VERIFACT

Relatório

Teste de intrusão em aplicação WEB

CLASSIFICAÇÃO:

RESTRITO

Realizado por

eSecurity CYBER SECURITY

Data:	Auditor:	Empresa:	Revisor:	Empresa:	Versão:
28/06/2022	Vinícius Leão	eSecurity	Alan Sanches	eSecurity	1.0

Sumário

1. Introdução

Este relatório tem como objetivo apresentar os riscos sistêmicos em aplicação web e seu impacto no negócio, em teste de intrusão e análise de vulnerabilidades que foram realizados entre os dias **09 de maio de 2022 a 20 de junho de 2022**.

1.1. Dados do alvo

Dados do Cliente:

- **Razão Social:** VERIFACT TECNOLOGIA LTDA
- **CNPJ:** 32.797.434/0001-50

Target:

- https://app.verifact.com.br/

Credenciais:

E-Mail:	Tipo:
testmaster@XXXXXX.com.br	Master
testegestor@XXXXXX.com.br	Subgestor da master
testeconvidado@XXXXXX.com.br	Convidado da master
testecomum@XXXXXX.com.br	Comum

2. Conclusão do teste de intrusão

Foram realizados diversos testes de segurança e tentativas de obtenção de informações ou dados de acessos restritos ou limitados, simulando um ataque real a partir da WEB. Nesta análise foram encontradas diversas proteções de segurança para evitar ataques simples e sofisticados no processo de coleta de informações fornecida pela plataforma, bem como em outros pontos do ambiente.

Dentre os testes realizados priorizamos ataques que consistiam na tentativa de manipulação do processo de coleta de dados e do material após a preservação, tais quais se encontram disponíveis na internet no momento do registro. Também buscamos sistematicamente manipular as informações do ambiente WhatsApp Desktop durante a coleta de informações, além das tentativas de alterações, manipulações ou falsificação destes dados, afins de forjar evidências.

Não foram encontradas vulnerabilidades conhecidas no ambiente, baseada na metodologia apresentada abaixo.

3. Metodologia utilizada

A metodologia utilizada para este teste de intrusão em aplicações WEB foi baseada no guia público e colaborativo "*OWASP Testing Guide versão 4".*

O OWASP Testing Guide v4 inclui uma estrutura de testes de penetração baseada nas "melhores práticas", que podem ser implementadas em testes de intrusão em ambiente web. Ele também inclui um guia de teste de penetração de "baixo nível" que descreve técnicas para testar os problemas mais comuns em aplicativos e serviços Web. Hoje, o Testing Guide é o

padrão para realizar o Teste de penetração de aplicativos da Web, e muitas empresas em todo o mundo o adotaram.

Para obter detalhes sobre a metodologia aplicada, visite a página no link abaixo:

https://www.owasp.org/index.php/OWASP_Testing_Project

3.1. OWASP Top Ten 2021 Project para pentest WEB

Durante a bateria de testes, iremos abranger centenas de possibilidades para encontrar e / ou provocar vulnerabilidades, além de coletar o máximo de informações possíveis sobre a aplicação e o ambiente que a hospeda, e então, analisar os riscos que essas informações poderão trazer ao negócio.

Será exercido maior esforço dos 10 grupos de vulnerabilidades mais comuns nos últimos anos, esse conjunto de 10 vulnerabilidades representam um número substancial de todas as vulnerabilidades em aplicações web reportadas.

O OWASP Top 10-2021 é baseado principalmente em mais de 40 envios de dados de empresas especializadas em segurança de aplicativos e uma pesquisa do setor que foi concluída por mais de 500 pessoas. Esses dados abrangem vulnerabilidades coletadas de centenas de organizações e mais de 100.000 aplicativos e APIs reais. Os 10 principais itens são selecionados e priorizados de acordo com esses dados de prevalência, em combinação com estimativas consensuais de explorabilidade, detectabilidade e impacto.

As top 10 vulnerabilidades que daremos foco nesse relatório são:

A01:2021-Broken Access Control: Restrições sobre o que os usuários autenticados têm permissão para fazer geralmente não são aplicadas corretamente. Os invasores podem explorar essas falhas para acessar funcionalidades e/ou dados não autorizados, como acessar contas de outros usuários, visualizar arquivos confidenciais, modificar dados de outros usuários, alterar direitos de acesso etc.

Estão inclusas nesta categoria as Common Weakness Enumerations (CWEs):

- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
- CWE-201: Exposure of Sensitive Information Through Sent Data
- CWE-352: Cross-Site Request Forgery.

Resultado: Em conformidade

A02:2021-Cryptographic Failures: Anteriormente conhecida como Exposição de dados confidenciais, que é mais um sintoma amplo do que uma causa raiz, o foco está nas falhas relacionadas à criptografia (ou falta dela). O que muitas vezes leva à exposição de dados confidenciais.

Estão inclusas nesta categoria as Common Weakness Enumerations (CWEs):

- CWE-259: Use of Hard-coded Password
- CWE-327: Broken or Risky Crypto Algorithm
- CWE-331 Insufficient Entropy.

Resultado: Em conformidade

A03:2021-Injection: Falhas de injeção, como SQL, NoSQL, OS e LDAP, ocorrem quando dados não confiáveis são enviados para um intérprete como parte de um comando ou consulta. Os dados hostis do invasor podem induzir o intérprete a executar comandos não intencionais ou acessar dados sem a devida autorização.

Estão inclusas nesta categoria as Common Weakness Enumerations (CWEs):

- CWE-79: Cross-site Scripting
- CWE-89: SQL Injection
- CWE-73: External Control of File Name or Path.

Resultado: Em conformidade

A04:2021- Insecure Design: Concentra-se nos riscos relacionados a falhas de design e arquitetura, com uma chamada para mais uso de modelagem de ameaças, padrões de design seguros e arquiteturas de referência.

Estão inclusas nesta categoria as Common Weakness Enumerations (CWEs):

- CWE-209: Generation of Error Message Containing Sensitive Information
- CWE-256: Unprotected Storage of Credentials
- CWE-501: Trust Boundary Violation, e CWE-522: Insufficiently Protected Credentials.

Resultado: Em conformidade

A05:2021-Security Misconfiguration: A configuração incorreta da segurança é o problema mais comum. Isso geralmente resulta de configurações padrão inseguras, incompletas ou ad hoc, armazenamento em nuvem aberta, cabeçalhos HTTP configurados incorretamente e mensagens de erro detalhadas que contêm informações confidenciais. Não apenas todos os sistemas operacionais, estruturas, bibliotecas e aplicativos devem ser configurados com segurança, mas devem ser corrigidos / atualizados em tempo hábil.

Estão inclusas nesta categoria as Common Weakness Enumerations (CWEs):

- CWE-16 Configuration
- CWE-611 Improper Restriction of XML External Entity Reference.

Resultado: Em conformidade

A06:2021-Vulnerable and Outdated Components: Componentes reconhecidamente vulneráveis ou sem suporte serão avaliados e mapeados para então serem explorados ou apontados durante o teste de intrusão.

Está inclusa nesta categoria a Common Weakness Enumerations (CWE):

- CWE-1104: Use of Unmaintained Third-Party Components.

Resultado: Em conformidade

A07:2021-Identification and Authentication Failures: As funções de aplicativos relacionadas à autenticação e ao gerenciamento de sessões são frequentemente implementadas incorretamente, permitindo que os invasores comprometam senhas, chaves ou tokens de sessão ou explorem outras falhas de implementação para assumir a identidade de outros usuários temporária ou permanentemente.

Estão inclusas nesta categoria as Common Weakness Enumerations (CWEs):

- CWE-297: Improper Validation of Certificate with Host Mismatch
- CWE-287: Improper Authentication
- CWE-384: Session Fixation.

Resultado: **Em conformidade**

A08:2021-Software and Data Integrity Failures: As falhas de software e integridade de dados estão relacionadas ao código e à infraestrutura que não protegem contra violações de integridade. Um exemplo disso é quando um aplicativo depende de plug-ins, bibliotecas ou módulos de fontes não confiáveis, repositórios e redes de entrega de conteúdo (CDNs). Um pipeline de CI / CD inseguro pode apresentar o potencial de acesso não autorizado, código malicioso ou comprometimento do sistema.

Estão inclusas nesta categoria as Common Weakness Enumerations (CWEs):

- CWE-829: Inclusion of Functionality from Untrusted Control Sphere
- CWE-494: Download of Code Without Integrity Check
- CWE-502: Deserialization of Untrusted Data.

Resultado: **Em conformidade**

A09:2021-Security Logging and Monitoring Failures: O registro e o monitoramento insuficientes, juntamente com a integração ausente ou ineficaz com a resposta a incidentes, permitem que os atacantes continuem atacando os sistemas, mantenham a persistência, façam o giro para mais sistemas e violem, extraiam ou destruam dados. A maioria dos estudos de violação mostra que o tempo para detectar uma violação é superior a 200 dias, geralmente detectados por partes externas, em vez de processos ou monitoramento interno.

Estão inclusas nesta categoria as Common Weakness Enumerations (CWEs):

- CWE-117 Improper Output Neutralization for Logs
- CWE-223 Omission of Security-relevant Information
- CWE-532 Insertion of Sensitive Information into Log File.

Resultado: **Em conformidade**

A10:2021-Server-Side Request Forgery (SSRF): As falhas de SSRF ocorrem sempre que um aplicativo da web busca um recurso remoto sem validar a URL fornecida pelo usuário. Ele permite que um invasor force o aplicativo a enviar uma solicitação criada para um destino inesperado, mesmo quando protegido por um firewall, VPN ou outro tipo de lista de controle de acesso à rede (ACL).

Resultado: **Em conformidade**

4. Modelo de Teste

O teste de intrusão foi realizado no modelo **Gray Box**, onde simulamos um teste de intrusão com uso de credenciais para testar o aplicativo em execução remota. Simulamos um ataque real, com objetivo de obter o máximo de informações sobre a aplicação e possíveis vulnerabilidades, além da escalabilidade delas.

5. Auditor responsável pelo projeto

Alan Sanches possui certificações internacionais de Hacker Ético (CEH) pela EC-CONCIL, Security+ pela CompTIA, Offensive Security Certified Professional (OSCP) e ISO/IEC ISO 27002, consultor em Segurança da Informação e possui 25 anos de experiência na área de Infraestrutura e Segurança Ofensiva.

Ministra treinamentos e palestras sobre Segurança Ofensiva, Defensiva, Ética Hacker e Técnicas de Intrusão nos maiores eventos de Tecnologia do Brasil como: Mind the Sec, Campus Party, LatinoWare, FLISOL, RoadSec, Hacking Day e FISL.

É Tecnólogo em Redes de Computadores e possui 3 Pós-Graduações, em Inteligência Estratégica, Master Business Information Security (MBIS) e Neurociência & Comportamento Humano.

Atualmente ministra treinamentos de Técnicas de Intrusão e Defesa Cibernética para a Polícia Civil do estado de São Paulo e treina equipes do Exército, Divisão de Inteligência da Marinha e ABIN.

LinkedIn: https://www.linkedin.com/in/alansanches/