Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Transformation – PicoCTF

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Transformation – Matheus Castilho |
| **N° Revisão** | 1 |
| **Data de publicação** | 25/02/2025 |
| **Link** | https://play.picoctf.org/practice/challenge/104?category=3&page=1 |

|  |  |  |
| --- | --- | --- |
| **Redação** | Matheus da Cunha Castilho | Estudante |
| **Revisão** | Sérgio Guidi Trovo | Coordenador |
| **Aprovação** | Sérgio Guidi Trovo | Coordenador |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 22/02/2025 | Produção |
| **1** | 25/02/2025 | Revisão |
| **2** | 25/02/2025 | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Fácil |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Engenharia Reversa |
| **Plataforma** | PicoCTF |
| **Área** | Red |

**Sumário**

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

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

[Flag](#_heading=h.3znysh7)

[Conclusão 7](#_heading=h.1t3h5sf)

[Referências 7](#_heading=h.4d34og8)

**Contextualização**

Neste CTF, é fornecido um arquivo contendo uma string criptografada, na qual deve-se encontrar a flag tendo como base um código em Python fornecido na descrição. Este CTF é indicado para aprender conceitos importantes de Engenharia Reversa.

**Desenvolvimento**

**Flag**

A screenshot of a computer

AI-generated content may be incorrect.

Ao baixar o arquivo fornecido, e abri-lo em um editor de texto, foi possível observar a seguinte string:

A screenshot of a computer

AI-generated content may be incorrect.

Analisando a string em um tradutor de texto, não foi possível encontrar nada relevante, levando a crer que eram apenas caracteres em chinês tradicional, porém sem significado válido.

Então, ao analisar a descrição do CTF, é possível encontrar um código em python que utiliza de uma variável chamada “flag”.

A screenshot of a computer

AI-generated content may be incorrect.

Testando o código, declarando uma váriavel de valor aleatório, temos:

A screen shot of a computer

AI-generated content may be incorrect.

A black background with orange and white text

AI-generated content may be incorrect.

Também é possível perceber que há um operador não muito comum do Python, o “<<”.

Pesquisando sobre este operador, temos que ele desloca o valor Unicode do caractere em 8 bits pra esquerda, ou seja, equivale a multiplicá-lo por 256.

Tendo isso em vista, é possível executar um print no código fornecido e observar a lista retornada, na qual é possível perceber que são retornados cinco valores.

A screen shot of a computer

AI-generated content may be incorrect.

Com isso, vemos que a flag é codificada utilizando dois caracteres por vez, e os unindo por meio de seus valores em ASCII. No ciclo, o primeiro caractere é transformado em ASCII e seu valor multiplicado por 256, enquanto o segundo é apenas transformado em ASCII. Após isso, são somados, e o valor dessa soma é convertido em um caractere. Podemos testar isso desta maneira:

A screen shot of a computer program

AI-generated content may be incorrect.

Então, para decodificar a string podemos utilizar o seguinte script, que segue a lógica descrita acima.

A screen shot of a computer

AI-generated content may be incorrect.

Ao executá-lo, temos a flag.

A black background with white text

AI-generated content may be incorrect.

**Conclusão**

Neste CTF foi possível observar conceitos básico de Engenharia Reversa assim como utiliza de maneira simples o ASCII e Unicode. Pode ser considerado uma bom início a Engenharia Reversa para usuários que já possuem um certo nível de lógica de programação. Apesar de ser considerado fácil, pode ser bem desafiador pois exige um nível de interpretação considerável e pode ser um pouco confuso por conter caracteres em chinês tradicional, que não são muito comuns para não falantes do idioma, levando o usuário a pensar que pode se tratar de um CTF envolvendo a tradução do string.

**Referências**

<https://www.w3schools.com/python/ref_func_chr.asp>

<https://www.w3schools.com/python/ref_func_ord.asp>

<https://www.treinaweb.com.br/blog/uma-introducao-a-ascii-e-unicode>