Trabalho Prático 1

Instruções

O trabalho prático deverá ser desenvolvido em grupos de três elementos e submetido via *Blackboard* até o fim do dia **21/03/2025**. O resultado da análise proposta deverá constar em um documento em formato *pdf* com, no máximo, 15 páginas (excluindo capa e referências).

Objetivo

O seu grupo faz parte da equipa de desenvolvimento de um serviço de *Cofre Digital*, sendo responsáveis pela identificação dos requisitos de cibersegurança e pela definição dos mecanismos de segurança mais adequados. Assim, o trabalho prático proposto tem por objetivo produzir uma análise de segurança para o serviço em desenvolvimento. A sua análise deverá conter (mas não estar limitada a):

- Os ativos relevantes do sistema do ponto de vista da proteção das propriedades de segurança da informação;
- As principais ameaças aos respetivos ativos;
- Uma análise de risco que sustente a priorização da resposta às ameaças identificadas durante fases seguintes do projeto, *i.e.*, desenvolvimento e operação do sistema;
- Uma lista de requisitos de segurança sustentada pelo seu estudo. Os requisitos devem ter em conta as ameaças de maior risco;
- Sugestões de respostas para os requisitos de segurança identificados.
  Notem que a equipa de desenvolvimento é representada pelos docentes da UC. Portanto, os esclarecimentos necessários sobre os requisitos funcionais ou outro detalhe que julguem relevantes para a análise de segurança deverão ser obtidos durante as aulas de *Práticas Laboratoriais*.

Descrição do *Cofre Digital*

O sistema em desenvolvimento suporta um serviço de *Cofre Digital* no qual utilizadores armazenam, de forma segura, ficheiros de qualquer tipo. O sistema é composto por três componentes principais, *i.e.*, *Servidor*, *Serviço web* e *Aplicação móvel*, e deve suportar a partilha de ficheiros das seguintes formas:

- Partilha de um ficheiro com um utilizador ou grupo de utilizadores do sistema;
- Partilha de um conjunto de ficheiros (*i.e.,* uma *pasta*) com um utilizador ou grupo de utilizadores do sistema.
  Qualquer utilizador do sistema poderá criar uma *pasta* contento um conjunto de ficheiros e partilhar esta pasta com um utilizador ou um grupo de utilizadores. Um grupo de utilizadores também poderá ser criado por qualquer utilizador do sistema, bastando conhecer os identificadores dos utilizadores ou os respetivos emails. Os grupos criados são identificados por um *nome* (*e.g.,* família, trabalho, etc). Uma restrição importante é que o proprietário de um ficheiro poderá conceder permissão de partilha dos seus ficheiros aos membros do grupo. Ou seja, ao partilhar um ficheiro ou pasta com um ou mais utilizadores, deverá indicar se estes poderão partilhá-lo com outros utilizadores.

As principais características e funcionalidades de cada componente do sistema são:

Servidor

O servidor é responsável por toda a lógica do serviço desenvolvido, incluindo registo e autenticação de utilizadores, controlo de acesso a ficheiros, criação e gestão de cofres, criação e gestão de grupos, criação e gestão de pastas, armazenamento de ficheiros, etc. Esta componente do sistema será composta por por um conjunto de microsserviços a correr em um *cloud provider*.

Algumas soluções já usadas pela empresa que prestará o serviço e que, idealmente, deverão ser mantidas no novo sistema são:

- Fedora Server 41
- Nginx 1.24.0
- PostgreSQL 10.22

Serviço web

Serviço oferecido a utilizadores onde poderão se registar no sistema, criar e gerir cofres, adicionar e remover ficheiros, criar e gerir pastas, criar e gerir grupos, gerir permissões de partilha, etc.

Aplicação móvel

Aplicação compatível com IOS e Android que suporta todas as funcionalidades disponíveis via *serviço web*. Além disso, a aplicação deverá manter uma cópia local do cofre para uso em modo *offline*. Neste modo, deverá ser possível também enviar um ficheiro de forma segura de um dispositivo móvel para outro. Ou seja, a transferência direta de um ficheiro entre dois dispositivos usando comunicação *bluetooth* (sem a intervenção do servidor).
Para reduzir os custos de desenvolvimento e manutenção, a aplicação deverá ser construída como uma *Progressive Web App* (PWA).

Requisitos globais

- É preciso garantir a confidencialidade do cofre e das comunicações
- É preciso garantir a integridade do cofre
- É preciso garantir a autenticidade dos utilizadores

Links úteis

- MITRE ATT&K
- OWASP TOP 10
- Elevation of Privilege (EoP) Threat Modeling Card Game
- OWASP Threat Modeling
- Common Weakness Enumeration
- National Vulnerability Database