INSTITUTO FEDERAL Rio Grande do Norte	**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	

Testes de Segurança

Para iniciar o TP, você precisará executar dois contêineres. Certifique-se de que o Docker está em execução em sua máquina e execute os seguintes comandos:

```
docker run -ti -d -p 8000:8000 qajuda/vulneravel
docker run -ti -d -p 80:80 qajuda/vulneravel-frontend
```

Depois de executar os comandos, acesse os seguintes endereços no seu navegador:

- `http://127.0.0.1:8000/api/doc/` - Para acessar a documentação da API (algumas falhas só poderão ser testadas aqui ou com um cliente REST, como Postman, Insomnia, Hopscotch, etc.)
- `http://127.0.0.1/` - Para acessar o frontend da aplicação

1. 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?

2. 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 que expõe uma vulnerabilidade de Command Injection, aproveite-se dessa falha para tentar encontra alguma pista por lá!*

   - Qual o nome de usuário (matricula) do invasor?

3. 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?

4. 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?