Relatório de Desafios - Wicked SA

Desafio 1: Acesso ao Painel de Autenticação

Passos:

1. **Iniciar Ação**: Clique no botão de login na página principal.
2. **Tentativa de Acesso**: Utilize o e-mail contato@wicked.com (encontrado na página principal) e a lista de palavras "rockyou.txt" para tentar acessar o painel de autenticação.
3. **Senha**: A senha "azerty" está na linha 2674 da lista de palavras.
4. **Observação da Bandeira**: Após a autenticação, localize e observe a bandeira correspondente.

Desafio 2: Token de Sessão

Procedimento:

1. **Acesso ao Painel**: Após a autenticação, vá até o painel do navegador onde os tokens de sessão são armazenados.
2. **Identificação do Token**: Encontre o "SessionToken" obtido após o login.
3. **Decodificação do Token**: Use o site https://jwt.io para decodificar o token JWT.
4. **Localização da Bandeira**: Procure a bandeira no campo "flag" do token decodificado.

Desafio 3: Elevação de Privilégios

Etapas:

1. **Acesso ao Painel de Tokens**: Com autenticação bem-sucedida, acesse o painel do navegador.
2. **Observação do Token**: Identifique o "SessionToken".
3. **Decodificação do JWT**: Use https://jwt.io para decodificar o token JWT.
4. **Alteração de Perfil**: Mude o valor de "role" de "employee" para "admin".
5. **Substituição do Token**: Troque o token antigo pelo novo com o parâmetro modificado.
6. **Acesso à Administração**: Vá para "/dashboard".
7. **Atenção à Bandeira**: Observe a bandeira na rota de administração.

Desafio 4: Download do Template XML

Instruções:

1. **Início do Processo**: Clique no botão de "download" para obter o modelo XML.
2. **Verificação da Bandeira**: Confira o valor da bandeira no campo "flag" do XML baixado.

Desafio 5: Modificação e Upload do XML

Passos:

1. **Edição do XML**: Altere o campo `<city>New York</city>` no modelo XML para:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE replace [<!ENTITY xxe "file:///etc/passwd"> ]>
<root>
  <person>
    <name>John Doe</name>
    <company>Wicked</company>
    <city>&xxe;</city>

<flag>TAC_2023{b1c2d3e4f5a6b7c8d9e0f1a2b3c4d5e6f7g8h9i0j1k2l3m4n5o6p7q8r9s0t1u2v3
</flag>
  </person>
</root>
```

2. **Upload do XML Modificado**: Realize o upload do XML alterado através do botão "upload".
3. **Observação da Bandeira**: Fique atento ao valor da bandeira na senha do último usuário após o upload.