



ZAP by
Checkmarx

GovWay Console di Configurazione

Analisi per la console di configurazione di GovWay

Site: <http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do>

Generated on Sat, 11 Apr 2026 17:04:50

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	6

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/configurazioneAuditing.do
Node Name	http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do ()(__i_hidden_locklabel_, __i_hidden_lockurl_, __i_hidden_lockvalue_, __csrf,dump,edit-mode,formatodump,log4j,stato, statoaudit)
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/configurazioneAuditing.do

Other Info	<p>appears to include user input in:</p> <p>a(n) [option] tag [value] attribute</p> <p>The user input found was:</p> <p>dump=disabilitato</p> <p>The user-controlled value was:</p> <p>disabilitato</p>
URL	http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do
Node Name	http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do ()(____i_hidden_locklabel____i_hidden_lockurl____i_hidden_lockvalue____csrf,dump,edit-mode,formatodump,log4j,stato,statoaudit)
Method	POST
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:</p> <p>http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do</p> <p>appears to include user input in:</p> <p>a(n) [input] tag [value] attribute</p> <p>The user input found was:</p> <p>edit-mode=end</p> <p>The user-controlled value was:</p> <p>end</p>
URL	http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do
Node Name	http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do ()(____i_hidden_locklabel____i_hidden_lockurl____i_hidden_lockvalue____csrf,dump,edit-mode,formatodump,log4j,stato,statoaudit)
Method	POST
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:</p> <p>http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do</p> <p>appears to include user input in:</p> <p>a(n) [input] tag [value] attribute</p> <p>The user input found was:</p> <p>formatodump=JSON</p> <p>The user-controlled value was:</p> <p>json</p>
URL	http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do
Node	http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do ()(____i_hidden_locklabel____i_hidden_lockurl____i_hidden_lockvalue____csrf,dump,edit-mode,formatodump,log4j,stato,statoaudit)

Name	__i_hidden_lockurl__,__i_hidden_lockvalue__,__csrf,dump,edit-mode,formatodump,log4j,stato,statoaudit)
Method	POST
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:</p> <p>http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do</p> <p>appears to include user input in:</p> <p>a(n) [option] tag [value] attribute</p> <p>The user input found was:</p> <p>log4j=abilitato</p> <p>The user-controlled value was:</p> <p>abilitato</p>
URL	http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do
Node Name	http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do ()(__i_hidden_locklabel__,__i_hidden_lockurl__,__i_hidden_lockvalue__,__csrf,dump,edit-mode,formatodump,log4j,stato,statoaudit)
Method	POST
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:</p> <p>http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do</p> <p>appears to include user input in:</p> <p>a(n) [option] tag [value] attribute</p> <p>The user input found was:</p> <p>stato=abilitato</p> <p>The user-controlled value was:</p> <p>abilitato</p>
URL	http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do
Node Name	http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do ()(__i_hidden_locklabel__,__i_hidden_lockurl__,__i_hidden_lockvalue__,__csrf,dump,edit-mode,formatodump,log4j,stato,statoaudit)
Method	POST
Attack	
Evidence	
Other Info	<p>User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:</p> <p>http://127.0.0.1:8080/govwayConsole/configurazioneAuditing.do</p> <p>appears to include user input in:</p>

Other Info	a(n) [option] tag [value] attribute The user input found was: statoaudit=abilitato The user-controlled value was: abilitato
Instances	6
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