Apresentação: Análise de Segurança com MobSF - InsecureBankV2

Autor: Vitor Cristiano Fellizatti

Faculdade: FATEC Araras

Data: 22/04/2025

Versão do App: Beta

Introdução

O projeto tem como objetivo aprender a utilizar a ferramenta MobSF (Mobile Security Framework) para realizar análise de vulnerabilidades em aplicativos Android. Foi escolhido o aplicativo InsecureBankV2, conhecido por conter falhas intencionais, ideal para testes de segurança.

Resultado da Análise

- Nota geral de segurança: 4.2 / 10
- Nível de risco: Alto
- Tamanho do APK: 3.4 MB
- Permissões perigosas:
- WRITE_EXTERNAL_STORAGE
- READ_SMS

Principais Vulnerabilidades Encontradas

1. Permissões Perigosas

Permitem que o app leia SMS e grave arquivos fora do sandbox, podendo causar vazamentos.

2. Criptografia Fraca

Uso de MD5 e Base64, que são inseguros. Isso permite que dados criptografados sejam facilmente quebrados.

3. Senha Hardcoded

Encontrada no código-fonte a string "admin123", comprometendo o controle de acesso.

4. Falta de Verificação SSL

HTTPS é usado, mas o certificado não é validado, permitindo ataques Man-in-the-Middle.

5. Log de Informações Sensíveis

Dados de login foram localizados nos logs do sistema, o que é um risco em ambientes compartilhados.

Recomendações

- Substituir MD5/Base64 por AES com chaves seguras.
- Remover credenciais hardcoded.
- Implementar SSL Pinning.
- Reduzir permissões ao mínimo necessário.
- Nunca registrar dados sensíveis nos logs.

Conclusão

MobSF é uma ferramenta poderosa para identificar riscos de segurança em apps Android. A experiência permitiu entender conceitos práticos de vulnerabilidades e boas práticas para o desenvolvimento seguro.