Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

flags are stepic – PicoCTF

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | flags are stepic – Matheus Castilho |
| **N° Revisão** | 1 |
| **Data de publicação** | 05/04/2025 |
| **Link** | <https://play.picoctf.org/practice/challenge/481?category=4&page=1&search=> |

|  |  |  |
| --- | --- | --- |
| **Redação** | Matheus Castilho | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do revisor | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 05/04/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

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

**Sumário**

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

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

[Encontrando](#_heading=h.3znysh7) possíveis alvos de exploração 4

Buscando a flag 4

[Conclusão](#_heading=h.1t3h5sf) 5

**Contextualização**

Neste CTF foram utilizados conceitos de esteganografia, e investigação forense para obter a flag. O processo de obtenção buscou encontrar strings escondidas em um arquivo de imagem, procurando desde os metadados do arquivo, até strings escondidas em seus binários. Com isso, foi possível obter a flag utilizando o stepic, que é uma ferramenta da qual é possível ocultar e recuperar dados de imagens por meio da biblioteca Pillow, do Python.

**Desenvolvimento**

Encontrando possíveis alvos de exploração

Em primeiro lugar, ao acessar o servidor web, podemos observar uma lista com diversas bandeiras e nomes de países.

A screenshot of a computer

AI-generated content may be incorrect.

Olhando a dica do CTF, vemos que ele pede para encontrar o país que não existe no meio desses.

A screenshot of a chat

AI-generated content may be incorrect.

Logo, um dos principais suspeitos seria o país “Upanzi”, que não existe, e pode ser nosso primeiro alvo de ataque.

A screenshot of a cellphone with a flag

AI-generated content may be incorrect.

Ao observar os Dev Tools, vemos que há um caminho de imagem em todas as imagens, chamado “flags”, com algumas imagens, incluindo a do alvo.

A screen shot of a computer program

AI-generated content may be incorrect.

Ao abrir no diretório, não é possível ver nada de diferente no css.

A screenshot of a computer

AI-generated content may be incorrect.

Buscando a flag

Ao baixar a imagem, é possível utilizar o exiftools para buscar metadados da imagem. Por ser um CTF de esteganografia é possível ter este direcionamento.

A screenshot of a computer

AI-generated content may be incorrect.

Rodando a ferramenta, não foi possível encontrar nada de útil.

Porém, ao observar o nome do CTF, é possível ver uma referência a biblioteca “stepic”, que pode esconder textos em imagens e recuperá-los também, utilizando o Pillow.

A screenshot of a computer

AI-generated content may be incorrect.

Com isso, é possível escrever um script para retirar estes textos de imagens já existentes, e assim, obter a flag.

A screenshot of a computer

AI-generated content may be incorrect.

**Conclusão**

O CTF utilizou técnicas de esteganografia, exigindo a análise de imagens e, principalmente, a biblioteca stepic, que permite extrair dados ocultos em arquivos de imagem. Após identificar a imagem suspeita, foi possível aplicar um script em Python utilizando Pillow e stepic para recuperar a flag embutida. Este CTF reforça o uso de ferramentas específicas para análise forense e manipulação de imagens, forçando o usuário a procurar ferramentas diferentes para buscar os textos escondidos.