GovWay Console di Configurazione

Analisi per la console di configurazione di GovWay

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

Generated on Tue, 24 Feb 2026 05:11:39

ZAP Version: 2.17.0

ZAP by [Checkmarx](#)

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances
[User Agent Fuzzer](#)	Informational	Systemic
[User Controllable HTML Element Attribute (Potential XSS)](#)	Informational	31

Alert Detail

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

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

Informational	User Controllable HTML Element Attribute (Potential XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)
Method	GET
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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [a] tag [title] attribute The user input found was: _tabKey_infoType=token The user-controlled value was: token policy
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do
	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do () (__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_4, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_4, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_4,

Node Name	__i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_4, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_4, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_4, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_4, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_4, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_4, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterValue_0,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/configurazionePolicyGestioneTokenList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_0=filtroTipoTokenPolicy The user-controlled value was: filtrotipotokenpolicy	
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do () (__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_4, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_4, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_4, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_4, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_4, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_4, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_4, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_4, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_4, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterValue_0,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/configurazionePolicyGestioneTokenList.do appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_0=retrieveToken The user-controlled value was: retrievetoken	
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do	
	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do ()	

Node Name	(__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_4, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_4, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_4, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_4, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_4, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_4, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_4, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_4, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_4, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterValue_0,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/configurazionePolicyGestioneTokenList.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/configurazionePolicyGestioneTokenList.do
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do () (__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_4, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_4, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_4, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_4, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_4, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_4, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_4, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_4, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_4, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll, filterName_0,filterValue_0,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/configurazionePolicyGestioneTokenList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: url_entry_8=configurazionePolicyGestioneTokenChange.do? _tabKey_infoType=&idPolicy=2 The user-controlled value was: configurazionepolicygestionetokenchange.do?_tabkey_infotype=&idpolicy=280	
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do () (__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll, filterName_0,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1)	
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/configurazionePolicyGestioneTokenList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: __i_hidden_title_iconUso_0_0=informazioniUtilizzoOggettoRegistro? idOggetto=280&tipoOggetto=TOKEN_POLICY&tipoRisposta=text The user-controlled value was: informazioniutilizzooggettoregistro? idoggetto=280&tipooggetto=token_policy&tiporisposta=text	
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do () (__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll, filterName_0,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1)	
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/configurazionePolicyGestioneTokenList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: __i_hidden_title_iconUso_0_4=proprietaOggettoRegistro? idOggetto=280&tipoOggetto=TOKEN_POLICY&tipoRisposta=text The user-controlled value was: proprietaoggettoregistro?idoggetto=280&tipooggetto=token_policy&tiporisposta=text	
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do	
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do () (__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll, filterName_0,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1)	
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/configurazionePolicyGestioneTokenList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: __i_hidden_title_iconUso_1_0=informazioniUtilizzoOggettoRegistro? idOggetto=281&tipoOggetto=TOKEN_POLICY&tipoRisposta=text The user-controlled value was: informazioniutilizzooggettoregistro? idoggetto=281&tipooggetto=token_policy&tiporisposta=text	
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do	

Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do () (__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll, filterName_0,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1)
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/configurazionePolicyGestioneTokenList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: __i_hidden_title_iconUso_1_4=proprietaOggettoRegistro? idOggetto=281&tipoOggetto=TOKEN_POLICY&tipoRisposta=text The user-controlled value was: proprietaoggettoregistro?idoggetto=281&tipooggetto=token_policy&tiporisposta=text
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do () (__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll, filterName_0,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1)
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/configurazionePolicyGestioneTokenList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_0=filtroTipoTokenPolicy The user-controlled value was: filtrotipotokenpolicy
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do () (__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll, filterName_0,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1)
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/configurazionePolicyGestioneTokenList.do appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_0=retrieveToken The user-controlled value was: retrievetoken
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do () (__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll, filterName_0,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1)
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/configurazionePolicyGestioneTokenList.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/configurazionePolicyGestioneTokenList.do
	Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do () (__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll, filterName_0,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1)
	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/configurazionePolicyGestioneTokenList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: selectcheckbox=280 The user-controlled value was: 280
URL		http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do
	Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do () (__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll, filterName_0,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1)
	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/configurazionePolicyGestioneTokenList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: url_entry_0=configurazionePolicyGestioneTokenChange.do? _tabKey_infoType=&idPolicy=280 The user-controlled value was: configurazionepolicygestionetokenchange.do?_tabkey_infotype=&idpolicy=280
URL		http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do
	Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do () (__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll, filterName_0,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1)
	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/configurazionePolicyGestioneTokenList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: url_entry_1=configurazionePolicyGestioneTokenChange.do? _tabKey_infoType=&idPolicy=281 The user-controlled value was: configurazionepolicygestionetokenchange.do?_tabkey_infotype=&idpolicy=281
URL		http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do? __prevTabKey__=f2d122d4-7088-4601-bfa7- 3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes
		http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_4,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_4,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_4,__i_hidden_title_iconUso_17_0,

Node Name	__i_hidden_title_iconUso_17_4,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_4,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_4,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_4,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4- 7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [a] tag [title] attribute The user input found was: _tabKey_infoType=token The user-controlled value was: token policy	
URL	[http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do? __prevTabKey__=f2d122d4-7088-4601-bfa7- 3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes](http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do)	
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_4,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_4,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_4,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_4,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_4,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_4,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_4,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4-	

	7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_0=filtroTipoTokenPolicy The user-controlled value was: filtrotipotokenpolicy
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_4,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_4,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_4,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_4,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_4,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_4,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_4,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_0=retrieveToken The user-controlled value was: retrievetoken
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_4,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_4,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_4,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_4,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_4,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_4,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0,

		__i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_4,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4- 7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&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/configurazionePolicyGestioneTokenList.do? __prevTabKey__=f2d122d4-7088-4601-bfa7- 3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes
Node Name		http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_4,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_4,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_4,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_4,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_4,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_4,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_4,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4- 7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: url_entry_8=configurazionePolicyGestioneTokenChange.do? _tabKey_infoType=token&idPolicy=2 The user-controlled value was: configurazionepolicygestionetokenchange.do?_tabkey_infotype=token&idpolicy=280
URL		http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do? __prevTabKey__=f2d122d4-7088-4601-bfa7- 3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes
		http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0,

	Node Name	__i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,search, selectcheckbox,url_entry_0,url_entry_1)
	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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: __i_hidden_title_iconUso_0_0=informazioniUtilizzoOggettoRegistro? idOggetto=280&tipoOggetto=TOKEN_POLICY&tipoRisposta=text The user-controlled value was: informazioniutilizzooggettoregistro? idoggetto=280&tipooggetto=token_policy&tiporisposta=text
URL		http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do? __prevTabKey__=f2d122d4-7088-4601-bfa7- 3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes
	Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,search, selectcheckbox,url_entry_0,url_entry_1)
	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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: __i_hidden_title_iconUso_0_4=proprietaOggettoRegistro? idOggetto=280&tipoOggetto=TOKEN_POLICY&tipoRisposta=text The user-controlled value was: proprietaoggettoregistro?idoggetto=280&tipooggetto=token_policy&tiporisposta=text
URL		http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do? __prevTabKey__=f2d122d4-7088-4601-bfa7- 3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes
	Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,search, selectcheckbox,url_entry_0,url_entry_1)
	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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: __i_hidden_title_iconUso_1_0=informazioniUtilizzoOggettoRegistro? idOggetto=281&tipoOggetto=TOKEN_POLICY&tipoRisposta=text The user-controlled value was: informazioniutilizzooggettoregistro? idoggetto=281&tipooggetto=token_policy&tiporisposta=text
URL		http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do? __prevTabKey__=f2d122d4-7088-4601-bfa7- 3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes

Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,search, selectcheckbox,url_entry_0,url_entry_1)	
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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: __i_hidden_title_iconUso_1_4=proprietaOggettoRegistro? idOggetto=281&tipoOggetto=TOKEN_POLICY&tipoRisposta=text The user-controlled value was: proprietaoggettoregistro?idoggetto=281&tipooggetto=token_policy&tiporisposta=text	
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do? __prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes	
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,search, selectcheckbox,url_entry_0,url_entry_1)	
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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [a] tag [title] attribute The user input found was: _tabKey_infoType=token The user-controlled value was: token policy	
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do? __prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes	
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,search, selectcheckbox,url_entry_0,url_entry_1)	
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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_0=filtroTipoTokenPolicy The user-controlled value was: filtrotipotokenpolicy	
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do? __prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes	
Node	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0,	

Name	__i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,search, selectcheckbox,url_entry_0,url_entry_1)	
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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4- 7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_0=retrieveToken The user-controlled value was: retrievetoken	
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do? __prevTabKey__=f2d122d4-7088-4601-bfa7- 3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes	
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,search, selectcheckbox,url_entry_0,url_entry_1)	
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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4- 7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&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/configurazionePolicyGestioneTokenList.do? __prevTabKey__=f2d122d4-7088-4601-bfa7- 3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes	
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,search, selectcheckbox,url_entry_0,url_entry_1)	
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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4- 7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: selectcheckbox=280 The user-controlled value was: 280	
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do? __prevTabKey__=f2d122d4-7088-4601-bfa7- 3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes	
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,search, selectcheckbox,url_entry_0,url_entry_1)	
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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: url_entry_0=configurazionePolicyGestioneTokenChange.do? _tabKey_infoType=token&idPolicy=280 The user-controlled value was: configurazionepolicygestionetokenchange.do?_tabkey_infotype=token&idpolicy=280
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do? __prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (__prevTabKey__,_tabKey_infoType,resetSearch)(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_4,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_4,_csrf,be_name_0,chkAll,filterName_0,filterValue_0,search, selectcheckbox,url_entry_0,url_entry_1)
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/configurazionePolicyGestioneTokenList.do?__prevTabKey__=f2d122d4-7088-4601-bfa7-3c2254e0cb29&_tabKey_infoType=token&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: url_entry_1=configurazionePolicyGestioneTokenChange.do? _tabKey_infoType=token&idPolicy=281 The user-controlled value was: configurazionepolicygestionetokenchange.do?_tabkey_infotype=token&idpolicy=281
Instances	31
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