**Relatório de exposição de vulnerabilidades no website da Union Corporation**

**Excessive Data Exposure**

**Sumário executivo**

Análise de segurança através de engenharia reversa em um website de propriedade de uma empresa fictícia. Alternativas para estabelecer uma postura de segurança e mitigar exposição excessiva de dados.

**Introdução**

Todos os requisitos foram seguidos de acordo com algumas regras especificadas no anexo (OTES12-P2.pdf). O ambiente de teste emulou o acesso que seria concedido a um usuário típico que visita o site da empresa.

**Descobertas**

Foi descoberta que ao menos uma brecha de segurança permite a redefinição de senha fornecendo somente um endereço de e-mail alvo. Com apenas conhecimentos básicos de engenharia reversa, o analista interceptou as requisições http e obteve endereço e parâmetros que expõem dados sensíveis sobre a conta do usuário em questão.

**Remediação**

Sugestão para correção do mecanismo de redefinição de senha:

Escrever método de redefinição com único propósito de enviar o link diretamente no e-mail requisitado;

Não retornar na requisição dado algum sobre url para redefinição com dados de nome de usuário, e-mail e token de acesso;

**Diagrama**