GovWay Console di Configurazione

Analisi per la console di configurazione di GovWay

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

Generated on Sat, 14 Mar 2026 15:11:58

ZAP Version: 2.17.0

ZAP by **Checkmarx**

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	0
Informational	1

Alerts

Name	Risk Level	Number of Instances
User Controllable HTML Element Attribute (Potential XSS)	Informational	68

Alert Detail

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/soggettiList.do
	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2,

Node Name	__i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do 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/soggettiList.do
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do 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/soggettiList.do
	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,

Node Name	__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_1=filtroDominio The user-controlled value was: filtrodominio
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_2=filtroTipoSoggetto The user-controlled value was: filtrotiposoggetto
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_3=filtroTipoCredenziali The user-controlled value was: filtrotipocredenziali
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2,

		__i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_4=filtroRuolo The user-controlled value was: filtroruolo
URL		http://127.0.0.1:8080/govwayConsole/soggettiList.do
	Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_5=filtroGruppo The user-controlled value was: filtrogruppo
URL		http://127.0.0.1:8080/govwayConsole/soggettiList.do
		http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2,

Node Name	__i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_6=filtroApiContesto The user-controlled value was: filtroapicontesto	
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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	

Other Info	XSS might be possible. The page at the following URL: http://127.0.0.1:8080 /govwayConsole/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_7=subtDatiProp The user-controlled value was: subtdatiprop	
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_8=filtroPropNome The user-controlled value was: filtropropnome	
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,	

		filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_9=filtroPropValore The user-controlled value was: filtropropvalore
URL		http://127.0.0.1:8080/govwayConsole/soggettiList.do
	Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_1=esterno The user-controlled value was: esterno
URL		http://127.0.0.1:8080/govwayConsole/soggettiList.do
		http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2,

Node Name	__i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_2=Fruitore The user-controlled value was: fruitore	
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_4=ModlRuolo1FonteQualsiasi The user-controlled value was: modiruolo1fontequalsiasi	

URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_8=authzContenutiTest The user-controlled value was: authzcontenutitest
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterValue_9=ZAP The user-controlled value was: zap
URL		http://127.0.0.1:8080/govwayConsole/soggettiList.do
	Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do 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/soggettiList.do
	Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do 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/soggettiList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do 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/soggettiList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_1=filtroDominio The user-controlled value was: filtrodominio	
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_2=filtroTipoSoggetto The user-controlled value was: filtrotiposoggetto	
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_3=filtroTipoCredenziali The user-controlled value was: filtrotipocredenziali	

URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_4=filtroRuolo The user-controlled value was: filtroruolo
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_5=filtroGruppo The user-controlled value was: filtrogruppo
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_6=filtroApiContesto The user-controlled value was: filtroapicontesto
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_7=subtDatiProp The user-controlled value was: subtdatiprop
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do

Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_8=filtroPropNome The user-controlled value was: filtropropnome	
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_9=filtroPropValore The user-controlled value was: filtropropvalore	
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_1=esterno The user-controlled value was: esterno	
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_2=Fruitore The user-controlled value was: fruitore	
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do	
	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf,	

	Node Name	filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_4=ModIRuolo1FonteQualsiasi The user-controlled value was: modiruolo1fontequalsiasi
URL		http://127.0.0.1:8080/govwayConsole/soggettiList.do
	Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_8=authzContenutiTest The user-controlled value was: authzcontenutitest
URL		http://127.0.0.1:8080/govwayConsole/soggettiList.do
	Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterValue_9=ZAP The user-controlled value was: zap
URL		http://127.0.0.1:8080/govwayConsole/soggettiList.do
	Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do ()(__fake__search__,_csrf, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do 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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
		http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3,

Node Name	__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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709- a978e7e49c2e&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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709- a978e7e49c2e&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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709- a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_1=filtroDominio The user-controlled value was: filtrodominio
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2,

Name	__i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709- a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_2=filtroTipoSoggetto The user-controlled value was: filtrotiposoggetto
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709- a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_3=filtroTipoCredenziali The user-controlled value was: filtrotipocredenziali
	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-

URL	460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709- a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_4=filtroRuolo The user-controlled value was: filtroruolo
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e- 460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709- a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_5=filtroGruppo The user-controlled value was: filtrogruppo
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e- 460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709- a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_6=filtroApiContesto The user-controlled value was: filtroapicontesto
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e- 460e-8709-a978e7e49c2e&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2,

Node Name	__i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_7=subtDatiProp The user-controlled value was: subtdatiprop
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value]

	attribute The user input found was: filterName_8=filtroPropNome The user-controlled value was: filtropropnome
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_9=filtroPropValore The user-controlled value was: filtropropvalore
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,

		filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709- a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_1=esterno The user-controlled value was: esterno
URL		http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e- 460e-8709-a978e7e49c2e&resetSearch=yes
Node Name		http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709- a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_2=Fruitore The user-controlled value was: fruitore
URL		http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e- 460e-8709-a978e7e49c2e&resetSearch=yes
		http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2,

Node Name	__i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_4=ModIRuolo1FonteQualsiasi The user-controlled value was: modiruolo1fontequalsiasi
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_8=authzContenutiTest The user-controlled value was: authzcontenutitest
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterValue_9=ZAP The user-controlled value was: zap
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __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_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2,

		__i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterName_9,filterValue_1,filterValue_2, filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709- a978e7e49c2e&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/soggettiList.do?__prevTabKey__=bc76888b-fa2e- 460e-8709-a978e7e49c2e&resetSearch=yes
	Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709- a978e7e49c2e&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/soggettiList.do?__prevTabKey__=bc76888b-fa2e- 460e-8709-a978e7e49c2e&resetSearch=yes
	Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709- a978e7e49c2e&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/soggettiList.do?__prevTabKey__=bc76888b-fa2e- 460e-8709-a978e7e49c2e&resetSearch=yes
	Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_1=filtroDominio The user-controlled value was: filtrodominio
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_2=filtroTipoSoggetto The user-controlled value was: filtrotiposoggetto
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_3=filtroTipoCredenziali The user-controlled value was: filtrotipocredenziali
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_4=filtroRuolo The user-controlled value was: filtroruolo
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch)

Node Name	(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_5=filtroGruppo The user-controlled value was: filtrogruppo	
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes	
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_6=filtroApiContesto The user-controlled value was: filtroapicontesto	
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes	
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_7=subtDatiProp The user-controlled value was: subtdatiprop	
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes	
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,filterValue_8,filterValue_9,search)	
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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-	

Info	a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_8=filtroPropNome The user-controlled value was: filtropropnome
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_9=filtroPropValore The user-controlled value was: filtropropvalore
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_1=esterno The user-controlled value was: esterno
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_2=Fruitore The user-controlled value was: fruitore
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_4=ModIRuolo1FonteQualsiasi The user-controlled value was: modiruolo1fontequalsiasi
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_8=authzContenutiTest The user-controlled value was: authzcontenutitest
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterValue_9=ZAP The user-controlled value was: zap
URL	http://127.0.0.1:8080/govwayConsole/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/soggettiList.do (__prevTabKey__,resetSearch) (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9, filterValue_1,filterValue_2,filterValue_4,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/soggettiList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&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	68
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