

Instituto Federal Norte de Minas
Gerais/Ciência da Computação
Disciplina: Sistemas de Informação

**Segurança: Plano de Correção das
falhas**

Outubro
2019

Instituto Federal Norte de Minas Gerais

Disciplina: Sistemas de Informação

Segurança: Plano de Correção de Falhas

Alunos: José Danilo, Rafael Teixeira, Roberto Ramos e Thamires Gonçalves

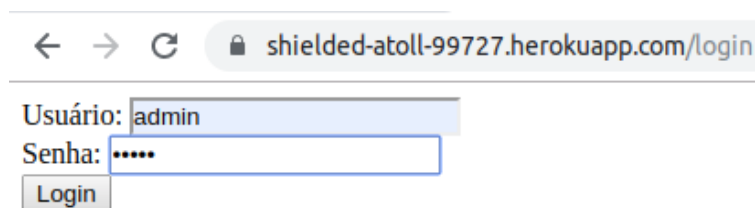
Professora orientadora: Luciana Balieiro

Outubro
2019

1 Descrição de atividades

O trabalho consiste em identificar falhas de segurança, inicialmente no "MiniApp". Falhas encontradas:

1) Senha padrão fraca;




← → ↻ shielded-atoll-99727.herokuapp.com/login

Usuário: admin

Senha:

Login

Figura 1: Login com usuário:"admin"e senha: "admin"



← → ↻ shielded-atoll-99727.herokuapp.com/login

Your login information was correct.

[Página principal](#)

Figura 2: Informações de login condizentes com o Banco de Dados



← → ↻ shielded-atoll-99727.herokuapp.com

Olá, Admin!

Como está?

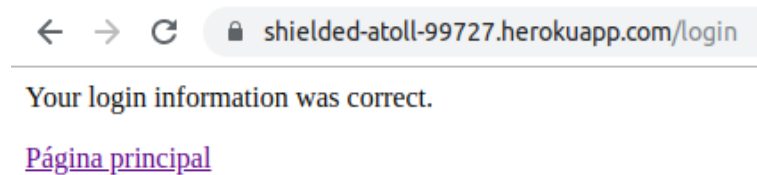
Figura 3: Acesso à pagina do usuário

Entrada como teste:



A screenshot of a web browser showing a login page. The address bar displays "shielded-atoll-99727.herokuapp.com/login". Below the address bar, there are two input fields: "Usuário:" with the text "teste" and "Senha:" with masked characters "....". A "Login" button is positioned below the password field.

Figura 4: Login com usuário:"teste"e senha: "teste"



A screenshot of the same web browser showing a success message. The address bar remains "shielded-atoll-99727.herokuapp.com/login". Below the address bar, the text "Your login information was correct." is displayed. Underneath this message is a purple underlined link labeled "Página principal".

Figura 5: Login correct



A screenshot of the web browser showing the user's main page. The address bar displays "shielded-atoll-99727.herokuapp.com". The page features a large, bold heading "Olá, Teste!" followed by the text "Como está?" in a smaller font.

Figura 6: Acesso à pagina do usuário

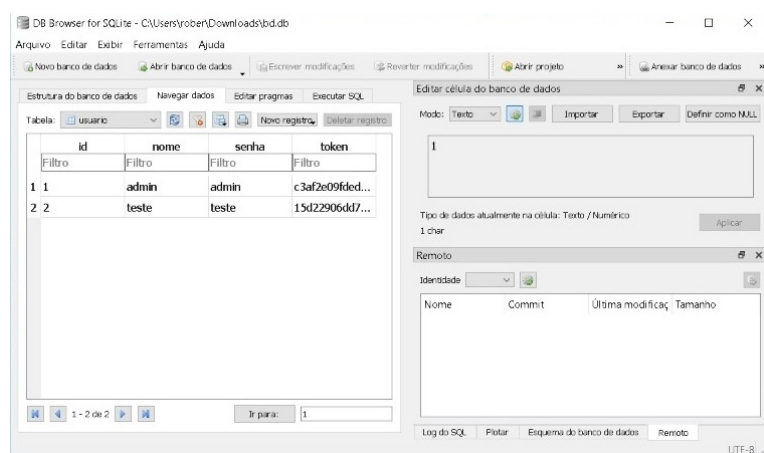
2) Ausência de opção de logout;

Olá, Teste!

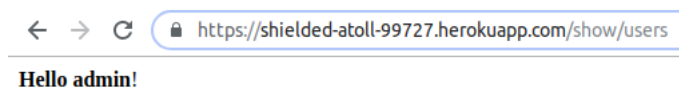
Como está?



3) Ausência de criptografia no banco de dados.



4) Acesso à pagina do sistema sem estar logado. (<https://shielded-atoll-99727.herokuapp.com/show/users>).



2 Falhas de Segurança 2ª parte

Ainda no MiniApp foi identificado uma outra falha na segurança: O SQL Injection.

Com o SQL Injection foi possível adicionar usuários personalizados, tornando assim possível obter acesso a dados restritos. Para isso foi necessário apenas inserir "'or"=' ' "no campo da senha, funcionando como se estivesse validando o usuário e senha vazios como uma combinação válida para efetuar o login.

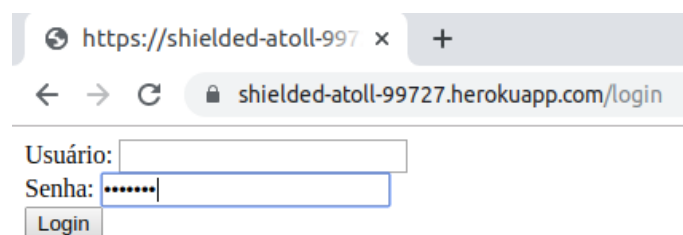
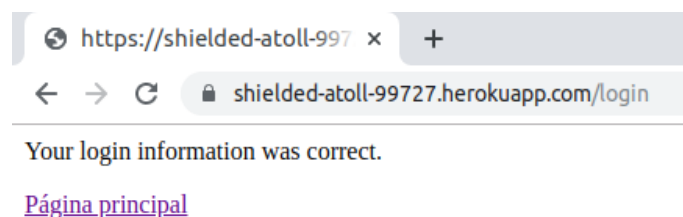
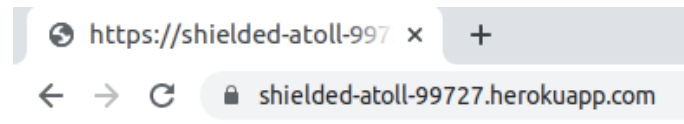


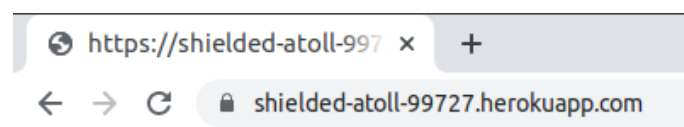
Figura 7: Falha de segurança SQL Injection





Olá, !

Como está?



Olá, Rafael!

Como está?