CONFORMIDADE EM TESTES DE SEGURANÇA

Introdução

Este documento foi criado como evidência e prova de auditoria, explicando os resultados de seus testes de segurança contínuos realizados pelo nosso time de segurança de produtos.

Nosso time de segurança de produtos (Security By Design) é especializado em executar uma ampla gama de testes de segurança para garantir a integridade e a segurança dos produtos. Realizamos avaliações detalhadas de segurança com base no escopo definido pelos projetos da empresa, procurando vulnerabilidades e reportando-as internamente de maneira coordenada e estruturada.

Nossos especialistas são altamente qualificados e utilizam as melhores práticas da indústria para identificar e mitigar potenciais riscos.

As avaliações de segurança realizadas pela nossa equipe incluem testes para uma ampla gama de vulnerabilidades, garantindo que todas as possíveis ameaças sejam identificadas e prontamente comunicadas às equipes de produtos para tratamento e mitigação.

Além disso, podemos contar com testes realizados por empresas de segurança parceiras, que trazem uma visão externa e independente, enriquecendo ainda mais a qualidade das avaliações de segurança.

Os testes de segurança conduzidos pelo nosso time são abrangentes e incluem a busca por vulnerabilidades que estão entre as mais críticas, conforme definido no **OWASP Top 10 - 2021**.

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures
A10:2021-Server-Side Request Forgery

Sumário Executivo

Tipos de Pentests

Nosso Red Team realiza os seguintes tipos de testes de segurança:

Teste de Caixa Preta (Black Box): Neste tipo de teste, nossos especialistas não possuem nenhum conhecimento prévio sobre a aplicação que está sendo testada. Eles simulam um ataque externo real, tentando identificar vulnerabilidades e falhas de segurança apenas com as informações que um atacante externo teria. Este método serve para avaliar a robustez da aplicação contra ataques genéricos e não direcionados.

Teste de Caixa Cinza (Grey Box): Os especialistas têm acesso parcial às informações sobre a aplicação, como diagramas de arquitetura, documentação técnica ou até mesmo algumas credenciais de acesso. Esse tipo de teste permite uma abordagem mais focada e eficiente, pois os pesquisadores podem explorar áreas específicas da aplicação com um entendimento melhor do seu funcionamento interno. É um equilíbrio entre os testes de caixa preta e caixa branca.

Teste de Caixa Branca (White Box): Neste caso, os especialistas têm acesso completo à aplicação, incluindo o código-fonte, a infraestrutura e a documentação. Eles realizam uma análise detalhada e abrangente para identificar vulnerabilidades e falhas de segurança. Este método é extremamente eficaz para encontrar vulnerabilidades complexas e lógicas, mas requer um alto nível de confiança nos pesquisadores, dada a quantidade de informação sensível a que eles têm acesso.

Escopo

O escopo dos testes de segurança realizados por nossa equipe é definido com base nas requisições e necessidades específicas das equipes de produtos. Esse alinhamento garante que os testes sejam direcionados para as áreas mais críticas e relevantes, atendendo às prioridades e aos objetivos de segurança estabelecidos por cada equipe de produto. Dessa forma, conseguimos proporcionar uma avaliação de segurança focada e eficaz, ajustada às particularidades e exigências de cada projeto.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Resultados

Período: últimos 12 meses - Mai/2023 a Mai/2024

ESCOPO	
SOLUÇÃO	PRODUTO
FLUIG	FLUIG fluig.com/portal

Vulnerabilidades reportadas (alta, média e baixa respectivamente):

Fonte: Dashboard controle pentest

Metodologia

Dependendo do escopo da avaliação, o nosso time de especialistas segue as metodologias e padrões discutidos nesta seção.

Aplicações Web

Durante a avaliação de segurança de uma aplicação web, uma ampla gama de vulnerabilidades é testada, incluindo aqueles definidos no OWASP Top 10 – 2021:

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures
A10:2021-Server-Side Request Forgery

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Algumas metodologias que também são seguidas nos testes realizados são:

OWASP Web Security Testing Guide
Penetration Testing Execution Standard (PTES)
NIST SP 800-115

API

Dependendo do escopo da avaliação, o nosso time de especialistas segue as metodologias e padrões discutidos nesta seção.
Para as avaliações de segurança das APIs, o foco dos testes está nas vulnerabilidades de segurança definidas no **OWASP Top 10 APIs - 2019**:

API1:2019-Broken Object Level Authorization
API2:2019-Broken User Authentication
API3:2019-Excessive Data Exposure
API4:2019-Lack of Resources & Rate Limiting
API5:2019-Broken Function Level Authorization
API6:2019-Mass Assignment
API7:2019-Security Misconfiguration
API8:2019-Injection
API9:2019-Improper Assets Management
API10:2019-Insufficient Logging & Monitoring

Aplicações Mobile

Durante a avaliação de segurança de aplicações móveis, o **OWASP MAS checklist** e o **OWASP Mobile Application Security Testing Guide** desempenham um papel predominante na cobertura de testes. Isso inclui vulnerabilidades fora das seguintes categorias:

- Arquitetura, Design e Modelagem de Ameaças
- Armazenamento e privacidade de dados
- Criptografia
- Autenticação e gerenciamento de sessão
- Comunicação de rede
- Interação com Plataforma
- Qualidade do código e configuração de construção
- Resiliência

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Considerações

A Declaração de Conformidade em Testes de Segurança, emitida pelo nosso Setor de Desenvolvimento Seguro (Security By Design), certifica que nossos produtos são submetidos a testes de segurança regulares realizados por nossa equipe de especialistas. Este documento assegura que nossos produtos estão alinhados aos mais altos padrões de segurança e que qualquer vulnerabilidade identificada recebe um tratamento.

Este documento reafirma o compromisso da TOTVS com a segurança e a qualidade dos nossos produtos. Nossas avaliações são conduzidas de maneira rigorosa e contínua por nossa equipe de especialistas, garantindo que todas as vulnerabilidades identificadas sejam prontamente comunicadas aos times de produtos para correção.

Nosso processo de avaliação e mitigação de riscos são cuidadosamente projetados para proteger nossos clientes e suas informações, assegurando a permanência de nossos produtos como soluções seguras e confiáveis. Estamos comprometidos em aprimorar continuamente nossas práticas de segurança para enfrentar os desafios emergentes e manter a confiança de nossos clientes.

TOTVS

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©