Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Ignite – Tryhackme

|  |  |
| --- | --- |
| **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** | Alexandre Gualiume Coruquieri | Coordenador |
| **Aprovação** | Alexandre Gualiume Coruquieri | Coordenador |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 07/09/2025 | Produção |
| **1** | 13/09/2025 | Revisão |
| **2** | 13/09/2025 | Aprovação |

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

**Sumário**

[Contextualização 3](#_Toc208670880)

[Desenvolvimento 3](#_Toc208670881)

[User.txt 3](#_Toc208670882)

[Root.txt 5](#_Toc208670883)

[Conclusão 6](#_Toc208670884)

[Referências 6](#_Toc208670885)

Contextualização

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

Desenvolvimento

User.txt

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

Texto

O conteúdo gerado por IA pode estar incorreto.

Figura 2 – Gobuster

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

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

Interface gráfica do usuário, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Figura 4 – Credenciais de acesso

Texto

O conteúdo gerado por IA pode estar incorreto.

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 shellTexto

O conteúdo gerado por IA pode estar incorreto.

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

Figura 6 – flag.txt

Tela de computador com texto preto sobre fundo branco

O conteúdo gerado por IA pode estar incorreto.

Root.txt

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

Texto

O conteúdo gerado por IA pode estar incorreto.

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

Texto

O conteúdo gerado por IA pode estar incorreto.

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

Texto

O conteúdo gerado por IA pode estar incorreto.

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>