

SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL
TERCEIRO ANO TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO

GABRIEL SZABO
ISABELLA AVELINA
JOÃO LUCAS MARTINS
MARIA EDUARDA MAKLOUF
MURILO MENDES
NATHALY VIEIRA
PEDRO AUGUSTO

ATIVIDADE INTEGRADA DO TERCEIRO BIMESTRE

SÃO PAULO
2023

GABRIEL SZABO
ISABELLA AVELINA
JOÃO LUCAS MARTINS
MARIA EDUARDA MAKLOUF
MURILO MENDES
NATHALY VIEIRA
PEDRO AUGUSTO

ATIVIDADE INTEGRADA DO TERCEIRO BIMESTRE

SÃO PAULO
2023

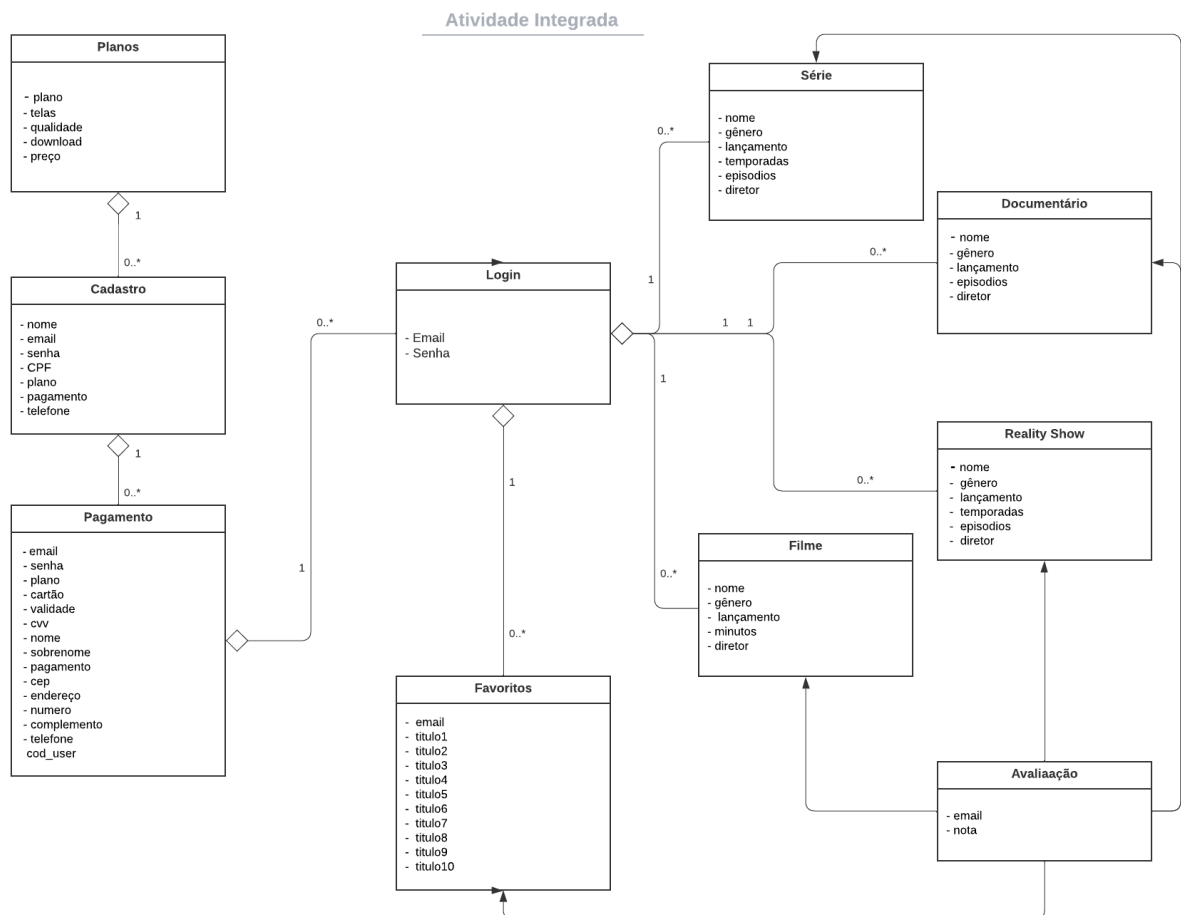
Resumo

Foi elaborada uma recriação da plataforma de streaming *Netflix*. Sendo assim, foi desenvolvido uma interface completa - com área de login, assinatura e espaço usuário-, além do banco de dados que armazena todos os dados do aplicativo - como os dados de pagamento do usuário e sua lista de conteúdo dentro da plataforma.

Atividade Integrada de TI do 3º Bimestre

Códigos e arquivos do Banco de Dados SQL e aplicativo Java script estão no repositório GitHub. Link dos nossos códigos e arquivos abaixo:
<https://github.com/nathalyjsvieira/Atividade-Integrada-de-TI-3-Bimestre>.

Etapa 1 - Diagrama MER




Etapa 2 - Aplicativo

O aplicativo foi desenvolvido espelhado na plataforma original, *Netflix*. Foi utilizado apenas “new ‘JFramequedeseja’ ().setVisible (true);” e tínhamos desejo de utilizar “JOptionPane” para impossibilitar a entrada de qualquer usuário dentro da plataforma.

Etapa 3 - Interface do aplicativo

A plataforma começa com a parte de “Login”:



The image shows the Netflix login screen. At the top, the word "NETFLIX" is displayed in red. Below it, there are two input fields: "Qual seu email:" and "Senha:". At the bottom, there are three red buttons: "ENTRAR" (twice) and "ASSINAR" (once).

- Aqui o usuário que já está cadastrado colocaria seu email em conjunto com a senha e entraria na plataforma. Os que não estão cadastrado iriam clicar em “ASSINAR” e iriam ser direcionados aos planos;



The image shows the Netflix subscription plans screen. At the top, the word "NETFLIX" is displayed in red. Below it, the text "Passo 1 de 3" and "ESCOLHA UM PLANO:" are visible. There are three red boxes representing different plans: BÁSICO, PADRÃO, and PREMIUM. Each box lists features and a price.

PLANO	Características	Preço
BÁSICO	2 Telas simultânea HD	R\$ 19,90
PADRÃO	4 Telas simultânea HD Download	R\$ 25,90
PREMIUM	4 Telas simultânea HD e 4k Download Primeiro mês grátis	R\$ 31,90

N

Passo 2 de 3

Nome completo:

CPF:

FORMA DE PAGAMENTO

☐ Débito

☐ Crédito

Número do cartão:

Data de vencimento:

CVV:

ENDEREÇO DE COBRANÇA

Endereço:

Bairro:

CEP:

Número:

Complemento:

Cidade:

Número de telefone:

PRÓXIMO

- Quando escolhido o plano o usuário iria ser direcionado para a área de pagamento onde colocaria seus dados e forma de pagamento;

N

Passo 3 de 3

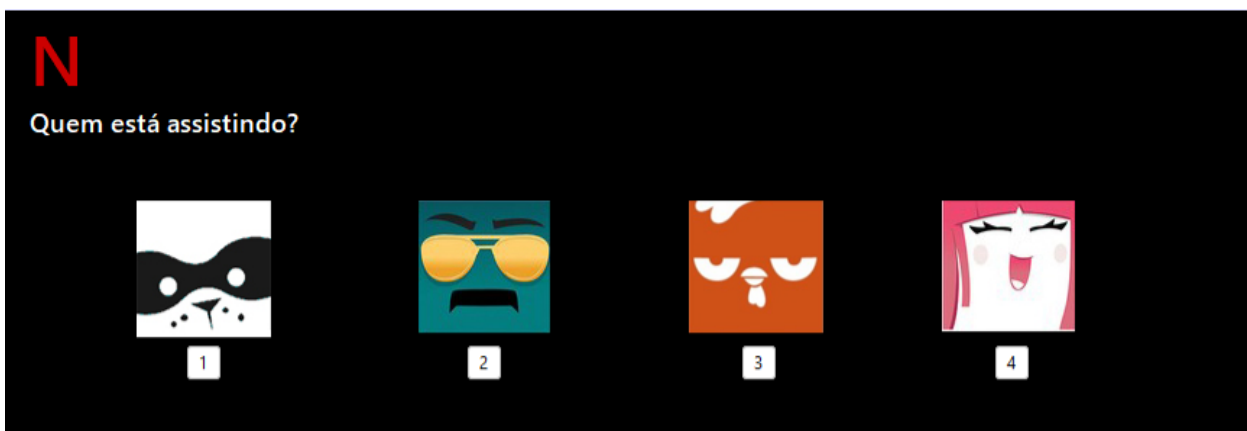
Digite seu email:

Crie uma senha:

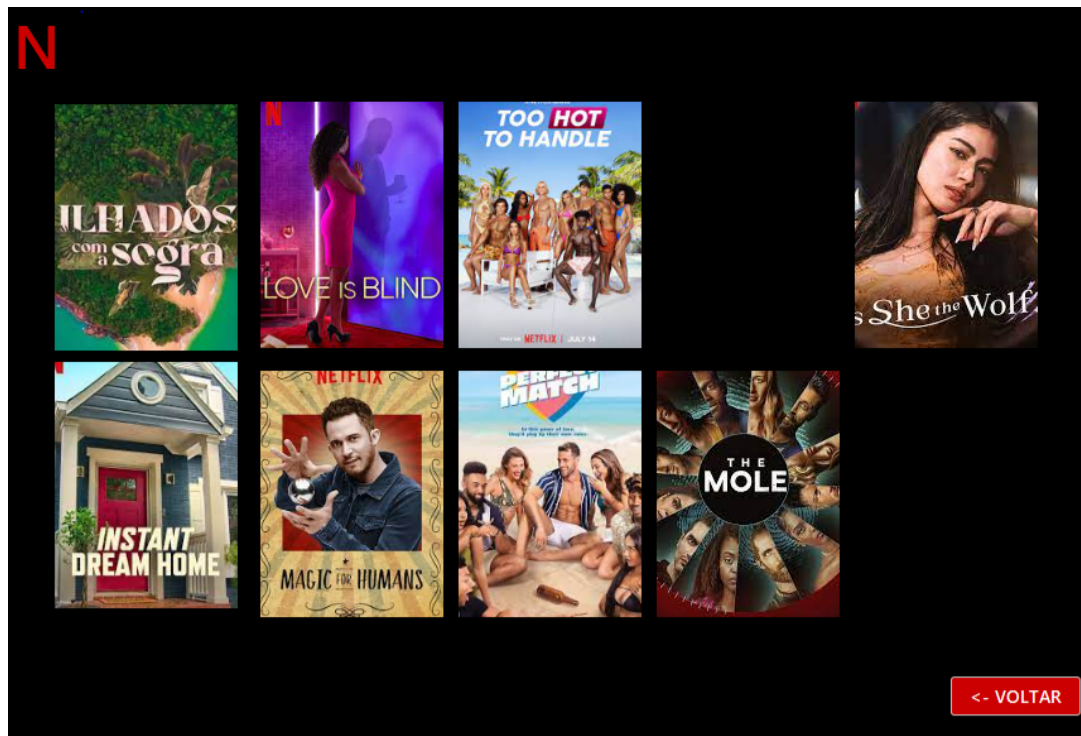
Confirme senha:

ASSINAR

- Completar o cadastro e assim é direcionado para o login novamente;



- O usuário faz seu login e escolher a conta que quer entrar e o que deseja assistir;



- Como exemplo, essa é a ilustração da parte de Reality Show;

Etapa 4 - Banco de dados

Criamos um banco de dados SQL para os seguintes dados: Cadastro, Login, Pagamento, Avaliação, Favoritos, Filmes, Séries, Documentários e Reality shows. Utilizamos o INSERT INTO e CREATE TABLE.

Consultas: nosso banco de dados pode ser prioritariamente consultado por email, id_user, plano, e gênero.

Etapa 5 - Conexão com o banco de dados

Etapa 6 - Tipos de Ataque

Phishing

Phishing é uma técnica de engenharia social usada para enganar os usuários da Internet por meio de fraude eletrônica para obter informações confidenciais, como nomes de usuário, senhas e detalhes de cartão de crédito. Basicamente, este ataque é

uma forma de fraude online em que um invasor se faz passar por uma entidade confiável para enganar a vítima e obter informações pessoais, como senhas, números de cartão de crédito ou informações financeiras. Isso geralmente é conseguido por meio de e-mails, mensagens de texto, sites ou mensagens instantâneas falsos que parecem legítimos, mas são projetados para induzir as pessoas a revelar informações confidenciais. Os criminosos usam essas informações para cometer fraudes, roubo de identidade e outros crimes cibernéticos. É importante estar ciente desses ataques e ter cautela ao fornecer informações pessoais online.

Para se prevenir é necessário um anti-spam e a Prolinx recomenda que você aposte na solução da Sophos ou no Office 365.

Ransomware

Ransomware é um tipo de malware de sequestro de dados que opera por meio de criptografia, usando os próprios arquivos pessoais da vítima como reféns e cobrando um resgate para restabelecer o acesso a esses arquivos. O resgate é cobrado em criptomoeda, tornando quase impossível rastrear os criminosos na prática. Esta é uma tática usada pelos cibercriminosos para extorquir dinheiro das vítimas e ameaçar a perda permanente de dados valiosos. As vítimas são muitas vezes forçadas a pagar um resgate para recuperar os seus dados, mas os criminosos não têm garantia de cumprir as suas promessas, o que pode resultar em perdas financeiras significativas. Portanto, a prevenção e a cibersegurança são fundamentais para evitar ataques de ransomware. Esse ataque poderia deixar a empresa inoperante por vários dias, para se proteger é necessário boas ferramentas, é importante manter o ambiente sempre atualizado e seguindo boas práticas de configuração.

DDOS Attack

Um ataque de negação de serviço é uma tentativa de tornar os recursos do sistema indisponíveis para o usuário. Um alvo típico é um servidor web, e o objetivo do ataque é indisponibilizar as páginas hospedadas na rede. O sistema foi desativado devido à sobrecarga, não hackeado. Esses ataques são frequentemente usados para prejudicar reputações, causar perdas financeiras ou simplesmente interromper serviços

online. A mitigação de ataques DDoS requer a proteção da sua infraestrutura contra cargas de tráfego maliciosas.

Para se prevenir desse tipo de ataque é importante usar balanceadores de carga e firewalls, os balanceadores de carga redirecionam o tráfego de um servidor para outro em um ataque DDoS. Implemente medidas de mitigação, ter um plano de resposta para ataques DDoS é altamente crucial.

Port scanning attack

Port scanner é uma ferramenta projetada para mapeamento de portas TCP e UDP. Este teste verifica o status da porta: se a porta está fechada, escutando ou aberta. Você pode especificar um intervalo de portas para seu aplicativo verificar (por exemplo, 25 a 80). Uma técnica de reconhecimento usada por invasores para mapear a topologia da rede e identificar possíveis pontos de entrada.

Para se manter livre desse tipo de ataque uma das formas é desativar portas não utilizadas

Cavalo de Troia

São arquivos, programas ou códigos que parecem legítimos e seguros, mas na verdade são códigos maliciosos. Os cavalos de Tróia são entregues como software legítimo (daí o nome) e geralmente são projetados para espionar vítimas ou roubar dados. Tudo o que você precisa fazer é seguir algumas regras simples de segurança na Internet e usar uma solução de segurança eficaz. Ele pode proteger seu computador contra a maioria dos cavalos de Tróia e outros programas maliciosos.

SQL injection

Um ataque de injeção de SQL é uma tentativa de comprometer a segurança de um aplicativo ou site onde um invasor insere comandos SQL maliciosos em um campo de entrada, como um formulário de pesquisa ou caixa de texto, para manipular o banco de dados subjacente. Isso pode permitir que um invasor acesse, alterar ou excluir dados do banco de dados e realizar ações não autorizadas. Esta é uma vulnerabilidade comum que pode ser evitada validando convenientemente os dados de entrada e

usando consultas parametrizadas. De acordo com o OWASP, as melhores práticas para evitar um ataque SQLi são conectar consultas, usar “procedimentos armazenados”, escapar de todas as entradas fornecidas pelo usuário e limitar os direitos de acesso. Usar a função addslashes tem o mesmo efeito que adicionar aspas mágicas. Mas só é usado quando conveniente. O que ele faz é colocar um caractere de escape antes das aspas simples ou duplas, antes da barra invertida e do caractere NULL.

Keylogger

Um keylogger é um sistema malicioso que registra tudo o que é digitado no teclado e encaminha para criminosos. Ou seja, monitora o teclado e captura mensagens secretas. Um computador protegido por um firewall, um bom antivírus, ferramentas antivírus e um navegador, sistema e sistema operacional bem ajustados impedirá muitos espiões digitais, aumentando o risco de parar os principais participantes antes de começarem.

Screenlogger

Os ataques de gravador de tela são softwares maliciosos que registram a atividade do usuário em um computador, incluindo imagens, pressionamentos de teclas e cliques do mouse. Essas informações são frequentemente expostas a invasores, que podem capturar informações confidenciais, como senhas, informações de login e privacidade do usuário, sem o conhecimento ou consentimento do usuário. Tais ataques representam uma ameaça à privacidade e à segurança dos dados. Para evitar esse tipo de ataque, é importante monitorar diferentes métodos, usar senhas fortes e considerar adicionar camadas adicionais de segurança.

Java

O Java é uma linguagem de programação que é executada em uma máquina virtual Java (JVM), e os "vírus" tradicionais, como os vírus de computador que afetam sistemas operacionais Windows ou outros, não são diretamente aplicáveis ao Java da mesma forma. No entanto, existem algumas ameaças que podem afetar aplicações Java:

1. Malware Java: Embora não sejam vírus tradicionais, existem malwares que são escritos em Java. Eles podem ser distribuídos como aplicativos ou applets Java maliciosos e podem explorar vulnerabilidades em máquinas Java desatualizadas.

2. Applets Maliciosos: Applets Java, que são pequenas aplicações que podem ser incorporadas em páginas da web, podem ser usados para disseminar malware. Os navegadores modernos desativaram o suporte a applets Java devido a preocupações de segurança, mas em ambientes mais antigos, eles ainda podem representar uma ameaça.

3. Vulnerabilidades de Segurança: Assim como qualquer software, a plataforma Java pode conter vulnerabilidades de segurança que podem ser exploradas por atacantes. É importante manter sua JVM e bibliotecas Java atualizadas para proteger contra ameaças conhecidas

Etapas 7 - Planos de Contenção

SQL injection, phishing, keyloggers e screenloggers.

Plano de Contenção para Proteção de Banco de Dados:

1. Avaliação de Riscos:

- Realize uma avaliação de riscos abrangente para identificar vulnerabilidades específicas no seu sistema.

2. Políticas de Segurança e Conscientização:

- Desenvolva políticas de segurança claras e promova uma cultura de conscientização sobre segurança entre os funcionários.

3. Firewall de Aplicação Web (WAF):

- Implemente um WAF para proteger contra-ataques de SQL injection e outros ataques na camada de aplicação.

4. Proteção contra SQL Injection:

- Utilize instruções SQL parametrizadas ou consultas preparadas para evitar a injeção de SQL.
- Valide e sanitize (limpe) todas as entradas de usuário antes de incorporá-las em consultas SQL.

5. Autenticação e Autorização:

- Implemente autenticação de dois fatores (2FA) sempre que possível.
- Defina políticas rigorosas de autorização para limitar o acesso de usuários privilegiados apenas ao necessário.

6. Monitoramento de Logs:

- Configure o registro de logs detalhados de todas as atividades no banco de dados.
- Implemente alertas de segurança para detectar padrões de acesso suspeitos.

7. Proteção contra Phishing:

- Eduque os funcionários sobre os perigos do phishing.
- Implemente filtros de e-mail e sistemas de detecção de phishing.

8. Antivírus e Anti-Malware:

- Mantenha sistemas antivírus e anti-malware atualizados em todos os dispositivos que acessam o banco de dados.

9. Proteção contra Keyloggers e Screenloggers:

- Implemente políticas de segurança que restrinjam o uso de software não autorizado em dispositivos de acesso ao banco de dados.

- Mantenha sistemas operacionais e software atualizados para corrigir vulnerabilidades conhecidas.

10. Testes de Segurança:

- Realize testes de penetração regulares para identificar vulnerabilidades.
- Realize simulações de phishing internas para treinar os funcionários e identificar áreas de fraqueza.

11. Plano de Resposta a Incidentes:

- Desenvolva um plano de resposta a incidentes detalhado que inclua etapas para conter e mitigar possíveis invasões.
- Treine sua equipe para responder rapidamente a incidentes de segurança.

12. Backup e Recuperação:

- Faça backups regulares e armazene-os offline em locais seguros.
- Teste regularmente a recuperação de dados a partir dos backups.

13. Conformidade com Regulamentações:

- Assegure-se de que seu banco de dados estejam em conformidade com as regulamentações de segurança relevantes, como o GDPR, HIPAA, etc., se aplicável.

14. Atualizações e Patches:

- Mantenha sistemas e software atualizados com as últimas correções de segurança.

15. Monitoramento Contínuo:

- Mantenha um programa de monitoramento contínuo para identificar ameaças emergentes e mudanças na infraestrutura de TI.

16. Treinamento Contínuo:

- Mantenha a equipe atualizada sobre as melhores práticas de segurança e as ameaças mais recentes.

17. Parcerias com Especialistas em Segurança Cibernética:

- Considere contratar especialistas em segurança cibernética para avaliar e aprimorar regularmente a segurança do seu banco de dados.

Referências

PROLINX. 7 principais tipos de ataques cibernéticos a empresas e como prevenir.

Disponível em: <<https://prolinx.com.br/tipos-de-ataques-ciberneticos/>>.

Training Institute: Library. Disponível em:
<https://training.fortinet.com/course/index.php/Certification:NSE_1>. Acesso em:
3 out. 2023.