Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Redaction gone wrong – PicoCTF

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Redaction gone wrong – Pedro Borges |
| **N° Revisão** | 1 |
| **Data de publicação** | 26/08/2025 |
| **Link** | https://play.picoctf.org/practice/challenge/290 |

|  |  |  |
| --- | --- | --- |
| **Redação** | Pedro Borges | Estudante |
| **Revisão** | Sérgio Guidi Trovo | Coordenador |
| **Aprovação** | Sérgio Guidi Trovo | Coordenador |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 21/04/2025 | Produção |
| **1** | 26/08/2025 | Revisão |
| **2** | 26/08/2025 | Aprovação |

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

**Sumário**

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

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

Can you find an important key that was not redacted properly?  
[Conclusão 3](#_heading=h.1t3h5sf)

**Contextualização**

O CTF "Redaction gone wrong" aborda a falha comum de esconder informações sensíveis de forma inadequada em documentos.

O desafio mostra como dados "ocultos" com redatores visuais ainda podem ser recuperados do conteúdo original.

“Agora você NÃO me vê.

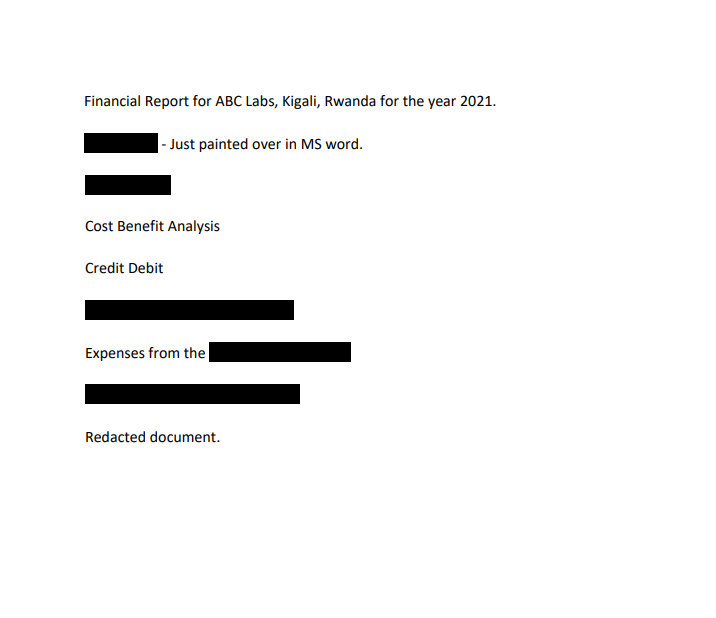
Este relatório contém alguns dados críticos, alguns dos quais foram redigidos corretamente, enquanto outros não. Você consegue encontrar uma chave importante que não foi redigida corretamente?”

**Desenvolvimento**

**Pergunta 1**

**Can you find an important key that was not redacted** **properly?**

Primeiro baixei o arquivo disponibilizado e percebi que se tratava de um PDF. Ao abrir o arquivo, notei que havia uma linha informando que certas frases haviam sido "redigidas" usando o próprio Microsoft Word. A partir disso, parti do pressuposto que as informações cobertas (vide imagem abaixo) haviam sido a censuradas de forma visualmente, e não de forma segura.



Com isso em mente, comecei a explorar o conteúdo do documento. Observei que as partes “censuradas” estavam cobertas por formas pretas, como caixas inseridas manualmente sobre o texto. Percebi que, mesmo sem enxergar o conteúdo coberto, ainda era possível selecionar o texto oculto. Então, selecionei essas áreas, copiei o conteúdo e colei em outro local utilizando a opção de colar como texto simples. Dessa forma, consegui visualizar claramente as informações que estavam escondidas sob as caixas pretas.

Seguindo esse processo, fui removendo as coberturas e, com isso, encontrei a flag do desafio escrita por baixo de uma dessas formas. Ela estava no formato picoCTF{...}. Assim, consegui recuperar a informação sensível que havia sido mal redigida e completei o desafio com sucesso.

**Conclusão**

Apesar de ser um desafio extremamente simples, O CTF ilustra de forma clara e didática um erro bastante comum na manipulação de documentos: a tentativa de censurar informações apenas cobrindo visualmente o texto, sem de fato removê-lo. Esse tipo de falha acontece com frequência no mundo real e pode expor dados sensíveis de maneira grave. O desafio reforça a importância de entender como as ferramentas funcionam e de aplicar boas práticas ao lidar com informações confidenciais.