Relatório Técnico

Teste de intrusão em aplicação WEB

Realizado por

Data:	Auditor:	Empresa:	Revisor:	Empresa:	Versão:
17/07/2020	Evely Macedo	eSecurity	Alan Sanches	eSecurity	1.1

Aviso legal

Este relatório destina-se apenas para o uso do indivíduo ou entidade ao qual está endereçado e pode conter informações que são privilegiadas, confidenciais e protegidas de divulgação, nos termos da legislação aplicável. Se o leitor deste aviso não é o destinatário pretendido, informamos que qualquer divulgação, distribuição ou cópia deste documento é estritamente proibido. Se você recebeu este documento por engano, por favor, avise-nos imediatamente por telefone, e-mail ou algum meio efetivo de comunicação.

Disclaimer

This report is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this disclaimer is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this document is strictly prohibited. If you received this document in error, please notify us immediately by telephone and return the original document to us at the post address below.

Sumário

1. Introdução 4
1.1. Dados do alvo 4
2. Conclusão do auditor 4
3. Metodologia utilizada 4
3.1. OWASP Top Ten 2017 Project 5
4. Modelo de Teste 7
5. Auditores designados para o projeto 7

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 **19 de junho à 10 de julho de 2020**.

1.1. Dados do alvo

Dados do Cliente:

Razão Social: Verifact Tecnologia LTDA ME

CNPJ: 32.797.434/0001-50

Responsável Técnico: Alexandre Munhoz

Contato: faleconosco@verifact.com.br

URL Alvo:

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

Credenciais:

Usuário:	testes@XXXXXXX.com.br
Tipo:	Cliente

2. Conclusão do auditor

Foram realizados diversos testes de segurança e tentativas de manipulação no processo de registro de evidências providas pela plataforma. Nesta análise foram encontradas diversas proteções de segurança para evitar ataques simples e sofisticados no processo de coleta de informações fornecido pela plataforma, bem como em outros pontos do sistema.

A partir do estudo realizado foi constatado que a Verifact possui medidas efetivas para evitar a manipulação do conteúdo registrado durante e depois de seu processo de registro de evidências digitais, coletando as informações conforme constam em sua origem. Também foi constatada a efetividade da segurança sobre os dados armazenados e outros pontos detalhados na metodologia descrita em seguida.

3. Metodologia utilizada

A metodologia utilizada para este teste será 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 2017 Project

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 10-2017 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:

A1:2017-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.

Status: Passou

A2:2017-Broken Authentication: 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.

Status: Passou

A3:2017-Sensitive Data Exposure: Muitos aplicativos da Web e APIs não protegem adequadamente dados confidenciais, como financeiro, assistência médica e PII. Os invasores podem roubar ou modificar esses dados com pouca proteção para realizar fraudes de cartão de crédito, roubo de identidade ou outros crimes. Os dados confidenciais podem ser comprometidos sem proteção extra, como criptografia em repouso ou em trânsito, e requer precauções especiais quando trocados com o navegador.

Status: Passou

A4:2017-XML External Entities (XXE): Muitos processadores XML mais antigos ou mal configurados avaliam referências de entidades externas em documentos XML. Entidades externas podem ser usadas para divulgar arquivos internos usando o manipulador de URI de arquivos, compartilhamentos de arquivos internos, varredura de portas internas, execução remota de código e ataques de negação de serviço.

Status: Passou

A5:2017-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.

Status: Passou

A6:2017-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.

Status: Passou

A7:2017-Cross-Site Scripting (XSS): As falhas do XSS ocorrem sempre que um aplicativo inclui dados não confiáveis em uma nova página da Web sem validação ou escape adequados ou atualiza uma página da Web existente com dados fornecidos pelo usuário usando uma API do navegador que pode criar HTML ou JavaScript. O XSS permite que os atacantes executem scripts no navegador da vítima, que podem seqüestrar sessões do usuário, desfigurar sites ou redirecionar o usuário para sites maliciosos.

Status: Passou

A8:2017-Insecure Deserialization: A desserialização insegura geralmente leva à execução remota de código. Mesmo que as falhas de desserialização não resultem em execução remota de código, elas podem ser usadas para executar ataques, incluindo ataques de repetição, ataques de injeção e ataques de escalonamento de privilégios.

Status: Passou

A9:2017-Using Components with Known Vulnerabilities: Componentes, como bibliotecas, estruturas e outros módulos de software, são executados com os mesmos privilégios que o aplicativo. Se um componente vulnerável for explorado, esse ataque poderá facilitar a perda séria de dados ou a aquisição de servidores. Aplicativos e APIs que usam componentes com vulnerabilidades conhecidas podem minar as defesas de aplicativos e permitir vários ataques e impactos.

Status: Passou

A10:2017-Insufficient Logging & Monitoring: 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.

Status: Não testado*

* Os testes foram realizados de modo remoto e durante os testes não fomos alertados ou bloqueados por nenhum sistema de monitoramento.

Outros testes: Realizamos testes de quebra criptográfica e integridade das provas geradas pela aplicação, além da injeção de conteúdo, remoção ou infecção das mesmas.

Status: Passou

Para obter detalhes sobre as TOP 10-2017 vulnerabilidades, visite a página no link abaixo:

4. Modelo de Teste

O teste de intrusão realizado utilizou o modelo **Gray Box**, onde foi fornecido apenas credenciais de nível usuário para testar o aplicativo em execução remota, com objetivo de encontrar vulnerabilidades de segurança, sem conhecer o funcionamento interno do próprio aplicativo. Simulamos um ataque real, com objetivo de obter o máximo de informações sobre a aplicação e possíveis vulnerabilidades, além da escalabilidade das mesmas.

5. Auditores designados para o projeto

Alan Sanches possui certificação internacional de Hacker Ético (CEH) pela EC-CONCIL e ISO/IEC ISO 27001, consultor em Segurança da Informação e possui 22 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 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/

Evely Macedo possui certificação internacional de Hacker Ético (CEH) pela EC-CONCIL e ISO/IEC ISO 27001, Pentester com mais de 3 anos de experiência em Segurança Ofensiva e Defensiva, especializou-se em testes de intrusão em aplicações WEB e Hardening, também é coordenadora da equipe de competições hacking (Hack a Flag) da eSecurity e graduanda em Ciências da Computação

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