GovWay Console di Configurazione

Analisi per la console di configurazione di GovWay

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

Generated on Sat, 14 Mar 2026 15:14:27

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	16

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/scopeList.do
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do ()(__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_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,_csrf,be_name_0,chkAll,filterName_0,filterName_1,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1,url_entry_2)
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/scopeList.do appears to include user input in: a(n) [input] tag [value]

Info	attribute The user input found was: filterName_0=filtroScopeContesto The user-controlled value was: filtroscopecontesto
URL	http://127.0.0.1:8080/govwayConsole/scopeList.do
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do ()(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_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,_csrf,be_name_0,chkAll,filterName_0,filterName_1, filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1,url_entry_2)
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/scopeList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_1=filtroApiContesto The user-controlled value was: filtroapicontesto
URL	http://127.0.0.1:8080/govwayConsole/scopeList.do
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do ()(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_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,_csrf,be_name_0,chkAll,filterName_0,filterName_1, filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1,url_entry_2)
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/scopeList.do appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_0=portaApplicativa The user-controlled value was: portaapplicativa
URL	http://127.0.0.1:8080/govwayConsole/scopeList.do
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do ()(__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_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,_csrf,be_name_0,chkAll,filterName_0,filterName_1, filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1,url_entry_2)
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/scopeList.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/scopeList.do
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do ()(_csrf,filterName_0,filterName_1, filterValue_0,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

Info	/govwayConsole/scopeList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_0=filtroScopeContesto The user-controlled value was: filtroscopecontesto
URL	http://127.0.0.1:8080/govwayConsole/scopeList.do
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do ()(_csrf,filterName_0,filterName_1, filterValue_0,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/scopeList.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: filterName_1=filtroApiContesto The user-controlled value was: filtroapicontesto
URL	http://127.0.0.1:8080/govwayConsole/scopeList.do
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do ()(_csrf,filterName_0,filterName_1, filterValue_0,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/scopeList.do appears to include user input in: a(n) [option] tag [value] attribute The user input found was: filterValue_0=portaApplicativa The user-controlled value was: portaapplicativa
URL	http://127.0.0.1:8080/govwayConsole/scopeList.do
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do ()(_csrf,filterName_0,filterName_1, filterValue_0,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/scopeList.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/scopeList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do (__prevTabKey__,resetSearch) (__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_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,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1, url_entry_2)
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/scopeList.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=filtroScopeContesto The user-controlled value was: filtroscopecontesto

URL	http://127.0.0.1:8080/govwayConsole/scopeList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do (__prevTabKey__,resetSearch)(__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_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,_csrf,be_name_0,chkAll,filterName_0,filterName_1,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1,url_entry_2)
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/scopeList.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=filtroApiContesto The user-controlled value was: filtroapicontesto
URL	http://127.0.0.1:8080/govwayConsole/scopeList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do (__prevTabKey__,resetSearch)(__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_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,_csrf,be_name_0,chkAll,filterName_0,filterName_1,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1,url_entry_2)
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/scopeList.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_0=portaApplicativa The user-controlled value was: portaapplicativa
URL	http://127.0.0.1:8080/govwayConsole/scopeList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do (__prevTabKey__,resetSearch)(__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_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,_csrf,be_name_0,chkAll,filterName_0,filterName_1,filterValue_0,search,selectcheckbox,url_entry_0,url_entry_1,url_entry_2)
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/scopeList.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/scopeList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do (__prevTabKey__,resetSearch)(_csrf,filterName_0,filterName_1,filterValue_0,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/scopeList.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=filtroScopeContesto The user-controlled value was: filtroscopecontesto
URL	http://127.0.0.1:8080/govwayConsole/scopeList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do (__prevTabKey__,resetSearch)(_csrf, filterName_0,filterName_1,filterValue_0,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/scopeList.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=filtroApiContesto The user-controlled value was: filtroapicontesto
URL	http://127.0.0.1:8080/govwayConsole/scopeList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do (__prevTabKey__,resetSearch)(_csrf, filterName_0,filterName_1,filterValue_0,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/scopeList.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_0=portaApplicativa The user-controlled value was: portaapplicativa
URL	http://127.0.0.1:8080/govwayConsole/scopeList.do?__prevTabKey__=bc76888b-fa2e-460e-8709-a978e7e49c2e&resetSearch=yes
Node Name	http://127.0.0.1:8080/govwayConsole/scopeList.do (__prevTabKey__,resetSearch)(_csrf, filterName_0,filterName_1,filterValue_0,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/scopeList.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	16
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