



ZAP by  
Checkmarx

# GovWay Console di Configurazione

Analisi per la console di configurazione di GovWay

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

Generated on Sat, 11 Apr 2026 17:16:44

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	57

## 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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
	<code>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()( __fake__ search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_2, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_2, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_2, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2,</code>

Node Name	<pre> __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_2,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,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) </pre>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a></p> <p>appears to include user input in:</p> <p>a(n) [td] tag [id] attribute</p> <p>The user input found was:</p> <pre> __fake__search__=search </pre> <p>The user-controlled value was:</p> <pre> searchformheader </pre>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<pre> http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_2, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_2, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_2, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_2,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,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) </pre>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterName_0=filtroProtocollo</p> <p>The user-controlled value was:</p> <p>filtroprotocollo</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<p><a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a> ( (__fake__search__,  __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2,  __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_2,  __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_2,  __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_2,  __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_2,  __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2,  __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2,  __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2,  __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2,  __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2,  __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2,  __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2,  __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2,  __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2,  __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2,  __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2,  __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2,  __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2,  __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2,  __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_2,_csrf,be_name_0,chkAll,  filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,  filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,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)</p>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterName_1=filtroTipoSA</p> <p>The user-controlled value was:</p>

	filtrtiposa
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<pre> http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_2, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_2, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_2, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_2,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,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) </pre>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterName_2=filtroTipoCredenziali</p> <p>The user-controlled value was:</p> <p>filtrtipocredenziali</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node	<pre> http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_2, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_2, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_2, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, </pre>

Name	<code>__i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_2,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,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)</code>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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><code>filterName_3=filtoRuolo</code></p> <p>The user-controlled value was:</p> <p><code>filtroruolo</code></p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<code>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_2, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_2, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_2, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_2,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,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)</code>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterName_4=filtroGruppo</p> <p>The user-controlled value was:</p> <p>filtrogruppo</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<p><a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a> ( (__fake__search__, __i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_2, __i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_2, __i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_2, __i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_2, __i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_2, _csrf, be_name_0, chkAll, filterName_0, filterName_1, filterName_2, filterName_3, filterName_4, filterName_5, filterName_6, filterName_7, filterName_8, filterValue_3, filterValue_7, filterValue_8, 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)</p>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterName_5=filtroApiContesto</p> <p>The user-controlled value was:</p>

	filtraopicontesto
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<pre>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_2, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_2, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_2, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_2,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,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)</pre>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterName_6=subtDatiProp</p> <p>The user-controlled value was:</p> <p>subtdatiprop</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node	<pre>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_2, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_2, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_2, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2,</pre>

Name	<code>__i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_2,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,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)</code>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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><code>filterName_7=filtroPropNome</code></p> <p>The user-controlled value was:</p> <p><code>filtropropnome</code></p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<code>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_2, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_2, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_2, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_2,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,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)</code>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterName_8=filtroPropValore</p> <p>The user-controlled value was:</p> <p>filtropropvalore</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<pre>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_2, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_2, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_2, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_2,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,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)</pre>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a></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>filterValue_3=ModIRuolo1FonteQualsiasi</p> <p>The user-controlled value was:</p>

	modiruolo1fontequalsiasi
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_2, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_2, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_2, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_2,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,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	<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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a></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>filterValue_7=authzContenutiTest</p> <p>The user-controlled value was:</p> <p>authzcontenutitest</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_2, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_2, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_2, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2,

Name	<code>__i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_2,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,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)</code>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterValue_8=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<code>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__, __i_hidden_title_iconUso_0_0,__i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0,__i_hidden_title_iconUso_10_2, __i_hidden_title_iconUso_11_0,__i_hidden_title_iconUso_11_2, __i_hidden_title_iconUso_12_0,__i_hidden_title_iconUso_12_2, __i_hidden_title_iconUso_13_0,__i_hidden_title_iconUso_13_2, __i_hidden_title_iconUso_14_0,__i_hidden_title_iconUso_14_2, __i_hidden_title_iconUso_15_0,__i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0,__i_hidden_title_iconUso_16_2, __i_hidden_title_iconUso_17_0,__i_hidden_title_iconUso_17_2, __i_hidden_title_iconUso_18_0,__i_hidden_title_iconUso_18_2, __i_hidden_title_iconUso_19_0,__i_hidden_title_iconUso_19_2, __i_hidden_title_iconUso_1_0,__i_hidden_title_iconUso_1_2, __i_hidden_title_iconUso_2_0,__i_hidden_title_iconUso_2_2, __i_hidden_title_iconUso_3_0,__i_hidden_title_iconUso_3_2, __i_hidden_title_iconUso_4_0,__i_hidden_title_iconUso_4_2, __i_hidden_title_iconUso_5_0,__i_hidden_title_iconUso_5_2, __i_hidden_title_iconUso_6_0,__i_hidden_title_iconUso_6_2, __i_hidden_title_iconUso_7_0,__i_hidden_title_iconUso_7_2, __i_hidden_title_iconUso_8_0,__i_hidden_title_iconUso_8_2, __i_hidden_title_iconUso_9_0,__i_hidden_title_iconUso_9_2,_csrf,be_name_0,chkAll, filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5, filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,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)</code>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>search=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a> ().__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a></p> <p>appears to include user input in:</p> <p>a(n) [td] tag [id] attribute</p> <p>The user input found was:</p> <p>__fake__search__=search</p> <p>The user-controlled value was:</p> <p>searchformheader</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a> ().__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterName_0=filtroProtocollo</p>

	The user-controlled value was: filtroprotocollo
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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:  <a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>  appears to include user input in:  a(n) [input] tag [value] attribute  The user input found was:  filterName_1=filtroTipoSA  The user-controlled value was:  filtrotiposa
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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:  <a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>  appears to include user input in:  a(n) [input] tag [value] attribute  The user input found was:  filterName_2=filtroTipoCredenziali  The user-controlled value was:  filtrotipocredenziali
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterName_3=filtroRuolo</p> <p>The user-controlled value was:</p> <p>filtroruolo</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<code>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)</code>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterName_4=filtroGruppo</p> <p>The user-controlled value was:</p> <p>filtrogruppo</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<code>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)</code>
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterName_5=filtroApiContesto</p> <p>The user-controlled value was:</p>

	filtraopicontesto
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterName_6=subtDatiProp</p> <p>The user-controlled value was:</p> <p>subtdatiprop</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterName_7=filtroPropNome</p> <p>The user-controlled value was:</p> <p>filtropropnome</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do ()(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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:

Other Info	<p><a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterName_8=filtroPropValore</p> <p>The user-controlled value was:</p> <p>filtrpropvalore</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a> ( (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a></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>filterValue_3=ModIRuolo1FonteQualsiasi</p> <p>The user-controlled value was:</p> <p>modiruolo1fontequalsiasi</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a> ( (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a></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>filterValue_7=authzContenutiTest</p> <p>The user-controlled value was:</p> <p>authzcontenutitest</p>

URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>filterValue_8=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.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>search=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
	<p>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__,resetSearch)(__fake__search__,_i_hidden_title_iconUso_0_0,_i_hidden_title_iconUso_0_2,_i_hidden_title_iconUso_10_0,_i_hidden_title_iconUso_10_3,_i_hidden_title_iconUso_11_0,_i_hidden_title_iconUso_11_3,_i_hidden_title_iconUso_12_0,_i_hidden_title_iconUso_12_3,_i_hidden_title_iconUso_13_0,_i_hidden_title_iconUso_13_3,_i_hidden_title_iconUso_14_0,_i_hidden_title_iconUso_14_3,_i_hidden_title_iconUso_15_0,_i_hidden_title_iconUso_15_2,_i_hidden_title_iconUso_16_0,_i_hidden_title_iconUso_16_3,_i_hidden_title_iconUso_17_0,_i_hidden_title_iconUso_17_3,_i_hidden_title_iconUso_18_0,_i_hidden_title_iconUso_18_3,_i_hidden_title_iconUso_19_0,</p>

Node Name	__i_hidden_title_iconUso_19_3,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,filterName_0,filterName_1, filterName_10,filterName_11,filterName_12,filterName_2,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_11, filterValue_12,filterValue_3,filterValue_8,filterValue_9,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	<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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a></p> <p>appears to include user input in:</p> <p>a(n) [td] tag [id] attribute</p> <p>The user input found was:</p> <p>__fake__search__=search</p> <p>The user-controlled value was:</p> <p>searchformheader</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_3,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_3,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_3,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_3,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_3,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,filterName_0,filterName_1, filterName_10,filterName_11,filterName_12,filterName_2,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_11, filterValue_12,filterValue_3,filterValue_8,filterValue_9,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	<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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_0=filtroProtocollo</p> <p>The user-controlled value was:</p> <p>filtroprotocollo</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	<p>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3, csrf,be_name_0,chkAll,filterName_0,filterName_1,filterName_10,filterName_11,filterName_12,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_11,filterValue_12,filterValue_3,filterValue_8,filterValue_9,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)</p>
Method	POST
Attack	
Evidence	
	<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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_1=filtroTipoSA</p> <p>The user-controlled value was:</p> <p>filtrotiposa</p>
URL	<p><a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a></p>
Node Name	<p>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake_search__, __i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3, csrf,be_name_0,chkAll,filterName_0,filterName_1, filterName_10,filterName_11,filterName_12,filterName_2,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_11, filterValue_12,filterValue_3,filterValue_8,filterValue_9,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)</p>
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_10=subtDatiProp</p> <p>The user-controlled value was:</p> <p>subtdatiprop</p>
URL	<p><a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a></p>
	<p>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__,</p>

Node Name	<code>resetSearch)(__fake_search__,__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_3,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_3,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_3,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_3,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_3,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,filterName_0,filterName_1, filterName_10,filterName_11,filterName_12,filterName_2,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_11, filterValue_12,filterValue_3,filterValue_8,filterValue_9,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)</code>
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_11=filtroPropNome</p> <p>The user-controlled value was:</p> <p>filtropropnome</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	<code>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake_search__,__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_3,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_3,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_3,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_3,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_3,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3,__i_hidden_title_iconUso_3_0,</code>

	<pre> __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,filterName_0,filterName_1, filterName_10,filterName_11,filterName_12,filterName_2,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_11, filterValue_12,filterValue_3,filterValue_8,filterValue_9,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) </pre>
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_12=filtroPropValore</p> <p>The user-controlled value was:</p> <p>filtropropvalore</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	<pre> http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(_fake_search__,__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_3,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_3,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_3,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_3,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_3,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,filterName_0,filterName_1, filterName_10,filterName_11,filterName_12,filterName_2,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_11, filterValue_12,filterValue_3,filterValue_8,filterValue_9,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) </pre>
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_2=filtroTipoCredenziali</p> <p>The user-controlled value was:</p> <p>filtrotipocredenziali</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	<pre> http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_3,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_3,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_3,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_3,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_3,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,__csrf,be_name_0,chkAll,filterName_0,filterName_1, filterName_10,filterName_11,filterName_12,filterName_2,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_11, filterValue_12,filterValue_3,filterValue_8,filterValue_9,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) </pre>
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_3=filtroRuolo</p> <p>The user-controlled value was:</p> <p>filtroruolo</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	<pre> http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_3,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_3,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_3,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_3,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_3,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,__csrf,be_name_0,chkAll,filterName_0,filterName_1, filterName_10,filterName_11,filterName_12,filterName_2,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_11, filterValue_12,filterValue_3,filterValue_8,filterValue_9,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) </pre>
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_4=filtroGruppo</p> <p>The user-controlled value was:</p> <p>filtrogruppo</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
	<pre> http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, </pre>

Node Name	<pre> __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_3,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_3,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_3,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_3,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_3,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,csrf,be_name_0,chkAll,filterName_0,filterName_1, filterName_10,filterName_11,filterName_12,filterName_2,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_11, filterValue_12,filterValue_3,filterValue_8,filterValue_9,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) </pre>
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_5=filtroApiContesto</p> <p>The user-controlled value was:</p> <p>filtroapicontesto</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	<pre> http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_3,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_3,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_3,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_3,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_3,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, </pre>

	<code>__i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,filterName_0,filterName_1, filterName_10,filterName_11,filterName_12,filterName_2,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_11, filterValue_12,filterValue_3,filterValue_8,filterValue_9,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)</code>
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a></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>filterValue_11=authzContenutiTest</p> <p>The user-controlled value was:</p> <p>authzcontenutitest</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	<code>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_3,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_3,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_3,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_3,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_3,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,filterName_0,filterName_1, filterName_10,filterName_11,filterName_12,filterName_2,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_11, filterValue_12,filterValue_3,filterValue_8,filterValue_9,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)</code>
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterValue_12=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
URL	<p><a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a></p>
Node Name	<p>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__, __i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2, __i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3, __i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3, __i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3, __i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3, __i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_3, __i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2, __i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_3, __i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_3, __i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_3, __i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_3, __i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3, __i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3, __i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3, __i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3, __i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3, __i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3, __i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3, __i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3, __i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3, __csrf, be_name_0, chkAll, filterName_0, filterName_1, filterName_10, filterName_11, filterName_12, filterName_2, filterName_3, filterName_4, filterName_5, filterName_6, filterName_7, filterName_8, filterName_9, filterValue_11, filterValue_12, filterValue_3, filterValue_8, filterValue_9, 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)</p>
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a></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>filterValue_3=ModIRuolo1FonteQualsiasi</p>

	<p>The user-controlled value was:</p> <p>modiruolo1fontequalsiasi</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	<pre>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0, __i_hidden_title_iconUso_14_3,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_3,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_3,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_3,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_3,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,__csrf,be_name_0,chkAll,filterName_0,filterName_1, filterName_10,filterName_11,filterName_12,filterName_2,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_11, filterValue_12,filterValue_3,filterValue_8,filterValue_9,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)</pre>
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterValue_9=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
	<pre>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,__i_hidden_title_iconUso_0_0, __i_hidden_title_iconUso_0_2,__i_hidden_title_iconUso_10_0, __i_hidden_title_iconUso_10_3,__i_hidden_title_iconUso_11_0, __i_hidden_title_iconUso_11_3,__i_hidden_title_iconUso_12_0, __i_hidden_title_iconUso_12_3,__i_hidden_title_iconUso_13_0, __i_hidden_title_iconUso_13_3,__i_hidden_title_iconUso_14_0,</pre>

Node Name	__i_hidden_title_iconUso_14_3,__i_hidden_title_iconUso_15_0, __i_hidden_title_iconUso_15_2,__i_hidden_title_iconUso_16_0, __i_hidden_title_iconUso_16_3,__i_hidden_title_iconUso_17_0, __i_hidden_title_iconUso_17_3,__i_hidden_title_iconUso_18_0, __i_hidden_title_iconUso_18_3,__i_hidden_title_iconUso_19_0, __i_hidden_title_iconUso_19_3,__i_hidden_title_iconUso_1_0, __i_hidden_title_iconUso_1_3,__i_hidden_title_iconUso_2_0, __i_hidden_title_iconUso_2_3,__i_hidden_title_iconUso_3_0, __i_hidden_title_iconUso_3_3,__i_hidden_title_iconUso_4_0, __i_hidden_title_iconUso_4_3,__i_hidden_title_iconUso_5_0, __i_hidden_title_iconUso_5_3,__i_hidden_title_iconUso_6_0, __i_hidden_title_iconUso_6_3,__i_hidden_title_iconUso_7_0, __i_hidden_title_iconUso_7_3,__i_hidden_title_iconUso_8_0, __i_hidden_title_iconUso_8_3,__i_hidden_title_iconUso_9_0, __i_hidden_title_iconUso_9_3,_csrf,be_name_0,chkAll,filterName_0,filterName_1, filterName_10,filterName_11,filterName_12,filterName_2,filterName_3,filterName_4, filterName_5,filterName_6,filterName_7,filterName_8,filterName_9,filterValue_11, filterValue_12,filterValue_3,filterValue_8,filterValue_9,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	<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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>search=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3, filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3, filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a></p> <p>appears to include user input in:</p> <p>a(n) [td] tag [id] attribute</p> <p>The user input found was:</p>

	<p>__fake__search__=search</p> <p>The user-controlled value was:</p> <p>searchformheader</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_0=filtroProtocollo</p> <p>The user-controlled value was:</p> <p>filtroprotocollo</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_1=filtroTipoSA</p> <p>The user-controlled value was:</p> <p>filtrotiposa</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>

Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_2=filtroTipoCredenziali</p> <p>The user-controlled value was:</p> <p>filtrotipocredenziali</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_3=filtroRuolo</p> <p>The user-controlled value was:</p> <p>filtroruolo</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_4=filtroGruppo</p> <p>The user-controlled value was:</p> <p>filtrogruppo</p>
URL	<p><a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a></p>
Node Name	<p>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)</p>
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_5=filtroApiContesto</p> <p>The user-controlled value was:</p> <p>filtroapicontesto</p>
URL	<p><a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a></p>
Node Name	<p>http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)</p>
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_6=subtDatiProp</p> <p>The user-controlled value was:</p> <p>subtdatiprop</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__, __csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_7=filtroPropNome</p> <p>The user-controlled value was:</p> <p>filtropropnome</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__, __csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterName_8=filtroPropValore</p> <p>The user-controlled value was:</p> <p>filtropropvalore</p>

URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a></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>filterValue_3=ModIRuolo1FonteQualsiasi</p> <p>The user-controlled value was:</p> <p>modiruolo1fontequalsiasi</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a></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>filterValue_7=authzContenutiTest</p> <p>The user-controlled value was:</p> <p>authzcontenutitest</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>filterValue_8=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
URL	<a href="http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</a>
Node Name	http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do (__prevTabKey__, resetSearch)(__fake__search__,_csrf,filterName_0,filterName_1,filterName_2,filterName_3,filterName_4,filterName_5,filterName_6,filterName_7,filterName_8,filterValue_3,filterValue_7,filterValue_8,search)
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/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes">http://127.0.0.1:8080/govwayConsole/serviziApplicativiList.do?__prevTabKey__=8fea4ae0-e038-4206-bbb8-d5a8d232f54b&amp;resetSearch=yes</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>search=ZAP</p> <p>The user-controlled value was:</p> <p>zap</p>
Instances	57
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>