Análise de Vulnerabilidades em Domínios WordPress de Instituições de Ensino

Gabriel Augusto Ocampos Vitorino[1], **Carlos Alberto da Silva**[2]

[1]Curso de Bacharelado em Sistemas de Informação - Faculdade de Computação (FACOM) ,
[2]Faculdade de Computação (FACOM),
Universidade Federal de Mato Grosso do Sul (UFMS),
CEP 79070-900 - Campo Grande - MS - Brazil

gabriel.vitorino@ufms.br, carlos.silva@ufms.br

Abstract. *This article presents a vulnerability analysis conducted on educational institution domains, focusing on the WordPress content management system (CMS) and using the WPScan tool. The analysis was carried out to highlight the weakness of WordPress services in these domains and reinforce the importance of keeping all website components updated, in order to minimize common vulnerabilities that these services might present.*

Resumo. *Este artigo apresenta uma análise de vulnerabilidades realizada em domínios de instituições de ensino, com foco no sistema de gerenciamento de conteúdo (CMS) WordPress, com a utilização da ferramenta WPScan. A análise foi realizada com o objetivo de evidenciar as fragilidades dos serviços WordPress destes domínios, e reforçar a importância de manter todos os componentes de um website atualizados, a fim de minimizar as vulnerabilidades comuns que os serviços podem apresentar.*

1. Introdução

Atualmente, vivemos na era da Indústria 4.0 [5], onde o mundo está se tornando cada vez mais informatizado, e a presença de empresas, órgãos e instituições no mundo digital de torna cada vez mais importante, especialmente no cenário pós-pandemia. Com essa contínua expansão, a presença das aplicações web no ecossistema das instituções se tornou essencial, visto que a rede web é um componente altamente presente no atual mundo digital. Além disso, a segurança cibernética é hoje um dos tópicos mais importantes, já que os dados com os quais estas instituições trabalham se tornaram também seus ativos mais valiosos. Por isso, têm-se uma grande importância nas ferramentas web utilizadas pelo mercado, sendo impreterível que elas estejam sempre atualizadas e sejam utilizadas com as melhores práticas, assim buscando evitar que apareçam vulnerabilidades e falhas de segurança.

Diante desse cenário, este trabalho propõe um uma análise de vulnerabilidades web em domínios que utilizam o sistema de gerenciamento de conteúdo (CMS) WordPress, especificamente em domínios de instituições de ensino que atuam no estado de Mato Grosso do Sul (MS). Com isso, este estudo busca evidenciar e compreender os principais riscos a que os serviços WordPress destes domínios estão expostos, além de propor medidas que podem ser adotadas para reforçar a sua segurança. Devido à natureza deste estudo, a identidade das instituições analisadas permanecerá em sigilo.

2. Trabalhos Relacionados

2.1. A Critical Review of WordPress Security Scanning Tools and the Development of a Next-Generation Solution (NCI - National College of Ireland) [19]

Esta pesquisa busca fazer uma análise de ferramentas empregadas na auditoria de segurança de serviços e plugins WordPress dentro de um domínio. Nesta análise, as ferramentas são avaliadas conforme sua efetividade, acessibilidade e otimização, através de *scans* realizados em ambientes de

teste. A partir destes resultados, o estudo então propõe o framework a ser utilizado para a avaliação, juntamente com uma nova ferramenta que é utilizada como referência. Por fim, são comparados e analisados os resultados de cada ferramenta através de casos de estudo.

2.2. Investigação de Vulnerabilidades em Aplicações Web Utilizadas por Empresas de Leilões Online e Instituições de Ensino à Distância (EAD) (UFMS - Universidade Federal de Mato Grosso do Sul) [3]

Voltado para a área de *pentest*, este estudo consiste em uma análise de vulnerabilidades de domínios web. Nele, é definido um escopo de 29 instituições a serem analisadas, englobando instituições de Ensino à Distância e plataformas de leilões online. São realizados *scans* para a detecção de vulnerabilidades, seguidos do processo de classificação e análise das principais vulnerabilidades encontradas, onde também são propostas recomendações para a correção de mitigação dos riscos presentes.

2.3. Análise de Vulnerabilidades Web em Universidade Privada (UFMS - Universidade Federal de Mato Grosso do Sul) [4]

Seguindo na área de análise de vulnerabilidades, este estudo traz uma análise do sistema web de uma universidade privada, visando evidenciar os ricos que organizações podem ter ao manter um sistema com grande quantidade de dispostivos. Para isso, a metodologia consistiu inicialmente na realização de *scans* para a deteção de subdomínios e endereços IP ativos, onde então foram feitas varreduras em busca de vulnerabilidades. Após a identificação de vulnerabilidades, o estudo busca evidenciar os principais riscos presentes no sistema, através da classificação e análise das vulnerabilidades mais severas encontradas, incluindo medidas corretivas e preventivas que a organização pode adotar, e reforçando a importância de uma gestão proativa e efetiva dos sistemas de segurança utilizados.

A partir destes trabalhos, este estudo se diferencia através da realização de uma análise de vulnerabilidades especificamente em serviços e plugins WordPress, em um escopo composto por 70 domínios de instituições de uma área e região específica. Com isso, é possível entender melhor os principais riscos presentes nas instituições do escopo, quando utilizam o WordPress, e auxiliar na sua gestão da segurança da informação, através da análise das vulnerabilidades mais relevantes.

3. Fundamentação Teórica

Este capítulo busca definir o escopo do estudo, além de apresentar os conceitos que fundamentam a análise de vulnerabilidades realizada. Para esta pesquisa foram analisados domínios web de 70 instituições de ensino que atuam no estado de Mato Grosso do Sul, tanto públicas como privadas, e tanto de ensino presencial como de Ensino à Distância (EaD).

O estudo se baseia na identificação e documentação de vulnerabilidades presentes nos serviços WordPress destes domínios, baseando-se no **Common Vulnerabilities and Exposures (CVE)** [6], um sistema de catalogação de vulnerabilidades de cibersegurança, mantido pela Mitre Corporation e patrocinado pelo Departamento de Segurança Interna dos Estados Unidos (DHS) e pela Agência de Cibersegurança e Segurança de Infraestrutura (CISA). O principal objetivo do CVE é oferecer uma forma padronizada de identificar, definir e catalogar vulnerabilidades publicamente conhecidas, reunindo as informações em um único sistema.

Em conjunto com o sistema CVE, neste estudo será realizada a classificação das vulnerabilidades encontradas, através do sistema **Common Vulnerability Scoring System (CVSS)** [16], utilizado para a classificação dos níveis de severidade em vulnerabilidades de cibersegurança. Essa anáslise utiliza um conjunto de métricas onde, com base na avaliação, cada vulnerabilidade recebe um score de severidade, medido de 0 a 10. Utilizando o CVSS para realizar a classificação das vulnerabilidades, é possível fazer uma análise objetiva dos possíveis impactos que elas podem causar, o que ajuda a direcionar a priorização dos esforços de correção.

4. Ferramentas

Para permitir a detecção, identificação e análise de vulnerabilidades nos domínios investigados, foram utilizadas neste estudo as seguintes ferramentas:

4.1. Oracle VirtualBox

Oracle VirtualBox [18] é um software de virtualização que possibilita a criação e execução de máquinas virtuais que podem ser individualmente configuradas, o que permite instanciar máquinas com diferentes arquiteturas, sistemas operacionais e especificações de *hardware*. Neste estudo o VirtualBox será utilizado para instanciar uma máquina virtual que contém o sistema operacional que será utilizado nos testes.

4.2. Kali Linux

Kali Linux [17] é uma distribuição Linux de código aberto baseada no Debian, voltada especificamente para atividades de cibersegurança como testes de penetração, auditoria de segurança, computação forense e engenharia reversa. Por isso, ele possui de forma integrada diversas ferramentas, configurações e *scripts* que podem ser utilizados para realizar auditorias de segurança de forma eficiente. No contexto deste estudo, o Kali Linux integra a ferramenta utilizada para a detecção e identificação de vulnerabilidades em domínios WordPress.

4.3. WPScan

WPScan [2] é uma ferramenta de código aberto voltada para auditoria de segurança em domínios que utilizam o sistema de gerenciamento de conteúdo (CMS) WordPress. Com ele, é possível escanear domínios, identificar e documentar as vulnerabilidades que eles possuem em seus serviços WordPress. Atualmente, o WPScan é considerado um dos padrões da indústria para testes de vulnerabilidades em domínios WordPress.

5. Metodologia

O principal objetivo deste estudo é identificar vulnerabilidades em serviços WordPress de domínios web de instituições de ensino no Mato Grosso do Sul. Para isso, a metodologia utilizada seguiu os seguintes passos:

5.1. Definição do Escopo e Preparação do Ambiente

O escopo desta análise consiste nos domínios web de 70 instituições de ensino que atuam no Estado do Mato Grosso do Sul. Nestes domínios estão inclusas tanto instituições públicas como privadas, e tanto instituições de ensino presencial como de Ensino à Distância (EaD). Para o ambiente de testes, foi criada uma máquina virtual utilizando o VirtualBox, e nela foi instalada e configurada uma distribuição do Kali Linux.

5.2. Identificação de Serviços WordPress

O primeiro passo da análise consiste em utilizar a ferramenta WPScan para escanear os domínios em busca de serviços WordPress. Ao realizar um scan simples utilizando a URL do domínio, o WPScan já é capaz de identificar serviços e *plugins* WordPress que estejam em execução, através de técnicas de *fingerprinting*. Caso o domínio não utilize qualquer serviço WordPress, o scan é abortado. Em alguns casos, o domínio identifica a tentativa de escaneamento e impede a sua execução, utilizando um *firewall* de aplicação web (WAF). Para estas situações, o teste é refeito utilizando a opção *Random User Agent*, que utiliza agentes (User-Agents) de navegadores reais nas requisições ao invés do agente do WPScan, evitando que o WAF do domínio detecte a execução do teste. O teste realizado para detectar serviços WordPress no domínio é um teste mais simples e rápido, que não detecta ou identifica vulnerabilidaes.

5.3. Varredura de Vulnerabilidades

Ao detectar que o domínio está utilizando WordPress, foi feito um novo teste, agora com conexão à API do WordPress, para ter acesso à base de vulnerabilidades do WPScan, e com ela detectar e identificar as vulnerabilidade presentes. Este teste é mais longo do que o teste básico, e sua duração depende da quantidade de serviços e *plugins* WordPress ativos no domínio. Após a conclusão deste teste, o relatório de resultado aponta as vulnerabilidades presentes em cada serviço e *plugin*.

5.4. Classificação e Documentação dos Resultados

Após os testes, são gerados os relatórios com os resultados obtidos, contendo tanto as vulnerabilidades documentadas na CVE, como também os *warnings*, alertas sobre falhas que podem eventualmente resultar em vulnerabilidades, que são documentados na base de dados do próprio WPScan. Com isso, a partir dos relatórios dos testes de cada domínio, foi feita a documentação das vulnerabilidades e *warnings* encontrados. Para as vulnerabilidades documentadas na CVE, foi realizada também a classificação de nível e score de severidade conforme o CVSS.

5.5. Proposição de Soluções

Com base nos resultados dos testes, foram propostas medidas preventivas e corretivas para as vulnerabilidades mais comuns e de maior severidade, com base na documentação CVE de cada uma, visando reduzir ou eliminar os riscos criados por cada vulnerabilidade, além de incentivar a melhora nas políticas de segurança das instituições para os domínios estudados.

6. Resultados

Inicialmente, foi realizado o teste básico para detectar e identificar serviços WordPress presentes em cada um dos 70 domínios do escopo, para então fazer a busca por vulnerabilidades nestes serviços. Neste teste, foi identificado que 50 dos domínios estudados não utilizam o WordPress. Com isso, dentro dos 20 domínios que o utilizam, foram encontradas vulnerabilidades em 18 deles, conforme apresentado na Figura 1.

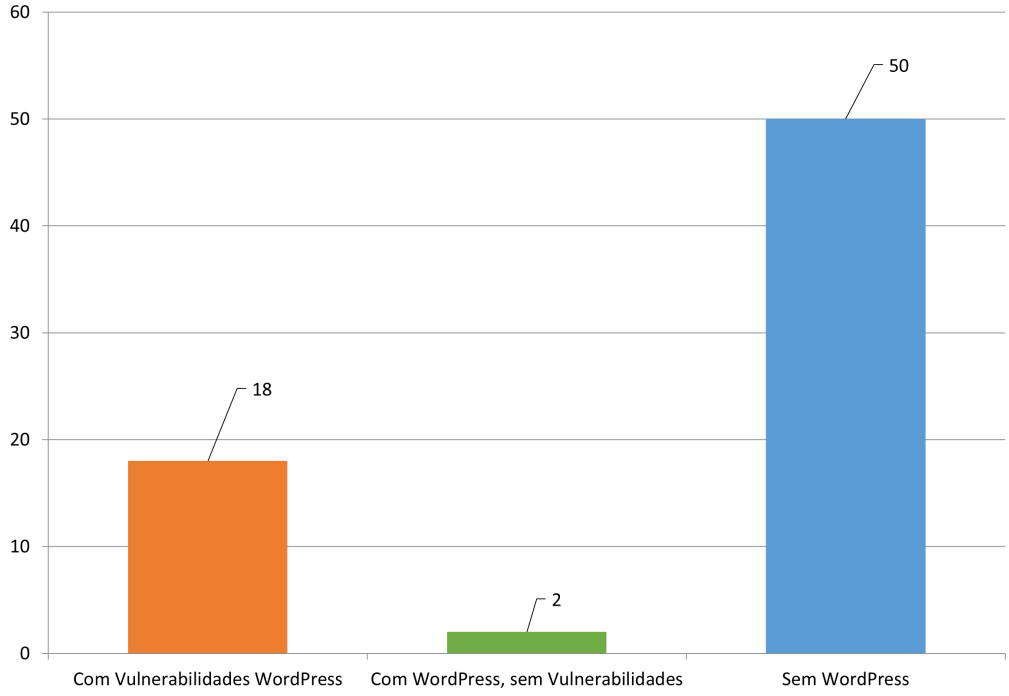

Figura 1. Presença de Serviços e Vulnerabilidades WordPress nos Domínios

A partir das varreduras realizadas nos domínios que utilizam o WordPress, foi identificado um total de 833 vulnerabilidades, sendo 705 vulnerabilidades documentadas pela CVE, e 128 *warnings* documentados pelo WPScan. Dentro destes resultados, foram identificadas no total 428 vulnerabilidades únicas com código CVE, com várias delas estando presentes em múltiplos domínios. Após isso, foi feita a classificação de severidade das vulnerabilidades, com base nas bases de dados da NVD e do WPScan, conforme apresentado na Figura 2.

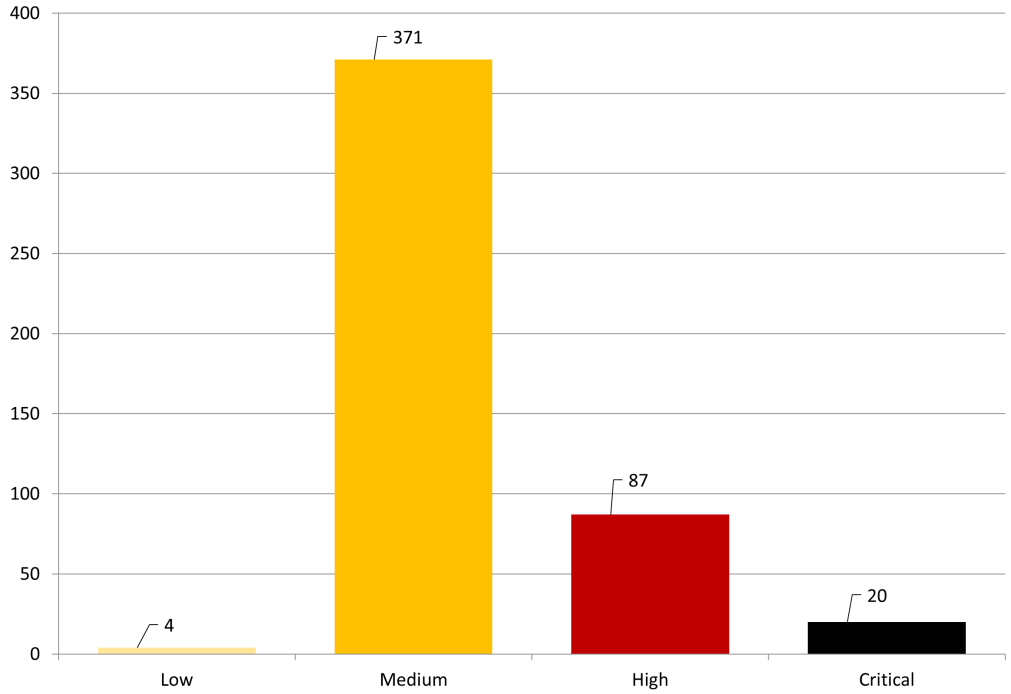

Figura 2. Classificação das Vulnerabilidades CVE

6.1. Vulnerabilidades de Maior Incidência

Durante a varredura realizada para detectar e identificar as vulnerabilidades, várias foram encontradas em múltiplos domínios. Com isso, as vulnerabilidades encontradas na maior quantidade de domínios tornam-se importantes pontos para análise. A Tabela 1 resume as vulnerabilidades que foram encontradas com maior frequência.

CVE	Descrição CVE	CVSS	Qtde
CVE-2024-50555	Elementor Website Builder < 3.29.1 - Contributor+ Stored XSS [1]	Medium (5.9)	7
CVE-2025-4566	Elementor < 3.30.3 - Contributor+ Stored XSS via Text Path Widget [14]	Medium (6.4)	6
CVE-2025-8081	Elementor < 3.30.3 - Admin+ Arbitrary File Read via Image Import [15]	Medium (4.9)	6
CVE-2023-6449	Contact Form 7 < 5.8.4 - Authenticated (Editor+) Arbitrary File Upload [12]	High (7.2)	5
CVE-2024-2242	Contact Form 7 < 5.9.2 - Reflected Cross-Site Scripting [13]	Medium (6.1)	5

Tabela 1. Vulnerabilidades Identificadas com Maior Frequência

Ao analisar as vulnerabilidades mais comuns, foi identificado que, apesar de apresentarem risco médio ou alto para a instituição, são de fácil correção e prevenção. Os principais riscos presentes

nestas vulnerabilidades consistem em falhas que permitem injeção de código malicioso via *Cross-Site Scripting* (XSS) ou manipulação de arquivos através de *upload* de arquivos maliciosos ou acesso indevido a arquivos sensíveis.

Apesar do alto risco, estas vulnerabilidades possuem as características de exigirem autenticação de usuário privilegiado (contribuidor ou administrador) e de serem facilmente corrigidas. Como o WordPress e seus *plugins* possuem equipes de desenvolvimento dedicadas, as principais vulnerabilidades são corrigidas em versões mais recentes. Por isso, neste caso, as vulnerabilidades mais comuns podem ser corrigidas através da atualização dos serviços e plugins afetados, sendo importante que as organizações façam o correto monitoramento e mantenham os sistemas sempre atualizados.

6.2. Vulnerabilidades de Maior Severidade

Além das vulnerabilidades que foram encontradas em maior número, também é importante analisar as que possuem maior grau de severidade, pois são elas que representam os maiores riscos para as instituições. A Tabela 2 resume as vulnerabilidades de maior severidade que foram encontradas, com base em suas classificações CVSS.

CVE	Descrição CVE	CVSS	Qtde
CVE-2020-36326	WordPress 3.7 to 5.7.1 - Object Injection in PHPMailer [8]	Critical (9.8)	2
CVE-2021-44223	WordPress < 5.8 - Plugin Confusion [9]	Critical (9.8)	2
CVE-2022-0320	Essential Addons for Elementor < 5.0.5 - Unauthenticated LFI [10]	Critical (9.8)	2
CVE-2023-32243	Essential Addons for Elementor 5.4.0 to 5.7.1 - Unauthenticated Privilege Escalation [11]	Critical (9.8)	2
CVE-2017-14723	WordPress 2.3.0-4.8.1 - $wpdb->prepare() Potential SQL Injection [7]	Critical (9.8)	1

Tabela 2. Vulnerabilidades Identificadas com Maior Severidade

Analisando as vulnerabilidades de maior severidade, foi possível observar que, similarmente às vulnerabilidades mais comuns, elas também apresentam alto risco à organização e podem ser corrigidas facilmente, através da atualização da versão do WordPress ou plugin afetado. No entanto, estas vulnerabilidades se diferenciam por serem de fácil exploração, seja por não exigirem autenticação ou por facilitarem escalonamento de privilégios. Além disso, algumas destas vulnerabilidades são de difícil detecção, o que permite que sejam exploradas sem que a organização descubra o ataque ou identifique a falha.

A partir destas análises, foi possível identificar a predominância de vulnerabilidades que trazem grandes riscos às organizações, mas que também podem ser facilmente corrigidas. Como o WordPress e seus plugins possuem equipes de desenvolvimento dedicadas, as principais vulnerabilidades identificadas tendem a ser rapidamente corrigidas através de atualizações e *patches*. Com isso, as organizações têm maior facilidade em corrigir as vulnerabilidades presentes e mitigar futuros riscos.

7. Conclusão

Através deste estudo, foi possível realizar uma análise prática de segurança WordPress em domínios do setor educacional no Mato Grosso do Sul, através da detecção, classificação e análise de vulnerabilidades WordPress. Assim, o estudo foi realizado com a utilização de ferramentas especializadas como Kali Linux e WPscan, e com o uso de métricas e padrões reconhecidos como a base de dados CVE e o sistema de classificação CVSS, que permitiram que a identificação e documentação de falhas fosse conduzida dentro dos padrões da área de auditoria de segurança da informação.

Com isso, os resultados não apenas reforçam a importância do acompamnhamento contínuo dos sistemas de segurança, como também evidenciam que é fundamental a adoção de uma abordagem proativa na gestão de segurança web pelas instituições, com a realização de auditorias, implementação de políticas e contínua manutenção preventiva, através correções e atualizações de sistemas.

Referências

[1] Automattic. *WPScan - CVE-2024-50555 - Elementor Website Builder < 3.29.1 - Contributor+ Stored XSS*. URL: https://wpscan.com/vulnerability/fc8e4264-fa78-44d2-8b6d-6c4305cd2280 (acesso em 25/10/2025).

[2] Automattic. *WPScan: WordPress Security Scanner*. URL: https://wpscan.com (acesso em 12/10/2025).

[3] Hatanael Lima Fernandes e Carlos Alberto da Silva. "Investigação de Vulnerabilidades em Aplicações Web Utilizadas por Empresas de Leilões Online e Instituições de Ensino à Distância (EAD)". Em: *Trabalho de Conclusão de Curso - Universidade Federal de Mato Grosso do Sul (UFMS)* (2025).

[4] Jonathas Guedes Borges e Carlos Alberto da Silva. "Investigação de Vulnerabilidades em Aplicações Web Utilizadas por Empresas de Leilões Online e Instituições de Ensino à Distância (EAD)". Em: *Trabalho de Conclusão de Curso - Universidade Federal de Mato Grosso do Sul (UFMS)* (2025).

[5] Adriano Pereira e Eugênio de Oliveira Simonetto. "Indústria 4.0 - Conceitos e Perspectivas para o Brasil". Em: *Revista Vale (Universidade Vale do Rio Verde - UninCor)* Volume 16 (2018).

[6] MITRE Corporation. *Common Vulnerabilities and Exposures - Overview*. URL: https://www.cve.org/About/Overview (acesso em 12/10/2025).

[7] MITRE Corporation. *CVE-2017-14723 - WordPress 2.3.0-4.8.1 - $wpdb->prepare() Potential SQL Injection*. URL: https://www.cve.org/CVERecord?id=CVE-2017-14723 (acesso em 26/10/2025).

[8] MITRE Corporation. *CVE-2020-36326 - WordPress 3.7 to 5.7.1 - Object Injection in PHPMailer*. URL: https://www.cve.org/CVERecord?id=CVE-2020-36326 (acesso em 26/10/2025).

[9] MITRE Corporation. *CVE-2021-44223 - WordPress < 5.8 - Plugin Confusion*. URL: https://www.cve.org/CVERecord?id=CVE-2021-44223 (acesso em 26/10/2025).

[10] MITRE Corporation. *CVE-2022-0320 - Essential Addons for Elementor < 5.0.5 - Unauthenticated LFI*. URL: https://www.cve.org/CVERecord?id=CVE-2022-0320 (acesso em 26/10/2025).

[11] MITRE Corporation. *CVE-2023-32243 - Essential Addons for Elementor 5.4.0 to 5.7.1 - Unauthenticated Privilege Escalation*. URL: https://www.cve.org/CVERecord?id=CVE-2023-32243 (acesso em 26/10/2025).

[12] MITRE Corporation. *CVE-2023-6449 - Contact Form 7 < 5.8.4 - Authenticated (Editor+) Arbitrary File Upload*. URL: https://www.cve.org/CVERecord?id=CVE-2023-6449 (acesso em 26/10/2025).

[13] MITRE Corporation. *CVE-2024-2242 - Contact Form 7 < 5.9.2 - Reflected Cross-Site Scripting*. URL: https://www.cve.org/CVERecord?id=CVE-2024-2242 (acesso em 26/10/2025).

[14] MITRE Corporation. *CVE-2025-4566 - Elementor < 3.30.3 - Authenticated (Contributor+) Stored Cross-Site Scripting via Text Path Widget*. URL: https://www.cve.org/CVERecord?id=CVE-2025-4566 (acesso em 26/10/2025).

[15] MITRE Corporation. *CVE-2025-8081 - Elementor < 3.30.3 - Authenticated (Administrator+) Arbitrary File Read via Image Import*. URL: https://www.cve.org/CVERecord?id=CVE-2025-8081 (acesso em 26/10/2025).

[16] National Vulnerability Database. *Common Vulnerability Scoring System*. URL: https://nvd.nist.gov/vuln-metrics/cvss (acesso em 12/10/2025).

[17] Offensive Security. *Kali Linux Features*. URL: https://www.kali.org/features (acesso em 12/10/2025).
[18] Oracle. *VirtualBox*. URL: https://www.virtualbox.org (acesso em 12/10/2025).
[19] Deepti Gupta e Vikas Sahni. "A Critical Review of WordPress Security Scanning Tools and the Development of a Next-Generation Solution". Em: *Tese de Mestrado - National College of Ireland (NCI)* (2023).