GovWay Console di Configurazione

Analisi per la console di configurazione di GovWay

Site: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do

Generated on Sat, 21 Mar 2026 17:19:46

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	0
Informational	2

Alerts

Name	Risk Level	Number of Instances
User Agent Fuzzer	Informational	Systemic
User Controllable HTML Element Attribute (Potential XSS)	Informational	86

Alert Detail

Informational	User Agent Fuzzer
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do

Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
Instances	Systemic
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

Informational	**User Controllable HTML Element Attribute (Potential XSS)**
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,

	filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [td] tag [id] attribute The user input found was: __fake__search__=search The user-controlled value was: searchformheader
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)

Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_0=filtroProtocollo The user-controlled value was: filtroprotocollo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_1=filtroServiceBinding The user-controlled value was: filtroservicebinding
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in:

Info	a(n) [input] tag [value] attribute The user input found was: filterName_10=filtroAutenticazioneTrasportoTipo The user-controlled value was: filtroautenticazionetrasportotipo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_11=filtroConfigurazioneRateLimitingStato The user-controlled value was:

	filtroconfigurazioneratelimitingstato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_12=filtroConfigurazioneValidazioneStato The user-controlled value was: filtroconfigurazionevalidazionestato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__,

Node Name	_tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_13=filtroConfigurazioneCacheRispostaStato The user-controlled value was: filtroconfigurazionecacherispostastato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3,

Node Name	__i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_14=filtroConfigurazioneMessageSecurityStato The user-controlled value was: filtroconfigurazionemessagesecuritystato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3,

Node Name	__i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_15=filtroConfigurazioneMTOMStato The user-controlled value was: filtroconfigurazionemtomstato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,

	filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_16=filtroConfigurazioneTrasformazione The user-controlled value was: filtroconfigurazionetrasformazione
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search,

	selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_17=filtroConfigurazioneTransazioni The user-controlled value was: filtroconfigurazionetransazioni
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	

Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_18=filtroConfigurazioneCorrelazioneApplicativaStato The user-controlled value was: filtroconfigurazionecorrelazioneapplicativastato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_19=filtroConfigurazioneDumpTipo The user-controlled value was: filtroconfigurazionedumptipo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute

	The user input found was: filterName_2=filtroGruppo The user-controlled value was: filtrogruppo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_20=filtroConfigurazioneCorsTipo The user-controlled value was:

	filtroconfigurazionecorstipo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_21=subtDatiProp The user-controlled value was: subtdatiprop
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,

Node Name	__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_22=filtroPropNome The user-controlled value was: filtropropnome
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3,

Node Name	__i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_23=filtroPropValore The user-controlled value was: filtropropvalore
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3,

Node Name	__i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_3=subtDatiConn The user-controlled value was: subtdaticonn
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,

	filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_4=filtroConnettoreTipo The user-controlled value was: filtroconnettoretipo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12,

	url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_5=filtroConnettoreTokenPolicy The user-controlled value was: filtroconnettoretokenpolicy
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	

Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_6=filtroConnettoreEndpoint The user-controlled value was: filtroconnettoreendpoint
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes

Other Info	appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_7=subtDatiConf The user-controlled value was: subtdaticonf
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was:

	filterName_8=filtroConfigurazioneStato The user-controlled value was: filtroconfigurazionestato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_9=filtroAutenticazioneTokenTipo The user-controlled value was: filtroautenticazionetokentipo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-

	5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_1=soap The user-controlled value was: soap
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3,

Node Name	__i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_11=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3,

Node Name	__i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_12=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3,

	__i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_13=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,

	filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_14=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST

Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_15=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_16=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute

	The user input found was: filterValue_17=Default The user-controlled value was: default
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_18=Abilitato The user-controlled value was:

	abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_19=Default The user-controlled value was: default
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,

Node Name	__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_2=AltroTag The user-controlled value was: altrotag
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3,

Node Name	__i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_22=algo The user-controlled value was: algo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3,

Node Name	__i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterValue_23=ZAP The user-controlled value was: zap
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,

	filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_5=api-config-test-jwt The user-controlled value was: api-config-test-jwt
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12,

	url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterValue_6=ZAP The user-controlled value was: zap
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	

Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_8=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes

Other Info	appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_9=AutenticazioneInternaRiconoscimentoApplicativoModI The user-controlled value was: autenticazioneinternariconoscimentoapplicativomodi
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_3, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_3, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13, filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19, filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15, filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22, filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,limit,search, selectcheckbox,url_entry_0,url_entry_1,url_entry_10,url_entry_11,url_entry_12, url_entry_13,url_entry_14,url_entry_15,url_entry_16,url_entry_17,url_entry_18,url_entry_19, url_entry_2,url_entry_3,url_entry_4,url_entry_5,url_entry_6,url_entry_7,url_entry_8, url_entry_9)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was:

	search=ZAP The user-controlled value was: zap
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [td] tag [id] attribute The user input found was: __fake__search__=search The user-controlled value was: searchformheader
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in:

Other Info	a(n) [input] tag [value] attribute The user input found was: filterName_0=filtroProtocollo The user-controlled value was: filtroprotocollo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_1=filtroServiceBinding The user-controlled value was: filtroservicebinding
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_10=filtroAutenticazioneTrasportoTipo The user-controlled value was: filtroautenticazionetrasportotipo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_11=filtroConfigurazioneRateLimitingStato The user-controlled value was: filtroconfigurazioneratelimitingstato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	

Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_12=filtroConfigurazioneValidazioneStato The user-controlled value was: filtroconfigurazionevalidazionestato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_13=filtroConfigurazioneCacheRispostaStato The user-controlled value was: filtroconfigurazionecacherispostastato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16,

	filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_14=filtroConfigurazioneMessageSecurityStato The user-controlled value was: filtroconfigurazionemessagesecuritystato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_15=filtroConfigurazioneMTOMStato The user-controlled value was: filtroconfigurazionemtomstato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0,

Node Name	filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_16=filtroConfigurazioneTrasformazione The user-controlled value was: filtroconfigurazionetrasformazione
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_17=filtroConfigurazioneTransazioni The user-controlled value was: filtroconfigurazionetransazioni

URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_18=filtroConfigurazioneCorrelazioneApplicativaStato The user-controlled value was: filtroconfigurazionecorrelazioneapplicativastato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was:

	filterName_19=filtroConfigurazioneDumpTipo The user-controlled value was: filtroconfigurazionedumptipo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_2=filtroGruppo The user-controlled value was: filtrogruppo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in:

Other Info	a(n) [input] tag [value] attribute The user input found was: filterName_20=filtroConfigurazioneCorsTipo The user-controlled value was: filtroconfigurazionecorstipo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_21=subtDatiProp The user-controlled value was: subtdatiprop
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_22=filtroPropNome The user-controlled value was: filtropropnome
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_23=filtroPropValore The user-controlled value was: filtropropvalore
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	

Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_3=subtDatiConn The user-controlled value was: subtdaticonn
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__,_tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_4=filtroConnettoreTipo The user-controlled value was: filtroconnettoretipo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__,_tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16,

	filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_5=filtroConnettoreTokenPolicy The user-controlled value was: filtroconnettoretokenpolicy
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_6=filtroConnettoreEndpoint The user-controlled value was: filtroconnettoreendpoint
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0,

Node Name	filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_7=subtDatiConf The user-controlled value was: subtdaticonf
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_8=filtroConfigurazioneStato The user-controlled value was: filtroconfigurazionestato

URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_9=filtroAutenticazioneTokenTipo The user-controlled value was: filtroautenticazionetokentipo
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was:

	filterValue_1=soap The user-controlled value was: soap
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_11=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in:

Other Info	a(n) [option] tag [value] attribute The user input found was: filterValue_12=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_13=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_14=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_15=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	

Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_16=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__,_tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_17=Default The user-controlled value was: default
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__,_tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16,

	filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_18=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_19=Default The user-controlled value was: default
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0,

Node Name	filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_2=AltroTag The user-controlled value was: altrotag
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_22=algo The user-controlled value was: algo

URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterValue_23=ZAP The user-controlled value was: zap
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was:

	filterValue_5=api-config-test-jwt The user-controlled value was: api-config-test-jwt
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__,_tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterValue_6=ZAP The user-controlled value was: zap
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__,_tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14,filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2,filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16,filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23,filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in:

Other Info	a(n) [option] tag [value] attribute The user input found was: filterValue_8=Abilitato The user-controlled value was: abilitato
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_9=AutenticazioneInternaRiconoscimentoApplicativoModI The user-controlled value was: autenticazioneinternariconoscimentoapplicativomodi
URL	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do (__prevTabKey__, _tabKey_tipologiaErogazione,resetSearch)(__fake__search__,_csrf,filterName_0, filterName_1,filterName_10,filterName_11,filterName_12,filterName_13,filterName_14, filterName_15,filterName_16,filterName_17,filterName_18,filterName_19,filterName_2, filterName_20,filterName_21,filterName_22,filterName_23,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1, filterValue_11,filterValue_12,filterValue_13,filterValue_14,filterValue_15,filterValue_16, filterValue_17,filterValue_18,filterValue_19,filterValue_2,filterValue_22,filterValue_23, filterValue_5,filterValue_6,filterValue_8,filterValue_9,search)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

Other Info	http://127.0.0.1:8080/govwayConsole/aspsErogazioniList.do?__prevTabKey__=936fe09e-d770-4435-982b-5ecb0cd9ce3b&_tabKey_tipologiaErogazione=erogazione&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: search=ZAP The user-controlled value was: zap
Instances	86
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031