Análise de vulnerabilidades em domínios WordPress: um estudo de caso em uma universidade pública

Gabriel Pastorello de Oliveira[1], Carlos Alberto da Silva

[1]Curso de Bacharelado em Ciência da Computação – Faculdade de Computação (FACOM)
Universidade Federal de Mato Grosso do Sul (UFMS).
Av. Costa e Silva, s/n. - Bairro Universitário - CEP 79070-900 - Campo Grande - MS.

{gabriel.pastorello, carlos.silva}@ufms.br

Abstract. *This article presents an analysis of the security vulnerabilities of the web domains of a public institution in the state of Mato Grosso do Sul, Brazil. Using the WPScan tool, the vulnerabilities present in the domains were identified and evaluated, with the aim of providing an overview of security conditions and proposing mitigation measures. The analysis revealed the existence of several vulnerabilities, highlighting the importance of proactive approaches to guarantee the protection of systems and avoid possible cyber attacks.*

Resumo. *Este artigo apresenta uma análise das vulnerabilidades de segurança dos domínios web de uma instituição pública no estado de Mato Grosso do Sul, Brasil. Utilizando a ferramenta WPScan, foram identificadas e avaliadas as vulnerabilidades presentes nos domínios, com o objetivo de fornecer um panorama das condições de segurança e propor medidas de mitigação. A análise revelou a existência de diversas vulnerabilidades, destacando a importância de abordagens proativas para garantir a proteção dos sistemas e evitar possíveis ataques cibernéticos.*

1. Introdução

A segurança cibernética é um tema de grande e crescente importância, devido ao aumento da dependência de sistemas *web* por parte das organizações e dos indivíduos.

No contexto educacional, os domínios *web* são essenciais para o funcionamento de atividades fundamentais, como no acesso a plataformas de ensino remoto, divulgação de informações e notícias à comunidade, no acesso a sistemas de gestão acadêmica e bibliotecas digitais.

Embora a identidade da organização envolvida permaneça confidencial por razões de segurança (contrato de confidencialidade), esta pesquisa tem como objetivo analisar as vulnerabilidades de segurança dos domínios *web* de uma instituição pública pertencente ao estado do Mato Grosso do Sul. Para isso, será utilizada a ferramenta *WPScan*, um escaneador de vulnerabilidades para sites desenvolvidos com o *WordPress*.

A análise será realizada com base nos seguintes objetivos específicos: identificar as vulnerabilidades de segurança dos domínios digitais da instituição e avaliar a criticidade das vulnerabilidades identificadas, e produz um relatorio tecnico das vulnerabilidades encontradas com seus respectivos niveis de criticidade dos domínios investigados, para que medidas correctivas possam ser tomadas, afim de evitar que um ataque cibernético ocorra e gere inconvenientes como interrupções de serviços, perda de dados ou danifiquem a reputação da entidade.

2. Trabalhos Relacionados

No trabalho de [DE QUEIROZ 2021] é apresentado uma análise das vulnerabilidades em servidores web de instituições de ensino de Mato Grosso do Sul, utilizando ferramentas de código aberto do Kali Linux. A técnica utilizada foi o pentesting, que consiste em simulações de ataques reais para avaliar os potenciais riscos de violações de segurança. Os resultados incluem a identificação de diversas

vulnerabilidades nos servidores web analisados, como falhas de autenticação, injeção de SQL e cross-site scripting. Já no trabalho de [COSTA and FEDRIZZI 2021] é apresentado um teste de segurança em redes de universidades, utilizando a ferramenta Nmap. A pesquisa foi realizada com o objetivo de identificar vulnerabilidades. Foram coletados dados referentes aos domínios das universidades e a ferramenta Nmap foi executada para descobrir a topologia de rede, a quantidade de redes, de *hosts* e as vulnerabilidades ativas. Os resultados mostraram um grande número de vulnerabilidades encontradas nas universidades analisadas, que merecem atenção e medidas de segurança.

3. Metodologia

Esta seção descreve quais foram o métodos utilizados durante a pesquisa que levaram a elaboração deste artigo.

3.1. Plano de Teste

Na segurança cibernética, diversos planos de testes podem ser implementados para diferentes finalidades. Com o objetivo de avaliar a segurança de sistemas web da universidade que utilizam o WordPress.

Uma avaliação será realizada utilizando a ferramenta WPScan [WPScan 2023], que é uma ferramenta gratuita e de código aberto, que pode ser utilizada para escanear domínios web que utilizam o WordPress como plataforma de gerenciamento de conteúdo.

A ferramenta será utilizada para o escaneamento de vulnerabilidades, em busca de vulnerabilidades de plugins, de temas, de configurações, entre outras. As vulnerabilidades encontradas serão listadas e analisadas para determinar sua criticidade.

3.2. Distribuições Linux para testes de penetração

Existem diversas distribuições Linux voltadas para testes de penetração, que incluem um conjunto de ferramentas para identificar uma variedade de vulnerabilidades. Algumas das distribuições Linux mais populares para testes de penetração incluem:

- Kali Linux [Kali 2023]
- Parrot Security OS [Parrot 2023]
- BlackArch Linux [BlackArch 2023]

Essas distribuições Linux incluem ferramentas para todas as fases do teste de penetração, desde o reconhecimento até a analise das vulnerabilidades.

3.3. Técnicas / Metodologias aplicadas

A Tabela 1 apresenta as várias técnicas e metodologias que foram utilizadas durante os testes, tanto como identificar, mapear, e efetivamente para encontrar as vulnerabilidades.

Tabela 1. Tabela de técnicas e metodologias utilizadas

Funcionalidade	**Técnica / Metodologia**
Identificação das tecnologias utilizadas nos *websites*	Wappalyzer
Distribuição Linux	Kali Linux
Criação de ambiente virtualizado para instalação do Kali Linux	VirtualBox
Identificação de vulnerabilidades	WPScan
Verificação e pesquisa de vulnerabilidades	https://nvd.nist.gov, https://cve.mitre.org, https://wpscan.com/vulnerability/

4. Estudo de Caso

Esta seção descreve como foi executado o plano de teste, e para seus resultados como um estudo de caso.

4.1. Seleção dos domínios

Os domínios alvos do estudo foram selecionados com base nos seguintes critérios:

- que utilizam o WordPress como plataforma de gerenciamento de conteúdo
- que estão ativos
- e que estão acessíveis ao público (internet).

4.2. Identificação dos domínios

Para identificar se os domínios utilizavam o *WordPress*, foi utilizada a ferramenta *Wappalyzer* [Wappalyzer 2023] que é capaz de identificar tecnologias presentes em servidores de *websites* Figura 4.2.

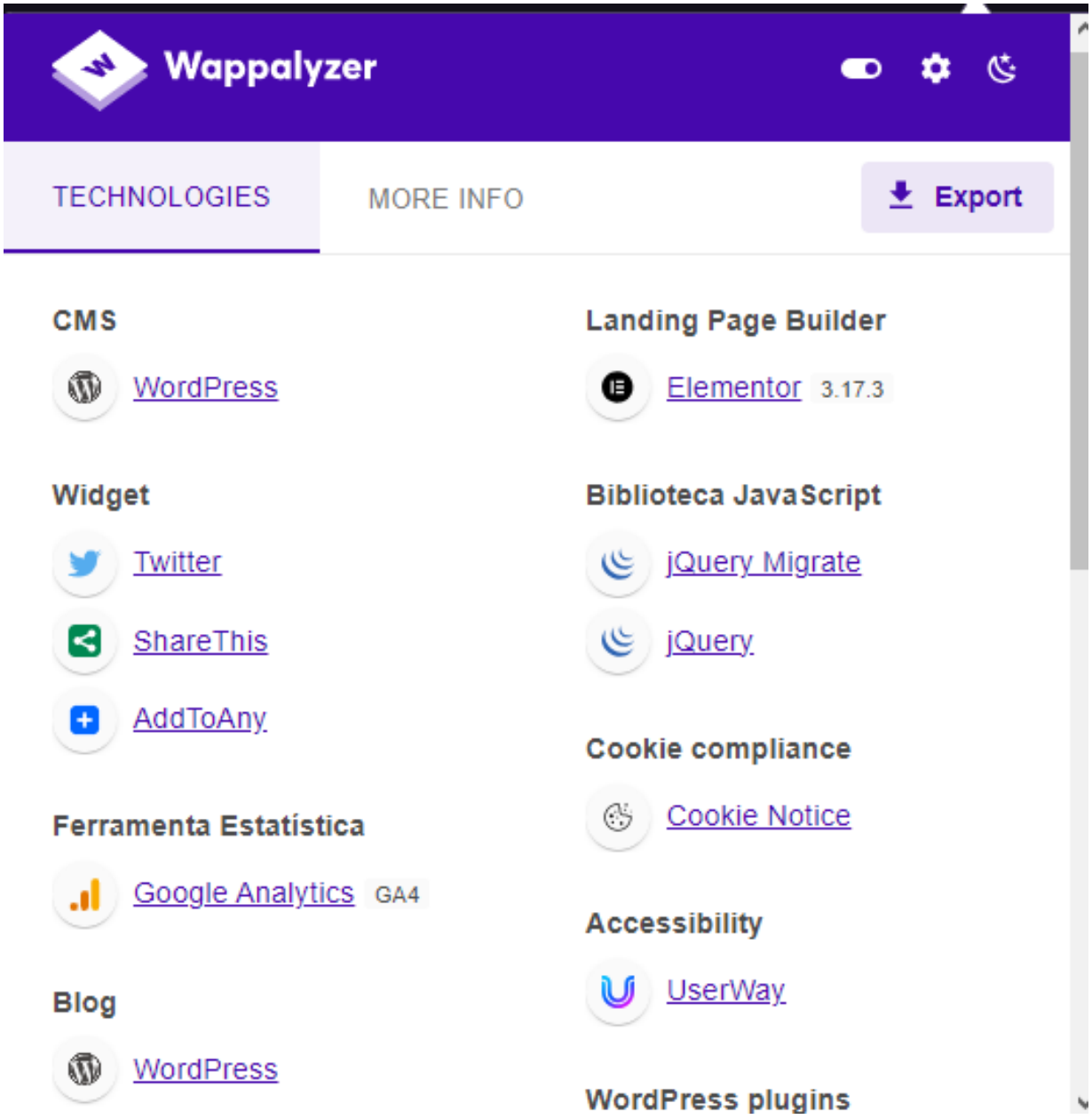

Figura 1. Exemplo de resultado obtido na aplicação da ferramenta Wappalyzer

Para a obtenção e verificação da disponibilidade de acesso das *URLs* utilizadas no estudo foram observadas as ativas e referenciadas no domínio principal da universidade alvo do estudo.

Após a identificação destes domínios, foi realizada uma análise manual, acessando-os um a um, para verificar se eles estavam ativos e acessíveis ao público.

4.3. Distribuição do Kali Linux

Para a realização do escaneamento de vulnerabilidades, foi utilizado o sistema operacional Kali Linux [Kali 2023].

O Kali Linux é uma distribuição Linux voltada para segurança da informação, que inclui uma ampla gama de ferramentas para testes de penetração e verificação de vulnerabilidades.

Esta distribuição foi instalada e executada em uma máquina virtual criada utilizando o software virtualizador de uso geral VirtualBox [VirtualBox 2023].

4.4. Scan de vulnerabilidades usando o WPScan

A ferramenta WPScan é uma ferramenta presente de forma padrão dentre as ferramentas do Kali Linux [Kali 2023], não sendo necessário fazer a sua instalação.

Esta ferramenta foi configurada para escanear os domínios selecionados em busca de vulnerabilidades com os seguintes parâmetros:

- –url URL: Obrigatório para informar a *URL* a ser testada.
- –random-user-agent: Utiliza um usuário aleatório em cada varredura.
- –api-token TOKEN: Parâmetro para que ao se informar um *TOKEN* obtido ao fazer um registro no seguinte link: https://wpscan.com/register a ferramenta exiba dados de vulnerabilidades.

4.5. Vulnerabilidades encontradas

Foram encontradas ao todo 20 vulnerabilidades diferentes nos testes realizado em 19 domínios distintos, levando em consideração as que o WPScan conseguiu determinar a versão do *plugin*, tema ou versão do WordPress, mas somente 14 dessas 20 possuíam um código CVE associado.

É válido citar que a ferramenta não conseguir identificar a versão, não implica que o website não está correndo risco de ser explorado, por exemplo: em um dos domínios testado, esta ferramenta reportou possíveis 31 problemas, que devem ter a devida atenção dos responsáveis para verificar o real risco.

Neste cenário, uma vulnerabilidade existe em 12 dos 19 domínios testados, mas suas versões não poderam ser determinada pelo WPScan.

4.6. Análise das vulnerabilidades

As vulnerabilidades encontradas que tiveram a versão confirmada, e que possuem um código CVE (*Common Vulnerabilities and Exposures*) foram analisadas para determinar sua criticidade, tendo como base o dados de vulnerabilidades do *National Vulnerability Database* (NVD) [NIST 2023].

Esta base de dados do NVD fornece informações sobre vulnerabilidades de segurança de software, incluindo o código CVE, sua criticidade e as recomendações para sua correção.

Na Tabela 2 apresenta a lista as vulnerabilidades encontradas que até o momento possuíam um código CVE associado, com suas respectivas criticidade identificadas.

Tabela 2. Tabela listando vulnerabilidades encontradas que possuíam código CVE

Vulnerabilidade	Cód. CVE	Severidade	Qtde. Dominios Vulneráveis
Contributor+ Stored XSS via Navigation Block	CVE-2023-38000	5.4 Média	17
Contributor+ Comment Disclosure	CVE-2023-39999	4.3 Média	17
Unauthenticated Post Author Email Disclosure	CVE-2023-5561	5.3 Média	17
Admin+ Stored XSS	CVE-2023-4502	4.8 Média	18
Cross-Site Request Forgery (CSRF)	CVE-2023-46189	8.8 Alta	7
Admin+ Stored Cross-Site Scripting	CVE-2022-1299	4.8 Média	2
Contributor+ Stored XSS via Shortcode	CVE-2022-4783	5.4 Média	2
Unauthenticated PHP Object Injection	CVE-2023-28782	RESERVADA	1
Reflected XSS	CVE-2023-2701	6.1 Média	1
Contributor+ Stored XSS	CVE-2023-0168	5.4 Média	1
Admin+ PHAR Deserialization	CVE-2023-3154	7.5 Alta	1
Admin+ Arbitrary File Read and Delete	CVE-2023-3155	7.2 Alta	1
Admin+ Local File Inclusion	CVE-2023-3279	4.9 Média	1
Admin+ SQLi	CVE-2023-0329	7.2 Alta	1

A análise das vulnerabilidades encontradas e descritas na Tabela 2 é possível notar que existe a ocorrência das vulnerabilidades *Admin+*, como maioria das vulnerabilidades descritas (6 em 14) com esta classificação, indicando que podem ser exploradas por usuários com o papel de administrador, destacando a importância de um gerenciamento adequado dos privilégios de usuários, e ressaltamos a existência de duas vulnerabilidades "*Unauthenticated*" que são vulnerabilidades sem necessidade de autenticação, o que as tornam particularmente perigosas, sendo uma delas sem uma severidade atualmente, mas marcada como reservada, ou seja, foi reservada por uma autoridade ou pesquisador de segurança porém ainda não teve seus detalhes publicados [CVE 2023].

Pode-se notar também que algumas vulnerabilidades afetam um grande número de domínios, como é o caso da "*Admin+ Stored XSS*" que foi encontrada em 18 dos 19 domínios testados (95%), o que sugere a necessidade de atenção imediata para resolver essas falhas de segurança e mitigar o impacto.

E também é importante notar que as criticidades das vulnerabilidades variam de 4,3 (média) a 8,8 (alta), com a maioria (9 em 14) caindo na faixa de criticidade média. Embora as vulnerabilidades de criticidade média não representem uma ameaça imediata, elas ainda devem ser abordadas para prevenir possíveis explorações.

5. Conclusão e Trabalhos Futuros

Neste estudo, analisamos uma série de vulnerabilidades identificadas em diferentes domínios da instituição objeto do estudo, cada uma com sua criticidade e impacto distintos. A compreensão detalhada dessas vulnerabilidades é crucial para suas futuras correções, e proteger os sistemas e *websites* contra possíveis ataques. Tal escaneamento dos *websites* permitiu identificar e localizar tais falhas de segurança encontradas, e o planejamento de medidas proativas de mitigação e correção.

Como trabalhos futuros, uma análise de todos os dominios desta universidade pública seria de interesse da administração atual, já que este estudo se limitou a apenas 19 dominios para avaliação dos riscos presentes. Em outra linha de investigação, existe a possibilidade de automatizar estes processos de pentesting para estes dominios de forma continua e automatica.

Referências

[BlackArch 2023] BlackArch (2023). Blackarch linux. `https://blackarch.org`. Acessado em 30 de Novembro de 2023.

[COSTA and FEDRIZZI 2021] COSTA, E. J. d. S. and FEDRIZZI, K. (2021). Teste de segurança usando o nmap nas universidades públicas e privadas.

[CVE 2023] CVE (2023). *Common Vulnerabilities and Exposures* (cve) reservado. https://www.cve.org/ResourcesSupport/FAQs. Acessado em 18 de Novembro de 2023.

[DE QUEIROZ 2021] DE QUEIROZ, L. G. (2021). Análise de vulnerabilidades em servidores web de ambientes educacionais de mato grosso do sul.

[Kali 2023] Kali (2023). Download do sistema kali linux. https://www.kali.org. Acessado em 15 de Novembro de 2023.

[NIST 2023] NIST (2023). *National Vulnerability Database (NVD)*. https://nvd.nist.gov/vuln/search. Acessado em 5 de Novembro de 2023.

[Parrot 2023] Parrot (2023). Parrot security os. https://www.parrotsec.org. Acessado em 30 de Novembro de 2023.

[VirtualBox 2023] VirtualBox (2023). Virtualbox. https://www.virtualbox.org. Acessado em 15 de Novembro de 2023.

[Wappalyzer 2023] Wappalyzer (2023). Ferramenta de identificação de tecnologias em *websites* wappalyzer. https://www.wappalyzer.com. Acessado em 15 de Novembro de 2023.

[WPScan 2023] WPScan (2023). Wpscan. https://wpscan.com. Acessado em 30 de Novembro de 2023.