**PROJETO INTEGRADOR DO 5º SEMESTRE: MEDIA SUGGESTER**

Ana Clara  
Bruno  
Igor  
João Nascimento  
Pedro Cruz

* **Introdução**

O aplicativo “Media Suggester” é uma plataforma de recomendação de Filmes e Séries desenvolvida em Flutter para dispositivos Android. Ele oferece uma experiência intuitiva e prática de recomendação de conteúdo para os usuários assistirem com base em seus gostos.

Principais Funcionalidades:

* Recomendação de Filmes e Séries: Os usuários recebem recomendações de filmes e séries com base em suas preferências, utilizando inteligência artificial.
* Busca de Filmes e Séries: Os usuários podem pesquisar as informações de algum filme ou série específica.
* Favoritos: Os usuários podem adicionar filmes e séries a sua lista de favoritos.
* Publicar Reviews: Os usuários podem fazer reviews de filmes ou séries, dando uma nota e falando o que acharam do conteúdo. Essa review ficará exposta para outros usuários.
* Visualizar reviews de outros usuários: Os usuários podem ler as reviews deixadas por outros usuários.

Tecnologias Utilizadas:

* Flutter: O aplicativo foi desenvolvido em Flutter, permitindo a criação de uma única base de código para Android e outras plataformas.
* Firebase: O aplicativo utiliza o Firebase para armazenamento de dados.
* Google: O aplicativo utiliza a API do Google para autenticação de seus usuários.
* TMDB: O aplicativo utiliza a API do The Movie DataBase para carregar as informações dos filmes e séries.
* Gemini: O aplicativo utiliza a inteligência artificial do Google para gerar as recomendações.
* API .NET: O aplicativo utiliza API desenvolvida pelo grupo em .NET(C#) para interagir e fazer requisições à API do Gemini.
* **Metodologia e Abordagem**

Emulador Android/iOS:

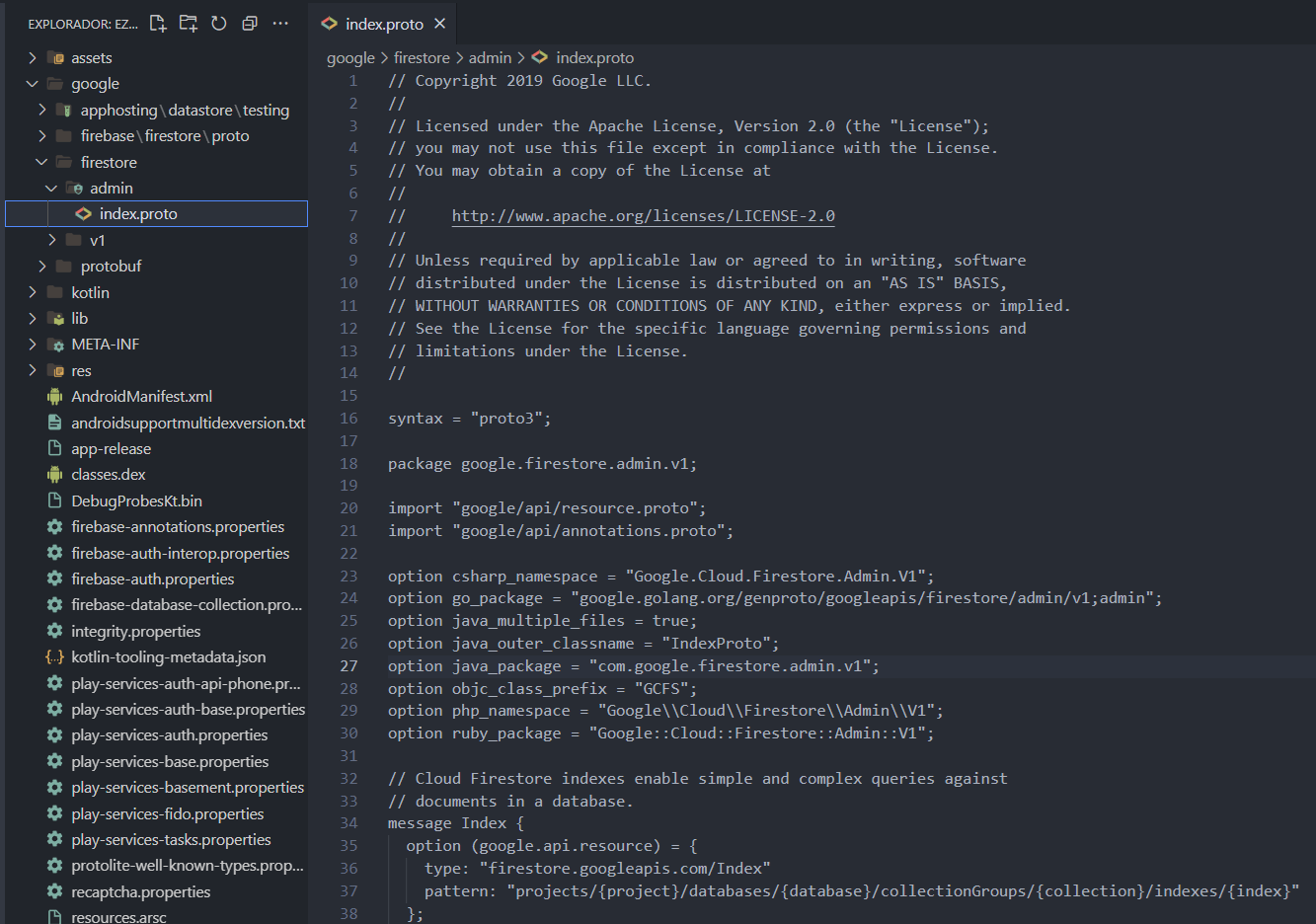
* Utilizado para simular o ambiente de execução do aplicativo em dispositivos virtuais.
* Permite testar o aplicativo em diferentes versões do sistema operacional e cenários de uso.

MobSF:

* Framework open-source utilizado para executar testes automatizados em busca de possíveis vulnerabilidades no sistema.
* **Testes de Vulnerabilidade**

Vulnerabilidade 1: Extração do arquivo .APK

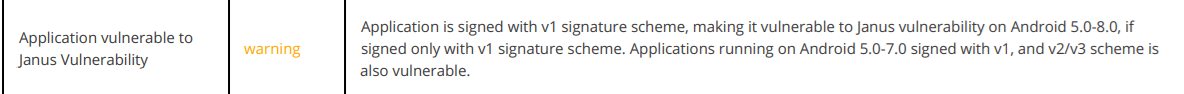
* Foi extraído o arquivo .APK (aplicativo compilado para Android), com a intenção de encontrar a chave da API do TMDB ou dados para a integração com o Firebase, porém nenhum dos dois foi encontrado.



* Caso as chaves fossem encontradas haveria uma grande vulnerabilidade, pois qualquer pessoa teria acesso ao nosso banco de dados no Firebase, ou a API do TMDB através de requisições com nossa conta.

Vulnerabilidade 2: Esquema de Assinatura V1(MobSF)

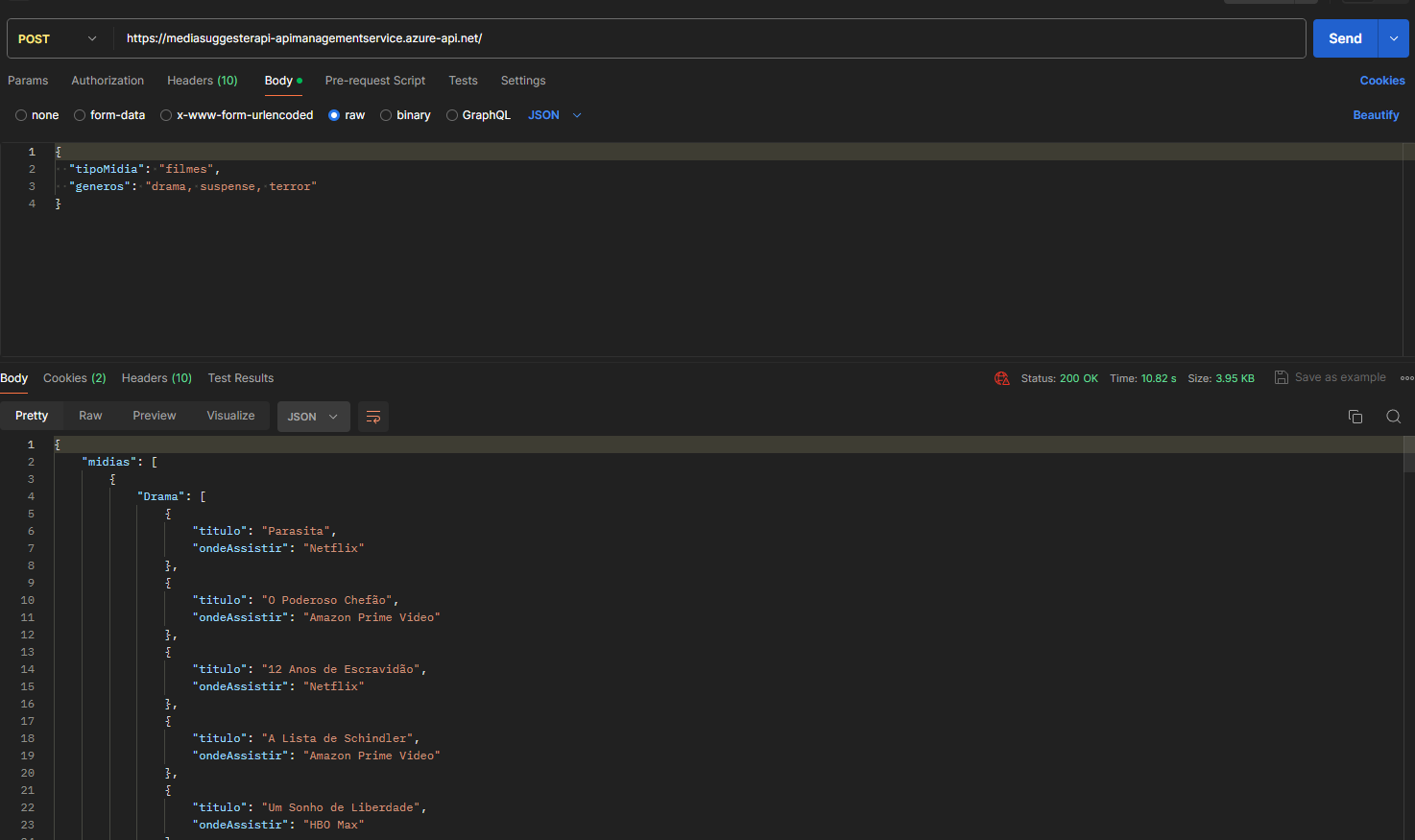
* A aplicação está assinada utilizando o esquema de assinatura v1, o que permite que a mesma seja instalada em dispositivos que possuem o Android 5.0-8.0 e versões abaixo.



* Este esquema de assinatura abre portas para uma vulnerabilidade conhecida como Janus, que permite a inserção de código malicioso em uma aplicação sem que a assinatura da mesma seja alterada, assim podendo ser distribuído sem que o Android perceba qualquer alteração maliciosa.
* Solução: Assinar a aplicação com um esquema de assinatura superior.

Vulnerabilidade 3: API .NET não possui autenticação

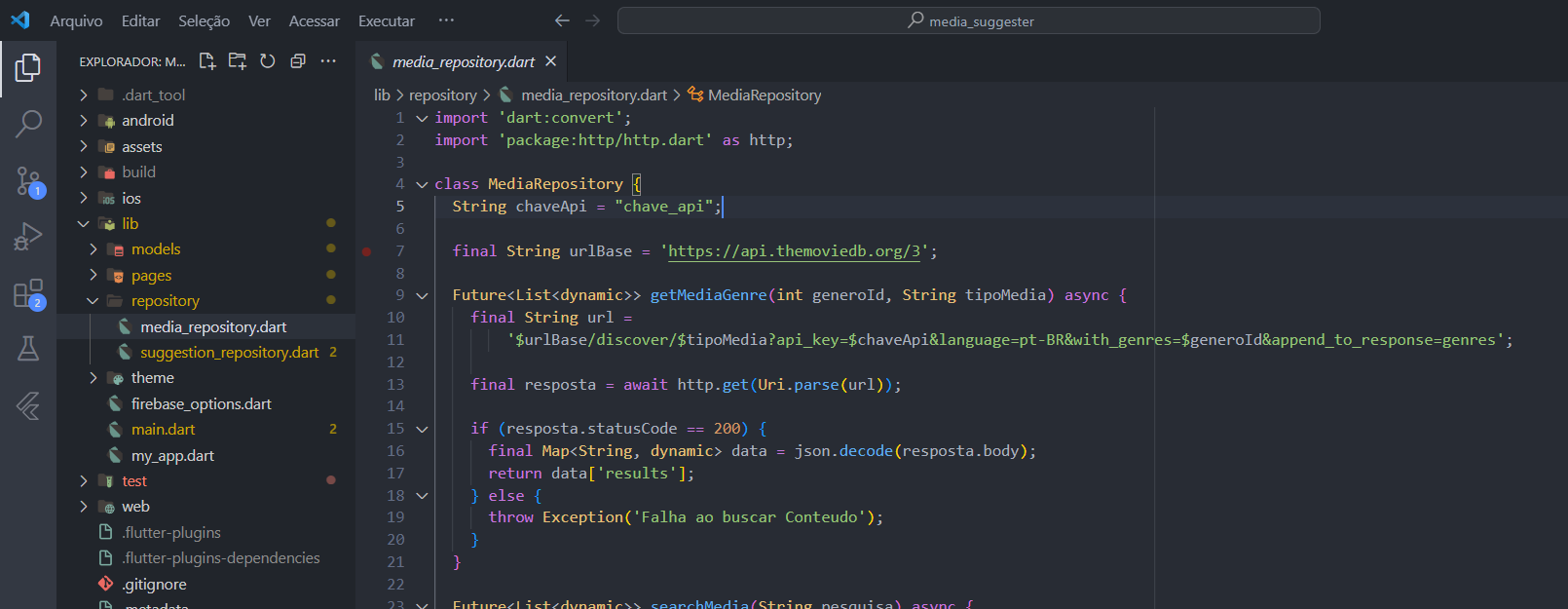
* A api não possui autenticação de usuário, permitindo que qualquer pessoa envie requisições para a mesma.



* Isso poderia acarretar no nosso limite de requisições permitidas gratuitamente à API do Gemini sendo atingido, causando custos para o grupo.
* Solução: Implementar autenticação obrigatória de usuário.

Vulnerabilidade 4: Projeto não possui arquivo .env

* O projeto não possui um arquivo para armazenar a chave da API e outros possíveis dados sensíveis, sendo necessário inserir manualmente no código (hardcoded).



* O nosso projeto está armazenado no GitHub, portanto se algum membro do grupo fizesse um commit sem omitir a chave a mesma ficara publica para qualquer usuário.
* Solução: Adicionar um arquivo .env ao projeto para armazenar dados sensíveis.
* **Conclusão**

Após a análise das vulnerabilidades apresentadas concluímos que são necessárias certas medidas para que a segurança seja garantida, como a configuração do arquivo .env, a implementação de autenticação na API .NET e a assinatura da aplicação com um esquema superior para que não sejam exploradas brechas de segurança comuns em versões antigas do Android.

Além disso, é possível notar que apesar de no momento contarmos com a atenção do grupo para que não sejam enviados dados sensíveis com chaves de API para o repositório do projeto, a configuração de um arquivo .env diminuiria drasticamente o risco dessas informações serem vazadas através da decompilação da APK.