UNIVERSIDADE DE BRASÍLIA

Faculdade do Gama

Sistemas de Banco de Dados 2

Trabalho Final (TF)

Problemas de Segurança e Invasões em Banco de Dados

Gabriel Moretti de Souza - 200018205

Brasília,
DF 2023

Definição da Tecnologia Pesquisada (o que são):

Os bancos de dados são coleções organizadas de informações que são armazenadas de forma estruturada, permitindo o acesso, manipulação e recuperação eficiente dos dados de uma organização, empresa ou outros. Eles desempenhas um papel crucial nas mesmas, pois são responsáveis por armazenar e gerenciar os dados necessários para as suas operações e negócios diários. No entanto, os bancos de dados estão sujeitos a diversos problemas de segurança e invasões, que podem comprometer a integridade, a confidencialidade e a disponibilidade dos dados de algumas maneiras diferentes.

Tais problemas de segurança em banco de dados podem incluir ataques cibernéticos, como invasões por hackers, roubo de informações sensíveis, injeções de SQL, acesso não autorizado, ataques DDoS (Distributed Denial of Service), entre outros. Essas violações podem ter consequências graves, como perda de dados, prejuízos financeiros, danos à reputação da empresa ou violações de privacidade.

Para esse relatório de pesquisa, serão utilizados como exemplos principais para explicação os problemas de “Injeção SQL” e de “Ataques DDoS”.

As injeções SQL são um tipo comum de ataque cibernético que exploram vulnerabilidades em aplicativos web que interagem com bancos de dados. Essas vulnerabilidades geralmente ocorrem quando os desenvolvedores não validam ou sanitizam adequadamente os dados inseridos pelos usuários em consultas SQL. Isso permite que um invasor possa inserir um código SQL malicioso nas entradas do aplicativo, explorando a falha para executar comandos não autorizados no banco de dados.

Por outro lado, os ataques DDoS são uma forma de ataque

cibernético em que um grande número de dispositivos conectados à internet ou rede são coordenados para enviar tráfego excessivo a um alvo específico, como um site, servidor ou serviço online. O objetivo desses ataques é sobrecarregar o alvo com uma quantidade massiva de solicitações, fazendo com que ele fique inacessível para os usuários legítimos.

Seguindo ao próximo tópico, serão explicados com mais detalhes os objetivos de tratar esse tipos de problema e como funcionam exatamente os problemas citados.

Objetivo(s) principal(is) da Tecnologia Pesquisada (como funcionam):

O objetivo principal da pesquisa sobre problemas de segurança e invasões em banco de dados é compreender as vulnerabilidades existentes e identificar as melhores práticas para proteger os dados armazenados. Isso inclui o desenvolvimento de medidas de segurança, como criptografia, autenticação, controle de acesso, monitoramento de atividades suspeitas, backups regulares e atualizações de software. O objetivo final é garantir a integridade, a confidencialidade e a disponibilidade dos dados em um ambiente de banco de dados.

Para entender o problema de injeção SQL melhor, imagine um formulário de login em um site que solicita um nome de usuário e senha. O aplicativo web, ao receber esses dados, constrói uma consulta SQL para verificar se as informações fornecidas são válidas. No entanto, se o desenvolvedor não tratar corretamente os dados inseridos, um invasor pode explorar essa falha inserindo código SQL adicional na entrada do nome de usuário.

Por exemplo, o invasor pode inserir o seguinte nome de usuário:

```
' OR '1'='1
```

Quando o aplicativo constrói a consulta SQL, ela pode ficar assim:

SELECT * FROM users WHERE username = '' OR '1'='1' AND password = 'senha'

Observe que o código ' OR '1'='1 foi inserido para que a condição 1=1 seja sempre verdadeira. Isso significa que o invasor será capaz de ignorar a verificação da senha e obter acesso não autorizado ao sistema.

Por outro lado, para entender melhor o problema de DDoS, imagine uma estrada com várias faixas de tráfego. Normalmente, o tráfego flui sem problemas, mas, em um ataque DDoS, uma grande quantidade de veículos maliciosos é enviada para essa estrada, congestionando todas as faixas e impedindo que o tráfego legítimo passe.

Esses ataques são chamados de "distribuídos" porque os atacantes geralmente controlam uma rede de dispositivos comprometidos, conhecidos como botnets, para lançar o ataque. Esses dispositivos podem ser computadores, servidores, roteadores ou até dispositivos da Internet das Coisas (IoT) que foram infectados com malware e se tornaram parte da botnet sem o conhecimento de seus proprietários.

Como se proteger:

Com relação aos problemas previamente citados, existem algumas medidas e práticas que podem ser tomadas para se proteger contra os mesmos.

Para a injeção SQL, podemos:

- Usar consultas parametrizadas ou prepared statements: Em vez de construir consultas SQL concatenando diretamente os dados fornecidos pelos usuários, utilize recursos oferecidos pelas

linguagens de programação e frameworks para criar consultas parametrizadas. Isso separa os dados dos comandos SQL, impedindo que os dados de entrada sejam interpretados como código.

- Validar e sanitizar os dados de entrada: Certifique-se de que os dados inseridos pelos usuários sejam validados e tratados corretamente antes de serem usados em consultas SQL. Remova caracteres especiais ou utilize funções de escape para evitar que o código malicioso seja interpretado.

- Princípio do menor privilégio: Certifique-se de que o usuário do banco de dados tenha apenas as permissões necessárias para realizar as operações requeridas pelo aplicativo. Isso limita o impacto de uma injeção SQL, caso ocorra.

- Manter o software atualizado: Mantenha seu banco de dados e aplicativos sempre atualizados, pois as atualizações frequentemente corrigem vulnerabilidades conhecidas.

- Implementar um firewall de aplicativos web (WAF): Um WAF pode ajudar a identificar e bloquear tentativas de injeção SQL, fornecendo uma camada adicional de proteção para o aplicativo.

- Limitar as informações detalhadas de erro: Não exiba mensagens de erro detalhadas para os usuários finais. Isso pode fornecer informações valiosas para um invasor entender a estrutura do banco de dados e explorar possíveis vulnerabilidades.

Para os ataques DDoS, podemos:

- Utilizar serviços de mitigação de DDoS: Contrate serviços especializados de mitigação de DDoS oferecidos por provedores de serviços de segurança. Esses serviços podem ajudar a detectar e filtrar o tráfego malicioso antes que ele atinja sua infraestrutura, protegendo seu site ou serviço.

- Configuração correta de firewalls e roteadores: Configure seus firewalls e roteadores para bloquear o tráfego indesejado, como tráfego suspeito ou vindo de endereços IP conhecidos por realizar ataques DDoS.

- Balancear carga e redundância: Distribua o tráfego entre vários servidores e recursos de rede para evitar que um único ponto se torne um gargalo e seja alvo fácil de um ataque DDoS. Além disso, tenha redundância em seus sistemas para garantir que, mesmo se um servidor for afetado, o serviço continue funcionando em outros servidores.

- Limitar a largura de banda: Configure limites de largura de banda em seus dispositivos de rede para evitar que um ataque DDoS consuma toda a sua capacidade de conexão.

- Monitorar tráfego e detecção precoce: Monitore regularmente o tráfego de rede e utilize ferramentas de detecção de ataques DDoS para identificar padrões incomuns ou tráfego malicioso. Isso pode ajudar a iniciar medidas de mitigação rapidamente.

- Configurar TTL baixo (Time-to-Live): Reduza o valor TTL em seus registros DNS para garantir que, em caso de um ataque DDoS, o tempo de propagação de DNS seja reduzido e você possa mudar rapidamente para outra infraestrutura de mitigação.

Vantagens da Tecnologia Pesquisada:

Algumas das vantagens da implementação de medidas de segurança em banco de dados incluem:

- Proteção dos dados sensíveis: As medidas de segurança ajudam a proteger informações confidenciais, como dados pessoais dos clientes, informações financeiras e segredos comerciais, contra

acesso não autorizado;

- Integridade dos dados: Ao adotar práticas de segurança adequadas, é possível garantir a precisão e a integridade dos dados, prevenindo a ocorrência de alterações não autorizadas ou corrupção dos mesmos;

- Cumprimento de regulamentações: Muitos setores, como saúde e financeiro, possuem regulamentações específicas para a proteção de dados. A implementação de medidas de segurança ajuda a cumprir essas regulamentações e evitar penalidades legais;

- Manutenção da reputação da empresa: Ao proteger os dados e evitar violações de segurança, as empresas preservam sua reputação junto aos clientes, parceiros e stakeholders, demonstrando compromisso com a privacidade e segurança dos dados.

Desvantagens da Tecnologia Pesquisada:

- Embora as medidas de segurança sejam essenciais para proteger os bancos de dados, também podem apresentar desvantagens, como:

- Complexidade e custo: A implementação de medidas de segurança pode exigir conhecimentos especializados e recursos financeiros significativos. Além disso, a manutenção e atualização dessas medidas também podem representar um desafio constante.

- Possíveis impactos na performance: Algumas medidas de segurança, como criptografia e autenticação rigorosa, podem afetar o desempenho do banco de dados, resultando em tempos de resposta mais lentos e maior carga de processamento.

- Risco de falsa sensação de segurança: Embora as medidas de segurança sejam implementadas, sempre existe o risco de

novas vulnerabilidades serem descobertas ou de invasores encontrarem formas de contornar as defesas existentes. Portanto, é importante manter-se atualizado sobre as melhores práticas de segurança e estar preparado para lidar com incidentes de segurança.

Exemplo(s) de uso interessante(s) em empresas, organizações, projetos ou instituições dessa tecnologia de Banco de Dados pesquisada (casos de ataques):

Como exemplo de um ataque que ocorreu envolvendo injeções SQL, podemos citar o ataque ao site “Yahoo!” em 2012, em que um grupo organizado de hackers conhecidos como D33Ds Company atacou um ponto fraco no banco de dados do site, afetando assim os dados de cerca de 450 mil usuários em todo o mundo, revelando endereços de e-mail e senhas mal criptografadas.

Apesar dos danos extensos, o site pôde usar a situação como um catalisador para mudanças, aumentando suas medidas de segurança, introduzindo proteções mais robustas e promovendo melhores práticas de senha entre seus usuários.

Por outro lado, como exemplo para um ataque DDoS, podemos citar um dos maiores ataques DDoS já registrados, que ocorreu em setembro de 2017 e visou afetar a empresa Google. Os invasores, assumidamente chineses, usaram diversas redes para enviar pacotes falsificados a 180000 servidores web, que por sua vez enviaram respostas ao Google.

Esse ataque resultou em um tráfego de 2,54 Tbps (Terabit por segundo), e foi divulgado 6 meses após seu acontecimento, resultando no aumento de segurança por parte da empresa.

Desse modo, visualizando os casos reais, é possível perceber as desvantagens que a falta de medidas de segurança podem

causar, envolvendo tanto a falta de integridade e proteção de dados sensíveis, quanto a complexidade necessária para implementar tais medidas quando percebidas em alguma situação.

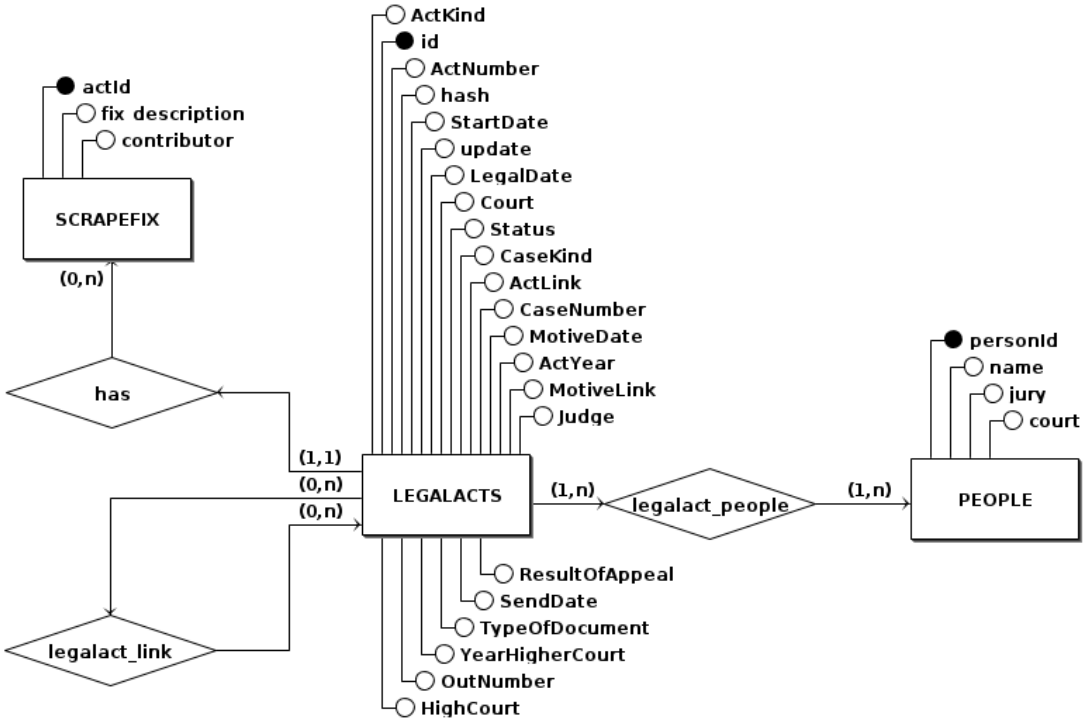
Base de Dados (documentação):

Podemos tomar como exemplo para uso a seguinte base de dados: “legalActs”.

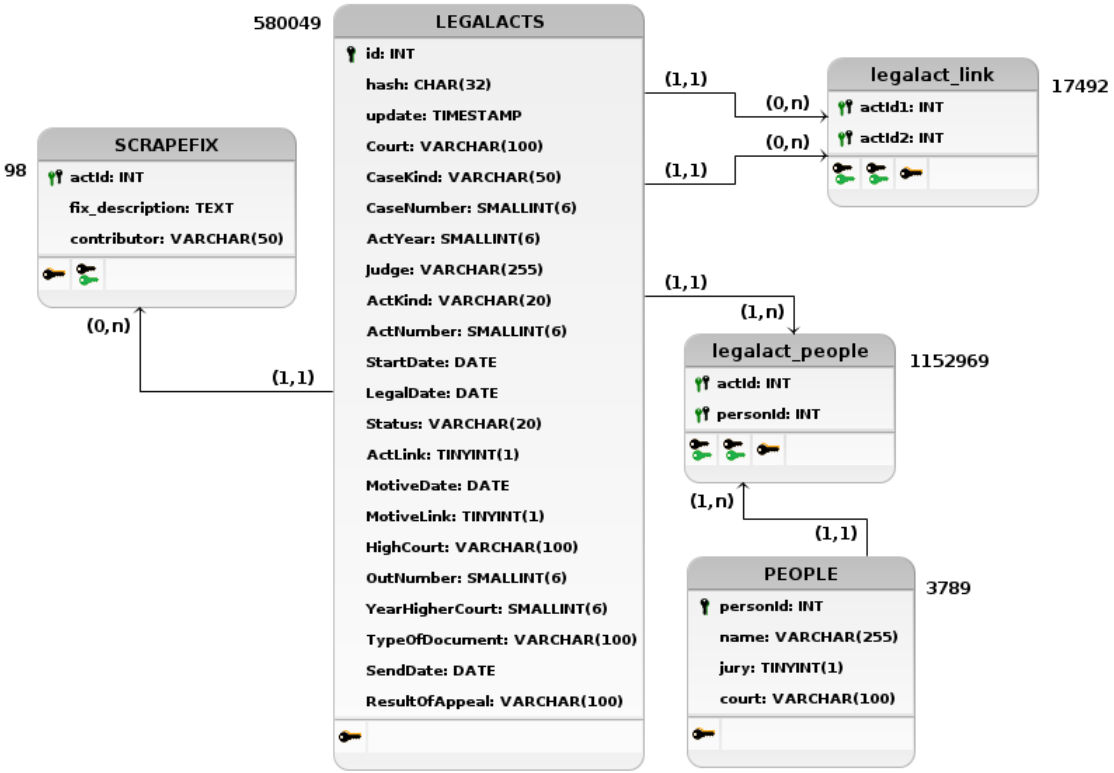
Essa base de dados representa mais de 500 mil casos de ações reais do tribunal búlgaro, e estão disponibilizados no site “Relational Dataset Repository”. As informações desses casos incluem as tabelas de casos, ligação entre os casos, contribuições de terceiros para alguma correção nos casos, pessoas participantes dos casos e as ligações entre os casos e essas pessoas. Ainda dentro da tabela de casos, podemos encontrar informações sobre o tribunal de cada um, sua data de início, o tipo de ação, o motivo da ação, o resultado, entre outros.

Seguindo o esquema da própria base de dados, temos o que segue para o Diagrama Entidade-Relacionamento (DER), seguido diretamente de seu Diagrama Lógico de Dados (DLD) resultante:

DER (Diagrama Entidade-Relacionamento):



DLD (Diagrama Lógico de Dados):



Segue o endereço virtual da base de dados utilizada, que se

encontra no próprio site da Relational Dataset Repository”, com suas devidas instruções de instalação citadas no endereço: https://relational.fit.cvut.cz/dataset/LegalActs

Bibliografias Pesquisadas:

OLIVEIRA, Ruy Flavio de. Segurança de Sistemas de Banco de Dados. Londrina: Editora e Distribuidora Educacional S.A., 2017. Disponível em: http://cm-kls-content.s3.amazonaws.com/201701/INTERATIVAS_2_0/SEGURANCA_DE_SISTEMAS_DE_BANCOS_DE_DADOS/U1/LIVRO_UNICO.pdf. Acesso em: 12 de Junho de 2023.

LEGAL ACTS. [S.l.]: [s.n.], [s.d.]. Disponível em: https://relational.fit.cvut.cz/dataset/LegalActs. Acesso em: 12 de Junho de 2023.

RELATIONAL DATASET REPOSITORY. [S.l.]: [s.n.], [s.d.]. Disponível em: https://relational.fit.cvut.cz/. Acesso em: 12 de Junho de 2023.

CLOUDFLARE. Famous DDoS Attacks. [S.l.]: Cloudflare, [s.d.]. Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/famous-ddos-attacks/. Acesso em: 12 de Junho de 2023.

ZDNET. Google says it mitigated a 2.54 Tbps DDoS attack in 2017, largest known to date. [S.l.]: ZDNet, 16 de outubro de 2020. Disponível em: https://www.zdnet.com/article/google-says-it-mitigated-a-2-54-tbps-ddos-attack-in-2017-largest-known-to-date/. Acesso em: 12 de Junho de 2023.

SOFTWARE LAB. Injeção SQL. [S.l.]: Software Lab, Maio de 2023. Disponível em: https://softwarelab.org/pt/injecao-sql/. Acesso em: 12 de Junho de 2023.