



Relatório de CTF

Título do CTF – Plataforma

| Informações do documento | |
|--------------------------|---|
| Referência | CTF de estudo – Vinícius Takashi |
| Nº Revisão | 1 |
| Data de publicação | 07/09/2025 |
| Link | https://tryhackme.com/room/ignite |

| | | |
|-----------|-------------------|------------|
| Redação | Vinícius Takashi | Estudante |
| Revisão | Nome do revisor | Orientador |
| Aprovação | Nome do aprovador | Diretor |

| Histórico de revisões | | |
|-----------------------|------------|-----------|
| Nº | Entregas | Descrição |
| 0 | 07/09/2025 | Produção |
| 1 | DD/MM/AAAA | Revisão |
| 2 | DD/MM/AAAA | Aprovação |

| Informações do CTF | |
|----------------------|----------------------------------|
| Nível de Dificuldade | Fácil |
| Tipo de acesso | Gratuito |
| Conceitos envolvidos | Priv Esc, RCE, reverse shell |
| Plataforma | Tryhackme, PicoCTF ou HackTheBox |
| Área | Red ou Blue |

Sumário

| | |
|------------------|---|
| Contextualização | 3 |
| Desenvolvimento | 3 |
| Pergunta 1 | 3 |
| Pergunta 2 | 3 |
| Pergunta 3 | 3 |
| Pergunta N | 3 |
| Conclusão | 3 |
| Referências | 3 |

CONTEXTUALIZAÇÃO

Esse documento tem o intuito de demonstrar as etapas para conclusão do CTF – Ignite.

DESENVOLVIMENTO

PERGUNTA 1

Para começar o desafio, foi necessário realizar a etapa de reconhecimento. Então, os primeiros passos foram rodar os comandos nmap e gobuster. A imagem a seguir mostra as respostas obtidas a partir desses comandos:

Figura 1 – Nmap

```
(kali@kali)-[~/ignite]
$ nmap 10.201.91.208 -sV -sC -T5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-07 17:24 EDT
Nmap scan report for 10.201.91.208
Host is up (0.20s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-robots.txt: 1 disallowed entry
|_ /fuel/
|_ http-title: Welcome to FUEL CMS
|_ http-server-header: Apache/2.4.18 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.80 seconds
```

Figura 2 – Gobuster

```
(kali@kali)-[~/ignite]
$ gobuster dir -u http://10.201.91.208 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.201.91.208
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.htaccess (Status: 403) [Size: 297]
/.htpasswd (Status: 403) [Size: 297]
/@ (Status: 400) [Size: 1134]
/.hta (Status: 403) [Size: 292]
/0 (Status: 200) [Size: 16597]
/assets (Status: 301) [Size: 315] [→ http://10.201.91.208/assets/]
/home (Status: 200) [Size: 16597]
/index (Status: 200) [Size: 16597]
/index.php (Status: 200) [Size: 16597]
/lost+found (Status: 400) [Size: 1134]
/offline (Status: 200) [Size: 70]
/robots.txt (Status: 200) [Size: 30]
/server-status (Status: 403) [Size: 301]
Progress: 4614 / 4615 (99.98%)

Finished
```

O passo seguinte foi analisar o endereço pelo navegador, o que trouxe algumas ideias. As imagens a seguir mostram algumas informações que podem ser usadas como formas de explorar:

Figura 3 – Versão da aplicação

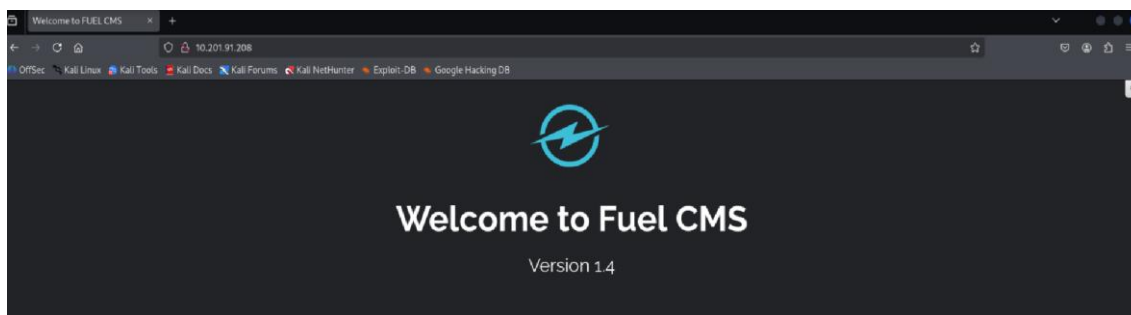
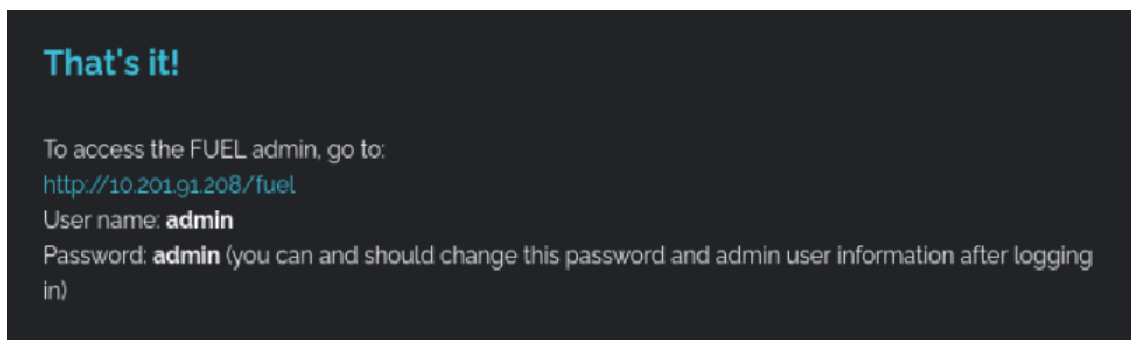


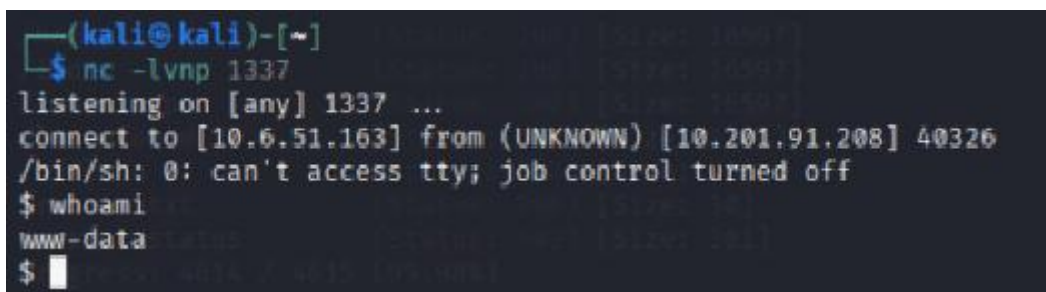
Figura 4 – Credenciais de acesso



Ao procurar a aplicação e a versão no exploit db, foi possível encontrar um exploit que funciona nessa versão. Esse exploit permite a realização de RCE. O próximo passo é executar o exploit e tentar encontrar uma maneira para realizar um reverse shell.

Após executar o exploit, foi possível entrar na máquina, mas foi necessário um reverse shell. Usando o site do pentestmonkey como auxílio, foi possível realizar o reverse shell.

Figura 5 – Reverse shell



Assim, foi possível encontrar a flag no diretório “/home/www-data” em um arquivo chamado flag.txt.

Figura 6 – flag.txt

```
Disallow: /fuel/www-data/ubuntu:/var/www  
cat /home/www-data/flag.txt  
6470e394cbf6dab6a91682cc8585059b
```

PERGUNTA 2

Para conseguir a segunda flag, foi preciso encontrar um jeito de obter acesso como root. Ao voltar para o navegador, foi possível encontrar uma dica de onde poderia estar as credenciais para o root naquela aplicação. A imagem a seguir mostra essa dica:

Figura 7 – dica

2

Install the database

Install the FUEL CMS database by first creating the database in MySQL and then importing the **fuel/install/fuel_schema.sql** file. After creating the database, change the database configuration found in **fuel/application/config/database.php** to include your hostname (e.g. localhost), username, password and the database to match the new database you created.

Essa parte deixou claro que poderia existir um arquivo que contém uma lista de usuários e senhas nesse endereço. Ao checar esse arquivo, foi possível encontrar uma possível senha para o root.

Figura 8 – database.php

```
$db['default'] = array(  
    'dsn' => '',  
    'hostname' => 'localhost',  
    'username' => 'root',  
    'password' => 'mememe',  
    'database' => 'fuel_schema',  
    'dbdriver' => 'mysqli',  
    'dbprefix' => '',  
    'pconnect' => FALSE,  
    'db_debug' => (ENVIRONMENT !== 'production'),  
    'cache_on' => FALSE,  
    'cachedir' => '',  
    'char_set' => 'utf8',  
    'dbcollat' => 'utf8_general_ci',  
    'swap_pre' => '',  
    'encrypt' => FALSE,  
    'compress' => FALSE,  
    'stricton' => FALSE,  
    'failover' => array(),  
    'save_queries' => TRUE
```

Ao testar essa senha, foi possível ter acesso como root. Então, no diretório raiz se encontrava o arquivo “root.txt” com a última flag.

Figura 9 – root.txt

```
root@ubuntu:~# cat root.txt
cat root.txt
b9bbcb33e11b80be759c4e844862482d
root@ubuntu:~#
```

CONCLUSÃO

Com a conclusão desse CTF, foi possível praticar e testar meus conhecimentos sobre RCE e reverse shell.

REFERÊNCIAS

<https://www.exploit-db.com/exploits/50477>

<https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>