# GovWay Console di Configurazione

Analisi per la console di configurazione di GovWay

## Site: http://127.0.0.1:8080/govwayConsole/configurazioneGenerale.do?configCaches=yes

### Generated on Sat, 14 Mar 2026 14:44:43

### 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 | 1 |

### 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/configurazioneGenerale.do?configCaches=yes |
| Node Name | http://127.0.0.1:8080/govwayConsole/configurazioneGenerale.do (configCaches) |
| Method | GET |
| Attack | |
| Evidence | |
| Other | 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 |

| | |
|---|---|
| Info | /govwayConsole/configurazioneGenerale.do?configCaches=yes appears to include user input in: a(n) [input] tag [value] attribute The user input found was: configCaches=yes The user-controlled value was: yes |
| 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 |