

UniBH

Gabriel Vitor Siqueira Costa, Gustavo Ferreira França de Abreu, Gustavo Teixeira Rocha Araujo, João Victor Teixeira Gomes Cota, Luiz Guilherme Vilaça de Moraes, Rafael Colombo Fernandes Silva

Guia com Medidas Protetivas de um Site

A segurança de sites é um dos pilares fundamentais da proteção de informações na era digital. Com o aumento constante de ataques cibernéticos e falhas exploradas em aplicações online, torna-se essencial adotar medidas protetivas que garantam a confiabilidade, a integridade e a disponibilidade dos sistemas.

Ataques mais comuns

SQL INJECTION-O invasor envia comandos maliciosos para o banco de dados através de formulários ou URLs, podendo ler, alterar ou apagar informações. Um exemplo comum é o Digitar algo como ' OR '1'='1 em um campo de login para tentar burlar a autenticação. Assim o sistema interpreta que o comando SQL seria algo verdadeiro

BRUTE FORCE- Um programa automatizado tenta milhares ou milhões de senhas por segundo até encontrar a correta. Exemplo:Ao entrar em uma tela de login. O programa tenta milhões de senhas comuns como "123456", "admin", "senha123".

TORJAN HORSE- Ele é um tipo de malware que se disfarça de um programa legítimo para enganar o usuário. Ele parece ser algo útil ou inofensivo, mas quando é instalado abre caminho para o atacante controlar o computador, roubar dados ou instalar outros vírus. Exemplo:Um arquivo enviado por e-mail com nome chamativo, como:

"Comprovante_pagamento.pdf.exe"

PHISHING- É um tipo de ataque em que o criminoso finge ser uma empresa ou pessoa confiável para enganar o usuário e fazer com que ele entregue informações sensíveis como: Senhas, dados bancários, códigos de verificação...

Exemplo:Ao receber um email dizendo "Sua conta foi bloqueada, clique aqui para atualizar seus dados.

Como se prevenir

SQL INJECTION-Prepared Statements: São consultas preparadas onde os dados do usuário não são misturados com o comando SQL. Ou seja seria uma separação clara do que seria um código SQL e um dado.

Exemplo **PRATICO INSERINDO O SEGUINTE COMANDO:**


```
-- Entrada maliciosa do usuário:  
email = "admin' OR '1'='1' --"
```

VULNERÁVEL

```
-- x VULNERÁVEL (concatenação)  
"SELECT * FROM usuarios WHERE email = '" + email + "'"
```

Assim o sistema valida como verdadeiro, com isso liberaria o acesso

SEGURO







```
--  SEGURO (prepared statement)
"SELECT * FROM usuarios WHERE email = ?"
```

Com isso o sistema buscaria que “**admin’ OR “1” = ‘1’** - - “ seria um email na qual nao existisse

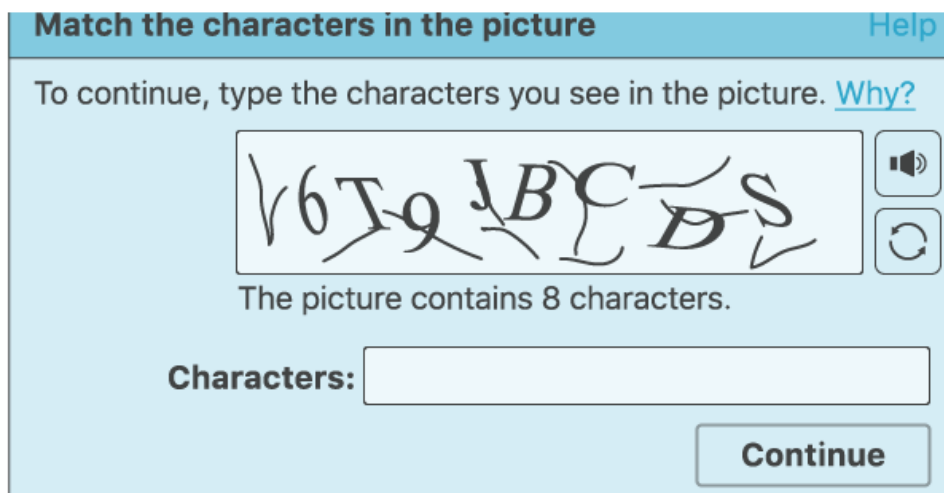
Validação se sanitização de entrada: Confere se o dado enviado pelo usuário é válido (ex.: apenas números, tamanho máximo, caracteres permitidos). Assim impedindo que comando maliciosos sejam processados

BRUTE FORCE- Rate limiting: O sistema bloqueia temporariamente o login após várias senhas erradas. Isso impede que programas testem milhares de senhas por minutos

Exemplo ao testar senhas:

- 1ª tentativa errada →  Permite nova tentativa
- 2ª tentativa errada →  Permite nova tentativa
- 3ª tentativa errada →  Aviso "Últimas tentativas"
- 4ª tentativa errada →  Bloqueio por 5 minutos
- 5ª tentativa errada →  Bloqueio por 30 minutos
- 6ª tentativa errada →  Bloqueio por 24 horas

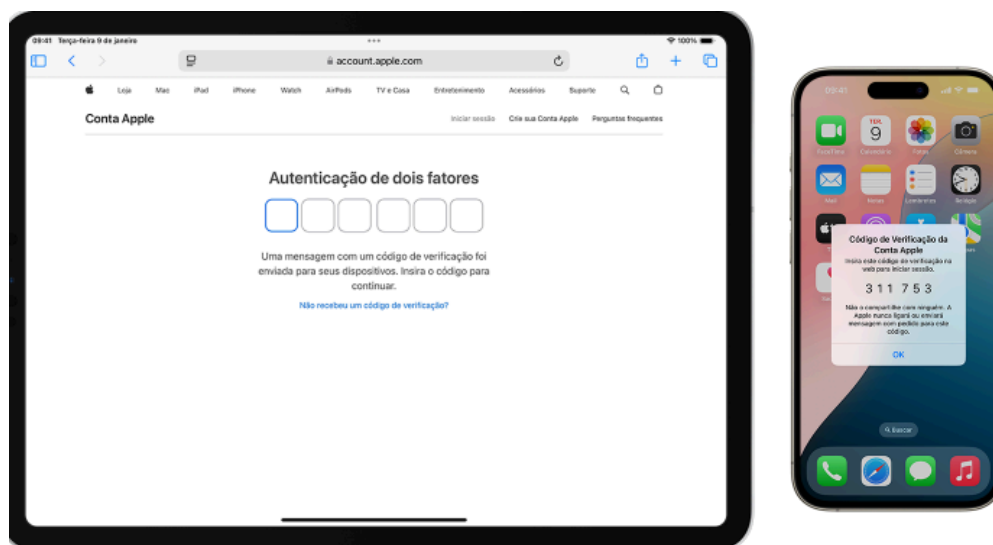
Captcha: Prova que o usuário é um humano. É realizado testes visuais na qual os humanos resolvem facilmente, já os robos não conseguem interpretar imagens distorcidas ou textos sobrepostos.



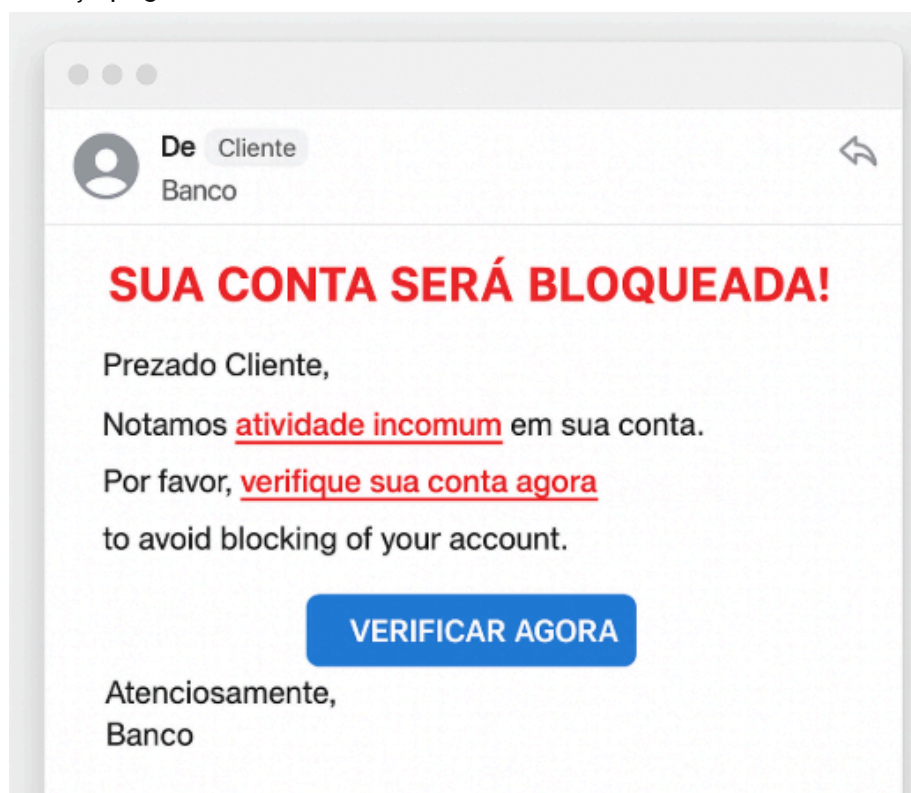
TROJAN HORSE- Verificação tecnica: Deve-se possui o antivirus sempre atualizado pois ele detecta e remove trojans antes que eles causem dano.

Sistemas atualizados: Atualizações e corrigem falhas que trojans usam para se instalar. Assim fecha portas que os malwares usariam para entrar.

PHISHING- Autenticação de dois fatores: O sistema requer não apenas aquilo que voce sabe(senha) mas também algo que voce possui(Código temporário) ou que voce é (Biometria). Após inserir a senha é solicitado um segundo fator de autenticação



Atentar a senso de urgência: O senso de urgência em phishing é uma técnica usada pelos criminosos para fazer a vítima agir rápido sem pensar. Eles criam mensagens que passam pressão, medo ou oportunidade limitada para que a pessoa clique em links, entregue dados ou faça pagamentos imediatamente.



Em vermelho consta os senso de urgência na qual é utilizado em maioria dos ataques

PREVENÇÃO DE FORMA GERAL

Educação ao Usuário: A educação do usuário é fundamental para a segurança digital, porque mesmo com sistemas protegidos, firewalls avançados e ferramentas modernas,

tudo pode falhar se o usuário não souber identificar riscos. O usuário é considerado o elo mais fraco porque, muitas vezes sem perceber, pode clicar em links maliciosos, baixar arquivos perigosos ou entregar informações confidenciais a golpistas.

Assim a educação ao usuário está interligada a várias formas de prevenção nas quais são

Manter sistemas, servidores e softwares sempre atualizados

Reconhecer mensagens suspeitas

Evitar download ou abertura de anexos desconhecidos

Utilizar conexões seguras (HTTPS).

Assim, concluímos que é necessário tanto investir na educação do usuário quanto implementar sistemas capazes de garantir confiança. A combinação entre boas práticas humanas e medidas técnicas fortalece a segurança digital, reduzindo vulnerabilidades e dificultando a ação de atacantes. Dessa forma, cria-se um ambiente mais protegido e confiável para todos.

Como ensinar pessoas mais velhas e desinformadas a se prevenir

Pessoas mais velhas ou com pouca experiência digital precisam de orientações claras e práticas. Por isso, é importante explicar de forma simples, evitando termos técnicos e usando exemplos do dia a dia. A melhor forma de ensinar é mostrando passo a passo como identificar algo suspeito e repetindo as instruções até que se tornem naturais.

Também ajuda criar regras fáceis de lembrar, como:

- Não clicar em links enviados por desconhecidos;
- Não baixar arquivos sem ter certeza da origem;
- Sempre desconfiar de mensagens muito urgentes;
- Conferir o remetente antes de digitar senhas ou dados pessoais.

Além disso, incentivar que elas perguntem a alguém de confiança quando tiverem dúvida reduz muito o risco de cair em golpes como phishing, trojans e sites falsos. Dessa forma, mesmo quem não entende muito de tecnologia consegue navegar com mais segurança.

Conclusão

A segurança de sites depende tanto das medidas técnicas quanto do comportamento dos usuários. Conhecer os ataques mais comuns e aplicar práticas de prevenção reduz significativamente os riscos. Além disso, orientar pessoas com menos conhecimento digital também é essencial, pois qualquer descuido pode abrir portas para invasores. Com sistemas atualizados, atenção aos sinais de golpe e boas práticas no uso da internet, criamos um ambiente digital mais seguro e confiável para todos.

