SEGURANÇA DE ACESSO

Michael, Gabriel, Samuel e Thalys

SOBRE O PROJETO

Projeto de tela de login com foco em boas práticas de autenticação e segurança.

Importância da segurança:

- Proteção dos dados;
- Evitar invasões;
- Preservar a privacidade.

```
setInterval(() => {
  db.query("UPDATE users SET verification_code = NULL, code_expires_at = NULL WHE
}, 10 * 60 * 1000); // Limpa códigos expirados a cada 10 minutos

// ------------Rota de Login------------ //

app.post("/login", async (req, res) => {
  const { email, password } = req.body;

  try {
    const [results] = await db
      .promise()
      .query(`SELECT id, password FROM users WHERE email = ?`, [email]);

    if (results.length === 0) {
      return res.status(401).json({ success: false, message: "Usuário ou senha in
    }

    const user = results[0];
    const isPasswordValid = await comparePassword(password, user.password);

    if (!isPasswordValid) {
      return res.status(401).json({ success: false, message: "Usuário ou senha in
    }

    // Login válido — pede autenticação de dois fatores
    return res.status(200).json({
      success: true,
      message: "Login válido. Código de verificação necessário.",
      userId: user.id,email
    });
```

VISÃO GERAL DO PROJETO

HTML/CSS

Utilizamos HTML como linguagem de marcação e CSS para estilização

JAVA SCRIPT

Utilizamos .Js para tornar as paginas mais interativas e dinâmicas

NODE.JS

Utilizamos para rodar o JavaScript fora do navegador, possibilitando o desenvolvimento de aplicações no lado do servidor (backend).

MYSQL

Utilizamos o MySql para nosso banco de dados.

DEMONSTRAÇÃO DO PROJETO

BOAS PRATICAS ADOTADAS

HASH E CRIPTOGRAFIA DE SENHAS

Utilizamos o Bcrypt , que é um algoritmo de hash criptográfico, baseado na cifra Blowfish

TOKENS (JWT / SESSÕES SEGURAS)

Após o login, o sistema gera um **token** que identifica o usuário.
Ele é usado para validar o acesso as rotas restritas.

TEMPO DE EXPIRAÇÃO E LOGOUT SEGURO

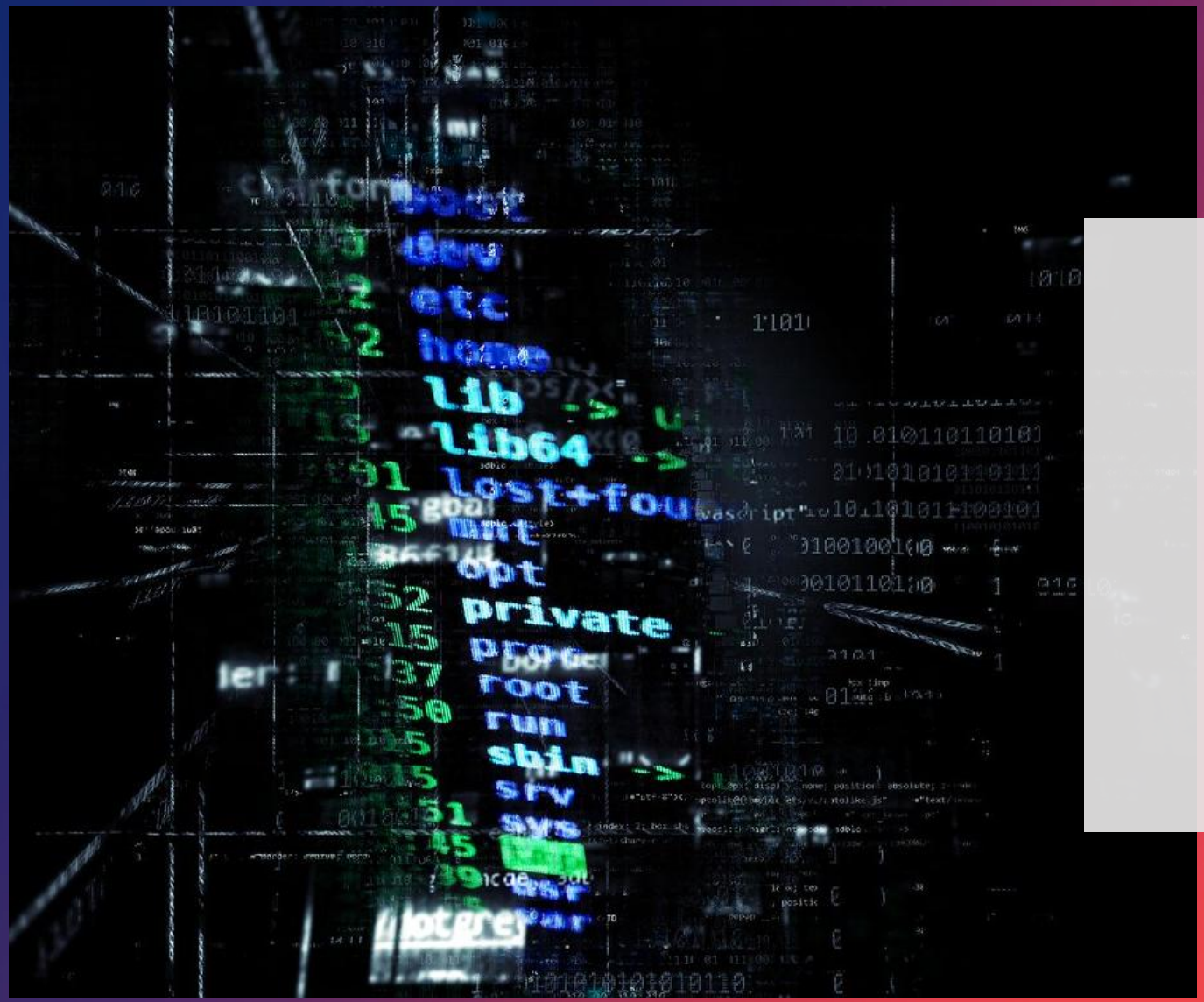
O token ou sessão deve **expirar após um tempo** para evitar acessos indevidos caso alguém roube o token.

POLÍTICA DE SENHA

Evita que usuários criem senhas fáceis de adivinhar. Recomenda usar **mínimo de 8 caracteres, letras maiúsculas, números e símbolos**.

VERIFICAÇÃO DE DOIS FATORES (2FA)

Adiciona uma **camada extra de segurança**: além da senha, o usuário precisa confirmar um código (SMS, e-mail ou app).



O QUANTO VOCÊ SE SENTE SEGURO NA INTERNET?

Você já sofreu alguma invasão ou golpe online?

Você costuma verificar se um site é seguro?

Você usa a mesma senha em vários lugares diferentes ?

PRINCIPAIS AMEAÇAS E ATAQUES

ATAQUE DE FORÇA BRUTA:

O invasor tenta **adivinhar a senha** testando várias combinações automaticamente (ex: “123456”, “senha123”).

SESSION HIJACKING:

O invasor **rouba o token ou cookie de sessão** de um usuário autenticado e se passa por ele.

SQL INJECTION:

O atacante insere **comandos maliciosos no campo de login** (ou outro formulário) para enganar o banco de dados.

CROSS-SITE SCRIPTING (XSS):

O invasor insere **códigos JavaScript maliciosos** em páginas web, que executam no navegador de quem acessa. Pode roubar cookies, dados ou redirecionar para páginas falsas.

PHISHING

Técnica de **enganar o usuário** com uma página de login falsa que imita a original, para roubar credenciais.

ATAQUES

73%

das empresas brasileiras foram vítimas de ransonware em 2024.

(IT FORUM)

83%

das companhias que sofreram ataques em 2023, e pagaram resgate após o ataque.

(IT FORUM)

R$ 2,1 MI.

valor médio pago por resgate no brasil

(UOL)

GRANDES ATAQUES REGISTRADOS

E seus impactos

MAIO DE 2017
WANACRY

Ransomware que explorou vulnerabilidade SMB (EternalBlue)

Impacto: ~200.000 computadores infectados (hospitais, empresas, governos), interrupção de serviços (ex.: NHS no Reino Unido), perdas operacionais significativas.

JUNHO DE 2017
NOTPETYA

Malware destrutivo com vetores de atualização de software

danos econômicos gigantescos (estimativas bilionárias), afetou grandes empresas globais (ex.: Maersk, Merck) e paralisou operações por dias/ semanas.

2013–2014
YAHOO

Vazamento massivo de credenciais

Impacto: estimativa de **até 3 bilhões** de contas afetadas; exposição de e-mails, senhas (hashes) e dados de perfil; enorme dano à reputação e perda de valor em transações (aquisição pelo Yahoo/Verizon foi impactada).

PREVENÇÕES E BOAS PRÁTICAS GERAIS

COMO SE PROTEGER (USUÁRIO)

- Use senhas fortes e únicas;
- Ative a verificação de duas etapas;
- Desconfie de links e Paginas Suspeitas;
- Não compartilhe suas senhas;
- Verifique a origem dos e-mails e mensagens;
- Evite Redes WI-FI Públicas;
- Monitore acessos e contas.

COMO SE PROTEGER (DEV)

- Sanitização de entradas (evitar SQL Injection);
- Limite de tentativas de login;
- Autenticação multifator;
- Monitoramento de acessos suspeitos;
- Atualizações e correções constantes.

CONCLUSÃO

- Proteger logins é essencial para evitar vazamentos e prejuízos.
- Um único ataque pode comprometer dados de clientes e empresas
- A prevenção é mais barata e eficiente que a recuperação
- Importância das boas praticas
- Ameaças comuns: Força Bruta, Phishing, Sql Injection, XSS e Ransomware

AGRADECEMOS

Segurança digital não é apenas responsabilidade do sistema, mas também do usuário. Cada login protegido é uma barreira a menos para o invasor.