Identificando vulnerabilidades em web sites

Gustavo Lube Machado de Melo[1], **Carlos Alberto da Silva**[2]

[1]Faculdade de Computação – Universidade Federal de Mato Grosso do Sul (UFMS)
Caixa Postal 549 – 79.070-900 – Campo Grande – MS – Brazil

gustavo.melo@ufms.br, carlos.silva@ufms.br

Abstract. *The purpose of this article is to deepen the understanding of cybersecurity and alert stakeholders to common errors that lead to digital vulnerabilities, allowing the mitigation and risk analysis. The study is based on practical experience involving the analysis of vulnerabilities in different web sites. Through this article, it becomes evident that there is a need for continuous and updated attention to online pages, as well as an awareness of the potential consequences of neglecting their correct maintenance.*

Resumo. *O propósito deste artigo é aprofundar o conhecimento em cibersegurança e alertar interessados aos erros comuns que causam diversas vulnerabilidades, permitindo a mitigação e análise de riscos. O estudo se baseou em uma experiência prática de análise de vulnerabilidades em diferentes web sites. Nesta pesquisa, ficou claro que há uma necessidade de atenção constante e atualizada das páginas de internet, bem como as possíveis consequências da falta ou incorreta manutenção das mesmas.*

1. Introdução

A interconectividade inerente à era digital tem proporcionado avanços extraordinários, mas também tem exposto organizações a um espectro cada vez mais sofisticado de ameaças cibernéticas [JornalAdvocacia 2023]. A crescente interdependência digital de setores vitais, como finanças, saúde e energia, destaca a urgência de aprimorar a resiliência contra tais ameaças, tornando este trabalho não apenas relevante, mas essencial para a compreensão e abordagem efetiva das vulnerabilidades digitais [Andritz 2023].

Ao longo deste estudo, serão abordados aspectos fundamentais relacionados às vulnerabilidades, incluindo as técnicas empregadas pelos agentes maliciosos para explorá-las, as consequências potenciais para sistemas e dados sensíveis, bem como a base de futuras medidas proativas e reativas, necessárias para fortalecer a postura de segurança digital. Este estudo surge de uma experiência prática, na qual foi feita uma análise abrangente de cibersegurança em diferentes web sites de uma empresa. Durante a experiência, ficou evidente que a presença de vulnerabilidades é comum, e que se torna crescente se não for monitorada.

Ao detectar um conjunto de vulnerabilidades em alguns web sites, foi possível atestar a importância crítica de medidas proativas na defesa do espaço digital. Simultaneamente, observou-se que a preservação da segurança em um web site não é uma garantia de imunidade perante os outros. Este estudo explora, de maneira aprofundada, a dinâmica entre web sites antigos e novos, mostrando como a contaminação de vulnerabilidades

pode se propagar como um vírus digital, comprometendo não apenas a integridade de um subdomínio específico, mas reverberando em cascata pelo servidor.

Este trabalho visa não apenas a contribuir para o conhecimento acadêmico em cibersegurança, mas também fornecer alertas outras empresas que buscam fortalecer a resiliência digital. Isso é essencial em um ambiente que é marcado pela constante evolução das ameaças cibernéticas e de seus possíveis estragos.

2. Trabalhos Relacionados

Esse trabalho apresenta mecanismos de pentest para descobrir vulnerabilidades em *websites* e servidores, no pretexto de identificar e analisar as falhas de segurança [Matheus 2023].

Nessa pesquisa é possível verificar, através de ferramentas de pentest do Kali Linux, *websites* que apresentam vulnerabilidades. O estudo foi feito em um caso de uma universidade pública em domínio WordPress [Gabriel 2023].

3. Metodologia

A metodologia adotada nesse trabalho consiste na organização de um plano de teste para enumerar as diferentes falhas, e destacar suas consequências. Para isso, aplicaram-se os seguintes passos:

1- Planejamento, onde foi definido o escopo, *web sites* para testes e limitações da empresa para o estudo, além de instalar o Kali Linux (sistema operacional com várias ferramentas e foco em segurança) [KaliLinux 2023];

2- Coleta de informações, utilizando *google dorking* (uso de *browsers* para encontrar informações ocultas na rede), análise manual dos *sites* a fim de encontrar informações para ataques, comandos do Linux para descobrir os respectivos domínios e endereços dos *sites*, além de ferramentas do Kali Linux como Nmap e Nping;

3- Análise de vulnerabilidades, encarregada pela análise de ferramentas automatizadas como Whatweb [KaliLinux 2023] e Nuclei [Nuclei 2023], utilização de opções dessas ferramentas para evitar bloqueio de rede, além da vistoria manual feita com o próprio navegador ou Burp Suite (ferramenta de testes de segurança *web* do Kali Linux);

4- Pesquisa sobre as vulnerabilidades, de forma a detalhar mais as falhas, classificar em níveis de severidade de acordo com o Sistema de Pontuação de Vulnerabilidade Comum (CVSS), citar algumas Exposições e Vulnerabilidades Comuns (CVEs), além de mostrar a consequência de alguns ataques. CVSS e CVE foram listados pela *National Vulnerability Database* (NVD) [NVD 2023];

5- Revisão e observação geral, onde foi considerada a ligação entre os subdomínios de um mesmo servidor e os frutos dessa conexão. Para finalizar, foi feita uma pesquisa para soluções das falhas encontradas.

4. Identificação e análise das vulnerabilidades

Esta seção apresenta quais vulnerabilidades foram identificadas, além de mostrar detalhes, severidade, exemplos de CVEs e possíveis estragos. Como a empresa pediu sigilo, não será divulgado nenhum dado que possam identifica-los.

4.1. Versões desatualizadas

Foi detectado que um dos subdomínios está com a versão do PHP (linguagem de programação web muito utilizada) em 5.6.31. O PHP 5.6 foi descontinuado oficialmente no dia 31 de dezembro de 2018 [PHP 2023] e, de acordo com o Sistema de Pontuação de Vulnerabilidade Comum (CVSS), versão do PHP não suportada é considerada uma falha crítica [Tenable 2023l]. As vulnerabilidades dessa versão são diversas [Cybersecurityhelp 2023b]. Uma das consequências é a indisponibilidade do servidor, ou até um ataque que provocam indisponibilidade do servidor ou *Denial of Service* (DoS).

A versão do Serviços de Informações de Internet da Microsoft (IIS) em mais de um subdomínio está na versão 7.5 (descontinuado em 14 de janeiro de 2020 [Microsoft 2023]), o que também é uma falha crítica [Tenable 2023j]. Como essa versão foi lançada para *Windows* 7 e *Windows Server* 2008 R2, é de se esperar que o sistema operacional seja antigo, o que abre para ainda mais problemas de segurança. Foram encontradas mais de 20 CVEs para esse IIS [Cybersecurityhelp 2023a], inclusive uma de nível crítico, com o possível controle total do sistema pelo atacante.

Como mencionado acima, é possível determinar o sistema operacional utilizado nos *hosts* de servidores o que, por ser antigo, leva a uma falha crítica [Tenable 2023k]. Por causa disso, inúmeras explorações graves são viáveis, o que provocam *Denial of Service* (DoS), execução de código remoto (execução de comandos não autorizados), elevação de privilégios do criminoso invasor (maior acesso e controle dos subdomínios), entre outros. Diversas CVEs de todos os níveis estão relacionadas a presença do *Windows* 7 [Cvedetails 2023a] e *Windows Server* 2008 R2 [Cvedetails 2023b].

Junto com esses, há o uso de uma aplicação web chamada CKAN em um outro subdomínio que foi detectada com a versão 2.8.2. Mais uma falha crítica de segurança [Tenable 2023a], tendo em vista que apenas as últimas versões são suportadas (atualmente 2.9.9 e 2.10.1 [CKAN 2023]). Foram encontradas quatro CVEs [SNYK 2023].

A Tabela 1 apresenta as vulnerabilidades encontradas com seus respectivos código CVE e grau de risco para os sites analisados:

Tabela 1. Tabela das vulnerabilidades encontradas

Objeto	Vulnerabilidade	Código CVE	Risco
PHP	Out-of-bounds write	CVE-2019-6977	Alto
	Integer underflow	CVE-2016-10166	Alto
IIS	Integer overflow	CVE-2015-1635	Crítico
	Permissions, Privileges, and Access Controls	CVE-2022-30209	Alto
CKAN	Arbitrary File Upload	CVE-2023-32321	Alto
	Improper Access Control	CVE-2022-43685	Alto

Tendo em vista o grande risco, é fortemente recomendado as atualizações desses sistemas e serviços.

4.2. Browsable Web Directories

Utilizando a técnica *google dorking*, é possível acessar diretórios que possuem informações sensíveis, ou áreas desativadas com códigos expostos e documentos antigos. A possibilidade dessa prática e o acesso a conteúdos indevidos possui a classificação de nível médio em CVSS [Tenable 2023d].

A página de destaque possui o diretório "/password.aspx", que é de acesso livre e permite trocar a senha de um usuário especificado. Como essa página retorna a mensagem "usuário não encontrado"e "senha incorreta"quando encontra um usuário válido, ela permite enumeração do mesmo. Além disso, como a página não possui nenhuma restrição, ela permite ataques de força bruta para descobrir tanto os usuários quanto a senha desses.

Embora isso pareça uma vulnerabilidade grave, as senhas do sistema são geradas automaticamente (com trocas periódicas) e é necessário um código de acesso para fazer login. Mesmo assim, é possível fazer a enumeração de qualquer usuário do sistema, o que é uma falha média [Tenable 2023e].

4.3. HTTP TRACE/TRACK permitido

Foi encontrado um subdomínio que suporta o comando TRACE. Esse comando é utilizado pelos atacantes para realizarem *debugs* nos servidores e possui CVSS média [Tenable 2023m]. Essa brecha foi detectada pelo Nuclei e posteriormente validado com o burpsuite de maneira manual.

4.4. Falta de HTTP security headers

A ferramenta Nuclei capturou a falta de diversos HTTP *security headers* em todos os sites testados. Esses são conjuntos de instruções que protegem usuários e sites de diversos ataques hackers. A falta deles culminam em brechas que possuem CVSS média ou leve.

Os principais *headers* não encontrados são:

- *Strict Transport Security* - Força comunicação HTTPS, evitando ataques do tipo *man in the middle* (MITM). Esse, consiste em capturar informações sensíveis passadas entre cliente e servidor de uma rede. A falta desse header é uma falha de nível médio [Tenable 2023f].
- *Content Security Policy* - Restringe conteúdos que navegadores conseguem carregar para evitar ataques clickjacking, por exemplo, que consiste em esconder links em botões para redirecionar as vítimas no intuito de roubar informações sigilosas. O nível de risco apersentado é baixo [Tenable 2023g].
- *X-Content-Type-Options* - Evita que o navegador deixe escapar conteúdo para MIME sniffing (prática que consiste em inspecionar bytes para deduzir o formato de arquivo dos dados contidos nele). Apresentado como nível de risco baixo [Tenable 2023h].
- *X-Frame-Options* - Controla permissão do navegador de renderizar ou não uma página, evitando *clickjacking*. Mais uma falha de risco baixo [Tenable 2023i].

4.5. Protocolo fraco de criptografia

TLS é um protocolo de criptografia que se aplica entre os computadores e o servidor de hospedagem no momento em que um site é acessado. Essa criptografia é essencial

para proteger ataques *man in the middle* (MITM), por exemplo, além de outras aplicações. Alguns sites testados foram detectados pelo Nuclei usando TLS 1.0 e TLS 1.1, sendo essas versões desatualizadas e, portanto, uma falha de nível médio [Tenable 2023b] [Tenable 2023c].

5. Observação sobre a ligação dos *web sites*

É preciso destacar que alguns dos subdomínios testados estavam bem protegidos. Entretanto, a vulnerabilidade de outros subdomínios pode contaminar os que estão inicialmente protegidos. O nome disso é *Cross-Site Contamination*, e consiste em contaminações de sites através de seus vizinhos em um mesmo servidor. A exemplo disso, foi encontrado um site bem protegido e atualizado, contido em um *host* que, por sua vez, possui IIS desatualizado (caso especificado em versões desatualizadas), o qual permite o ataque *Cross-Site* mencionado. Portanto, é de suma importância a proteção de todos os *web sites* como um todo. A tabela abaixo dita as soluções para os problemas encontrados:

Tabela 2. Tabela de soluções para as vulnerabilidades encontradas

Objeto	Solução	Maior risco
Versões desatualizadas	Manter atualizados sistemas e serviços	Crítico
Browsable web directories	Deletar ou isolar diretórios antigos e sensíveis	Médio
HTTP TRACE/TRACK	Desabilitar método TRACE encontrado	Médio
Falta de security headers	Adicionar os headers que não estão ativos	Médio
Protocolo fraco de criptografia	Reconfigurar TLS para versão mais atualizada	Médio

6. Conclusão e trabalhos futuros

Compreender e enfrentar as complexidades da cibersegurança tornou-se uma imperativa necessidade na atual era digital, marcada pela crescente interconectividade. Este trabalho buscou explorar, de maneira abrangente, as vulnerabilidades digitais, destacando não apenas as técnicas empregadas por agentes maliciosos, mas também as potenciais consequências que permeiam setores vitais da sociedade. A análise prática realizada em diversos websites revelou que a presença de vulnerabilidades é comum e, se negligenciada, pode se propagar como um vírus digital, comprometendo a integridade de sistemas e a proteção de todas as pessoas envolvidas. A abordagem metodológica permitiu identificar falhas e classificá-las em níveis de severidade, utilizando diversas ferramentas e pesquisas detalhadas sobre as vulnerabilidades. Este estudo não apenas contribui para o conhecimento acadêmico em cibersegurança, mas também oferece alertas para empresas que buscam se fortalecer. Em um cenário caracterizado pela constante evolução das ameaças cibernéticas, a compreensão dos impactos e análises discutidos neste trabalho tornam-se cruciais para a defesa efetiva do espaço computacional, além da preservação da integridade dos sistemas e de seus usuários.

Como trabalhos futuros, está planejado a aplicação de novos *pentests* para identificar mais vulnerabilidades, fazer novos relatórios com apontamento de riscos, além de aprofundar ainda mais os conhecimentos de segurança. Portanto, os trabalhos seguintes visam ampliar a proteção e prevenção de mais atacantes criminosos.

Referências

Andritz (Acessado em novembro de 2023). Site discutindo sobre o aumento da digitalização. https://www.andritz.com/spectrum-en/latest-issues/issue-39/digitalization-as-a-megatrend.

CKAN (Acessado em novembro de 2023). Versões suportadas ckan. https://docs.ckan.org/en/2.10/maintaining/releases.html.

Cvedetails (Acessado em novembro de 2023a). Vulnerabilidades windows 7. https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-17153/opbyp-1/Microsoft-Windows-7.html.

Cvedetails (Acessado em novembro de 2023b). Vulnerabilidades windows server 2008. https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-11366/year-2018/Microsoft-Windows-Server-2008.html.

Cybersecurityhelp (Acessado em novembro de 2023a). Vulnerabilidades iis 7.5. https://www.cybersecurity-help.cz/vdb/microsoft/microsoft_iis/7.5/.

Cybersecurityhelp (Acessado em novembro de 2023b). Vulnerabilidades php 5.6.31. https://www.cybersecurity-help.cz/vdb/php_group/php/5.6.31/.

Gabriel, P. D. O. (2023). Análise de vulnerabilidades em domínios wordpress: um estudo de caso em uma universidade pública.

JornalAdvocacia (Acessado em novembro de 2023). Site discutindo sobre o aumento dos ataques cibernéticos. https://jornaldaadvocacia.oabsp.org.br/noticias/aumento-dos-ataques-ciberneticos-uma-ameaca-global-no-mundo-digital/.

KaliLinux (Acessado em novembro de 2023). Sistema utilizado no estudo. https://www.kali.org.

Matheus, V. S. (2023). Aprimorando a cibersegurança em ambientes digitais: um estudo de caso de identificação de vulnerabilidades.

Microsoft (Acessado em novembro de 2023). Ciclo de vida iis. https://learn.microsoft.com/en-us/lifecycle/products/internet-information-services-iis.

Nuclei (Acessado em novembro de 2023). Ferramenta de analise de vulnerabilidades web. https://github.com/projectdiscovery/nuclei.

NVD (Acessado em novembro de 2023). National Vulnerability Database (NVD), National Institute of Standards and Technology (NIST). https://nvd.nist.gov/vuln/search/.

PHP (Acessado em novembro de 2023). Site mostrando versões de php. https://kinsta.com/blog/php-versions/.

SNYK (Acessado em novembro de 2023). Vulnerabilidades ckan 2.8.2. https://security.snyk.io/package/pip/ckan/2.8.2.

Tenable (Acessado em novembro de 2023a). Severidade ckan versão não suportada. https://www.tenable.com/plugins/nessus/176633.

Tenable (Acessado em novembro de 2023b). Severidade criptografia fraca 1.0. https://www.tenable.com/plugins/was/112496.

Tenable (Acessado em novembro de 2023c). Severidade criptografia fraca 1.1. https://www.tenable.com/plugins/was/112546.

Tenable (Acessado em novembro de 2023d). Severidade diretórios sensíveis pesquisáveis. https://www.tenable.com/plugins/nessus/40984.

Tenable (Acessado em novembro de 2023e). Severidade enumeração de usuários. https://www.tenable.com/plugins/was/98203.

Tenable (Acessado em novembro de 2023f). Severidade falta de security header. https://www.tenable.com/plugins/was/98056.

Tenable (Acessado em novembro de 2023g). Severidade falta de security header. https://www.tenable.com/plugins/was/112551.

Tenable (Acessado em novembro de 2023h). Severidade falta de security header. https://www.tenable.com/plugins/was/112529.

Tenable (Acessado em novembro de 2023i). Severidade falta de security header. https://www.tenable.com/plugins/was/98060.

Tenable (Acessado em novembro de 2023j). Severidade iis versão não suportada. https://www.tenable.com/plugins/was/113029.

Tenable (Acessado em novembro de 2023k). Severidade os versão não suportada. https://www.tenable.com/plugins/nessus/122615.

Tenable (Acessado em novembro de 2023l). Severidade php versão não suportada. https://www.tenable.com/plugins/nessus/58987.

Tenable (Acessado em novembro de 2023m). Severidade trace/track permitidos. https://www.tenable.com/plugins/nessus/11213.