Engenharia de Segurança

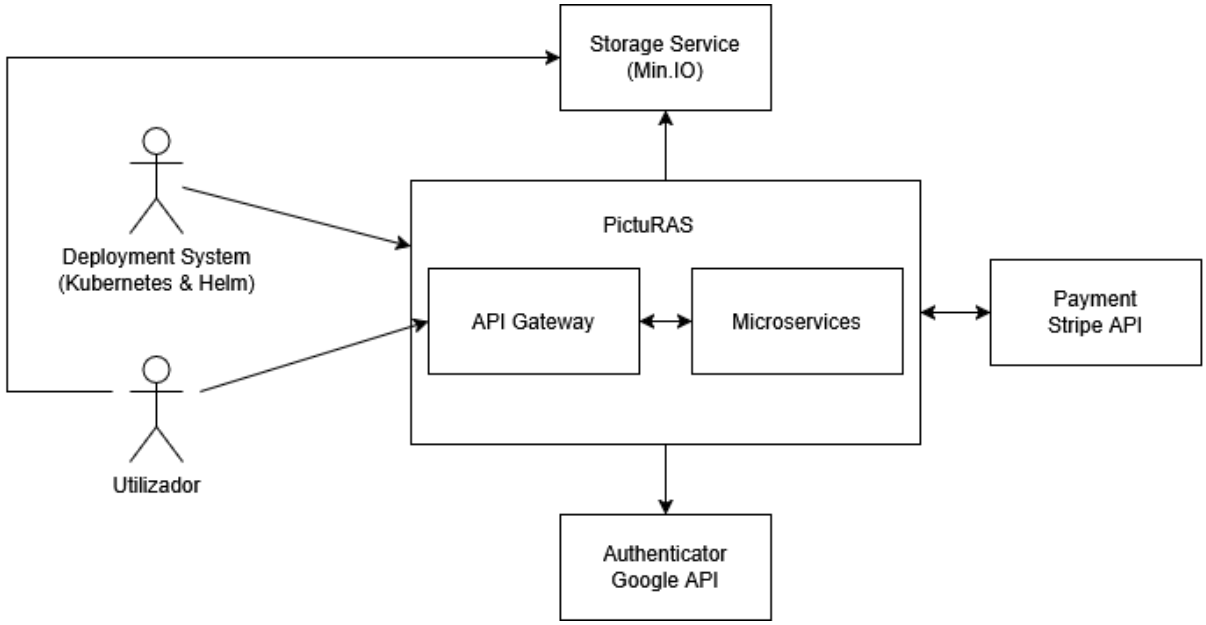
Hands-On 2

PictuRAS Threat Model

Eduardo Cunha PG55939

Fevereiro 2025

Modelo de Fluxo de Data



1. Ameaças a que o PictuRAS está sujeito

Ataque de Brute Force

Um atacante pode adivinhar as credenciais de um utilizador (como nome de utilizador e/ou palavra-passe) através de múltiplas tentativas de login.

Como fazer:

1. Identificação do Alvo

Identificar o formulário de login da aplicação web, que é o ponto de entrada para testar combinações de credenciais.

2. Recolha de Informações

Recolher informações sobre a aplicação, como:

- Nomes de utilizadores comuns (ex: admin).
- Listas de palavras-passe comuns.
- Regras de validação de palavras-passe (ex: número mínimo de caracteres, uso de maiúsculas e números).

3. Automatização do Ataque

Utilizar ferramentas ou scripts para automatizar o envio de múltiplas tentativas de login. (ex. Hydra: Uma ferramenta de brute force que suporta vários protocolos (HTTP, HTTPS, FTP, etc.)).

Como resolver:

1. Implementar limites de tentativas de login, bloqueando temporariamente a conta após um número definido de tentativas falhadas.

2. Utilizar CAPTCHA para distinguir entre utilizadores humanos e bots, dificultando a automatização de tentativas de login.

A verdade é que temos implementado a autenticação de dois fatores (2FA), o que aumenta significativamente a segurança do sistema mesmo que uma palavra-passe seja crackeada. No entanto, é importante ter em mente que o 2FA, apesar de ser uma medida robusta, não é infalível. Um invasor pode recorrer a outras técnicas para contornar esta proteção

2. Ameaças devidamente defendidas:

SQL Injection:

Um atacante injeta código malicioso nas queries SQL para aceder e/ou manipular a base de dados.

Mitigação:
No caso do PictuRAS, estamos a utilizar o MongoDB, uma base de dados NoSQL, que não está sujeita a ataques de SQL Injection.

Não está garantida a segurança contra ataques NoSQL Injection

Armazenamento Inseguro de Palavras-passe:

As palavras-passe são armazenadas em texto simples ou com algoritmos de hashing fracos, o que facilita a sua descoberta em caso de violação de dados.

Mitigação:
No PictuRAS, utilizamos algoritmos de hashing forte, como o bcrypt, para armazenar as palavras-passe de forma segura. O bcrypt inclui um "salt" (valor aleatório) para garantir que hashes idênticas tenham resultados diferentes, aumentando a segurança.

Phishing:

Um atacante engana o utilizador, levando-o a revelar as suas credenciais através de emails, mensagens ou websites falsos.

Mitigação:
Para combater o phishing, implementámos autenticação de dois fatores (2FA). Além da palavra-passe, o utilizador precisa de fornecer um código temporário para aceder à sua conta. Isto adiciona uma camada extra de segurança, mesmo que as credenciais sejam comprometidas.

Ataques de Replay:

Um atacante intercepta e reutiliza tokens de autenticação para se fazer passar por um utilizador legítimo.

Mitigação:
Utilizamos tokens com tempo de vida limitado, como JWT (JSON Web Tokens), que expiram após um período definido. Além disso, implementámos mecanismos de renovação de tokens para garantir que apenas tokens válidos e recentes são aceites.

Acesso Não Autorizado:

Um utilizador acede a recursos ou funcionalidades do sistema sem as permissões adequadas.

Mitigação:
Implementámos controlos de acesso rigorosos, baseados no modelo RBAC (Role-Based Access Control). Neste modelo, cada utilizador tem um "role" específico que define as suas permissões. Além disso, verificamos as

permissões em cada operação sensível para garantir que apenas utilizadores autorizados podem aceder a determinados recursos.