GovWay Console di Configurazione

Analisi per la console di configurazione di GovWay

Site: http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do?_tabKey_infoType=aa

Generated on Sat, 11 Apr 2026 17:08:23

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
Session Management Response Identified	Informational	1
User Controllable HTML Element Attribute (Potential XSS)	Informational	1

Alert Detail

Informational	Session Management Response Identified
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do?_tabKey_infoType=aa
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (_tabKey_infoType)(__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, search,selectcheckbox,url_entry_0,url_entry_1)
Method	POST
Attack	

Evidence	JSESSIONID_GW_CONSOLE
Other Info	cookie:JSESSIONID_GW_CONSOLE
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/
CWE Id	
WASC Id	
Plugin Id	10112

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?_tabKey_infoType=aa
Node Name	http://127.0.0.1:8080/govwayConsole/configurazionePolicyGestioneTokenList.do (_tabKey_infoType)(__i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_4, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_4, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_4, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_4, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_4, __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_4, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_4, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_4, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_4, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_4, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_4, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_4,_csrf,be_name_0,chkAll,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?_tabKey_infoType=aa 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	1
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