



ZAP by  
Checkmarx

# 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 17:25:18

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
<a href="#">User Controllable HTML Element Attribute (Potential XSS)</a>	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	<a href="http://127.0.0.1:8080/govwayConsole/auditing.do">http://127.0.0.1:8080/govwayConsole/auditing.do</a>
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: <a href="http://127.0.0.1:8080/govwayConsole/auditing.do">http://127.0.0.1:8080/govwayConsole/auditing.do</a>

Other Info	<p>appears to include user input in:</p> <p>a(n) [input] tag [value] attribute</p> <p>The user input found was:</p> <p>contoggetto=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/auditing.do">http://127.0.0.1:8080/govwayConsole/auditing.do</a>
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	<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><a href="http://127.0.0.1:8080/govwayConsole/auditing.do">http://127.0.0.1:8080/govwayConsole/auditing.do</a></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>datafine=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/auditing.do">http://127.0.0.1:8080/govwayConsole/auditing.do</a>
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	<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><a href="http://127.0.0.1:8080/govwayConsole/auditing.do">http://127.0.0.1:8080/govwayConsole/auditing.do</a></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>datainizio=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/auditing.do">http://127.0.0.1:8080/govwayConsole/auditing.do</a>
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	<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><a href="http://127.0.0.1:8080/govwayConsole/auditing.do">http://127.0.0.1:8080/govwayConsole/auditing.do</a></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	<a href="http://127.0.0.1:8080/govwayConsole/auditing.do">http://127.0.0.1:8080/govwayConsole/auditing.do</a>
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	<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><a href="http://127.0.0.1:8080/govwayConsole/auditing.do">http://127.0.0.1:8080/govwayConsole/auditing.do</a></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>id=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/auditing.do">http://127.0.0.1:8080/govwayConsole/auditing.do</a>
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	<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><a href="http://127.0.0.1:8080/govwayConsole/auditing.do">http://127.0.0.1:8080/govwayConsole/auditing.do</a></p> <p>appears to include user input in:</p>

Other Info	<p>a(n) [input] tag [value] attribute</p> <p>The user input found was:</p> <p>oldid=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/auditing.do">http://127.0.0.1:8080/govwayConsole/auditing.do</a>
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	<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><a href="http://127.0.0.1:8080/govwayConsole/auditing.do">http://127.0.0.1:8080/govwayConsole/auditing.do</a></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>utente=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
Instances	7
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html</a>
CWE Id	<a href="#">20</a>
WASC Id	20
Plugin Id	<a href="#">10031</a>