

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

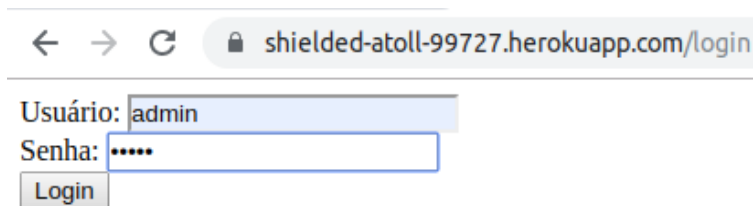
Outubro  
2019

# 1 Descrição de atividades

## 2 Falhas encontradas no Miniapp em 11/10/2019

Falhas encontradas:

### 1) Senha padrão fraca;



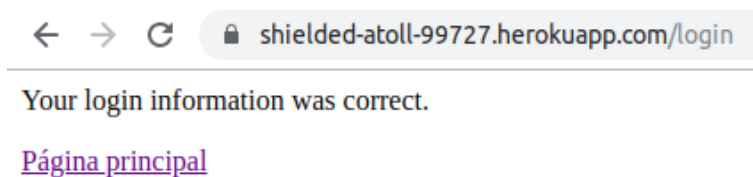
← → ↻ shielded-atoll-99727.herokuapp.com/login

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:

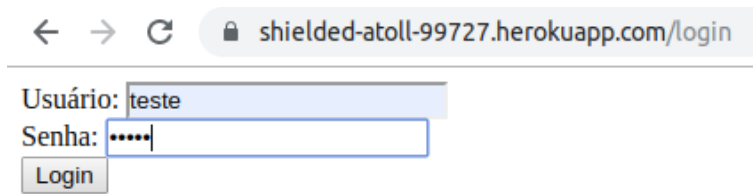


Figura 4: Login com usuário: "teste" e senha: "teste"

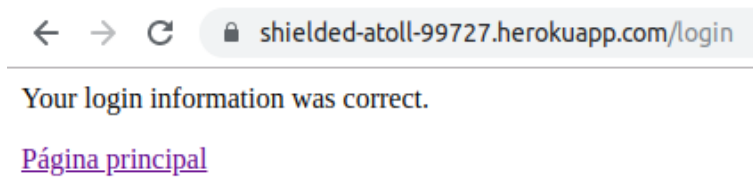
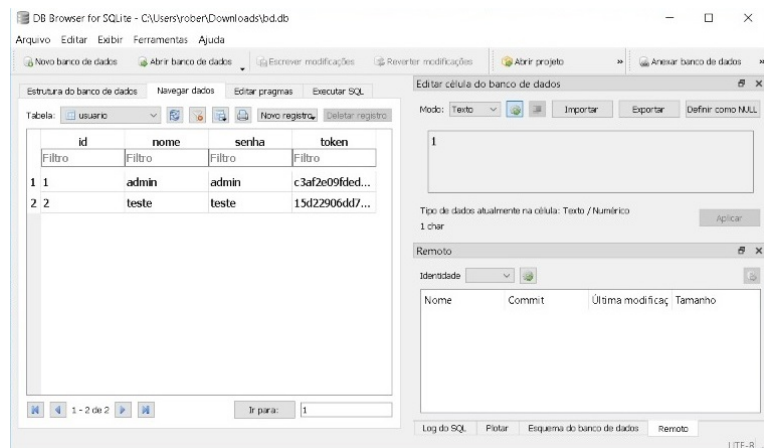


Figura 5: Login correct

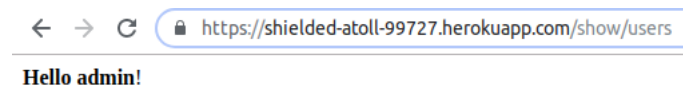


Figura 6: Acesso à pagina do usuário

- 2) Ausência de opção de logout;
- 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>).



### 3 Falhas de Segurança em Miniapp 31/10/2019

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.

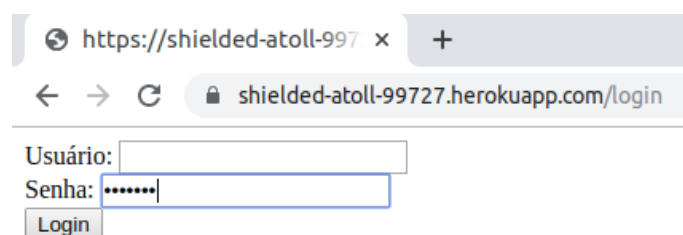
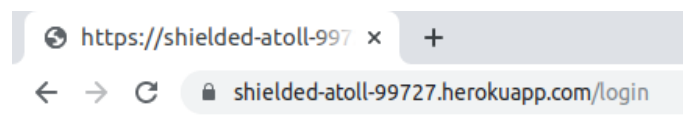
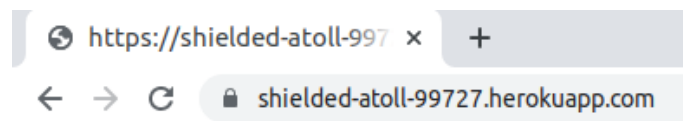


Figura 7: Falha de segurança SQL Injection



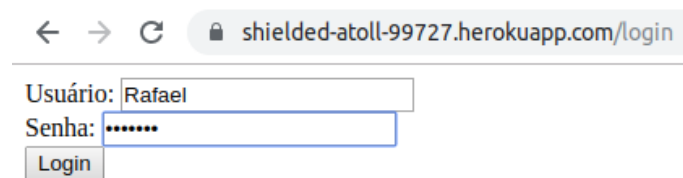
Your login information was correct.

[Página principal](#)



# Olá, !

Como está?



← → ↻ [shielded-atoll-99727.herokuapp.com/login](https://shielded-atoll-99727.herokuapp.com/login)

Usuário:

Senha:

Login

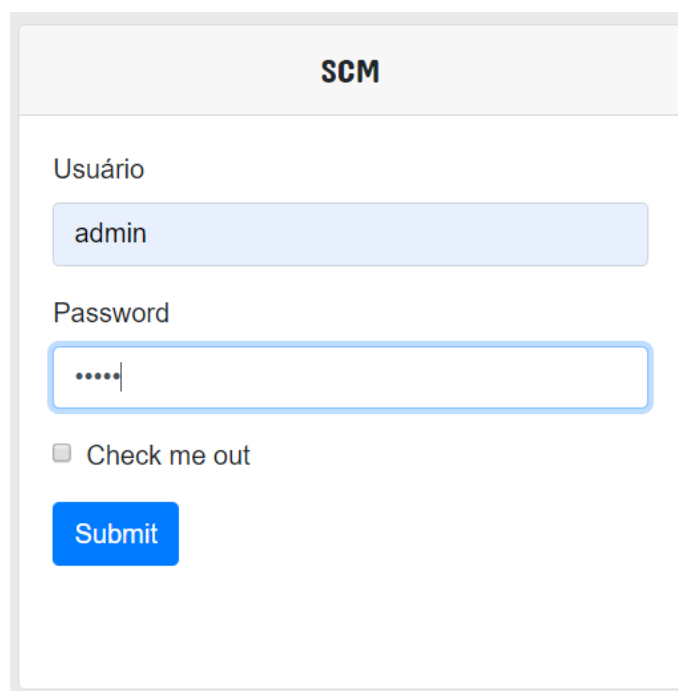


Com o SQLInjection, foi possível abrir a tela de login com qualquer usuário digitável, pois a verificação de senha retorna sempre "true" quando é inserido 'or'="" no campo senha.



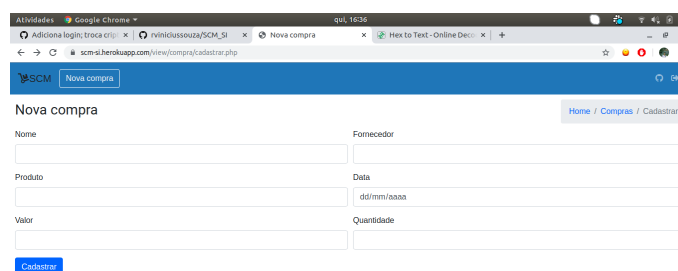
## 4 Falhas de Segurança em SCM 01/11/2019

1) Senha padrão fraca;



The image shows a login interface for a system labeled "SCM". It contains two input fields: "Usuário" (Username) with the value "admin" and "Password" with masked characters ".....". Below the password field is a checkbox labeled "Check me out" and a blue "Submit" button.

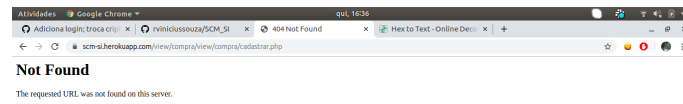
Figura 8: Login com usuário: "admin" e senha: "admin"



The image shows a web browser window displaying the "Nova compra" (New purchase) form in the SCM system. The form includes fields for "Nome" (Name), "Fornecedor" (Supplier), "Produto" (Product), "Data" (Date), "Valor" (Value), and "Quantidade" (Quantity). The "Data" field is pre-filled with "dd/mm/aaaa". A blue "Cadastrar" (Register) button is at the bottom left. The browser's address bar shows the URL "scm-si.herokuapp.com/View/compra/cadastrar.php".

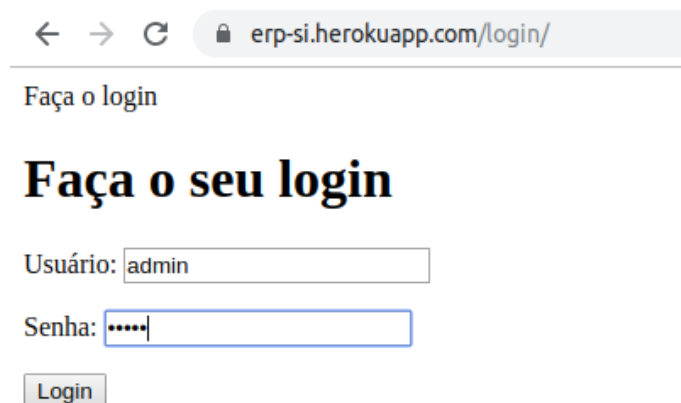
## 2)NotFound

A opção "Nova compra" continua disponível mesmo na própria tela. Quando clicamos 2 vzs o link é alterado e da erro.



## 5 Falhas de segurança ERP em 28/11/2019

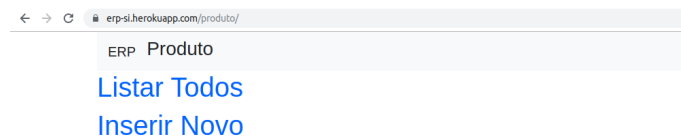
### 1) Senha padrão fraca



A screenshot of a web browser showing the login page for `erp-si.herokuapp.com/login/`. The browser's address bar shows the URL. Below the address bar, the text "Faça o login" is displayed. The main heading is "Faça o seu login". There are two input fields: "Usuário:" with the value "admin" and "Senha:" with masked characters ".....". A "Login" button is located below the password field.

Figura 9: Login com usuário:"admin" e senha: "admin"

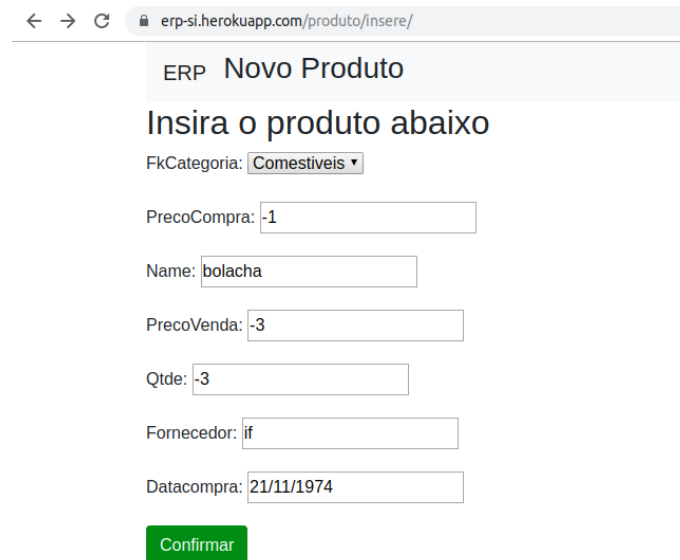
### 2) Ausência de opção de logout



A screenshot of a web browser showing the product management page for `erp-si.herokuapp.com/produto/`. The browser's address bar shows the URL. Below the address bar, the text "ERP Produto" is displayed. There are two links: "Listar Todos" and "Inserir Novo", both in blue text.

### 3) Adicionar produtos

Aceita adição de quantidades negativas de produtos, preço de compra e preço de venda.



ERP Novo Produto

Insira o produto abaixo

FkCategoria: Comestiveis ▼

PrecoCompra: -1

Name: bolacha

PrecoVenda: -3

Qtde: -3

Fornecedor: if

DataCompra: 21/11/1974

Confirmar

Figura 10: Inserindo quantidade negativa de um novo produto

22	tesstt	Louco	-20.0	-50.0	10	EASGDH	1 de Janeiro de 2019
23	bolacha	Comestiveis	-1.0	-3.0	-3	if	21 de Novembro de 1974
24	bolacha	Comestiveis	-1.0	-3.0	-3	if	21 de Novembro de 1974

[Voltar](#)

Figura 11: Produtos adicionados