

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: Rafael Teixeira Rezende
Roberto Ramos Ferreira

Professor orientador: Luciana Balieiro Cosme

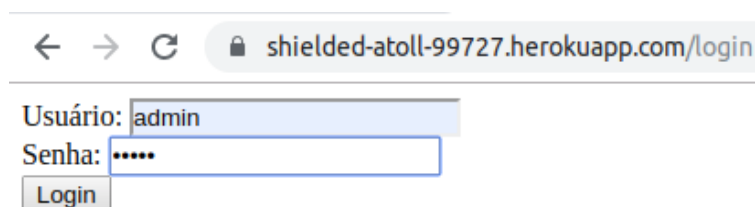
Outubro
2019

1 Descrição de atividades

Esse relatório foi desenvolvido por acadêmicos do curso de Bacharel em Ciência da Computação do Instituto Federal do Norte de Minas Gerais - Campus Montes Claros com a finalidade de encontrar falhas nos serviços disponibilizados, a princípio pela professora Luciana Balieiro (Miniapp) e posteriormente pela turma (ERP, SCM, CMS, CRM,).

2 Falhas encontradas no Miniapp em 11/10/2019

1) Senha padrão fraca;
Entrada como admin:



← → ↻ 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



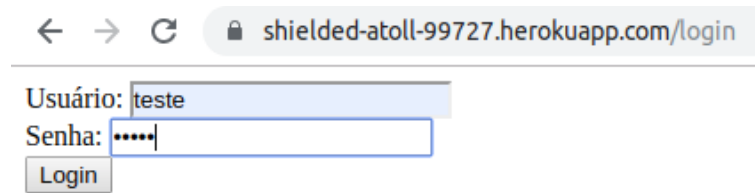
← → ↻ shielded-atoll-99727.herokuapp.com

Olá, Admin!

Como está?

Figura 3: Acesso à pagina do usuário

Entrada como teste:



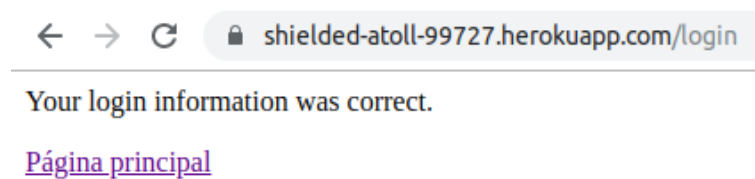
← → ↻ shielded-atoll-99727.herokuapp.com/login

Usuário: teste

Senha:

Login

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



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

Your login information was correct.

[Página principal](#)

Figura 5: Login correct



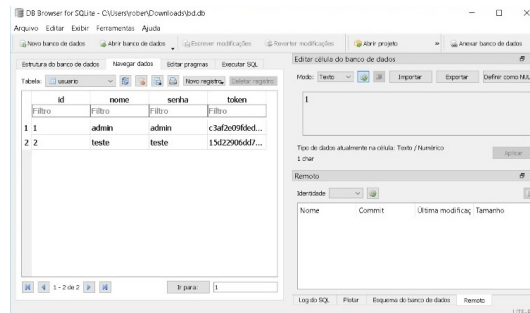
← → ↻ shielded-atoll-99727.herokuapp.com

Olá, Teste!

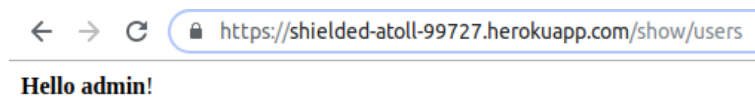
Como está?

Figura 6: Acesso à página 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.

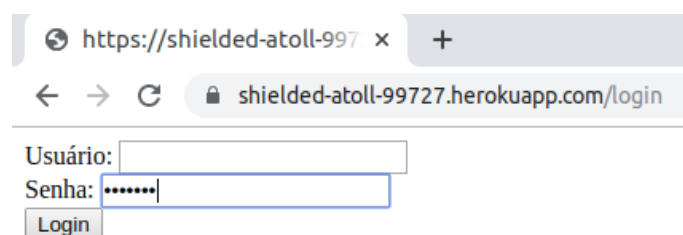
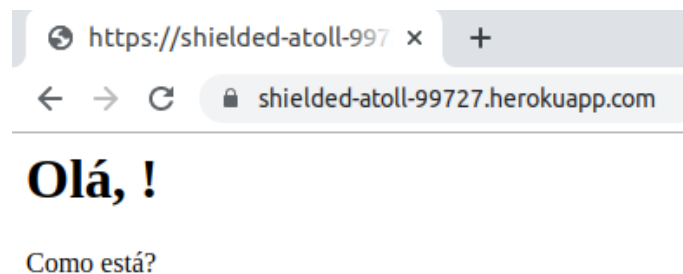
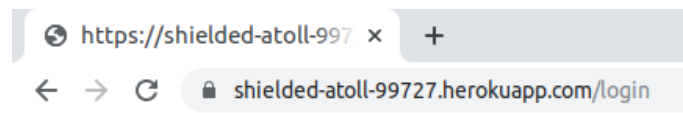
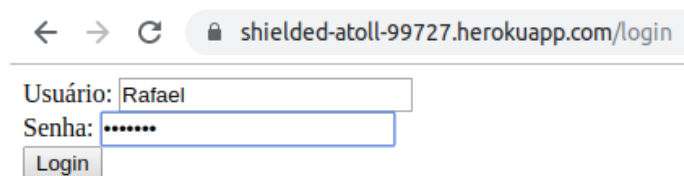



Figura 7: Falha de segurança SQL Injection





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

Usuário:

Senha:

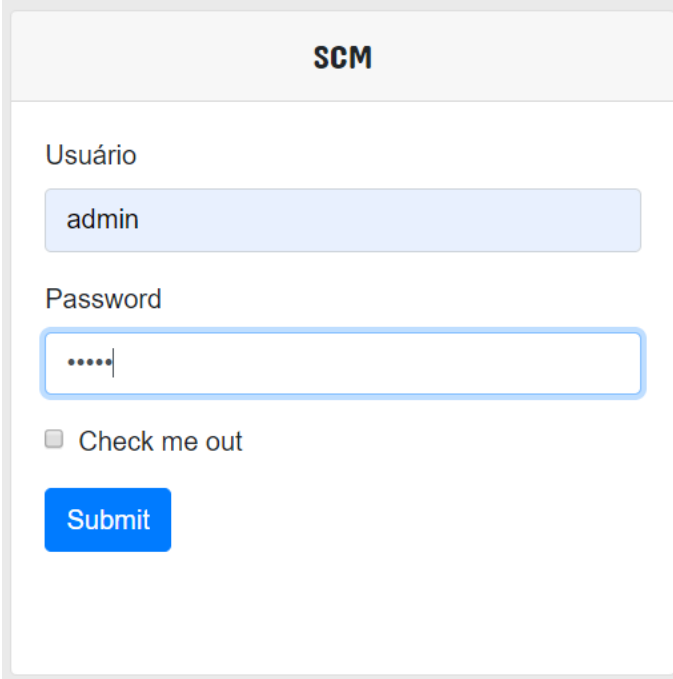
Login



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.

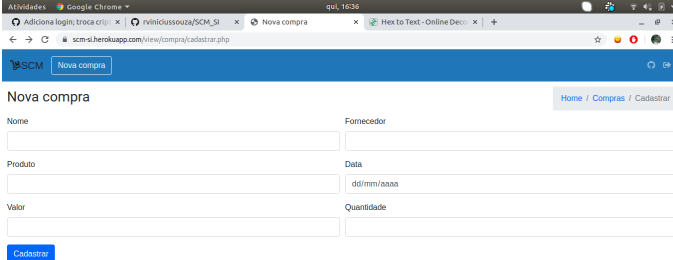
4 Falhas de Segurança em SCM 01/11/2019

1) Senha padrão fraca;



The image shows a login interface for a system labeled "SCM". It contains two input fields: "Usuário" (User) 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.

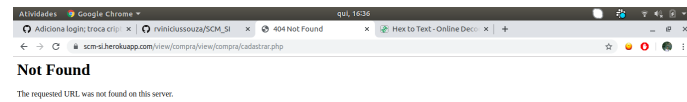
Figura 8: Login com usuário: "admin" e senha: "admin"



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). A "Cadastrar" (Register) button is at the bottom left. The browser's address bar shows the URL "scm-vi.herokuapp.com/view/compra/cadastrar.php".

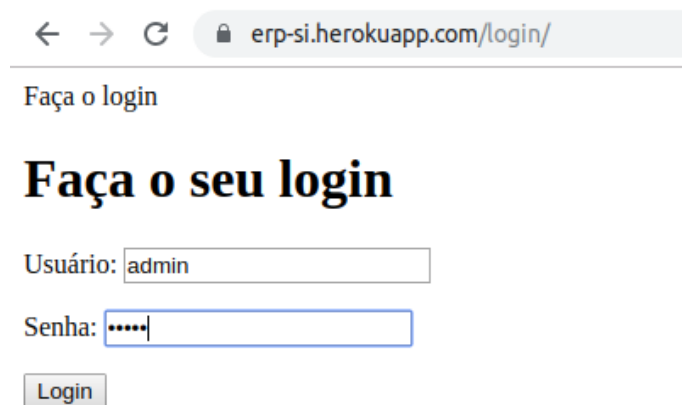
2)NotFound

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

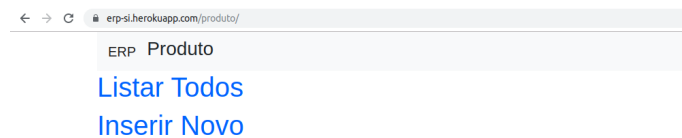
1) Senha padrão fraca



A screenshot of a web browser showing the login page for `erp-si.herokuapp.com/login/`. The page has a title "Faça o login" and a large heading "Faça o seu login". Below the heading, there are two input fields: "Usuário:" with the text "admin" and "Senha:" with masked characters ".....". A "Login" button is positioned below the password field.

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

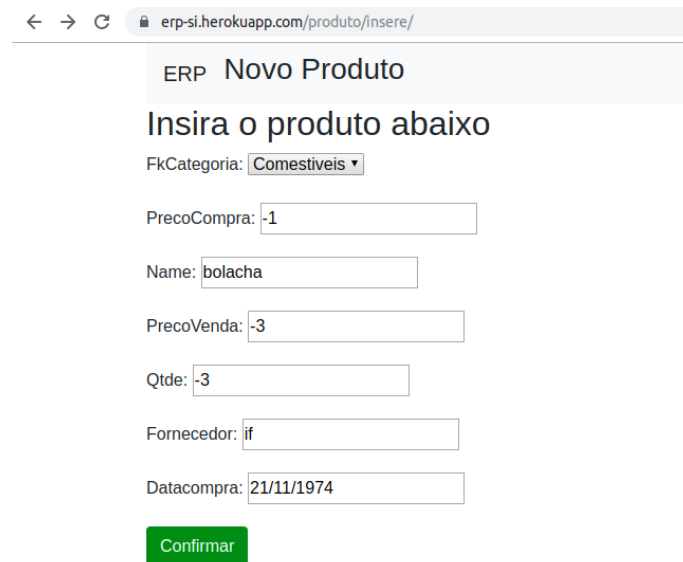
2) Ausência de opção de logout



A screenshot of a web browser showing the product management page for `erp-si.herokuapp.com/produto/`. The page has a title "ERP Produto" and two links: "Listar Todos" and "Inserir Novo".

3) Adicionar produtos

Aceita adição de valores negativos em adição 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

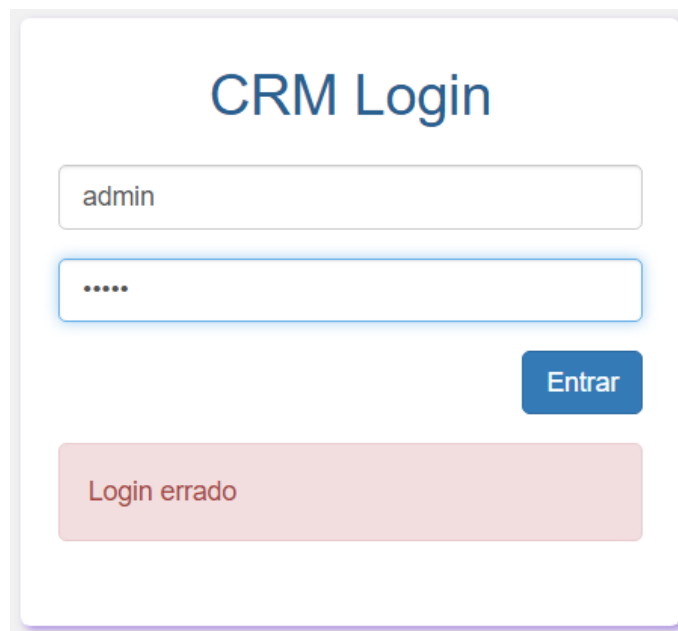
Figura 10: Inserindo quantidade negativa de um novo produto

22	testt	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

6 Falhas de segurança CRM em 03/12/2019



The image shows a web form titled "CRM Login". It contains two input fields: the first is labeled "admin" and the second is masked with five dots. To the right of the second field is a blue button labeled "Entrar". Below the input fields is a red rectangular box containing the text "Login errado" in red.

Figura 12: Não foi mais possível acessar através do usuário: "admin" e senha: "admin"

7 Falhas de segurança SCM em 03/12/2019

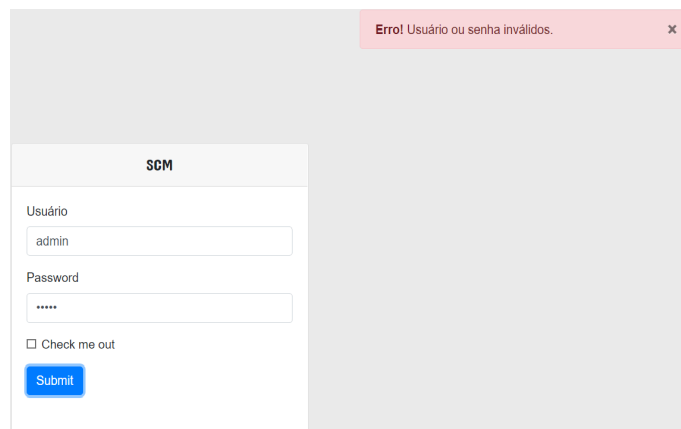


Figura 13: Não foi mais possível acessar através do usuário:” admin” e senha: ”admin”

8 Brute Force 13/12/2019

Todas as aplicações estão sujeitas a receber um ataque de brute force por não conter um sistema de segurança que bloqueie excessivas tentativas de login seguidas, ainda que faça uso de uma senha mais complexa do que o habitual permanece sendo apenas questão de tempo o sucesso do ataque.