Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Título do CTF – Plataforma

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | CTF de estudo – **Vulnerability Capstone** |
| **N° Revisão** | 1 |
| **Data de publicação** | 8/9/2025 |
| **Link** | https://tryhackme.com/room/vulnerabilitycapstone |

|  |  |  |
| --- | --- | --- |
| **Redação** | Nome do realizador | Guilherme Ronca |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | DD/MM/AAAA | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Pago |
| **Conceitos envolvidos** | Reverse Shell, Reconnaissance, Exploits |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs)

[Subtítulo caso necessário 3](#_heading=h.30j0zll)

[Desenvolvimento 3](#_heading=h.1fob9te)

[Conclusão 7](#_heading=h.1t3h5sf)

[Referências 7](#_heading=h.4d34og8)

**Contextualização**

O objetivo do CTF é ensinar estudantes do TryHackMe a pesquisar por vulnerabilidades já encontradas e utilizá-las com o intuíto de de invadir sistemas em risco.

**Desenvolvimento**

Primeiramente, começo com o nmap do sistema:

A computer screen shot of a program

AI-generated content may be incorrect.

Com o http aberto podemos ver que o IP está rodando uma página web, assim coloco o número de IP no navegador.

A screenshot of a computer

AI-generated content may be incorrect.

Procuro por informações dentro da página e encontro a seguinte:

A screen shot of a computer screen

AI-generated content may be incorrect.

Com esse usuário e senha, vou para esse link e preencho os campos.

A screenshot of a computer

AI-generated content may be incorrect.

Dentro do site, consegui a informação da versão serviço rodando dentro do sistema. A Fuel CMS 1.4.1. Pesquisando no Exploit Database encontrei o seguinte exploit.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Tentei rodar e a principio tudo estava a caminho, porém todo comando que eu tentei rodar, o sistema só voltava system. Com isso tentei procurar outros exploits.

A blue and white screen

AI-generated content may be incorrect.

Tentei o segundo, que era um código ruby:

A screenshot of a computer

AI-generated content may be incorrect.

Porém, não obtive sucesso. Tentei mais uma vez com o terceiro exploit do ExploitDBm, um código em python2:

A computer screen shot of a computer code

AI-generated content may be incorrect.

Novamente o exploit não funcionou para esse sistema. Pesquisando um pouco mais descobri um outro exploit em um github feito pelo user anir0y. Copiei para a minha máquina e rodei.

A screenshot of a computer screen

AI-generated content may be incorrect.

Rodando o shell, eu consegui acesso ao sistema. Fazendo a procura da flag dentro do sistema, fui navegando dentro do servidor utilizando comandos do Linux, até que enfim encontrei o diretório home, que continha a flag.txt:

A screenshot of a computer

AI-generated content may be incorrect.

**Conclusão**

O CTF em si não foi técnicamente díficil, porém o maior desafio foi encontrar um exploit funcional para o sistema. Me fez refletir sobre bug hunting e ter conhecimento necessário em programação e sistemas para conseguir desenvolver os meus próprios exploits.

**Referências**

ANIR0Y. **fuel-cms.py**. Gist. Disponível em: <https://gist.github.com/anir0y/8529960c18e212948b0e40ed1fb18d6d#file-fuel-cms-py>. Acesso em: 9 set. 2025.

ZANNI, Alexandre. **Fuel CMS 1.4.1 - Remote Code Execution (2)**. Exploit Database. Disponível em: <https://www.exploit-db.com/exploits/49487>. Acesso em: 9 set. 2025.

**NVD - CVE-2018-16763**. Nist.gov. Disponível em: <https://nvd.nist.gov/vuln/detail/CVE-2018-16763>.