

Resolução desafio HackerSec

Nome: Noob

Categoria: Criptografia e Cifras (Iniciante)

Pontuação: 5 pontos

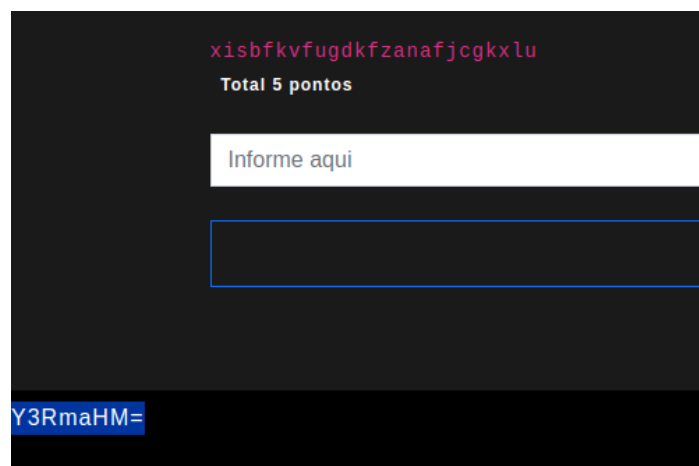
Descrição: Um desafio que envolve criptografia, permitindo ao usuário compreender melhor sua atuação e exercício do raciocínio para resolver falhas.

Resolução

Inicialmente em todo desafio, é importante analisar o código-fonte da página, para que o mesmo possa ser observado e analisado e o atacante consiga extrair o máximo de informações possíveis para obter a *flag*. Ao descer até o final da página do código-fonte, é possível observar, na linha **415** o seguinte código:

```
412  
413     </div>  
414 </main>  
415 <p style="color: #000">Y3RmaHM=</p>  
416 <br>  
417 <footer class="footer text-white-50">  
418     <div class="container">
```

Essa tag HTML possui a edição de cor do CSS, ocultando o texto na página em que aparece, pois é camuflada com a mesma cor do background. Apertando CTRL + A na página inicial é possível ver o texto oculto, pois é marcado com a seleção e fica visível.



Iremos decifrar esse texto, para obter alguma informação legível e compreensível.

Você pode utilizar as ferramentas da própria plataforma para resolver a criptografia, indo ao cabeçalho da página e clicando em “Ferramentas”, após isso em “Criptografia” e selecionando a opção “Decode”.

Ao inserir o código encontrado no campo de criptografia para que seja decifrado, iremos obter a seguinte informação:



The screenshot shows a web interface with a dark background. At the top, there is a white input field containing the text "Y3RmaHM=". Below this field is a button labeled "Consultar". Underneath the button, there is a dark grey box containing the text "Tipo = base64" and "Decrypt = ctfhs".

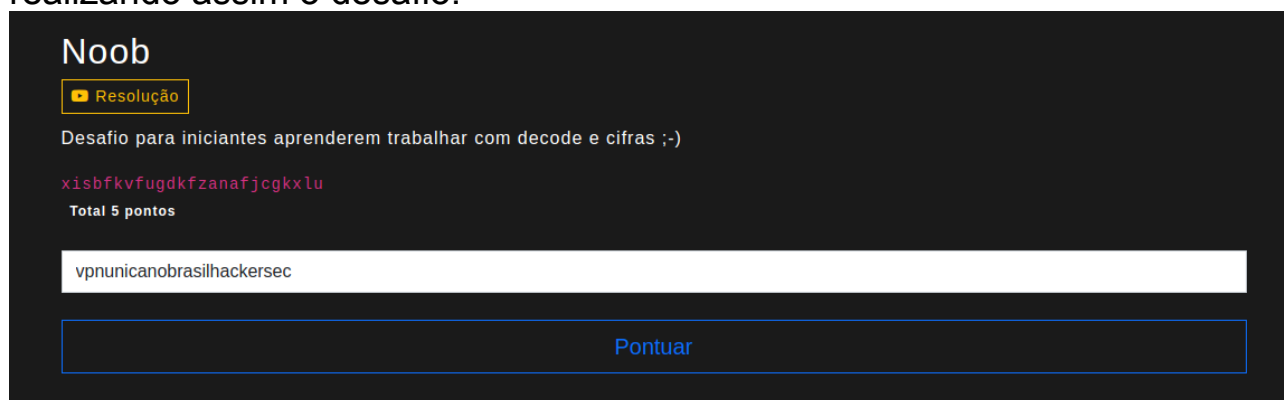
O texto decifrado é "ctfhs", devemos armazenar essa informação em um bloco de notas ou algum lugar que possa ser consultado com facilidade quando for necessário.

Após isso, ainda há o texto que não está legível na página inicial, devemos explorar para conseguirmos decifrá-lo e obter a *flag*. O texto da página inicial está com a Cifra de Vigenère, uma cifra que usa diversas cifras de César em várias partes do texto, possui uma criptografia polialfabética e necessita de uma chave para criptografar e decifrar.

Iremos copiar essa cifra de Vigenère e acessar novamente o campo de ferramentas para que seja decifrado, entretanto, dessa vez iremos selecionar o campo "Cifras" ao invés do "Criptografia" e após isso selecionaremos "Vigenère" para que possamos decifrar a *flag*. Com o texto criptografado em mãos iremos clicar em "Selecione a ação" e optaremos por "decifrar", após isso inserimos o texto cifrado no campo "Insira o texto" e a senha será a que conseguimos decifrar inicialmente "ctfhs" e salvamos no bloco de notas.

Ao inserirmos tanto o texto a ser decifrado, quanto a senha para decifrá-lo e realizarmos a consulta, obteremos acesso à *flag*: "vpnunicanobrasilhackersec".

Devemos inserir ela na página inicial do desafio e clicar em "Pontuar" realizando assim o desafio.



The screenshot shows a challenge page titled "Noob". It has a yellow button labeled "Resolução". Below the button, it says "Desafio para iniciantes aprenderem trabalhar com decode e cifras ;-)". There is a line of red text: "xisbfkvfugdkgfzanafjcgkxlu". Below that, it says "Total 5 pontos". There is a white input field containing the text "vpnunicanobrasilhackersec". At the bottom, there is a button labeled "Pontuar".

Considerações finais

Este é um ótimo desafio para o exercício de lógica na exploração de falhas, fazendo com que o atacante procure por informações sensíveis no código fonte, aprenda a lidar com criptografia e explore novas formas de ver uma página web.

Desejo boa sorte e bons estudos na jornada do hacking e lembre-se: Com foco e persistência, você pode chegar a lugares jamais imaginados!

Um grande abraço :D

Contato

@undergroundbyters (Twitter)