GAC119 - REO 2: Projeto de Mitigação de Riscos - Design Seguro

Mateus Carvalho Gonçalves - 201810245
Pedro Antônio de Souza - 201810557

Introdução

Este trabalho objetiva produzir um projeto de mitigação de riscos e ameaças da aplicação **Quero falar**, baseado nos problemas levantados na atividade 1 deste REO. Por isso, o modelo STRIDE novamente é utilizado para apoiar a organização das ideias.

Spoofing (Propriedade violada: autenticação)

Para mitigar os dois problemas relacionados a Spoofing descritos no documento de análise de riscos, pode ser feita uma implementação razoavelmente simples de autenticação de usuário, com login e senha. Assim, para utilizar a aplicação, as mulheres deverão se cadastrar no sistema informando seus dados pessoais, dentre os quais se destaca o CPF. Esse documento deve ser coletado e validado em APIs da Receita Federal para diminuir as probabilidades de criação de perfis falsos. Além disso, para prevenir problemas legais, deve ser adicionado ao Termo de Uso do software uma seção sobre Políticas de Identidade.

Para mais, como o sistema utilizará um mecanismo de controle de acesso e um dos grupos de usuário compõem entidades de segurança estatais, como descrito na seção Elevation of Privilege, regras de autenticação mais severas devem ser implementadas, como senhas com mais caracteres e autenticação de dois fatores, por exemplo.

Tampering (Propriedade violada: integridade)

Para minimizar os riscos de violação de integridade dos dados, é importante que toda entrada seja validada e tratada. Dessa forma, reduz-se a chance de injeção de código, por exemplo, ao higienizar e validar o tipo e sintaxe da informação fornecida pelo usuário.

Também, é importante criptografar dados sensíveis ao armazená-los. Assim, mesmo que um atacante tenha acesso aos dados, não será possível alterá-los sem a posse da chave de criptografia.

Repudiation (Propriedade violada: autenticidade)

Problemas de repudiação acontecem quando uma ação não é autêntica, ou seja, não foi o próprio usuário que a executou, ou quando este alega que não executou. Desta forma,

um dos principais problemas que o sistema em questão pode ter é a prática de trotes. Como dito na seção Spoofing, um cadastro forte e com validação de dados é uma medida paliativa para isso, pois o usuário executor pode ser identificado quando necessário.

Ainda, um caso similar na aplicação em questão é a ação de apertar o botão de pânico por acidente. Uma medida para isso pode ser a implementação de uma caixa de confirmação rápida que também assegure a segurança de uma vítima de violência em casos reais.

Novamente, destaca-se a importância de adicionar seções nos Termos de Uso do software para alertar os usuários sobre o mau uso do app e isentar a empresa dos casos abordados.

Information Disclosure (Propriedade violada: confidencialidade)

Para evitar os riscos de violação de confidencialidade dos dados apontados no documento de análise de riscos, é fundamental implementar um bom gerenciamento de sessão de usuário. Então, para evitar manipulações na sessão, as informações de credenciais e papel do usuário devem ser armazenadas apenas no lado do servidor.

Além da preocupação com as sessões, o uso de criptografia também pode minimizar os riscos de acesso indevido aos dados. Assim, ao utilizar criptografia de ponta-a-ponta nas transmissões de áudio e vídeo, garante-se que um atacante não conseguirá assisti-la sem possuir a chave de criptografia. Também, como já mencionado na seção Tampering, é importante criptografar todos os dados sensíveis ao armazená-los.

Denial of Service (Propriedade violada: disponibilidade)

Para evitar ataques de negação de serviço, o sistema deve permitir que apenas usuários autorizados e autenticados consumam altos níveis de CPU. Contudo, mesmo utilizando essa estratégia, a negação de serviço poderá ocorrer caso haja um alto consumo legítimo de CPU.

Portanto, dada a necessidade de alta disponibilidade da aplicação, também é importante que o sistema seja hospedado em um serviço de nuvem com escalabilidade automatizada. Assim, um *balancer* pode ajustar múltiplas máquinas para comportar grandes demandas de processamento.

Elevation of Privilege (Propriedade violada: autorização)

Para preservar a autorização necessária para cada tipo de usuário sobre as funcionalidades, é fundamental implementar mecanismos de permissionamento ou controle

de acesso, como as listas de controle de acesso (do inglês access control list, ou ACL), além de aplicar boas práticas de codificação nesse sentido.

No caso em questão, a aplicação possui dois grupos principais: o grupo padrão, definido pelas mulheres usuárias, e a entidade de segurança, definido por usuários que trabalham para os órgãos de segurança que policiam e atendem os chamados via app.

Cada um desses grupos deve possuir permissões específicas do que é possível fazer no sistema. Portanto, uma boa prática é, ao definir as permissões de um usuário ou grupo, sempre limpar os dados e adicionar o que convém. Ainda, um caso a ser analisado é o destrinchamento do grupo entidade de segurança em subgrupos, caso existam funções e atribuições diferentes entre usuários desse grupo.