GovWay Console di Configurazione

Analisi per la console di configurazione di GovWay

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

Generated on Sat, 11 Apr 2026 17:25:41

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	7

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/auditing.do
Node Name	http://127.0.0.1:8080/govwayConsole/auditing.do ()(__i_hidden_locklabel_,__i_hidden_lockurl_,__i_hidden_lockvalue_,_csrf,contoggetto,datafine,datainizio,edit-mode,id,oldid,statooperazione,tipooggetto,tipooperazione,utente)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/auditing.do

Other Info	appears to include user input in: a(n) [input] tag [value] attribute The user input found was: contoggetto=ZAP The user-controlled value was: zap
URL	http://127.0.0.1:8080/govwayConsole/auditing.do
Node Name	http://127.0.0.1:8080/govwayConsole/auditing.do ()(__i_hidden_locklabel_,__i_hidden_lockurl_,__i_hidden_lockvalue_,_csrf,contoggetto,datafine,datainizio,edit-mode,id,oldid,statooperazione,tipooggetto,tipooperazione,utente)
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/auditing.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: datafine=ZAP The user-controlled value was: zap
URL	http://127.0.0.1:8080/govwayConsole/auditing.do
Node Name	http://127.0.0.1:8080/govwayConsole/auditing.do ()(__i_hidden_locklabel_,__i_hidden_lockurl_,__i_hidden_lockvalue_,_csrf,contoggetto,datafine,datainizio,edit-mode,id,oldid,statooperazione,tipooggetto,tipooperazione,utente)
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/auditing.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: datainizio=ZAP The user-controlled value was: zap
URL	http://127.0.0.1:8080/govwayConsole/auditing.do
Node	http://127.0.0.1:8080/govwayConsole/auditing.do ()(__i_hidden_locklabel_,

Name	__i_hidden_lockurl_,__i_hidden_lockvalue_,_csrf,contoggetto,datafine,datainizio,edit-mode,id,oldid,statooperazione,tipooggetto,tipooperazione,utente)
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/auditing.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: edit-mode=end The user-controlled value was: end
URL	http://127.0.0.1:8080/govwayConsole/auditing.do
Node Name	http://127.0.0.1:8080/govwayConsole/auditing.do ()(__i_hidden_locklabel_,__i_hidden_lockurl_,__i_hidden_lockvalue_,_csrf,contoggetto,datafine,datainizio,edit-mode,id,oldid,statooperazione,tipooggetto,tipooperazione,utente)
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/auditing.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: id=ZAP The user-controlled value was: zap
URL	http://127.0.0.1:8080/govwayConsole/auditing.do
Node Name	http://127.0.0.1:8080/govwayConsole/auditing.do ()(__i_hidden_locklabel_,__i_hidden_lockurl_,__i_hidden_lockvalue_,_csrf,contoggetto,datafine,datainizio,edit-mode,id,oldid,statooperazione,tipooggetto,tipooperazione,utente)
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://127.0.0.1:8080/govwayConsole/auditing.do appears to include user input in:

Other Info	a(n) [input] tag [value] attribute The user input found was: oldid=ZAP The user-controlled value was: zap
URL	http://127.0.0.1:8080/govwayConsole/auditing.do
Node Name	http://127.0.0.1:8080/govwayConsole/auditing.do ()(__i_hidden_locklabel_, __i_hidden_lockurl_,__i_hidden_lockvalue_,_csrf,contoggetto,datafine,datainizio,edit-mode, id,oldid,statooperazione,tipooggetto,tipooperazione,utente)
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/auditing.do appears to include user input in: a(n) [input] tag [value] attribute The user input found was: utente=ZAP The user-controlled value was: zap
Instances	7
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