


| | | |
|---|---|-------------------------|
|  | INSTITUTO FEDERAL DO RN Campus Natal-Central | |
| | Disciplina: Teste de Software | |
| | Professor(a): Plácido A. Souza Neto | |
| | Discente: | Matrícula: |
| | Curso: TADS | Semestre: 2024.1 |
| | Lista 2.4: Testes de Segurança | |

Introdução

Para iniciar o TP, você precisará clonar o repositório do projeto e garantir que está na pasta raiz do mesmo. Antes de seguir para a execução dos contêineres, certifique-se de que o Docker está instalado e em execução na sua máquina. Se estiver tudo certo, siga os passos abaixo:

1. Clone o repositório do projeto:

```
git clone https://github.com/IFRN/testes-de-seguranca.git
cd testes-de-seguranca
```

2. Inicie os contêineres necessários executando o comando:

```
docker compose up -d
```

3. Após a execução bem-sucedida do comando, acesse os seguintes endereços no seu navegador:

- <http://127.0.0.1:8000/api/doc/> - Para acessar a documentação da API. Algumas falhas de segurança podem ser exploradas diretamente por aqui ou através de um cliente REST, como Postman, Insomnia, ou Hopscotch.
- <http://127.0.0.1/> - Para acessar o frontend da aplicação.

Acesso ao Sistema

Cada aluno da turma já possui um usuário cadastrado no sistema. Para fazer login, utilize o número da sua matrícula como nome de usuário e a senha padrão 123. Esse acesso inicial permitirá que você explore as vulnerabilidades do sistema e responda às questões propostas no TP.

Acesso à Documentação da API

Ao acessar a documentação da API em <http://127.0.0.1:8000/api/doc/>, você precisará fazer login através do Swagger para testar os endpoints protegidos. Utilize o botão **Authorize** localizado no canto superior direito da interface Swagger, e insira seu *access token* que pode ser conseguido através do endpoint `/login/`.

Ao explorar as vulnerabilidades e responder às questões, envie suas respostas através do **formulário**. Não se esqueça de utilizar seu e-mail `@escolar.ifrn.edu.br` ao submeter o formulário.

Imagine que você é um detetive da segurança e conseguiu se infiltrar no sistema da Plácido Drive. Utilize um SQL Injection para acessar a lista de todos os usuários. Seu objetivo é verificar se há algum usuário que não deveria estar lá. *Dica: existe um endpoint que deveria retornar os dados só do seu usuário, mas se usado corretamente poderá trazer informações que deveriam ser sigilosas!*

- O invasor colocou uma mensagem no lugar de seu nome completo, qual a mensagem?
1. Você descobriu um usuário que parece estar fora do lugar. Agora, é hora de descobrir seu nome de usuário. Os relatórios indicam que o invasor deixou uma mensagem na raiz da aplicação. *Dica: o endpoint de exclusão de arquivos expõe uma vulnerabilidade de Command Injection, aproveite-se dessa falha para tentar encontrar alguma pista por lá!*
 - Qual o nome de usuário (matrícula) do invasor?
 2. Agora que você descobriu qual o username do usuário malicioso, encontre qual o arquivo que ele fez upload. Você precisa entrar na conta dele alterando a senha de acesso! *Dica: Existe uma grave falha na implementação da funcionalidade de alterar senha, talvez ela permita que você troque a senha do usuário!*
 - Qual foi o nome do arquivo enviado por ele?
 3. Agora é só entrar na conta do usuário malicioso e fazer download do arquivo que ele enviou. Lá estará o código secreto para completar a tarefa!
 - Qual foi a mensagem secreta final deixada pelo nosso invasor?