



ZAP by
Checkmarx

GovWay Console di Configurazione

Analisi per la console di configurazione di GovWay

Site: <http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc>

Generated on Sat, 11 Apr 2026 17:12:48

ZAP Version: 2.17.0

ZAP by [Checkmarx](#)

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	0
Informational	1

Alerts

Name	Risk Level	Number of Instances
User Controllable HTML Element Attribute (Potential XSS)	Informational	16

Alert Detail

Informational	User Controllable HTML Element Attribute (Potential XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc
	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo) (<code>__i_hidden_title_iconUso_0_0</code> , <code>__i_hidden_title_iconUso_0_2</code> , <code>__i_hidden_title_iconUso_10_0</code> , <code>__i_hidden_title_iconUso_10_2</code> , <code>__i_hidden_title_iconUso_11_0</code> , <code>__i_hidden_title_iconUso_11_2</code> , <code>__i_hidden_title_iconUso_12_0</code> , <code>__i_hidden_title_iconUso_12_2</code> , <code>__i_hidden_title_iconUso_13_0</code> , <code>__i_hidden_title_iconUso_13_2</code> , <code>__i_hidden_title_iconUso_14_0</code> , <code>__i_hidden_title_iconUso_14_2</code> , <code>__i_hidden_title_iconUso_15_0</code> , <code>__i_hidden_title_iconUso_15_2</code> , <code>__i_hidden_title_iconUso_16_0</code> , <code>__i_hidden_title_iconUso_16_2</code> , <code>__i_hidden_title_iconUso_17_0</code> , <code>__i_hidden_title_iconUso_17_2</code> , <code>__i_hidden_title_iconUso_18_0</code> , <code>__i_hidden_title_iconUso_18_2</code> ,

Node Name	<code>__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,filterValue_1,filterValue_2,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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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=filtroServiceBinding</p> <p>The user-controlled value was:</p> <p>filtroServiceBinding</p>
URL	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc
Node Name	<code>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo) (__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,filterValue_1,filterValue_2,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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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=filtroGruppo</p> <p>The user-controlled value was:</p> <p>filtrogruppo</p>
URL	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc
Node Name	<p>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo)</p> <p>(__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,filterValue_1,filterValue_2,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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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_1=soap</p> <p>The user-controlled value was:</p> <p>soap</p>
URL	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc
Node Name	<p>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo)</p> <p>(__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,filterValue_1,filterValue_2,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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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_2=AltroTag</p> <p>The user-controlled value was:</p> <p>altrotag</p>
URL	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc
	<p>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo)</p> <p>(__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,</p>

Node Name	__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,filterValue_1,filterValue_2,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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc
Node Name	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo) (_csrf,filterName_0,filterName_1,filterName_2,filterValue_1,filterValue_2,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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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>

	filtroprotocollo
URL	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc
Node Name	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo) (_csrf,filterName_0,filterName_1,filterName_2,filterValue_1,filterValue_2,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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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=filtroServiceBinding</p> <p>The user-controlled value was:</p> <p>filtroservicebinding</p>
URL	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc
Node Name	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo) (_csrf,filterName_0,filterName_1,filterName_2,filterValue_1,filterValue_2,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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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=filtroGruppo</p> <p>The user-controlled value was:</p> <p>filtrogruppo</p>
URL	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc
Node Name	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo) (_csrf,filterName_0,filterName_1,filterName_2,filterValue_1,filterValue_2,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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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_1=soap</p> <p>The user-controlled value was:</p> <p>soap</p>
URL	<p>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</p>
Node Name	<p>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo) (_csrf,filterName_0,filterName_1,filterName_2,filterValue_1,filterValue_2,search)</p>
Method	<p>POST</p>
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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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_2=AltroTag</p> <p>The user-controlled value was:</p> <p>altrotag</p>
URL	<p>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</p>
Node Name	<p>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo) (_csrf,filterName_0,filterName_1,filterName_2,filterValue_1,filterValue_2,search)</p>
Method	<p>POST</p>
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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc
Node Name	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo) (_csrf,filterName_0,filterName_1,filterValue_0,filterValue_1,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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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=filtroServiceBinding</p> <p>The user-controlled value was:</p> <p>filtrservicebinding</p>
URL	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc
Node Name	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo) (_csrf,filterName_0,filterName_1,filterValue_0,filterValue_1,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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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=filtroGruppo</p> <p>The user-controlled value was:</p> <p>filtrgruppo</p>
URL	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc
Node Name	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo) (_csrf,filterName_0,filterName_1,filterValue_0,filterValue_1,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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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_0=soap</p> <p>The user-controlled value was:</p> <p>soap</p>
URL	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc
Node Name	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo) (_csrf,filterName_0,filterName_1,filterValue_0,filterValue_1,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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</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_1=AltroTag</p> <p>The user-controlled value was:</p> <p>altrotag</p>
URL	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc
Node Name	http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do (tipoAccordo) (_csrf,filterName_0,filterName_1,filterValue_0,filterValue_1,search)
Method	POST
Attack	
Evidence	
Other	<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>http://127.0.0.1:8080/govwayConsole/accordiServizioParteComuneApiList.do?tipoAccordo=apc</p> <p>appears to include user input in:</p> <p>a(n) [input] tag [value] attribute</p>

Info	The user input found was: search=ZAP The user-controlled value was: zap
Instances	16
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031