Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

EvilGPT – Tryhackme

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | EvilGPT – Eike G. Barbosa |
| **N° Revisão** | 1 |
| **Data de publicação** | 24/03/2025 |
| **Link** | https://tryhackme.com/room/HackfinityBattleEncore |

|  |  |  |
| --- | --- | --- |
| **Redação** | Eike G. Barbosa | Estudante |
| **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** | Gratuito |
| **Conceitos envolvidos** | Prompt Injection |
| **Plataforma** | Tryhackme |
| **Área** | Red |

**Sumário**

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

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

[What is the root flag? 3](#_heading=h.3znysh7)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

**Contextualização**

Este CTF, chamado Evil GPT, consiste em você tentar burlar o filtro de uma IA, não muito inteligente e rodar os comandos para poder ter acesso a Flag.txt

**Desenvolvimento**

**What is the root flag?**

Primeiro conectamos no servidor com um “netcat” no ip e na porta.

Interface gráfica do usuário, Site

O conteúdo gerado por IA pode estar incorreto..

Podemos ver que podemos rodar alguns comandos, para tentar achar a flag.

Então vou usar o comando “ls”

**Comando usado:** ls -la

Texto

O conteúdo gerado por IA pode estar incorreto.

Após isso, podemos notar que a I.A não é tão inteligente, já que ela corrige os comandos que nós tentamos, como por exemplo o comando “cd”

Interface gráfica do usuário

O conteúdo gerado por IA pode estar incorreto.

Rodando o “ls -la” pelos diretórios, podemos notar que não há nenhuma flag nos diretórios padrões.   
Então vamos olhar o /root

Texto

O conteúdo gerado por IA pode estar incorreto.

Podemos achar a “flag.txt”, porém não o conteúdo dentro do arquivo. Vamos tentar pegar ela então. Porém, temos um problema, a I.A não aceita o “cat”.

Texto

O conteúdo gerado por IA pode estar incorreto.

Vamos tentar com o “sudo” na frente do comando, para tentar ter total privilégio.

Interface gráfica do usuário, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

**Conclusão**

Este CTF é feito para testar a sua paciência e também a sua noção de diretórios, burlando o filtro que tem na IA para resolver o desafio.

**Referências**

Não há.