PROJETO EYEWEB

Introdução Base de Dados

1º Ano de CTeSP de Cibersegurança

Trabalho realizado por:

José Samuel da Rocha Oliveira – Nº 2024172

Tiago Filipe Sousa Carvalho – Nº 2024180

Vanina Kollen – Nº 2024056

Francisco Rafael Carocinho Ribeiro – Nº 2024123

Emanuel Jorge Seixas – Nº 2024079

Ana Rita da Silva Monteiro – Nº 2024041

abril 2025

ÍNDICE

1.- INTRODUÇÃO

A gestão de riscos associados a ativos informáticos é essencial para garantir a segurança e a continuidade operacional das organizações. O Simulador de Gestão de Riscos de Dados foi desenvolvido com o objetivo de facilitar este processo, permitindo a catalogação de ativos, a identificação de ameaças e o cálculo automático de um índice de risco com base em parâmetros predefinidos.

A aplicação inclui funcionalidades como o registo de ativos e ameaças, o cálculo do risco utilizando uma fórmula simples e um dashboard interativo para a análise de estatísticas. Além disso, a base de dados foi estruturada com base em princípios como relacionamentos 1:N, normalização, views e stored procedures, garantindo eficiência no armazenamento e na consulta dos dados.

Este sistema visa apoiar a gestão de riscos, proporcionando uma abordagem sistemática e fundamentada para a tomada de decisões, contribuindo assim para a proteção dos ativos informáticos da organização.

2.- CONCEITOS BÁSICOS

2.1.- O QUE É UMA BASE DE DADOS

Uma base de dados é um conjunto organizado de informações estruturadas ou de dados geralmente armazenados eletronicamente em um sistema informático. Normalmente, uma base de dados é controlada por um sistema de gestão de bases de dados (DBMS). Em conjunto, os dados e o DBMS, juntamente com as aplicações que estão associadas aos mesmos, são referidos como um sistema de base de dados, muitas vezes reduzidos para uma única base de dados.

2.2.- O QUE É UMA TABELA

Uma tabela, em base de dados, está dividida em linhas e colunas onde são registrados os dados dentro da base e consiste na estrutura principal e essencial de uma base de dados. O uso de tabelas permite evitar redundâncias.

3.- RELACIONAMENTOS, NORMALIZAÇÃO E INTEGRIDADE

ESTRUTURA DAS TABELAS PARA UM RELACIONAMENTO 1:N

Antes de perceber como devem organizar-se, é preciso saber o que é um relacionamento. Um relacionamento ou cardinalidade, em base de dados, trata-se da interação entre entidades ou tabelas, facilitando e melhorando o desempenho das consultas. Existem distintos tipos de relacionamentos e cardinalidades: relacionamento 1:1, cardinalidade 1:N, cardinalidade N:M, etc. O relacionamento 1:N (também conhecido como um-para-muitos) faz referência a quando uma instância, ou ocorrência, de uma entidade A se relaciona com muitas instâncias de outra entidade B, mas isto não ocorre vice-versa, senão que uma instância da entidade B se relaciona com uma única instância da entidade A. Para poder estabelecer um relacionamento 1:N, é preciso utilizar uma chave estrangeira. Existem distintos tipos de chaves no âmbito de bases de dados, como: a chave primária, chave estrangeira, chave candidata, chave secundária, etc. Uma chave estrangeira consiste numa coluna referente à chave primária de outra tabela.

COLUNAS PARA GARANTIR A NORMALIZAÇÃO DAS TABELAS

A normalização de tabelas trata-se de organizar as informações numa base de dados para melhorar o desempenho, administração e evita complicações e a possibilidade de que se torne demasiado complexa de analisar. Para implementar a normalização numa base de dados, é necessário aplicar uma série de regras que atribui estruturas definidas aos dados. Existem 8 formas normais e regras como: a primeira forma normal (1FN), a segunda forma normal (2FN), a terceira forma normal (3FN), etc. Por exemplo, na primeira forma (1FN), estabelece grupos lógicos de maneira que não existam repetições além de identificar a chave primária da tabela. Na segunda forma normal (2FN) assegura que os registros da tabela dependam da chave primária e na terceira forma normal (3FN) os atributos que dependem de outro que não é uma chave, são separados.

COMO GARANTIR A INTEGRIDADE REFERENCIAL

A integridade de uma base de dados faz referência à qualidade que caracteriza aos dados que são exatos, precisos e consistentes, concedendo proteção contra perdas ou intervenções

que produzam danos. Existem 5 tipos de integridade de dados: de identidade, física, referencial, do domínio e definida pelo utilizador. A integridade referencial cria relacionamentos entre as identidades seguindo uma lógica, se estes relacionamentos são quebrados, os dados perdem-se. Para proteger a integridade dos dados numa base de dados é preciso aplicar técnicas de defesa nos pontos de entrada, métodos e ferramentas além de restrições para limitar a possibilidade de uma vulnerabilidade afetar o acesso aos dados.

4.- ARMAZENAMENTO, REGISTROS E ESTRUTURA

COMO CADASTRAR E ARMAZENAR UM ATIVO COM NOME, CATEGORIA E CRITICIDADE NO BANCO DE DADOS

Para cadastrar um ativo, cria-se uma tabela com os campos: nome (texto), categoria (texto) e criticidade (numérico, tipicamente 1-5). A operação de armazenamento é feita através do comando INSERT, que adiciona registros à tabela. É crucial definir uma chave primária (ID) para identificação única e implementar validações para garantir a integridade dos dados. A criticidade deve seguir uma escala predefinida para manter a consistência na avaliação dos ativos.

COMO REGISTAR UMA AMEAÇA, INCLUINDO TIPO, IMPACTO E PROBABILIDADE

O registo de ameaças requer uma tabela com os campos: tipo (texto para classificação), impacto (numérico, escala 1-5) e probabilidade (numérico, escala 1-5). Deve incluir-se uma chave estrangeira (ID do ativo) para estabelecer a relação com a tabela de ativos. O comando INSERT é utilizado para adicionar novas ameaças, com restrições (CHECK) para limitar os valores de impacto e probabilidade à escala definida, assegurando dados válidos e consistentes.

COMO ESTRUTURAR A CONSULTA PARA CALCULAR AUTOMATICAMENTE O RISCO USANDO A FÓRMULA (RISCO = IMPACTO X PROBABILIDADE)

O cálculo do risco pode ser implementado de três formas principais: 1) Através de uma consulta SELECT que multiplica impacto por probabilidade; 2) Usando colunas geradas (em PostgreSQL) que calculam e armazenam automaticamente este valor; 3) Criando uma VIEW que apresenta o risco calculado em tempo real. Para maior flexibilidade, pode-se adicionar uma classificação qualitativa (ex.: "Alto", "Médio", "Baixo") baseada em intervalos do valor calculado.

5.- CONSULTAS COMPLEXAS, VIEWS E STORED PROCEDURES

COMO IMPLEMENTAR CONSULTAS COMPLEXAS PARA FILTRAR ATIVOS POR CRITICIDADE E AMEAÇAS POR IMPACTO

Basicamente, para filtrar ativos por criticidade e ameaças por impacto, precisamos juntar as informações das duas tabelas: ativos e ameaças. Depois aplicar os filtros que interessam, por exemplo, dá para ver só os ativos mais críticos ou as ameaças com impacto mais alto. O importante aqui é ter as tabelas bem ligadas com aquelas chaves que conectam uma tabela na outra, e usar essas conexões pra conectar os dados. Também dá pra criar uns índices nessas colunas que são mais pesquisadas como a criticidade ou o impacto para deixar tudo mais rápido. Isso ajuda a puxar os dados mais depressa.

FORMAS QUE AS VIEWS PODEM SER UTILIZADAS PARA EXIBIR DADOS RESUMIDOS NO DASHBOARD

Resumidamente as views deixam as consultas mais fáceis e atualizam automaticamente quando os dados mudam e ainda ajudam a organizar melhor as informações no painel. As views são tipo atalhos para consultas que a gente usa. Em vez de ficar a escrever a mesma cena várias vezes, dá para criar uma view e já tá lá sempre que precisar. No dashboard, elas servem para mostrar este tipo de informação:

Quantos ativos têm risco alto;

Ameaças mais comuns;

Um resumo geral do risco de cada ativo;

COMO STORED PROCEDURES PODEM SER USADAS PARA AUTOMATIZAR CÁLCULOS DE RISCO

As stored procedures são uma espécie de scripts que ficam guardados na base de dados e rodam automaticamente quando as usamos. No caso do cálculo de risco(exemplo(impacto x probabilidade)), em vez de ficar a calcular isso a toda a hora dá pra criar uma stored procedure que já faz isso sozinha. Aqui estão alguns exemplos em que elas são usadas:

Automatiza o cálculo de risco sempre que tem uma nova ameaça;

Atualiza os valores sem precisar mexer em cada registro manualmente;

Garantir que todos os cálculos sejam feitos sempre do mesmo jeito, sem erro;

Fica mais prático porque basta rodar a stored procedure uma vez e já resolve tudo de uma vez só

6.- FORMATOS DE EXPORTAÇÃO E RELATÓRIO CONSOLIDADO

QUAIS FORMATOS DE EXPORTAÇÃO DE RELATÓRIOS PODEM SER IMPLEMENTADOS (CSV, PDF, JSON)

Implementar funções que extraem os dados da base, formatam conforme o tipo de ficheiro e disponibilizam para download. Para CSV e JSON, basta converter os dados em tabelas estruturadas. Para PDF, usar bibliotecas que permitam a criação de relatórios formatados com tabelas e gráficos.

COMO GERAR UM RELATÓRIO CONSOLIDADO COM ESTATÍSTICAS DOS ATIVOS E SEUS RISCOS ASSOCIADOS

Criar consultas SQL que agreguem informações dos ativos e os seus riscos, utilizando JOIN e GROUP BY. Usar views para facilitar a reutilização dessas consultas e stored

procedures para automatizar cálculos de risco. Os dados consolidados podem ser exibidos no dashboard e exportados nos formatos desejados.

7.- CONCLUSÃO

O Simulador de Gestão de Riscos de Dados constitui uma solução eficaz para a identificação, avaliação e monitorização dos riscos associados a ativos informáticos. Através de funcionalidades como o registo detalhado de ativos e ameaças, o cálculo automatizado de riscos e a visualização de estatísticas, a aplicação permite uma gestão mais estruturada e informada dos riscos.

A aplicação dos conceitos de banco de dados, como relacionamentos 1:N, normalização e o uso de views e stored procedures, assegura um sistema eficiente e escalável. Com isso, a ferramenta contribui para uma melhor tomada de decisão na minimização de riscos, promovendo a segurança e a proteção dos ativos essenciais nas organizações.

Em suma, o simulador oferece uma abordagem integrada e prática para a gestão de riscos, proporcionando às empresas os meios necessários para prevenir ameaças e proteger a sua infraestrutura digital de forma eficaz.

8.- PROJETO – EYEWEB

8.1.- O QUE É EYEWEB

EyeWeb é um projeto com o objetivo de criar uma ferramenta capaz de analisar a segurança de websites e senhas. Com o EyeWeb, é possível verificar a integridade de sites, identificando possíveis ameaças e vulnerabilidades, bem como avaliar a força das senhas e confirmar se já foram comprometidas em vazamentos de dados.

Caso uma senha seja identificada como vazada, o nosso site irá alertar o utilizador e fornecer detalhes sobre as informações expostas, permitindo assim que tome medidas rápidas para reforçar a segurança.

Este projeto consiste numa ferramenta desenvolvida para melhorar a segurança digital dos utilizadores, focando-se na análise de websites e palavras-passe. O principal objetivo é ajudar

a identificar potenciais ameaças online e garantir que as palavras-passe utilizadas são seguras e não estão comprometidas.

A funcionalidade de análise de websites permite verificar se um site pode ser malicioso, avaliando fatores como histórico de ameaças, certificados de segurança e possíveis ligações suspeitas. Já a funcionalidade de verificação de palavras-passe permite ao utilizador saber se a sua senha é forte e se já foi exposta em bases de dados comprometidas. Caso tenha sido, o sistema indica quando e onde ocorreu essa exposição, ajudando o utilizador a tomar as medidas necessárias para proteger as suas contas.

O software foi desenvolvido para ser intuitivo e acessível, permitindo que qualquer pessoa, independentemente dos seus conhecimentos técnicos, consiga utilizá-lo para reforçar a sua segurança online.

8.2.- **OBJETIVO**

O objetivo deste projeto é disponibilizar uma ferramenta útil e acessível para reforçar a segurança digital dos utilizadores. A aplicação permite identificar possíveis riscos ao navegar na internet e avaliar a segurança das palavras-passe utilizadas. Desta forma, pretende-se minimizar a exposição a ataques informáticos, como o roubo de dados e acessos não autorizados, contribuindo para uma navegação mais segura.

Com este sistema, os utilizadores poderão:

- Verificar se um website é seguro antes de o acederem;
- Avaliar se as suas palavras-passe são fortes e se já foram expostas em fugas de dados;
- Receber sugestões para melhorar a proteção das suas contas e informações pessoais.

Este projeto procura sensibilizar para a importância da cibersegurança e disponibilizar uma solução prática e eficaz para garantir maior privacidade e proteção de dados.

8.3.- **PÚBLICO-ALVO**

O público-alvo do projeto são pessoas e empresas que querem melhorar a sua privacidade e a segurança dos seus dados.

8.4.- **CRITÉRIOS DE SUCESSO**

O sucesso deste projeto será avaliado com base em vários fatores que garantem a eficácia, a usabilidade e o impacto da ferramenta na segurança digital dos utilizadores. Para que o projeto seja considerado bem-sucedido, devem ser cumpridos os seguintes critérios:

1. **Precisão**: A ferramenta deve identificar corretamente websites maliciosos e avaliar a força das palavras-passe, incluindo verificações de fugas de dados.
2. **Usabilidade**: A interface deve ser intuitiva e de fácil utilização, permitindo que qualquer utilizador consiga realizar as análises de forma simples e rápida.
3. **Segurança e Privacidade**: Nenhuma informação pessoal deve ser armazenada ou partilhada. As análises devem ser seguras e temporárias.
4. **Desempenho**: A ferramenta deve ter uma resposta rápida, sem falhas, garantindo eficiência na análise de sites e senhas.
5. **Adoção**: O número de utilizadores e o feedback positivo indicam a utilidade e aceitação da ferramenta.
6. **Cumprimento de prazos e orçamento**: O projeto deve ser concluído dentro do cronograma e orçamento estabelecidos.

Esses critérios garantirão que o projeto atenda aos objetivos e tenha um impacto positivo na segurança digital dos utilizadores.

8.5.- **COMUNICAÇÃO**

A comunicação entre a equipa e o cliente será feita por e-mail da empresa, através do qual um membro da equipa terá acesso. Assim, o cliente poderá fazer perguntas e solicitar melhorias ou soluções caso o software não funcione como esperado.

8.6.- **REQUISITOS**

8.6.1.- FUNCIONAIS

1. **Análise de Websites**

   O utilizador deve conseguir inserir a URL de um site para obter uma avaliação sobre a sua segurança, identificando se o site é seguro ou se há risco de ser malicioso.

2. **Verificação de Senhas**

   A ferramenta deve permitir que o utilizador insira uma senha para que seja analisada quanto à sua complexidade. A ideia é avaliar se a senha é forte o suficiente e, caso tenha sido comprometida em alguma violação de dados, informar onde isso aconteceu.

3. **Relatórios Claros**

   Depois da análise de um site ou senha, o sistema deverá gerar um relatório simples e direto, com informações sobre os riscos encontrados e sugestões sobre como melhorar a segurança.

4. **Alertas de Senhas Vazadas**

   Se a senha inserida já foi exposta em algum vazamento de dados, a ferramenta deverá alertar o utilizador e informar em qual violação ela foi encontrada, para que ele possa tomar ações, como trocar a senha.

5. **Interface Simples e Intuitiva**

   O objetivo é que o utilizador consiga fazer tudo de maneira rápida e sem complicações. A interface deve ser simples, permitindo que qualquer pessoa, independentemente do seu conhecimento técnico, consiga utilizar a ferramenta com facilidade.

8.6.2.- NÃO FUNCIONAIS

1. **Desempenho Rápido**

   A ferramenta deve ser ágil. O utilizador não deve esperar muito tempo para ver os resultados das análises, seja para sites ou senhas.

2. **Segurança Garantida**

   Nenhuma informação sensível do utilizador, como senhas ou dados pessoais, deve ser guardada no sistema. A análise deve ser feita de forma temporária e segura, sem riscos para o utilizador.

3. **Compatibilidade com Diferentes Navegadores**

   A ferramenta deve funcionar bem nos navegadores mais usados (como Chrome, Firefox e Edge) e também ser otimizada para ser usada em dispositivos móveis, para que as pessoas possam acessá-la de qualquer lugar.

4. **Capacidade de Crescer**

   O sistema deve ser capaz de crescer, caso seja necessário. Ou seja, se no futuro mais pessoas começarem a usar ou o sistema precisar de mais funcionalidades, ele deve continuar a funcionar sem problemas.

5. **Disponibilidade Constante**

   A ferramenta deverá estar disponível sempre, 24/7. O sistema precisa ser estável, com o mínimo de interrupções e manutenção, para que o utilizador possa usá-lo sempre que precisar.

6. **Privacidade Respeitada**

   O foco é a privacidade do utilizador. O sistema não deverá exigir registo de dados pessoais e, de maneira alguma, deverá guardar ou partilhar informações sensíveis sem o consentimento explícito do utilizador.

7. **Acessibilidade para Todos**

   A interface precisa ser acessível para qualquer pessoa, incluindo aquelas com limitações de visão. O sistema deverá ser compatível com leitores de tela e ter alternativas visuais para garantir que todos consigam utilizá-lo com facilidade.

8.7.- ANÁLISE DAS NECESSIDADES E PRIORIDADES

8.7.1.- NECESSIDADES

1. **Segurança das Senhas e Sites**

   O utilizador precisa de uma ferramenta que consiga analisar senhas e sites para garantir que estão seguros. É fundamental verificar se a senha já foi comprometida em vazamentos de dados e, se sim, onde aconteceu, para que o utilizador possa tomar medidas de proteção.

2. **Simples e Fácil de Usar**

   A ferramenta deve ser fácil de usar, sem complicações. O objetivo é que qualquer pessoa consiga usar a plataforma para verificar senhas ou sites sem precisar ser um especialista em segurança, tudo de forma clara e prática.

3. **Verificar Senhas e Sites de Forma Rápida**

   O utilizador quer uma maneira rápida e eficiente de verificar se as suas senhas são fortes e se os sites que visita estão seguros. A ferramenta deve mostrar essas informações de forma clara, ajudando o utilizador a proteger suas contas e dados.

4. **Privacidade e Confidencialidade**

   As informações dos utilizadores devem ser protegidas a todo custo. Nenhuma senha ou dado pessoal deve ser armazenado ou partilhado. O sistema tem de garantir que a privacidade seja sempre respeitada.

8.7.2.- PRIORIDADES

1. **Alta Prioridade**
   - Segurança e Proteção: A prioridade número um é garantir que o sistema analise senhas e sites de forma segura e eficaz, sem comprometer os dados dos utilizadores.
   - Facilidade de Uso: A interface da ferramenta deve ser simples e intuitiva, para que qualquer pessoa consiga usar sem dificuldades, sem ter de aprender nada complexo.

2. **Média Prioridade**
   - Relatórios Simples e Úteis: Embora os relatórios sobre senhas e sites sejam importantes, eles não devem ser complicados. A ideia é que as informações sejam diretas, com dicas claras sobre como melhorar a segurança.
   - Verificação de Vazamentos de Senhas: Saber se a senha foi vazada em algum ataque é uma funcionalidade importante, mas a verificação da força da senha e da segurança do site deve vir em primeiro lugar.

3. **Baixa Prioridade**
   - Escalabilidade no Futuro: Embora o sistema deva ser escalável para futuras melhorias, no início, o foco será garantir que ele funcione bem e de forma estável.
   - Suporte a Vários Idiomas: A tradução para diferentes idiomas pode ser feita depois, quando o sistema estiver completamente funcional e a sua base de utilizadores já estiver estabelecida.

8.8.- **LIMITAÇÕES DO PRODUTO**

1. **Dependência da Entrada do Utilizador**

   O sistema depende das senhas e sites que o utilizador fornece. Ou seja, para funcionar corretamente, é necessário que o utilizador insira as informações certas. Sem essas entradas, a ferramenta não pode fazer a verificação.

2. **Necessita de Internet**

   A aplicação precisa de uma conexão à internet para funcionar. Isso significa que não será possível usar a ferramenta sem acesso à web.

3. **Limitações na Verificação de Sites**

   A análise de sites para verificar se são maliciosos depende de fontes externas e bases de dados. Se essas fontes não estiverem atualizadas ou não forem acessíveis, a análise pode não ser totalmente precisa.

4. **Limitações na Avaliação de Senhas**

   Embora a ferramenta verifique se a senha é forte com base em certos critérios, ela não consegue prever todos os tipos de ataques, como os de engenharia social ou phishing.

5. **Funcionalidades Iniciais**

   O foco inicial da ferramenta está em funções básicas, como verificar a força das senhas e analisar a segurança dos sites. Algumas funcionalidades mais avançadas poderão ser adicionadas no futuro.

6. **Privacidade e Dados**

   O sistema não guarda nenhum dado dos utilizadores. Isso é bom para a privacidade, mas também significa que não podemos criar um histórico das análises feitas.

8.9.- **DESIGN**

8.9.1.- CENÁRIO DE SUCESSO PRINCIPAL

1. OBJETIVOS DO PROJETO

O nosso projeto tem como objetivo criar uma ferramenta simples e eficaz para ajudar os utilizadores a proteger as suas senhas e verificar se os sites que visitam são seguros. A plataforma será fácil de usar e rápida, permitindo que qualquer pessoa, independentemente dos seus conhecimentos em segurança digital, consiga utilizá-la sem problemas. O sucesso será medido pela experiência do utilizador: se a ferramenta for prática e realmente ajudar a melhorar a segurança online. A interface será clara e intuitiva, com navegação simples. Além disso, a rapidez na análise das senhas e sites será uma prioridade. O objetivo final é que os utilizadores se sintam seguros e confiantes ao usar a ferramenta, protegendo as suas informações de forma eficiente.

2. ANÁLISE DAS NECESSIDADES DOS UTILIZADORES

Para garantir que a ferramenta atenda às necessidades dos utilizadores, fizemos uma análise com base em pesquisas e feedback direto. As principais necessidades identificadas foram:

- **Necessidade de Senhas Seguras e Comprovadas:** Os utilizadores precisam de uma forma simples de garantir que as suas senhas são fortes e seguras, além de verificar se já foram comprometidas em vazamentos de dados.
- **Verificação de Sites e Segurança Online:** Os utilizadores querem saber se os sites que visitam são seguros, especialmente com o aumento de ataques cibernéticos e fraudes online.
- **Facilidade de Uso e Acessibilidade:** A ferramenta deve ser simples e intuitiva, permitindo que qualquer pessoa consiga verificar as suas senhas e sites sem conhecimentos técnicos.
- **Privacidade e Confidencialidade:** Os utilizadores querem garantir que as suas senhas e informações não sejam armazenadas ou partilhadas com terceiros.
- **Rapidez e Eficiência:** A ferramenta deve ser rápida, processando as informações sem grandes esperas, para garantir uma experiência de uso sem frustrações.

3. MÉTRICAS DE SUCESSO

As métricas de sucesso definem como vamos avaliar o impacto e o desempenho da nossa ferramenta. Elas são baseadas nas necessidades dos utilizadores e nos objetivos do projeto. As principais métricas são:

- **Taxa de Adoção da Ferramenta:** Medir o número de utilizadores que começam a usar a plataforma. O sucesso será maior se mais pessoas adotarem a ferramenta.
- **Satisfação dos Utilizadores:** A satisfação será avaliada por feedback direto e inquéritos. Se os utilizadores acharem a ferramenta útil e fácil de usar, é um bom sinal.
- **Tempo de Resposta:** A ferramenta deve ser rápida e fornecer resultados em tempo real, garantindo uma experiência sem frustrações.
- **Taxa de Precisão:** A precisão das análises será medida pela eficácia em identificar senhas fracas e sites inseguros.

8.10.- **INTERFACE GRÁFICA**

O utilizador ao aceder ao site vai aceder a uma página principal em que vai ter uma animação de entrada de um olho, e depois aparece o conteúdo. A página inicial vai ter o nome em grande centralizado, e vai ter uma pequena frase logo embaixo a dizer "descubra se o seu email, palavra passe, utilizador e número de telefone foi compartilhado pela internet!" ou algo do género. E em seguida vai ter uma barra em baixo que o utilizador vai poder ver se foi vazado ou não. Vai ter uma pequena página de "about" com interações gráficas animadas.

8.11.- **FUNCIONAMENTO DO SITE**

O utilizador ao inserir qualquer uma das informações que quer verificar, elas vão aparecer em diferentes tipos de "ficheiros" que deram leaked, e vai aparecer se tem algum tipo de informação extra relacionado com o que ele inseriu. Vai aparecer para ele quando é que essa informação foi divulgada na internet e quando foi colocada no site.

Ele também vai poder verificar se um link de algum site já foi identificado como malicioso antes, e que tipo de malware foi encontrado nele. O site também vai mostrar se o link do site selecionado foi alvo de ataques ou não, e a data em que isso aconteceu. Também vai dizer quando é que esse site foi identificado como malicioso e quando foi inserido na base de dados.

8.12.- **ADMINISTRAÇÃO DO SITE**

O administrador vai ter uma página separada há parte. Em que ao entrar, ele vai ter uma interface bem mais simples e menos animada, porque importa é a eficiência de preenchimento de dados e a organização deles na base de dados. Ele vai ter um botão em que vai dizer "novo ficheiro encontrado" na categoria de "info-leaked", em que vai inserir todos os dados desse ficheiro, e vai dar para relacionar dados entre o tipo de informação divulgada. Ao inserir o ficheiro vai dizer a data em que ele foi publicado na internet para todos verem, e quando foi adicionado ao site. Também vai ter outra aba em que vai dizer "informação separada encontrada" também na categoria de "info-leaked". Em que vai dar para meter dados que não foram encontrados em ficheiros mas divulgados na internet por pessoas com intenções maliciosas. Vai dar para relacionar esses dados com outros dados que foram encontrados com ele também. Vai dar para editar todos os ficheiros que foram colocados lá e editar ou apagar informação adicionada anteriormente, caso ela tenha sido alterada ou deletada do público, e a mesma coisa será aplicada para informação que foi adicionada separadamente.

O administrador também vai ter outra categoria chamada de "sites maliciosos" em que vai poder adicionar links de sites que foram encontrados com algum tipo de malware neles, e vai especificar que tipo de malware foi encontrado neles, se é seguro para navegar ou não. Também vai informar se foi alvo de algum tipo de ataque hacker e vai dizer o dia em que aconteceu e o tipo de ataque que aconteceu. Vai dar para editar todos os links foram colocados lá e editar ou apagar cada um dos links adicionados anteriormente, caso eles tenham sido alterados ou deletados do público.

9.- **WEBGRAFIA**

- Blog DNC - "Tipos de Cardinalidade: o que é e conheça os tipos - Blog DNC" (Acedido o 25 de março de 2025)
https://www.escoladnc.com.br/blog/entendendo-os-tipos-de-cardinalidade-em-modelagem-de-bancos-de-dados/

- Linkedin - "Explorando os diferentes tipos de chaves em Bancos de Dados" (Acedido o 25 de março de 2025)
https://pt.linkedin.com/pulse/explorando-os-diferentes-tipos-de-chaves-em-bancos-cordeiro-de-sousa

- Linkedin - "Chaves em bancos de dados relacionais" (Acedido o 7 de abril de 2025)
https://pt.linkedin.com/pulse/chaves-em-bancos-de-dados-relacionais-henrique-paes-de-souza

- Ebaconline - "O que é a normalização de bases de dados e como fazê-la?" (Acedido o 7 de abril de 2025)
https://ebaconline.com.br/blog/normalizacao-de-bases-de-dados

- IBM - "O que é integridade de dados?" (Acedido o 7 de abril de 2025)
https://www.ibm.com/br-pt/topics/data-integrity

- Linkedin - "Integridade em Banco de Dados" (Acedido o 7 de abril de 2025)
https://pt.linkedin.com/pulse/integridade-em-banco-de-dados-paulo-planez-diniz

- Medium - "Normalização em Bancos de Dados" (Acedido o 7 de abril de 2025)
https://medium.com/@diegobmachado/normaliza%C3%A7%C3%A3o-em-banco-de-dados-5647cdf84a12

- PostgreSQL - "PostgreSQL: Documentation: 17: INSERT" (Acedido o 25 de março de 2025)
https://www.postgresql.org/docs/current/sql-insert.html

- W3schools - "SQL Constraints" (Acedido o 25 de março de 2025)
https://www.w3schools.com/sql/sql_constraints.asp

- PostgreSQL - “PostgreSQL: Documentation: 17: 5.4. Generated Columns” (Acedido o 25 de março de 2025)

https://www.postgresql.org/docs/current/ddl-generated-columns.html

- PostgreSQL - “PostgreSQL: Documentation: 17: CREATE VIEW” (Acedido o 25 de março de 2025)

https://www.postgresql.org/docs/current/sql-createview.html

- W3schools - “SQL CREATE TABLE Statement” (Acedido o 25 de março de 2025)

https://www.w3schools.com/sql/sql_create_table.asp

- PostgreSQL - “PostgreSQL INSERT” (Acedido o 25 de março de 2025)

https://neon.tech/postgresql/postgresql-tutorial/postgresql-insert