Faculdade Adventista
BAHIA

Relatório de Análise de Vulnerabilidades

Professores: Jean do Ouro e Erik Lago

Classificação: PÚBLICA

Última Revisão: 28/12/2022

CONTEÚDO

Sumário

1. SUMÁRIO EXECUTIVO

Este relatório reflete os resultados da análise de vulnerabilidades da plataforma (aplicações web) Lightspeed Retail (X-Serie) (https://developers.vendhq.com/). A análise de vulnerabilidade foi realizada no período de 24 de novembro a 28 de novembro de 2022.

1.1 Sobre Projeto de Desenvolvimento Profissional

Projeto desenvolvido pelos alunos da Faculdade Adventista da Bahia que consiste em encontrar vulnerabilidades em aplicações web das empresas que participam do programa da **Bugcrowd,** uma plataforma de segurança coletiva mais inteligente da indústria, e que utiliza a **Crowdsourced Security** como ferramenta para eliminar o desequilíbrio, aproveitando os pesquisadores de segurança do **Whitehat** para encontrar e eliminar vulnerabilidades.

1.2 Código de Ética

Os alunos graduando do Curso de Gestão da Tecnologia da Informação da Faculdade Adventista da Bahia aplicam e mantêm os seguintes princípios:

• Integridade: a integridade dos pentesters estabelece confiança e, portanto, fornece a base para a confiança em seu julgamento;

• Objetividade: os pentesters possuem o mais alto nível de objetividade profissional na coleta, avaliação e comunicação de informações sobre a atividade ou processo que está sendo examinado, fazendo uma avaliação equilibrada de todas as circunstâncias relevantes para suas análises e não são indevidamente influenciados por seus próprios interesses ou por outros na formação de julgamentos;

• Confidencialidade: os pentesters respeitam o valor e a propriedade das informações que recebem e não divulgam informações sem a devida autoridade, a menos que haja uma obrigação legal ou profissional de fazê-lo;

• Competência: os pentesters aplicam os conhecimentos, habilidades e experiência necessários no desempenho dos serviços de análise de vulnerabilidades e testes de intrusão.

2. INTRODUÇÃO

Foi realizado análises de vulnerabilidades na plataforma Lightspeed, conforme definido no "Escopo" deste relatório, cujos resultados serão abordados adiante. Os testes de segurança foram realizados no período de 24/11/2022 a 28/11/2022 e seu objetivo foi identificar vulnerabilidades e propor recomendações para sua correção.
As fragilidades identificadas foram avaliadas e priorizadas de acordo com seu risco relativo e medidas para sua remediação também foram propostas.

2.1 Termo de responsabilidade

Todo o trabalho de avaliação para a elaboração deste documento foi realizado de acordo com as práticas de mercado e em conformidade com as obrigações e regulamentos impostos tanto pela legislação vigente, quanto pelo que foi estabelecido pelo orientador Jean Ouro.
As informações contidas neste relatório estão sujeitas e limitadas pelas condições descritas nas seções de “Escopo” e “Objetivos” e conforme as condições acordadas para a realização das atividades de análise de vulnerabilidades.
Em qualquer auditoria ou avaliação autorizada, o tempo e os recursos são naturalmente limitados e, portanto, quando comparado ao tempo e recursos potencialmente ilimitados disponíveis para partes com intenção maliciosa, a existência de vulnerabilidades será verificada, mas a inexistência de todos e quaisquer tipos de fragilidades não pode ser assegurado absolutamente.
Neste contexto, embora tenham sido feitos todos os esforços para auditar e avaliar a segurança do ambiente computacional da Lightspeed Retail (X-Serie), este relatório não garante de forma alguma o estabelecimento de um sistema impenetrável. Sendo assim, a FADBA e os Pentesters não se responsabilizam por qualquer perda ou dano direto ou indireto causado por qualquer falha ou violação dos sistemas desta da plataforma de viagem.

Por fim, as informações deste relatório têm classificação PÚBLICA e devem ser usadas apenas pela Lightspeed Retail (X-Serie) e pela FADBA, sendo de inteira e única responsabilidade de ambas.

2.1 Análise da organização

O Lightspeed Retail (X-Serie) é um programa público de recompensas por bugs no Bugcrowd, tendo como objetivo é construir relacionamentos mais fortes com a comunidade de segurança, recompensando os pesquisadores de segurança por seu trabalho na descoberta de vulnerabilidade de segurança.

Objetivo

O objetivo dos testes foi fornecer informações confiáveis sobre a segurança do ambiente computacional da Lightspeed Retail (X-Serie). Dessa forma, a avaliação identificou vulnerabilidades e quantificou sua criticidade, para que as mesmas possam ser geridas, resolvidas e, consequentemente, ajudar a prevenir o mau funcionamento e/ou perda financeira por meio de fraudes, fornecer diligências a regulações a clientes, e proteger a marca contra a perda de reputação.

2.3 Escopo

Os testes realizados foram do tipo “White Box” e seguiram uma abordagem com base nos limites impostos pela empresa. Portanto, o principal objetivo alcançado através da adoção de metodologia, detalha adiante, que consistiu em priorizar e otimizar as validações realizadas, fornecendo garantias em termos de cobertura ao minimizar as chances de uma falha evidente escapar ao processo de análise. Ademais, foram reunidas informações sobre a organização para que seja possível determinar o ambiente em que ela opera e a relevância desse ambiente para o processo de gestão de riscos de segurança da informação. Nesse sentido, foram realizados testes básicos de verificação de segurança em IPs obtidos indiretamente, isto é, IPs que são públicos e que foram conseguidos através de consulta ao “DNSdumpster” - ferramenta de pesquisa de domínio gratuitos que visam descobrir hosts relacionados a um domínio, conforme mostrados na Figura 1.

Figura 1 - Mapeamento dos endereços IP para o domínio “www.derbund.ch”

2.4 Limites

Todos os devidos cuidados foram tomados com base na especificação e critérios da empresa (Lightspeed Retail (X-Serie)) e as orientações do professor (FADBA) para não prejudicar o funcionamento da empresa, a fim de não causar impacto em seus sistemas ou interferir nos negócios diários da plataforma.

o fazem parte do escopo: Escalonamento de privilégios e problemas de IDOR Escalonamento de privilégios e problemas de IDOR (Insecure Direct Object References) que têm acesso de leitura/visualização a endpoints no escopo da mesma loja varejista

- injeção de CSV
- Injeção de hiperlink
- Falsificação de conteúdo
- Sequestro de link quebrado
- Redirecionamentos abertos sem demonstrar impacto de segurança adicional, como roubo de tokens para um domínio arbitrário
- Ataque homógrafo de nome de domínio internacionalizado (IDN)
- Injeção de HTML
- Navegação na guia
- Enumeração de usuários ou lojas de varejo
- Entrar/sair CSRF
- ataques de força bruta
- Limites de taxa ausentes
- Negação de serviço distribuída
- Relatórios relacionados a problemas de auto-DoS
- Problemas relacionados ao tempo limite excessivo da sessão
- Falha ao invalidar a sessão
- Relatórios de ferramentas ou varreduras automatizadas
- Sinalizadores de cookies ausentes em cookies não confidenciais
- Ataques MITM sobre conexões HTTP inseguras
- Presença de atributo de preenchimento automático em formulários da web
- Ataques que exigem acesso físico ao dispositivo de um usuário

- Técnicas de engenharia social (phishing, vishing, etc.)
- Divulgação de impressão digital/banner em serviços comuns/públicos
- Problemas de configuração de e-mail, incluindo configurações de SPF, DKIM e DMARC
- Divulgação de arquivos ou diretórios públicos conhecidos (por exemplo, robots.txt)
- Uso de uma biblioteca sabidamente vulnerável ou obsoleta (sem evidência de exploração)
- Vulnerabilidades em aplicativos de terceiros que fazem uso da API X-Series
- Vulnerabilidades que afetam usuários de navegadores ou plataformas não suportados ou desatualizados
- Qualquer acesso a dados em que o usuário alvo precise estar operando um dispositivo móvel roteado ou extraído de um backup de dispositivo móvel
- "Self" XSS (exigimos evidências de como o XSS pode ser usado para atacar outro usuário do Lightspeed)
- XSS armazenado no escopo de qualquer tipo de relatório no recurso "Relatório"
- Problemas de XSS em Angular
- Problemas relacionados a políticas de recuperação de senha e conta, como expiração de link de redefinição ou complexidade de senha
- Falta de tokens CSRF (a menos que haja evidência de ação real e sensível do usuário não protegida por um token)
- Relatórios de ataques relacionados a SSL/TLS (por exemplo, BREACH/BEAST/CRIME), cifras inseguras e protocolos, a menos que você tenha uma prova de conceito funcional e não apenas um relatório de um scanner
- Quaisquer serviços hospedados de terceiros (por exemplo, support.vendhq.com) sem prova de conceito que demonstre impacto sobre os usuários do Lightspeed
- Problemas sem impacto de segurança claramente identificado, como clickjacking em um site estático, cabeçalhos de segurança ausentes, métodos HTTP específicos em uso ou mensagens de erro descritivas
- Envios de ex-funcionários da Lightspeed dentro de um ano após sua saída da Lightspeed
- Bugs de segurança em software relacionados a uma aquisição por um período de 90 dias após qualquer anúncio público
- Bugs divulgados publicamente em software da Internet até 3 dias após sua divulgação
- Quaisquer serviços operados por integrações de terceiros sem prova de conceito que demonstre impacto sobre os usuários do Lightspeed provavelmente não serão elegíveis para recompensas

- Envios relacionados ao ponto de extremidade da API de solicitação de token no aplicativo Lightspeed Retail POS (X) para iOS
- Envios relacionados à fixação SSL móvel
- Validação inconsistente de caracteres entre os campos de formulário da interface do usuário e a API, sem impacto claro na segurança

Além disso, não foi permito realização de testes nos seguintes alvos:

partners.vendhq.comdhq.com

your-store.vendecommerce.com

partnerportal.vendhq.com

vendhq.force.com

vendimageuploadcdn.global.ssl.fastl.net

3 DETALHAMENTO DOS SOFTWARES INSTALADOS

ANÁLISE E RASTREAMENTO

Insights de domínio do Facebook	**Parse.ly**	**Insights de domínio do Facebook**	Hotjar	Google Analytics
DoubleClick Floodlight	**comScore**	Twitter Analytics	Linker de conversão do Google	**Google Universal Analytics**

FRAMEWORKS

Firebase	Bug Bounty	Next.js

REDE DE DISTRIBUIÇÃO DE CONTEÚDO

Cloudflare	API de bibliotecas AJAX	CDN JS	GStatic Google Static Content
jQuery CDN	jsDelivr	BootstrapCDN	CloudFront

MOBILE

Viewport Meta	Compatível com iPhone / Celular	Conteúdo móvel não escalonável	Compatível com Apple Mobile Web App

JAVASCRIPT LIBRARIES AND FUNCTIONS

Underscore.js	html5shiv	Reagir	Lodash
JQuery hospedado pelo Google	Hammer JS	core-js	Webpack

SERVER NAME

Cloudflare DNS	Amazon Route 53

WEB HOSTING PROVIDERS

Cloudflare Hosting	Amazon

EMAIL HOSTING PROVIDERS

SPF	DMARC

SSL CERTIFICATES

SSL por padrão	Amazon SSL

WEB SERVERS

nginx	Verniz	Apache

CDN VERIFIED

Amazon CloudFront

4 METODOLOGIA

As etapas a seguir, foram conduzidas para fornecer uma avaliação dos riscos com base na norma ABNT NBR ISO/IEC 27005:2011 com intuito de determinar eventos que possam causar uma perda potencial e auxiliar na adequação dos controles de segurança do ambiente testado:

• **Identificação de Ameaças:** identificar ameaças e potenciais de comprometer ativos (como informações, processos e sistemas);

• I**dentificação de Vulnerabilidade:** analisar vulnerabilidades que podem ser exploradas por ameaças para comprometer os ativos;

• **Determinação do nível das Vulnerabilidades:** A análise das vulnerabilidades é baseada nas consequências e na probabilidade de um cenário de incidente e suas consequências.

• **Avaliação das consequências:** determinar medidas apropriadas através do entendimento das vulnerabilidades por meio análise dos riscos para a tomada de decisões sobre ações futuras

4.1 Identificação de Ameaças

A primeira fase da avaliação concentrou-se na coleta, análise e estruturação de informações sobre os itens do escopo, utilizando principalmente técnicas de análise passiva, além de normas, fontes públicas como sites, blogs e mecanismos de pesquisa, que foram consultadas para obtenção e reconhecimento de informações sobre o ambiente testado. Isso é feito para coletar informações necessárias para conduzir as demais fases dos testes. Vale ressaltar que uma ameaça pode surgir de dentro ou de fora da organização e isso significa que nenhuma ameaça será ignorada. Dessa forma,

as ameaças foram identificadas genericamente e classificadas de acordo com a sua gravidade percebida.

4.2 Identificação das Vulnerabilidades

Testes automatizados e manuais foram combinados para confirmar a maioria das vulnerabilidades potenciais. Pois, uma vulnerabilidade que não tem uma ameaça correspondente pode não requerer a implementação de um controle no presente momento, mas convém que ela seja reconhecida como tal e monitorada, no caso de haver mudanças. Sendo assim, ao testar de diferentes formas os aspectos críticos, as falhas de segurança que não foram descobertas por determinado método puderam ser encontradas e avaliadas conforme o CVSS (Common Vulnerability Scoring System).

4.3 Determinação do nível das Vulnerabilidades

A análise das vulnerabilidades designa valores para a probabilidade e para as consequências de um risco. Esses valores (com base CVSS) foram atribuídos aos resultados das análises manuais e automatizadas verificando quanto à sua integridade e razoabilidade a fim de se diminuir o risco de vulnerabilidades não identificadas (falsos negativos) para um nível aceitável. Com isso, as descobertas foram avaliadas e reavaliadas individualmente para verificar se elas representavam, de fato, vulnerabilidades.

4.4 Avaliação das consequências

O relatório foi construído com base no escopo que empresa Lightspeed Retail (X-Serie) disponibilizou no site da bugcrowd.com. Para as futuras decisões a serem tomadas convém que as consequências, a probabilidade e o grau de confiança na identificação e determinação do nível das vulnerabilidades também sejam considerados. Por fim, é importante ressaltar que foi seguido à risca o que foi solicitado e todo o progresso geral com informações sobre a realização dos testes juntamente com os resultados da avaliação foram aqui documentados e serão entregues na forma deste relatório.

4.5 Ferramentas Utilizadas

As ferramentas mencionadas abaixo foram executadas no Kali Linux Versão 2021.2.

- **DNSdumpster.com:** é uma ferramenta GRATUITA de pesquisa de domínio que pode descobrir hosts relacionados a um domínio. E encontrar hosts visíveis da perspectiva dos invasores é uma parte importante do processo de avaliação de segurança.
- **NMAP:** é uma ferramenta de código aberto para exploração de rede e auditoria de segurança. Ela foi desenhada para escanear rapidamente redes amplas, embora também funcione muito bem contra hosts individuais. O Nmap utiliza pacotes IP em estado bruto (raw) de maneira inovadora para determinar quais hosts estão disponíveis na rede, quais serviços (nome da aplicação e versão) os hosts oferecem, quais sistemas operacionais (e versões de SO) eles estão executando, que tipos de filtro de pacotes/firewalls estão em uso, e dezenas de outras características.
- **OWASP ZAP -** Zed Attack Proxy (ZAP) é uma ferramenta gratuita de teste de penetração de código aberto mantida sob a égide do Open Web Application Security Project (OWASP). O ZAP foi projetado especificamente para testar aplicativos da web e é flexível e extensível. Em sua essência, o ZAP é conhecido como um "proxy man-in-the-middle". Ele fica entre o navegador do testador e o aplicativo da web para que possa interceptar e inspecionar mensagens enviadas entre o navegador e o aplicativo da web, modificar o conteúdo se necessário e, em seguida, encaminhar esses pacotes para o destino. Ele pode ser usado como um aplicativo independente e como um processo daemon.
- **BuiltWith -** é uma ferramenta de criação de perfil de website, geração de leads, análise competitiva e inteligência de negócios que fornece adoção de tecnologia, dados de comércio eletrônico e análise de uso para a internet. O rastreamento da tecnologia BuiltWith inclui widgets, análises, estruturas, sistemas de gerenciamento de conteúdo, anunciantes, redes de distribuição de conteúdo, padrões da web e servidores da web.
- **Nessus:** definido pela Tenable como a solução número um de avaliação de vulnerabilidades para profissionais de segurança. Tendo como característica a precisão Six Sigma, apresentando a menor taxa de falso-

positivos do setor. Possui ampla e profunda cobertura, com mais de 56 mil CVEs (Common Vulnerabilities and Exposures) e mais de 142 mil plugins já publicados e com crescimento exponencial voltados para a identificação de vulnerabilidades.

5 EQUIPE TÉCNICA

NOME	RESPONSABILIDADE	CONTATO
Roseane de Souza Neves	Reconhecimento do ambiente, Teste, elaboração de conceitos e produção do relatório.	desouzanevesroseane@gmail.com
Bruna Silva	Reconhecimento do ambiente, Teste, elaboração de conceitos e produção do relatório.	Ssbru24@gmail.com

6 CRONOGRAMA DE ATIVIDADES

ATIVIDADE	DATA DA REALIZAÇÃO
Pesquisas e reconhecimento de sistemas computacionais envolvidos no escopo.	24 de novembro de 2022
Provas de conceito e conclusão dos testes.	24 de novembro de 2022
Avaliação de riscos e esboço do relatório.	07 de novembro de 2022
Conclusão e revisão final do relatório	01 de dezembro de 2022

7 NÍVEIS DE CRITICIDADE

Para categorizar o impacto e a exploração de vulnerabilidades, os níveis de criticidade usados na seção “Vulnerabilidades Encontradas” estão de acordo com a Versão 3 do Common Vulnerability Scoring System (CVSS v3) do NIST, o qual utiliza a pontuação básica composta pelo tipo de acesso, a complexidade de acesso e o nível de autenticação exigido para explorar uma determinada vulnerabilidade, bem como o impacto relacionado à confidencialidade, integridade e disponibilidade. A pontuação aplicada às vulnerabilidades varia de 0 a 10 pontos e é normalizada categorizando-as em níveis críticos, altos, médios e baixos de criticidade.

- **Vetor de Acesso (AV):** descreve a fonte necessária de ataque para explorar uma vulnerabilidade, cujos valores possíveis são Local (L), Rede Adjacente (A) ou Rede (N);
- **Complexidade do Acesso (AC):** está relacionado à complexidade das condições que precisam estar em vigor para uma exploração bem-sucedida. Os valores possíveis são Alto (H), Médio (M) e Baixo (L);
- **Autenticação (AU):** refere-se aos níveis de autenticação que um invasor precisa transmitir para explorar uma vulnerabilidade. Os valores possíveis são Requer Várias Instâncias (M), Requer Instância Única (S) e Nenhum Requerido (N);
- **Confidencialidade (C), Integridade (I), Disponibilidade (A):** quando há impacto na confidencialidade, integridade ou disponibilidade, e cujos possíveis valores são Nenhum (N), Parcial (P) e Completo (C).

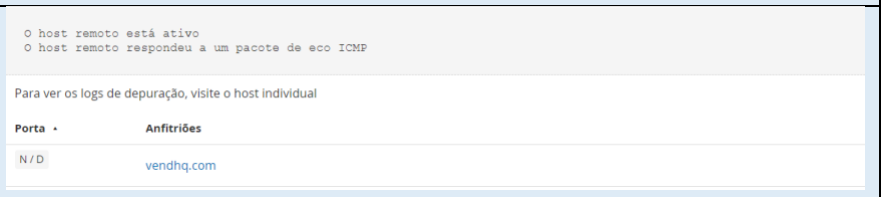
Diante do exposto, os níveis de criticidade definidos podem ser visualizados na Tabela 1, a seguir, de acordo com o resultado da soma de seus fatores de risco, juntamente com seu respectivo significado. Tais níveis foram utilizados para representar o risco e a criticidade calculados para cada uma das vulnerabilidades que identificadas.

Tabela 1 - Níveis de criticidade e descrição.

CRITICIDADE	DESCRIÇÃO
Crítica	• Pontuação Base do CVSS: 9 a 10 pontos; • Exploração trivial; • Perda de confidencialidade, integridade e disponibilidade. **A remediação imediata é crítica para os negócios.**
Alta	• Pontuação Base do CVSS: de 6 a 8.9 pontos; • Exploração quase trivial; • Perda ou de confidencialidade, ou de integridade ou de disponibilidade. **A remediação é crítica para os negócios.**
Média	• Pontuação Base do CVSS: de 4 a 6.9 pontos; • Exploração possível e comum, mas requer habilidades; • Sério impacto na confidencialidade, integridade e disponibilidade. **Ações corretivas são exigidas dentro de um prazo razoável.**

Baixa	• Pontuação Base do CVSS: de 0.1 a 3.9 pontos; • Exploração possível, mas difícil e improvável; • Impacto mensurável na confidencialidade, integridade e disponibilidade. **Ações corretivas são recomendadas.**
Informativa	**Nenhuma vulnerabilidade real foi identificada, mas há informações que podem ser relevantes para melhorar a segurança do ambiente.**

8 VULNERABILIDADES ENCONTRADAS

ID da Vulnerabilidade 1	
Criticidade	Informativo
Título	DESCOBER DE HOST
Descrição	O Nessus foi capaz de determinar se o host remoto está ativo usando um ou mais dos seguintes tipos de Ping: - Um ping ARP, desde que o host esteja na sub-rede local e o Nessus esteja sendo executado na Ethernet. - Um Ping ICMP. - Um Ping TCP, no qual o plugin envia para o host remoto um pacote com o flag SYN, e o host responderá com um RST ou um SYN/ACK. - Um Ping UDP (por exemplo, DNS, RPC e NTP).
URL afetado	https://www.vendhq.com/
Evidência	
Recomendação	Ative o suporte para TLS 1.2 e / ou 1.3 e desative o suporte para TLS 1.1.

ID da Vulnerabilidade 2	
Criticidade	Informativo
Título	Identificação de portas abertas

Descrição	As portas 21, 25, 53, 80, 110, 119, 135, 143, 443, 2000, 5060, 8008 estão abertas e sem filtro do firewall no servidor rodando alguns serviços.
URL afetado	derbund.ch
Evidência	
Recomendação	É recomendado que proteja seu alvo com um filtro de IP.

ID da Vulnerabilidade 3	
Criticidade	Informativo
Título	INFORMAÇÕES DE VARREDURA DO NESSUS
Descrição	Este plug-in exibe, para cada host testado, informações sobre a própria verificação: - A versão do conjunto de plug-ins. - O tipo de scanner (Nessus ou Nessus Home). - A versão do Nessus Engine. - O(s) scanner(s) de porta usado(s). - O intervalo de portas digitalizado. - O tempo de ida e volta do Ping - Se as verificações de gerenciamento de patches credenciadas ou de terceiros são possíveis. - Se a exibição de patches substituídos está habilitada - A data da varredura. - A duração da verificação. - O número de hosts verificados em paralelo. - O número de verificações feitas em paralelo.
URL afetado	https://www.vendhq.com/

Evidência	Versão do Nesso: 10.4.1 Construção do Nessus: 20091 Versão do feed do plug-in: 202212011347 Edição do scanner usada: Nessus Home Sistema operacional do scanner: WINDOWS Distribuição do scanner: win-x86-64 Tipo de escaneamento: Normal Scan name: descoberta de host Política de varredura usada: descoberta de host IP do scanner: 10.41.18.23 AVISO: Nenhum scanner de porta foi ativado durante a verificação. Isso pode levar a resultados incompletos. Intervalo de portas: padrão Ping RTT: 185,457 ms Testes completos: não Testes experimentais: não Depuração de plug-in ativada: não Nível de paranóia: 1 Detalhismo do relatório: 1 Verificações seguras: sim Otimize o teste: sim Cheques credenciados: não Verificações de gerenciamento de patches: Nenhuma Exibir patches substituídos: sim (plugin de substituição lançado) Escaneamento CGI: desabilitado Testes de aplicativos da Web: desativado Número máximo de hosts: 256 Verificações máximas: 5 Tempo limite de recuperação: 5 Backports: Nenhum Permitir edição pós-digitalização: Sim Data de início da varredura: 01/12/2022 15:01 E. Horário padrão da América do Sul Duração da varredura: 34 segundos
Recomendação	Configure o servidor da web remoto para usar HSTS.

ID da Vulnerabilidade 4	
Criticidade	Informativo
Título	Vulnerabilidade via Google Maps (street)
Descrição	FICAR LOCALIZADA A SEDE EM MONTRESL, QUEBEC NO CANADÁ, QUE TEM MAIS DE 17 FILIAIS ESPALHADAS PELO MUNDO.

Evidência	 

9 QUADRO SWOT DA SEGURANÇA DO SITE

12 CONCLUSÕES E RECOMENDAÇÕES GERAIS

Conforme detalhado no item 6, e de acordo com as vulnerabilidades encontradas nos testes, é possível concluir que o sucesso de um ataque pode

resultar em perdas financeiras, de ativos ou de recursos, além de causar danos à imagem da plataforma. Portanto, sua remediação é média para os negócios, exigindo que seja providenciada em curto intervalo de tempo.

A abordagem dos testes realizados não considera a probabilidade do agente de ameaça, nem responde por qualquer um dos vários detalhes técnicos associados à sua aplicação específica. Qualquer um desses fatores poderia afetar significativamente a probabilidade global de um atacante encontrar e explorar uma vulnerabilidade particular. Esta classificação também não leva em conta o impacto real sobre o negócio. É necessário que a área específica de segurança da plataforma defina qual o grau de risco de segurança das aplicações que está disposta a aceitar.

Cabe ressaltar, que novas ameaças, novas vulnerabilidades e mudanças na probabilidade ou nas consequências podem vir a ampliar os riscos anteriormente avaliados como pequenos. Convém que a análise crítica dos riscos pequenos e aceitos considere cada risco separadamente e em conjunto, a fim de avaliar seu impacto potencial agregado. Se os riscos não estiverem dentro da categoria "informativo" ou "baixo", convém que eles sejam tratados utilizando-se uma ou mais de uma das opções consideradas.

13 REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27005:2011: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**. Rio de Janeiro: 2011

OWASP. **OWASP Testing Guide. 2017**. Disponível em: <https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents>. Acesso em novembro de 2021.

OWASP. **OWASP Top Ten. 2017**. Disponível em: <https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project>. Acesso em dezembro 2021.

LAB, Access Security. **Relatório de Análise de Vulnerabilidades e Testes de Intrusão** Disponível em: <https://anubis.website/docs/report_access_pentest_anbistrade.pdf> Acesso em novembro de 2021.

EMPRESARIAS, Soluções. **TERMO ESPECÍFICO DO PRODUTO – VAMPS**. Disponível em: <https://www.vivo.com.br/content/dam/vivo-sites/vivo-com-br/pdf/para-empresas/regulatorio/solucoes-digitais/termo-especifico-vamps.pdf>. Acesso em novembro 2021

As partes acima identificadas têm, entre si, justo e certado o presente Contrato de Prestação de Serviços de Teste de Intrusão (Pentest), que se regerá pelas cláusulas seguintes e pelas condições descritas no presente.

1) DO OBJETO

O presente contrato tem por objeto, a realização de Teste de Intrusão (Pentest), a ser realizado pela CONTRATADA junto à CONTRATANTE, sendo que referidos testes somente poderão ser realizados nos dias e horários acordados, discriminados na Cláusula 2ª. A CONTRATADA conduzirá um PENETRATION TESTING contra e-commerce/rede/sistema **Lightspeed Retail (série X).**

Tais testes, consistem em simulações de ataques reais, resultando na descoberta de falhas da configuração e/ou vulnerabilidades. Vulnerabilidades estas que possam vir a permitir que a CONTRATANTE sofra impactos com ataques direcionados, perdendo a disponibilidade, integridade e confidencialidade de informações e sistemas.

2) DA EXECUÇÃO DOS SERVIÇOS

2.1 Escopo

O PENETRATION TESTING escolhido foi do tipo BLACKBOX (Sem conhecimento de informações), ou seja, a única informação oferecida pela CONTRATANTE foi uma URL.

O trabalho deve ser executado no seguinte escopo:

https://developers.vendhq.com/

A CONTRATADA tem permissão de explorar o Escopo em sua Integralidade

2.2 Limitações do Escopo

A CONTRATANTE determina as seguintes limitações à realização dos referidos testes:

ATIVIDADES/ATAQUES DE TESTES DE SEGURANÇA FÍSICA, WEBSITES DE FRONT-END DE MÍDIA PAGA, DDOS, PHISHING, SOFTWARE / EXTENSÕES MALICIOSOS, TESTES DE INSCRIÇÕES E AUTENTICAÇÕES, OUTROS DOMÍNIOS, SUBDOMÍNIOS OU CAMINHOS NÃO LISTADOS NA SEÇÃO DE DESTINOS, APLICATIVOS IOS E ANDROID, VARREDURAS AUTOMATIZADAS AGRESSIVAS, POIS PROVAVELMENTE IRÃO BLOQUEÁ-LO (POR AWS), ATAQUES QUE REQUEREM ACESSO FÍSICO AO DISPOSITIVO DE UM USUÁRIO, TODOS OS APLICATIVOS DE TERCEIROS OU BIBLIOTECAS / DEPENDÊNCIAS QUE NÃO ESTÃO SOB CONTROLE DA TAMEDIA, ATAQUES QUE REQUEREM ACESSO FÍSICO OU ADMINISTRATIVO À HOSPEDAGEM DO SISTEMA, VULNERABILIDADES QUE AFETAM USUÁRIOS DE

NAVEGADORES OU PLATAFORMAS DESATUALIZADOS, COOKIES AUSENTES SÃO SEGUROS OU HTTPONLY, CLICKJACKING E PROBLEMAS QUE SÓ PODEM SER EXPLORADOS POR MEIO DE CLICKJACKING, CABEÇALHOS DE SEGURANÇA HTTP AUSENTES, ESPECIFICAMENTE (HTTPS://OWASP.ORG/WWW-PROJECT-SECURE-HEADERS/), POR EXEMPLO.

2.3 JANELA DE TESTES

Referidos testes, deverão ser realizados dentro do horário comercial, ou seja, de segunda à sexta-feira das 09:00 às 18 :00 horas.

Todas as fases do teste poderão ser acompanhadas e supervisionadas à critério da CONTRATANTE. Caso opte pelo acompanhamento, tal supervisão somente poderá ser realizada pelo responsável indicado e qualificado pela CONTRATANTE na Cláusula 3ª.

O teste de invasão deverá obedecer às seguintes fases:

1 Planejamento;

2 Descoberta;

3 Ataque (exploração);

4. Relatório de recomendações

5. Reunião para apresentação do relatório de recomendações e descrição das atividades executada durante o teste.

6. Reavaliação, novo teste pós remediação

7. Relatório final pós remediação

3) DAS RESPONSABILIDADES

A responsabilidade da CONTRATADA restringe-se apenas detectar e apontar os riscos existentes com relação à integridade e vulnerabilidade dos sistemas da CONTRATANTE e tão somente, apresentar formas para minimizá-los.

O trabalho desenvolvido pela CONTRATADA não tem como objetivo corrigir as possíveis vulnerabilidades, tampouco, proteger a CONTRATANTE contra-ataques internos e externos.

As recomendações feitas pela CONTRATADA de vem ser validadas antes de serem colocadas em produção, a CONTRATADA não se responsabilizará por erros de implementações.

Será de responsabilidade da CONTRATANTE, garantir a segurança ao acesso dos relatórios entregues pela CONTRATADA, bem como a indicação dos responsáveis pelo acompanhamento da realização dos referidos testes, conforme disposto no competente TERMO DE ACORDO DE CONFIDENCIALIDADE DE INFORMAÇÕES em sua cláusula 4ª, item 4.2, anexo á este instrumento, sendo a pessoa indicada pela CONTRATANTE, devidamente qualificada abaixo:

Responsável nomeado pela CONTRATANTE:

NOME DA EMPRESA: Vend by Lightspeed

CNPJ: **14.239.647/0001-85**

TELEFONE: (21) 3282-5412

E-MAIL: PAULO.RICARDO@IACT.COM.BR

CLIENTE: ROSEANE DE SOUZA NEVES E BRUNA SILVA

4) DO PRAZO CONTRATUAL

O presente contrato terá validade única e exclusivamente durante o período de realização da atividade contratada, ou seja, 40 (quarenta) horas testes, a partir da data da assinatura do presente contrato, podendo ser prorrogado por comum acordo entre as partes até a conclusão dos serviços contratados.

O presente contrato poderá ser rescindido ocorrendo pelo menos uma das seguintes situações:

a) por mútuo consentimento;

b) por qualquer das partes, mediante manifestação por escrito com antecedência mínima de 30 (trinta) dias, se a outra parte descumprir quaisquer obrigações assumidas no presente Contrato.

Fica estipulada a multa de 20% (vinte por cento), sobre o valor contratual, na qual incorrerá a parte que infringir qualquer uma das cláusulas deste contrato, ressalvada à parte inocente o direito de poder considerar simultaneamente rescindido o presente contrato, independentemente de qualquer outra formalidade judicial ou extrajudicial. A multa será sempre paga integralmente seja qual for o prazo decorrido do presente contrato ficando claro que o pagamento dessa multa não exime o pagamento de outras despesas inerentes ao contrato.

5) DO PAGAMENTO

Em contrapartida aos serviços contratados, a CONTRATANTE pagará à CONTRATADA, o valor **de R$ 2,500,00(DOIS MIL E QUIENTOS REAIS)** por **30 HRS** de serviços prestados, que serão pagos da seguinte forma:
A não efetivação do pagamento na forma e prazo pactuados acima, por culpa da CONTRATANTE fica estipulada a multa de 10% (dez por cento), juros moratórios à razão de 1% (um por cento) ao mês e correção monetária, além de outras despesas decorrentes de cobrança judicial ou extrajudicial.

6) DA AUTORIZAÇÃO

Para que seja alcançado o objetivo da atividade contratada e, para que esta possa ser realizada em sua integralidade, a CONTRATANTE, neste ato, AUTORIZA a CONTRATADA, a realizar o Teste de Intrusão (pentest), objeto do presente contrato, devendo-se sempre, ambas as partes, assegurar a segurança das informações obtidas e fornecidas, bem como, cumprirem com seus deveres de confidencialidade de informações, devidamente pactuado

entre as partes, conforme TERMO DE CONFIDENCIALIDADE DE INFORMAÇÕES, parte integrante do presente contrato.

7) DAS CONDIÇÕES GERAIS

Este Contrato constitui o único documento que regula os direitos e obrigações das partes, com relação aos serviços contratados, ficando expressamente cancelado e revogado, todo e qualquer entendimento ou ajuste porventura existente que não esteja explicitamente consignado neste Contrato.
Caso as partes envolvidas deixem de exigir em qualquer tempo o cumprimento de quaisquer cláusulas ou condições deste contrato, a parte prejudicada não ficará impedida de, quando o entender, fazer com que a parte inadimplente cumpra rigorosamente todas as condições contratuais.
Caso a CONTRATADA admitir em benefício do CONTRATANTE qualquer atraso no pagamento das mensalidades ou no cumprimento de qualquer outra obrigação contratual, essa tolerância não poderá ser considerada como alteração das condições deste contrato, pois se constituirá em ato de mera liberdade da CONTRATADA.
As partes contratantes elegem o foro da comarca de São Paulo, cujo foro é o único competente, com renúncia expressa de qualquer outro por mais privilegiado que seja, para dirimir as questões que porventura surgirem na execução do presente Contrato.
E, por estarem justos e contratados, cientes e de acordo com todas as cláusulas e condições do presente Contrato de Prestação de Serviços de Teste de Intrusão (Penterster), assinam este instrumento em duas vias para um só efeito na presença das testemunhas abaixo.

Cachoeira-BA, 01de Dezembro de 2022

ROSEANE DE SOUZA NEVES
CONTRATADA

BRUNA SILVA
CONTRADADA

Vend by Lightspeed
CONTRATANTE

TESTEMUNHAS:

Nome: _____

CPF: _____

Nome: _____

CPF: _____