Pentest 2024 Q1

VANTICO

04 de Março de 2024

Contents

List of Figures

1 DECLARAÇÃO E RESPONSABILIDADE

Este documento serve como uma declaração oficial sobre o desempenho do pentest na aplicação web da empresa VANTICO. Com o objetivo de identificar e avaliar possíveis vulnerabilidades nos sistemas da empresa.

O teste foi conduzido seguindo um conjunto de diretrizes éticas e com o propósito de identificar possíveis vulnerabilidades e pontos de entrada que poderiam ser explorados por indivíduos mal-intencionados.

Este documento atesta a conclusão do pentest de acordo com os termos estabelecidos e tem como objetivo informar a VANTICO sobre as atividades conduzidas durante este processo de avaliação de segurança.

2 Sumario Executivo

Este documento possui duas seções:

Sumario Executivo: Esta seção fornece uma visão geral das atividades de teste, objetivos e descobertas críticas.

Relatório Técnico: Este segmento fornece uma descrição detalhada das vulnerabilidades descobertas durante a avaliação, incluindo sua classificação, localização, impacto potencial e prova de conceito.

Este pentest tem como objetivo fornecer à equipe da VANTICO uma compreensão clara do estado atual de segurança do seu serviço. O teste oferece recomendações acionáveis para aprimorar sua resistência contra possíveis ameaças cibernéticas.

É importante observar que, embora este relatório ofereça insights valiosos sobre o estado de segurança dos serviços durante o período de teste, ele não representa a segurança geral do sistema. Alterações feitas após o teste e novos elementos introduzidos no sistema podem alterar o status de segurança. Portanto, é altamente recomendável manter uma vigilância contínua, realizar testes regulares e implementar remediações oportunas para manter uma postura de segurança robusta. ## Escodo do teste

Os testes foram conduzidos utilizando o escopo fornecido pelo cliente na carta de compromisso, se atendo somente a sua aplicação.

2.1 Resultado Executivo

O teste recentemente conduzido revelou um apenas uma vulnerabilidades, as quais precisam ser corrigidas para evitar possíveis explorações.

Vulnerabilidades	Criticidade	CVSS
Insecure Direct Object Reference (IDOR) - Upload de arquivos	Média	6.8

2.2 Referência à Classificação de Risco

Abaixo está uma tabela com informações relacionadas à classificação das falhas e o total de vulnerabilidades.

Severidade	Descrição	Quantidade
Critica	Severidade máxima, elas possibilitam controle total ou parcial do sistema operacional, execução remota de código (RCE) e acesso a outros ambientes da estrutura de rede corporativa.	0
Alta	Severidade elevada, vazamento de dados e exSposição de informações sensíveis, permitindo reconhecimento dos processos internos.	0
Média	Severidade moderada, pode desencadear ataques subsequentes, comprometendo parcialmente a estrutura.	1
Baixa	Severidade baixa, não ameaça a segurança, fornece informações técnicas úteis para o conhecimento, não requer correção urgente.	0
informativa	Severidade informativa, informações técnicas ou contextuais, não representam riscos significativos.	0