Aluno **RGM**
Iago Alves **11242400738**

Relatório Técnico

1. Introdução

Este relatório apresenta a implementação de um **sistema seguro de autenticação**, desenvolvido para a disciplina de Políticas de Segurança da Informação. O objetivo é garantir que as credenciais dos usuários sejam armazenadas e protegidas contra ataques de força bruta e dicionário, utilizando ***SALT*** e ***bcrypt*** para hashing de senhas.

2. Lógica da Implementação

2.1. Registro de Usuários

1. O sistema solicita um **nome de usuário** e uma **senha**.
2. A senha fornecida passa por uma validação de segurança.
3. Um **SALT único** é gerado para o usuário.
4. A senha é **criptografada com bcrypt** e armazenada no banco de dados.
5. O registro falha caso o nome de usuário já exista ou a senha seja fraca.

2.2. Processo de Login

1. O sistema solicita o **nome de usuário** e a **senha**.
2. Busca-se o **SALT** correspondente ao usuário no banco de dados.
3. O sistema gera o hash da senha digitada e a compara com o hash armazenado no BD.
4. Se a senha estiver correta, é solicitado um **código de verificação** (autenticação multifator).
5. Caso o usuário falhe no login **5 vezes**, ele é temporariamente bloqueado.

3. Medidas de Segurança Aplicadas

- **Uso de bcrypt e SALT único para cada usuário**: Garante que as senhas sejam armazenadas de forma segura, dificultando ataques de dicionário e força bruta.
- **Autenticação Multifator (MFA)**: Implementado como um desafio extra, exigindo um código de verificação de 6 dígitos.
- **Proteção contra tentativas excessivas de login**: O sistema bloqueia o usuário temporariamente após 5 falhas consecutivas.

- **Validação de senha forte**: O registro de usuários requer uma senha que atenda aos seguintes critérios:
    - Pelo menos 6 caracteres
    - Pelo menos uma letra maiúscula
    - Pelo menos uma letra minúscula
    - Pelo menos um número
    - Pelo menos um caractere especial

4. Teste de Força Bruta e Ataques de Dicionário

Para verificar a segurança das senhas, foi realizado um teste de ataque de dicionário utilizando uma lista de senhas comuns.

Para isso, dois usuários foram criados ignorando os critérios de validação de senha forte. Enquanto um usuário foi cadastrado seguindo os critérios de validação de senha forte.

4.1. Resultados

Foram cadastrados três usuários: dois com senhas fracas e um com senha forte. Os tempos de quebra foram:

- **Usuário 1 (senha fraca - "1234")**: senha quebrada em **0.41 segundos**.
- **Usuário 2 (senha fraca - "12345678")**: senha quebrada em **1.99 segundos**.
- **Usuário 3 (senha forte)**: senha **não foi quebrada**.

Isso demonstra que o uso de senhas fortes aumenta significativamente a segurança contra ataques de dicionário.

5. Melhorias Extras Implementadas

Além das exigências da atividade, foram implementadas as seguintes melhorias:

- **Validação de senha forte**: Reduz vulnerabilidades a ataques de força bruta.
- **Autenticação multifator (MFA)**: Adiciona uma camada extra de segurança.
- **Registro de tentativas de login**: Mantém logs de acessos e falhas para auditoria. O registro inclui o usuário, data e hora e **endereço IP**.

6. Conclusão

O sistema desenvolvido atende aos requisitos de segurança, implementando hashing seguro com bcrypt e proteção contra ataques. Os testes de força bruta demonstraram a importância de senhas fortes, reforçando a necessidade de boas práticas de segurança na autenticação de usuários.