# GovWay Console di Configurazione

Analisi per la console di configurazione di GovWay

## Site: http://127.0.0.1:8080/govwayConsole/import.do

## Generated on Sat, 14 Mar 2026 14:57:41

## 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 |
|---|:---:|:---:|
| User Agent Fuzzer | Informational | Systemic |
| User Controllable HTML Element Attribute (Potential XSS) | Informational | 2 |

## Alert Detail

| Informational | User Agent Fuzzer |
|---|---|
| Description | Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response. |
| URL | http://127.0.0.1:8080/govwayConsole/import.do |
| Node Name | http://127.0.0.1:8080/govwayConsole/import.do |
| Method | GET |
| Attack | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |
| Evidence | |
| Other Info | |
| URL | http://127.0.0.1:8080/govwayConsole/import.do |
| | |

| | | |
|---|---|---|
| Node Name | http://127.0.0.1:8080/govwayConsole/import.do | |
| Method | GET | |
| Attack | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) | |
| Evidence | | |
| Other Info | | |
| URL | http://127.0.0.1:8080/govwayConsole/import.do | |
| Node Name | http://127.0.0.1:8080/govwayConsole/import.do | |
| Method | GET | |
| Attack | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1) | |
| Evidence | | |
| Other Info | | |
| Instances | Systemic | |
| Solution | | |
| Reference | https://owasp.org/wstg | |
| CWE Id | | |
| WASC Id | | |
| Plugin Id | 10104 | |

| 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/import.do?__prevTabKey__=75fdd773-f1fd-494f-b6db-df0610c3f98b&modalita=import&resetSearch=yes |
| Node Name | http://127.0.0.1:8080/govwayConsole/import.do (__prevTabKey__,modalita,resetSearch) |
| Method | GET |
| 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/import.do?__prevTabKey__=75fdd773-f1fd-494f-b6db-df0610c3f98b&modalita=import&resetSearch=yes appears to include user input in: a(n) [a] tag [title] attribute The user input found was: modalita=import The user-controlled value was: importa |
| URL | http://127.0.0.1:8080/govwayConsole/import.do?__prevTabKey__=75fdd773-f1fd-494f-b6db-df0610c3f98b&modalita=import&resetSearch=yes |
| Node Name | http://127.0.0.1:8080/govwayConsole/import.do (__prevTabKey__,modalita,resetSearch) |
| Method | GET |
| 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 |

| | |
|---|---|
| Other Info | /govwayConsole/import.do?__prevTabKey__=75fdd773-f1fd-494f-b6db-df0610c3f98b&modalita=import&resetSearch=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: resetSearch=yes The user-controlled value was: yes |
| Instances | 2 |
| 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 |