Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

St3g0 – picoCTF

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | St3g0 – Pedro Borges |
| **N° Revisão** | 1 |
| **Data de publicação** | 24/04/2025 |
| **Link** | https://play.picoctf.org/practice/challenge/305?category=4&difficulty=2&page=2 |

|  |  |  |
| --- | --- | --- |
| **Redação** | Nome do realizador | Pedro Borges |
| **Revisão** | Sérgio Guidi Trovo | Coordenador |
| **Aprovação** | Sérgio Guidi Trovo | Coordenador |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 06/04/2025 | Produção |
| **1** | 24/04/2025 | Revisão |
| **2** | 24/04/2025 | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Médio |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Forense e esteganografia |
| **Plataforma** | PicoCTF |
| **Área** | Red |

**Sumário**

[Contextualização 2](#_heading=h.gjdgxs)

[Desenvolvimento 2](#_heading=h.1fob9te)

[Download this image and find the flag. 2](#_heading=h.3znysh7)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

**Contextualização**

Um CTF hospedado na plataforma picoCTF, entitulado St3g0 e com flags indicando que é um desafio de dificuldade mediana, na área de forense e envolve conceitos de esteganografia.

**Desenvolvimento**

**Download this image and find the flag.**

A plataforma começa fornecendo uma imagem para baixarmos. Após o download, vejo que o nome e extensão da imagem são, respectivamente, pico.flag, png. (Print da imagem abaixo)

A white text on a grey background

AI-generated content may be incorrect.

Uma vez que o desafio já deu indícios (no título e nas flags) que haveria algo relacionado a esteganografia, fui direto buscar alguma ferramenta em que eu poderia utilizar essa técnica no arquivo .png.

Encontrei a biblioteca *zsteg* que instalei no meu terminal Kali Linux através do comando *gem install zsteg*, a palavra gem indicando que a ferramenta foi desenvolvida na linguagem de programação Ruby.

Após a instalação da ferramenta e lendo a sua documentação, utilizei o comando *zsteg pico.flag.png* e obtive o seguinte resultado:

A screenshot of a computer screen

AI-generated content may be incorrect.

Logo no primeiro retorno já me devolveu a flag em plain text, e assim conclui o desafio.

**Conclusão**

Apesar de estar catalogado como um CTF de dificuldade média, ele é bastante simples. O desafio demonstrou o uso básico de esteganografia em arquivos de imagem, reforçando a importância de conhecer ferramentas específicas como o zsteg.

**Referências**

Documentação zsteg <https://github.com/zed-0xff/zsteg>