

UXD Cycle 2 - RQ 3 - Numbers

MSAT Interface

Project: Alpha

S. No.	Name (Bug title)	Tool	Type	Fix Location	Assignee
1	XSS_CONFIG		XSS	12.4 XSSFILTER.java	Varma
2	EQ_CHECK		EQ	6.3 LoopHelper.java	Max
3	CO_SELF		CO	11.2 StringComparer.java	
4	XSS_REQUEST		XSS	5.4 HttpSender.java	John
5	DMI_EMPTY		DM	3.3 DatabaseHelper.java	Elina
6	BC_EQUALS		BC	2.4 HttpReceiver.java	Tom
7	BIT_CHECK		BIT	3.3 NetworkConnect.java	John
8	CN_CLONE		CN	6.7 CloneMessage.java	Max
9	DE_EXCEPTION		DE	2.2 StringPlacer.java	Elina
10	DMI_RANDOM		DMI	3.7 DatabaseConnect.java	Elina
11	EQ_EQUALS		EQ	1.3 StringCheck.java	John
12	IJU_TEST		IJU	9.3 DatabaseTest.java	John
13	IL_LOOP		IL	7.2 FormValidate.java	Tom
14	CI_FINAL		CI	1.6 MessageSender.java	Max
15	SQL_CONSTANT		SQL	3.5 DatabaseInsert.java	Elina

Filters

☒ Select All ☐ Deselect All

☒ tool1

☒ tool2

☒ tool3

☒ tool4

☒ tool5

☒ tool6

☒ tool7

☒ tool8

☒ tool9

☒ tool10

Bugs
☐ My Bugs
☒ All Bugs

Vulnerability Type
☐ SQL Injection
☐ XSS

Bug Description

XSS: Anti cross-site scripting filter (XSS_CONFIG)

Wrap the HTTP request object in a specialized HttpServletRequestWrapper that will perform filtering.

Fix Now

Know More

MSAT Interface

Project: Alpha - Selected Bug Description

XSS: Anti cross-site scripting filter (XSS_CONFIG)

You should configure it as the first filter in your chain (web.xml) and it's generally a good idea to let it catch every request made to your site. The actual implementation should consist of two classes, the actual filter is quite simple, it wraps the HTTP request object in a specialized HttpServletRequestWrapper that will perform the filtering.

he wrapper overrides the `getParameterValues()`, `getParameter()` and `getHeader()` methods to execute the filtering before returning the desired field to the caller. The actual XSS checking and stripping is performed in the `stripXSS()` private method.

Suggested Quick Fixes:

```

<filter>
<filter-name>XSSFilter</filter-name>
<filter-class>com.example.xss.XSSFilter</filter-class>
</filter>
<filter-mapping>
<filter-name>XSSFilter</filter-name>
<url-pattern>/</url-pattern>
</filter-mapping>

```

Apply

Filters

☐ Select All ☐ Deselect All

☐ tool1

☐ tool2

☐ tool3

☐ tool4

☐ tool5

☐ tool6

☐ tool7

☐ tool8

☐ tool9

☐ tool10

MSAT Interface

Project: Alpha - Selected Bug Description

XSS: Anti cross-site scripting filter (XSS_CONFIG)

You should configure it as the first filter in your chain (web.xml) and it's generally a good idea to let it catch every request made to your site. The actual implementation should consist of two classes, the actual filter is quite simple, it wraps the HTTP request object in a specialized HttpServletRequestWrapper that will perform the filtering.

he wrapper overrides the `getParameterValues()`, `getParameter()` and `getHeader()` methods to execute the filtering before returning the desired field to the caller. The actual XSS checking and stripping is performed in the `stripXSS()` private method.

Suggested Quick Fixes:

```

<filter>
<filter-name>XSSFilter</filter-name>
<filter-class>com.example.xss.XSSFilter</filter-class>
</filter>
<filter-mapping>
<filter-name>XSSFilter</filter-name>
<url-pattern>/</url-pattern>
</filter-mapping>

```

Apply

 The Revert option helps to carry traceability of bugs in your codebase with respect to multiple tools analysis. The **number** represent bugs fixed by the commit and **number** represent the new bugs introduced with this commit.

Filters

☐ Select All ☐ Deselect All

☐ tool1

☐ tool2

☐ tool3

☐ tool4

☐ tool5

☐ tool6

☐ tool7

☐ tool8

☐ tool9

☐ tool10

MSAT Interface

Project: Alpha - Selected Bug Description

XSS: Anti cross-site scripting filter (XSS_CONFIG)

You should configure it as the first filter in your chain (web.xml) and it's generally a good idea to let it catch every request made to your site. The actual implementation should consist of two classes, the actual filter is quite simple, it wraps the HTTP request object in a specialized HttpServletRequestWrapper that will perform the filtering.

he wrapper overrides the `getParameterValues()`, `getParameter()` and `getHeader()` methods to execute the filtering before returning the desired field to the caller. The actual XSS checking and stripping is performed in the `stripXSS()` private method.

Suggested Quick Fixes:

```
<filter>
<filter-name>XSS_CONFIG</filter-name>
<filter-class>org.apache.struts2.views.defaults.DefaultServletWrapper</filter-class>
</filter>
<filter>
<filter-name>XSS_CONFIG</filter-name>
<filter-class>org.apache.struts2.views.defaults.DefaultServletWrapper</filter-class>
</filter>
```

Apply

Filters

☒ Select All ☐ Deselect All

☒ tool1

☒ tool2

☒ tool3

☒ tool4

☒ tool5

☒ tool6

☒ tool7

☒ tool8

☒ tool9

☒ tool10

S. No.	Commit ID	Time Stamp	tool1	tool2	tool3	tool4	tool5	tool6	tool7	tool8	tool9	tool10	Total	Revert
1	fcd121	15-06-2019 09:56	0 1	0 2	2 0	2 1	0 1	0 2	2 0	2 1	0 1	0 2	3 4	
2	efd008	16-06-2019 14:09	0 1	1 1	0 1	0 2	0 1	1 1	0 1	0 2	0 1	1 1	2 6	
3	vcs113	16-06-2019 15:23	2 0	2 1	0 1	1 1	2 0	2 1	0 1	1 1	2 0	2 1	4 5	
4	fes254	16-06-2019 17:45	0 1	0 2	2 0	2 1	0 1	0 2	2 0	2 1	0 1	0 2	3 6	
5	xsd785	17-06-2019 09:35	0 1	1 1	0 1	0 2	0 1	1 1	0 1	0 2	0 1	1 1	2 3	
6	fcd121	18-06-2019 09:56	2 0	2 1	0 1	1 1	2 0	2 1	0 1	1 1	2 0	2 1	2 5	
7	edf008	19-06-2019 14:09	0 1	0 2	2 0	2 1	0 1	0 2	2 0	2 1	0 1	0 2	4 5	
8	vc113	19-06-2019 15:23	0 1	1 1	0 1	0 2	0 1	1 1	0 1	0 2	0 1	1 1	4 4	
9	fse254	19-06-2019 17:45	2 0	2 1	0 1	1 1	2 0	2 1	0 1	1 1	2 0	2 1	3 2	
10	xds785	20-06-2019 09:35	0 1	0 2	2 0	2 1	2 0	2 1	2 0	2 1	0 1	0 2	1 1	
11	fgd547	20-06-2019 10:23	0 1	1 1	2 0	2 1	2 0	2 1	2 0	2 1	0 1	1 1	0 2	