Relatório de CTF

Título do CTF – Plataforma

Informações do documento	
Referência	CTF de estudo – Vinícius Takashi
N° 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		
N°	**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

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 rodas os comandos nmap e gobuster. A imagem a seguir mostra as respostas obtidas a partir desses comandos:

Figura 1 – Nmap

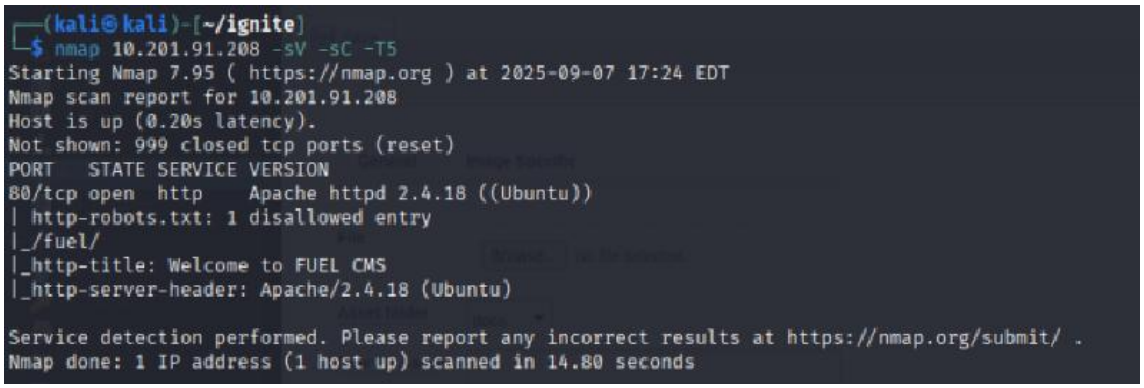
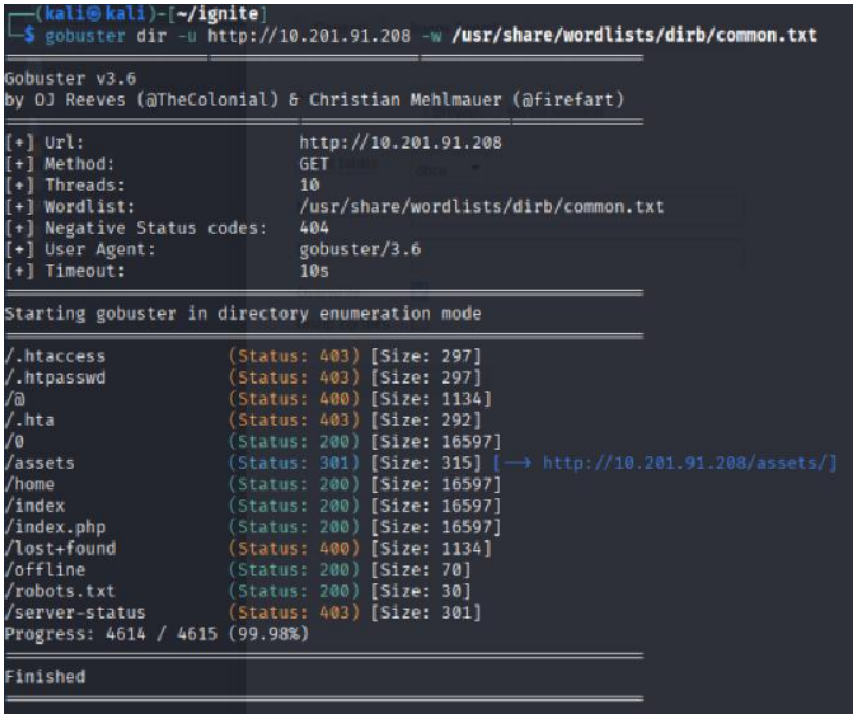


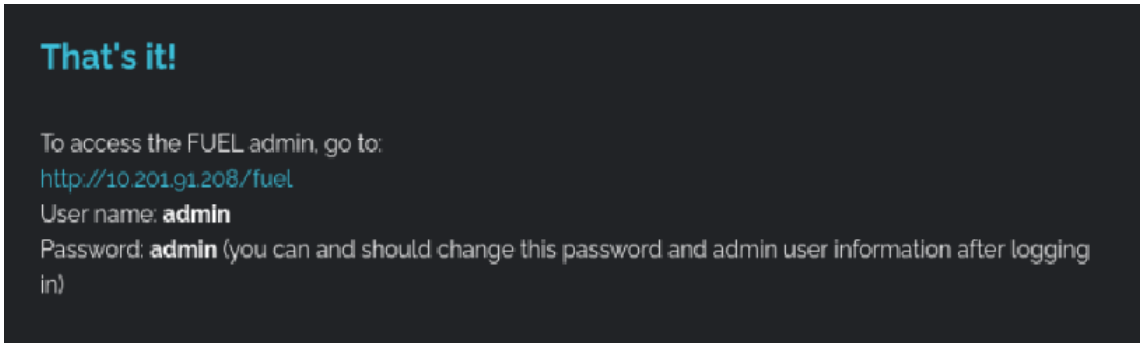
Figura 2 – Gobuster



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

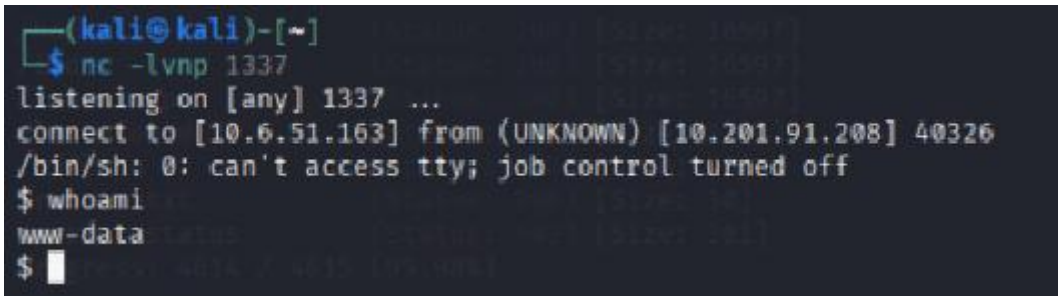
Figura 4 – Credenciais de acesso



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.

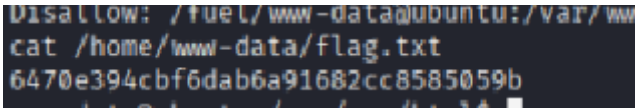
Após executar o exploit, foi possível entrar na máquina, mas foi necessário um reverse shell. Usando o site do pentestmonkey como auxílio, foi possível realizar o reverse shell.

Figura 5 – Reverse shell



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

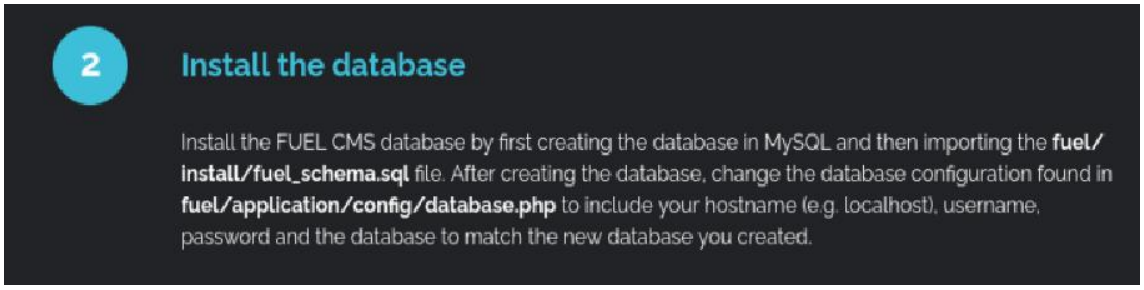
Figura 6 – flag.txt



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

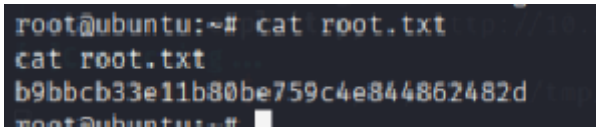


Essa parte deixou claro que poderia existir um arquivo que contêm uma lista de usuários e senhas nesse endereço. Ao checar esse arquivo, foi possível encontrar uma possível senha para o root.

Figura 8 – database.php

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



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