ATAQUES:

1. Manipular Dados;
2. Injetar SQL;
3. Executar Força Bruta;
4. Roubar Credenciais;
5. Injetar Código Malicioso

EVIL USER STORIES

1. Como usuário malicioso, pretendo manipular dados para alterar a visualização de relatórios e a visualização do quadro de vagas, mostrando (falsamente) vagas ociosas.

Critérios de Aceitação:

a) Identificar a fonte da manipulação de dados e isolar imediatamente o acesso desautorizado; removendo as alterações indevidas e restaurando os dados afetados.
b) Avaliar o impacto da manipulação de dados, incluindo quais relatórios e informações foram alterados.
c) Analisar logs do sistema para identificar como o usuário malicioso conseguiu manipular os dados.
d) Exportar relatórios usando código ou programas que são executados em um servidor, em vez de serem executados no lado do cliente (front-end).
e) Identificar pontos de vulnerabilidade para evitar explorações futuras.
f) Implementar monitoramento contínuo para detectar atividades suspeitas e intrusões no sistema, utilizando alertas automáticos para notificar a equipe de segurança sobre possíveis anomalias.

2. Como usuário malicioso, pretendo injetar SQL para poder modificar o cadastro de alunos, de serviços ou de funcionários.

Critérios de Aceitação:

a) Identificar e isolar imediatamente a parte vulnerável do sistema onde a injeção ocorreu e corrigir o código fonte para evitar futuros ataques de injeção de SQL .
b) Utilizar consultas parametrizadas ou prepared statements para prevenir essas vulnerabilidades.
c) Restaurar os dados afetados a partir de backups confiáveis, se disponíveis, certificando se os backups estão livres de vulnerabilidades e que foram criados antes do incidente.
d) Conduzir uma revisão abrangente da segurança do sistema para identificar outras potenciais vulnerabilidades.

3. Como usuário malicioso, irei aplicar a força bruta para invadir contas no sistema por meio de credenciais usadas frequentemente

Critérios de Aceitação:

a) Após um número específico de tentativas falhas de login para o mesmo usuário, a partir do mesmo endereço IP e/ou endereço MAC, bloquear temporariamente a conta para frustrar tentativas de força bruta.

b) Exigir senhas fortes, combinando letras, números e caracteres especiais, dificultando o processo de adivinhação.
c) Adicionar uma camada extra de segurança exigindo uma segunda forma de autenticação além da senha (Autenticação de Dois Fatores (2FA)
d) Introduzir atrasos entre as tentativas de login, tornando os ataques mais lentos e menos eficazes.
e) Utilizar sistemas de detecção para identificar padrões de login incomuns, como múltiplas tentativas falhadas em curto espaço de tempo (Monitoramento de Anomalias).
f) Implementar captchas que se adaptem conforme a suspeita de atividade maliciosa, aumentando a dificuldade quando necessário.
g) Informar aos usuários sobre atividades suspeitas em suas contas para que possam agir rapidamente, caso necessário.

4. Como usuário malicioso, irei invadir as funcionalidades do sistema por meio de credenciais roubadas

Critérios de Aceitação:

a) Todas as credenciais comprometidas devem ser imediatamente revogadas e desativadas.
b) Compreender o método de invasão para entender como as credenciais foram comprometidas.
c) Determinar o escopo do incidente, incluindo quais sistemas, dados e funcionalidades foram comprometidos para a contenção eficaz e proteção de ativos críticos.
d) Implementar um processo seguro para que os usuários legítimos possam redefinir ou recuperar suas credenciais.
e) Notificar todos os usuários afetados por meio de comunicações claras e transparentes e fornecer orientações para mitigar danos adicionais.

5. Como usuário malicioso, pretendo injetar um código malicioso de modo a acessar ou modificar dados

Critérios de Aceitação:

a) Identificar e isolar imediatamente a parte afetada do sistema onde o código malicioso foi injetado.
b) Remover o código malicioso do sistema e corrigir a vulnerabilidade no código-fonte.
c) Avaliar o alcance do ataque para determinar quais dados foram acessados ou modificados, considerando o impacto no sistema, nos dados e na confidencialidade das informações.
d) Se possível, restaurar os dados afetados a partir de backups recentes e confiáveis, certificando que os backups não estão comprometidos e foram feitos antes do incidente.
e) Implementar monitoramento contínuo para identificar atividades suspeitas no sistema, utilizando ferramentas de detecção de intrusões para identificar possíveis ameaças.
f) Realize treinamentos com a equipe para garantir que todos estejam cientes das práticas de segurança e das ameaças potenciais.