Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v11i3.18336

ESTUDO COMPARATIVO DE FERRAMENTAS DE VARREDURA APLICADAS A SITES INSTITUCIONAIS - ESTUDO DE CASO

COMPARATIVE STUDY OF SCANNING TOOLS APPLIED TO INSTITUTIONAL WEBSITES - CASE STUDY

ESTUDIO COMPARATIVO DE HERRAMIENTAS DE ESCANEO APLICADAS A SITIOS INSTITUCIONALES - ESTUDIO DE CASO

Diny Silvane Teixeira e Silva[1]
Paula Renatha Nunes da Silva[2]

RESUMO: À medida que as ameaças cibernéticas aumentam, os sistemas institucionais públicos correm mais perigo e precisam de estratégias de detecção e mitigação de riscos. Essa tendência enfatiza a necessidade de adoção contínua de melhores técnicas de identificação e mitigação de riscos. Uma abordagem para detecção automática de vulnerabilidades é o uso de Ferramentas de Varredura de Vulnerabilidades Web. Entre as opções disponíveis, destacam-se os scanners open-source, que oferecem alternativas acessíveis e eficazes para instituições que buscam segurança digital sem altos custos de implementação. Este estudo compara os relatórios de varreduras realizadas em um site institucional de uma universidade pública utilizando três ferramentas gratuitos - ZAP, Skipfish, Wapiti - e o software comercial Burp Suite. Com essa avaliação, busca-se determinar se os scanners de vulnerabilidades gratuitos podem ser suficientes para automatizar o processo de detecção de vulnerabilidades em aplicações web institucionais. Dessa forma, espera-se contribuir para a definição de boas práticas na segurança digital nesse contexto.

Palavras-chave: Ferramentas de Varredura. Vulnerabilidades Web. Sistemas Institucionais. Scanner Open-source. Ameaças cibernéticas.

ABSTRACT: As cyber threats continue to rise, public institutional systems face greater risks and require strategies for threat detection and risk mitigation. This trend highlights the ongoing need to adopt improved techniques for identifying and mitigating vulnerabilities. One approach to automatic vulnerability detection is the use of Web Vulnerability Scanning Tools. Among the available options, open-source scanners stand out as accessible and effective alternatives for institutions seeking digital security without high implementation costs. This study compares the vulnerability scanning reports of a public university's institutional website using three free tools—ZAP, Skipfish, and Wapiti—alongside the commercial software Burp Suite. Through this evaluation, the study aims to determine whether free vulnerability scanners can sufficiently automate the detection process in institutional web applications. In this way, it seeks to contribute to the establishment of best practices in digital security within this context.

Keywords: Scanning Tools. Web Vulnerabilities. Institutional Systems. Open-source Scanner. Cyber Threats.

[1]Discente do curso de Engenharia Física da Universidade Federal do Oeste do Pará UFOPA, Universidade Federal do Oeste do Pará –UFOPA.
[2]Doutora em Engenharia Elétrica pela Universidade Federal do Pará - UFPA. Professora, orientadora. Universidade Federal do Oeste do Pará –UFOPA.

RESUMEN: A medida que las amenazas cibernéticas continúan en aumento, los sistemas institucionales públicos enfrentan mayores riesgos y requieren estrategias para la detección de amenazas y la mitigación de riesgos. Esta tendencia resalta la necesidad constante de adoptar mejores técnicas para la identificación y mitigación de vulnerabilidades. Una de las estrategias para la detección automática de vulnerabilidades es el uso de Herramientas de Escaneo de Vulnerabilidades Web. Entre las opciones disponibles, destacan los escáneres de código abierto, que ofrecen alternativas accesibles y eficaces para instituciones que buscan seguridad digital sin incurrir en altos costos de implementación. Este estudio compara los informes de escaneo de vulnerabilidades de un sitio web institucional de una universidad pública utilizando tres herramientas gratuitas—ZAP, Skipfish y Wapiti—junto con el software comercial Burp Suite. A través de esta evaluación, se busca determinar si los escáneres de vulnerabilidades gratuitos pueden ser suficientes para automatizar el proceso de detección de vulnerabilidades en aplicaciones web institucionales. De esta manera, se espera contribuir a la definición de buenas prácticas en seguridad digital dentro de este contexto.

Palabras clave: Herramientas de Escaneo. Vulnerabilidades Web. Sistemas Institucionales. Escáner de Código Abierto. Amenazas Cibernéticas.

INTRODUÇÃO

A insegurança cibernética se destaca como um dos principais riscos globais para a próxima década, afetando diretamente a infraestrutura digital ou serviços que sustentam sistemas críticos, incluindo internet, telecomunicações, serviços públicos, sistema financeiro ou energia (World Economic Forum, 2024). No Brasil, dados recentes apontam um aumento significativo nas vulnerabilidades e incidentes cibernéticos de governo reportados, passando de 8.530 casos em 2022 para 14.654, em 2024 (CTIR Gov, 2025). Esse aumento alinhado ao avanço da transformação digital no setor público e a crescente necessidade da internet para acesso a serviços públicos essenciais enfatiza a adoção insuficiente de práticas de identificação, prevenção, gerenciamento e mitigação de riscos, o que além de comprometer a segurança das informações, fragiliza a soberania digital do país e a confiança da população nos sistemas institucionais (Tribunal de Contas da União, 2024).

Para enfrentar esses desafios, o governo brasileiro tem implementado estratégias que incluem a elaboração do Framework de Privacidade e Segurança da Informação, o qual contém um guia de Gerenciamento de Vulnerabilidades (Secretaria de Governo Digital, 2025). A estratégia de gerenciamento de vulnerabilidades proposta abrange 3 ciclos: ciclo de detecção, ciclo de relatórios e ciclo de remediação (Secretaria de Governo Digital, 2023). Para atender esta

estratégia, as ferramentas de varredura são muito úteis pois automatizam o rastreio contínuo de vulnerabilidades.

No presente estudo, buscou-se comparar o desempenho de quatro ferramentas de varredura de vulnerabilidades web, algumas delas listadas no Guia de Gerenciamento de Vulnerabilidades proposto pela Secretaria de Governo Digital (2023) do Brasil — Zed Attack Proxy (ZAP), Skipfish, Wapiti e Burp Suite — aplicadas a um site institucional de uma Universidade Pública. A pesquisa destaca a importância de adotar soluções eficientes e acessíveis, especialmente no setor público, para garantir conformidade com legislações como a Lei Geral de Proteção de Dados (LGPD) e atender aos requisitos recomendados por órgãos de controle como o Tribunal de Contas da União (TCU).

MÉTODOS

VULNERABILIDADES EM APLICAÇÕES WEB

Segundo a Associação Brasileira de Normas Técnicas (2022), uma vulnerabilidade pode ser definida como o ponto fraco do elemento gerido pela segurança. Em geral, trata-se de um ativo que possui falhas em seu código, processo ou implantação, tornando-o suscetível à exploração que podem comprometer seu funcionamento, fornecer acesso indevido aos dados vinculados à aplicação e, em alguns casos, facilitar a propagação de outras ameaças à segurança do ambiente. Os invasores ou indivíduos mal-intencionados tentam explorar a vulnerabilidade para obter acesso indevido a dados ou comprometer funcionalidades para fins ilícitos.

Um grande número de ferramentas de varredura de vulnerabilidades comercias e de código aberto está disponível para avaliar a configuração de segurança dos ativos geridos (OWASP Foundation, 2025). Para ajudar a padronizar as definições de vulnerabilidades descobertas, é preferível usar ferramentas que mapeiam vulnerabilidades para um ou mais dos seguintes esquemas e linguagens de vulnerabilidade, configuração e classificação de plataforma reconhecidos pelo setor: Common Vulnerabilities and Exposures (CVE), Common Configuration Enumeration (CCE), Open Vulnerability and Assessment Language (OVAL), Common Platform Enumeration (CPE), Common Vulnerability Scoring System (CVSS) e/ou Formato de Extensible Configuration Checklist Description Format (XCCDF) (Center for Internet Security, 2021).

FERRAMENTAS DE VARREDURA DE VULNERABILIDADE WEB DE CAIXA PRETA

Há dois tipos de Ferramentas de Varredura de Vulnerabilidades de aplicações Web: Análise de Código Estático (Static Application Security Testing – SAST) e Varreduras Dinâmicas (Dynamic Application Security Testing – DAST) (Lavens et al., 2022). As ferramentas SAST têm uma abordagem de caixa branca e possuem acesso ao código-fonte da aplicação para analisar a qualidade do código. Os scanners DAST são ferramentas com abordagem de caixa preta e não tem acesso à estrutura interna da aplicação e simulam ataques reais (Secretaria de Governo Digital, 2023). As ferramentas DAST são populares porque não dependem da tecnologia ou linguagem da aplicação web, funcionando em qualquer sistema baseado na web (Alazmi e De Leon, 2022).

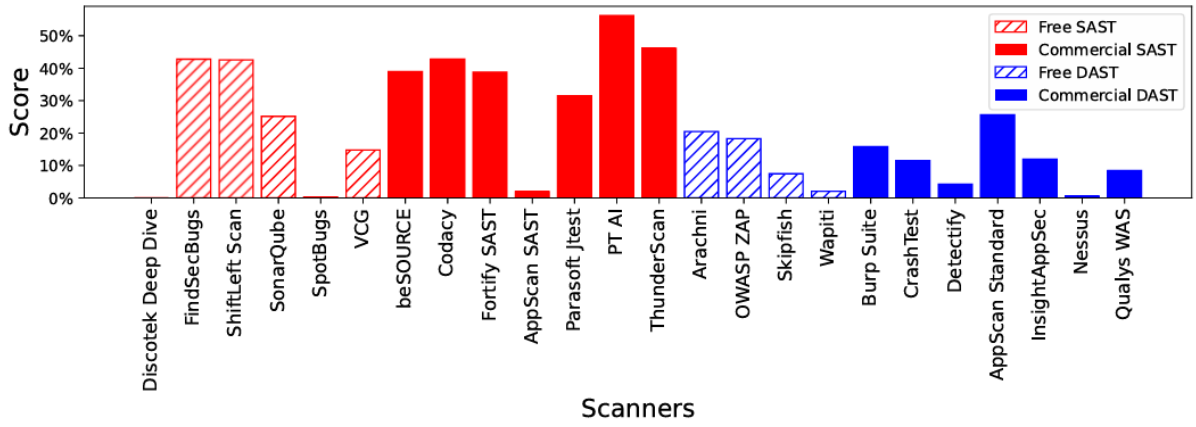
Os scanners DAST foram as ferramentas utilizadas neste estudo. Conforme Lavens et al (2022), o funcionamento dos scanners de vulnerabilidade web de caixa preta possui quatro fases principais:

1. Configuração: Define o alvo (URL) e os parâmetros do teste.
2. Rastreamento (crawling): Mapeia recursivamente páginas, queries e formulários a partir da URL alvo.
3. Ataque (fuzzer): Para cada ponto de entrada e tipo de vulnerabilidade é gerado um módulo de ataque que envia uma grande quantidade de solicitações à aplicação.
4. Análise de respostas: Examina a respostas da aplicação e fornece relatório indicando as vulnerabilidades.

SELEÇÃO DAS FERRAMENTAS

O estudo conduzido por Lavens et al (2022) realizou uma Avaliação Quantitativa do Desempenho de Detecção do ferramentas de varredura de vulnerabilidades Web. O resultado do desempenho das ferramentas analisadas está apresentado na Figura 1.

Figura 1 – Pontuação média de cada scanner num estudo de avaliação Desempenho de Ferramentas de Varredura de Vulnerabilidades Web.



Fonte: Lavens, et al (2022).

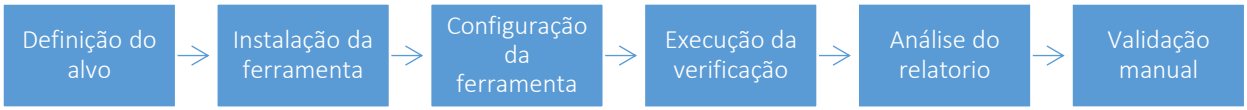
Foram selecionados os scanners gratuitos ZAP, Skipfish e Wapiti e comparados com o desempenho do software comercial Burp Suite. Conforme Alazmi e De Leon (2022), esses scanners também estão entre os que mais apareceram em estudos sobre o tema. Além disso, elas estão entre as ferramentas de varredura de vulnerabilidades sugeridas no Guia de Gerenciamento de Vulnerabilidades publicado pelo Governo Federal e na página da Open Web Application Security Project (OWASP) (Secretaria de Governo Digital, 2023; OWASP Foundation, 2025).

A seguir, descreve-se as características dos scanners selecionados neste estudo:

- **ZAP (ZED Attack Proxy):** Desenvolvido pela Checkmarx, na versão 2.16.0, é um software Open Source compatível com sistema operacional Windows, Unix/Linux e Macintosh. Pode ser operado tanto utilizando a interface gráfica quanto via linha de comando.
- **Skipfish:** Na versão 2.10b, com licença Open Source, compatível apenas com ambiente Linux e pode ser executado apenas por linha de comando.
- **Wapiti:** Lançado pela Informática Gesfor, em sua versão 3.0.4, cm licença Open Source, compatível com Windows, Unix/Linux e Macintosh e utiliza linha de comando.
- **Burp Suite:** Fornecido pela PortSwigger, na versão 2024.11.2, possui licença comercial, oferece suporte a maioria das plataformas e é operado por meio de interface gráfica.

Os passos seguidos para executar os testes estão na Figura 2.

Figura 2 – Passos para execução dos testes.



Fonte: Adaptado de Kritikos et al (2019).

A Tabela 1 apresenta as configurações empregadas nas ferramentas testadas. Todas elas realizaram a varredura no mesmo alvo.

Tabela 1 – Características gerais dos testes.

Ferramenta	Execução	Sistema Operacional	Entrada	Saída
ZAP	Interface gráfica	Windows 11	Tradicional Spider e Ajax Spider If Modern with Chrome Headless	Relatório HTML
Skipfish	Linha de comando	Kali Linux 2024.4	skipfish -o [diretório de saída do relatório] URL	Relatório HTML
Wapiti	Linha de comando	Kali Linux 2024.4	wapiti -u URL	Relatório HTML
Burp Suite	Interface Gráfica	Windows 11	Crawl and audit	Relatório HTML

Fonte: Autores (2025).

Foram selecionados dois relatórios de cada ferramenta para análise comparativa neste estudo. No período de varredura não houve atualização na aplicação. Também foi realizado o teste com o scanner comercial Burp para comparação com os resultados das ferramentas gratuitas. Neste scanner foi selecionado o tipo de varredura “Crawl and audit” primeiramente na configuração padrão e depois na configuração pré-definida “Deep” para ampliar a cobertura da varredura e obter uma melhor compreensão da postura de segurança do site.

RESULTADOS

Nos relatórios emitidos pelos scanners ZAP, Wapiti e Burp são apresentadas a descrição das vulnerabilidades encontradas e as sugestões de mitigação. Esse detalhamento das vulnerabilidades encontradas nos ativos de informação é indispensável para a elaboração do

Relatório de Avaliação de Vulnerabilidades, conforme o modelo proposto no Programa de Privacidade e Segurança da Informação do Governo Federal (Secretaria de Governo Digital, 2023).

Vale ressaltar que apenas o Skipfish não fornece a descrição detalhada das vulnerabilidades encontradas nem sugere medidas de mitigação dos riscos. Ele apenas lista dos problemas identificados e sua respectiva localização.

A lista de vulnerabilidade encontradas por ferramenta, tipo, nível de risco, data e quantidade está disposta na Tabela 2.

Tabela 2 – Lista de vulnerabilidade encontradas.

Tipo de vulnerabilidade	**Risco**	**Quantidade**	
ZAP		10/01/2025	20/01/2025
Personally Identifiable Information (PII) Disclosure	Alto	1	1
Configuração Incorreta Entre Domínios	Médio	17	17
Content Security Policy (CSP) Header Not Set	Médio	67	66
Missing Anti-clickjacking Header	Médio	38	37
Vulnerable JS Library	Médio	1	1
Cookie No HttpOnly Flag	Baixo	66	65
Cookie Without Secure Flag	Baixo	64	63
Cookie with SameSite Attribute None	Baixo	3	3
Cookie without SameSite Attribute	Baixo	65	64
Cross-Domain JavaScript Source File Inclusion	Baixo	793	781
Divulgação de Data e Hora – Unix	Baixo	276	304
Divulgação de Informações – Comentários Suspeitos	Informativo	139	137
Information Disclosure – Sensitive Information in URL	Informativo	1	1
Modern Web Application	Informativo	64	63
Re-examine Cache-control Directives	Informativo	46	45

Tipo de vulnerabilidade	Risco	Quantidade	
Retrieved from Cache	Informativo	116	118
Session Management Response Identified	Informativo	80	80
Skipfish		**14/01/2025**	**27/02/2025**
Resource fetch failed	Informativo	1	1
New 404 signature seen	Aviso interno	1	1
New 'X-*' header value seen	Informativo	4	4
New 'Via' header value seen	Informativo	1	1
Wapiti		**14/01/2025**	**27/02/2025**
Content Security Policy Configuration	Não classificado	1	2
HTTP Secure Headers	Não classificado	2	4
HttpOnly Flag cookie	Não classificado	8	9
Secure Flag cookie	Não classificado	7	8
Burp Suit		**17/01/2025** Modo: Padrão	**19/01/20205** Modo: Deep
Session token in URL	Médio	0	4
Cookie without HttpOnly flag set	Baixa	1	1
Vulnerable JavaScript dependency	Baixo	1	0
Cacheable HTTPS response	Informativo	1	1
Cookie without HttpOnly flag set	Informativo	1	1
Cross-domain script include	Informativo	1	1
Cross-site scripting (reflected)	Informativo	0	11
Email 708gente708s disclosed	Informativo	2	1
Frameable response (potential Clickjacking)	Informativo	1	1
Input returned in response (reflected)	Informativo	0	26
Robots.txt file	Informativo	0	1
TLS certificate	Informativo	0	1
TLS cookie without secure flag set	Informativo	1	1
User agente-dependent response	Informativo	0	12

Fonte: Dados extraídos dos relatórios emitidos pelo Zap, Wapiti, Burp Suit , Skipfish e Zalewski et al (2025).

DISCUSSÃO

Uma comparação entre as vulnerabilidades encontradas nos relatórios emitido pelas ferramentas de varredura de vulnerabilidades utilizadas nos testes está disposta na Tabela 3.

Tabela 3 – Comparação das principais vulnerabilidade encontradas por cada scanner.

Tipo de Vulnerabilidade	ZAP	Wapiti	Skipfish	Burp Suite	Impacto Potencial
Divulgação de Informações Sensíveis	PII Disclosure	Não identificado	Não identificado	Email addresses disclosed	Pode facilitar ataques de phishing e spam
Headers de Segurança Ausentes (CSP, X-Frame-Options)	Content Security Policy (CSP) Header Not Set, Missing Anti-clickjacking Header	Content Security Policy Configuration	Não identificado	Frameable response (potential Clickjacking)	Pode facilitar ataques de clickjacking e Cross-Site Scripting (XSS)
Uso de Bibliotecas JavaScript Vulneráveis	Vulnerable JS Library	Não identificado	Não identificado	Vulnerable JavaScript dependency	Pode variar de acordo com o contexto de uso do componente
Cookies Sem Proteção (HttpOnly, Secure, SameSite)	Cookie No HttpOnly Flag, Cookie Without Secure Flag, Cookie with SameSite Attribute None, Cookie without SameSite Attribute	HttpOnly Flag cookie, Secure Flag cookie	Não identificado	Cookie without HttpOnly flag set, TLS cookie without secure flag set	Pode permitir sequestro de sessão
Inclusão de JavaScript de Domínio Cruzado	Cross-Domain JavaScript Source File Inclusion	Não identificado	Não identificado	Cross-domain script include	Alerta informativo para certificar-se de que os scripts de domínio de terceiros utilizados são confiáveis
Vazamento de Informações na URL	Information Disclosure - Sensitive Information in URL	Não identificado	Não identificado	Session token in URL	Exposição de informações sensíveis a terceiros em URLs

Tipo de Vulnerabilidade	ZAP	Wapiti	Skipfish	Burp Suite	Impacto Potencial
Falhas no Cache e Controle de Armazenamento	Re-examine Cache-control Directives, Retrieved from Cache	Não identificado	Não identificado	Cacheable HTTPS response	Armazenamento de informações sensíveis no cache local
Arquivo Robots.txt Expõe Informações	Divulgação de Informações - Comentários Suspeitos	Não identificado	Não identificado	Robots.txt file	Exposição de informações que podem ajudar invasões
Erros e Respostas Inesperadas do Site	Não identificado	Não identificado	Resource fetch failed, New 404 signature seen	Input returned in response (reflected)	Alerta informativo para verificação
Configuração Incorreta Entre Domínios	Configuração Incorreta Entre Domínios	Não identificado	Não identificado	Não identificado	Pode permitir que domínios de terceiros façam solicitações de leitura entre domínios usando APIs (Application Programming Interface) não autenticadas
Divulgação de Data e Hora – Unix	Divulgação de Data e Hora – Unix	Não identificado	Não identificado	Não identificado	Alerta informativo para verificar se os dados do carimbo de data/hora são dados sensíveis e podem ser agregados para revelar padrões exploráveis.
Cross-site scripting (XSS)	Não identificado	Não identificado	Não identificado	Cross-site scripting (reflected)	Explorável para roubo de credenciais
Entradas Informativas Não Específicas	Session Management Response Identified	HTTP Secure Headers	New 'Via' header value seen, New 'X-*' header value seen	TLS certificate, User agent-dependent response	Alertas informativos ou indicação de boas práticas, e não necessariamente se tratam vulnerabilidades a serem corrigidas

Fonte: Dados extraídos dos relatórios emitidos pelo Zap, Wapiti, Burp Suit , Skipfish e Zalewski et al (2025).

A análise comparativa dos relatórios gerados pelos scanners ZAP, Wapiti e Skipfish evidencia que cada ferramenta possui um foco distinto na identificação de vulnerabilidades, não havendo unanimidade entre elas, em nenhuma das categorias identificadas. O ZAP foi o scanner que identificou o maior número de vulnerabilidades, com destaque para exposição de dados sensíveis. O Wapiti apresentou boa performance na verificação de headers de segurança e cookies inseguros, enquanto o Skipfish se restringiu à detecção de problemas de infraestrutura e HTTPS. O ZAP foi a ferramenta open source mais abrangente, mas, assim como as outras não dispensa a necessidade de confirmação manual das vulnerabilidades encontradas.

A vulnerabilidade Exposição de Informações Sensíveis (PII), por exemplo, identificada pelo ZAP, é um falso positivo. Na verdade, trata-se de endereços de e-mail divulgados, conforme indicado no alerta informativo do Burp, e outros dados pessoais e funcionais não protegidos pela LGPD. Esse caso evidencia um desafio comum em scanners automatizados, que podem gerar falsos positivos ou negativos (Amankwah et al, 2020), exigindo validação manual para precisão dos achados (Cruz et al, 2023).

A escolha de ferramentas de varredura de vulnerabilidades para ambientes institucionais, especialmente no setor público deve considerar a abrangência de detecção, custo-benefício e a facilidade de implementação. Diante disso, os resultados levam a concluir que o ZAP é melhor alternativa gratuita dentre as ferramentas testadas, cobrindo as principais vulnerabilidades da OWASP Top 10 e fornecendo relatórios detalhados para mitigação.

Contudo, considerando que nenhuma ferramenta open source isolada cobre todas as vulnerabilidades da aplicação, a combinação de diferentes scanners aliada à confirmação manual dos achados relatados pode proporcionar uma varredura mais eficiente (Cruz et al, 2023). Vale ressaltar que uma abordagem ideal de segurança deve combinar diferentes scanners para cobrir tanto falhas estruturais (testes de caixa branca) (Doupé et al, 2012) quanto vulnerabilidades exploráveis diretamente na aplicação (testes de caixa preta), garantindo uma defesa mais ampla contra ataques cibernéticos.

CONCLUSÃO

Neste trabalho foi apresentada a comparação entre scanners open source e comerciais para a avaliação da segurança cibernética de sites institucionais visando identificar a melhor abordagem para garantir a segurança de sites institucionais. Para isso, foram analisados os

relatórios gerados por três scanners gratuitos (ZAP, Skipfish e Wapiti) e um scanner pago (Burp Suite) em um site de uma universidade pública.

Dentre as ferramentas gratuitas analisadas, o ZAP foi a ferramenta mais abrangente e apresentou o melhor desempenho. Entretanto, considerando o custo-benefício e a facilidade de implementação, o estudo demonstra que utilizar mais de um scanner open source e realizar a validação manual é a melhor abordagem para uso dos scanners de caixa preta gratuitos.

O uso dessas ferramentas aliado a adaptação das diretrizes Framework de Privacidade e Segurança da Informação à realidade da instituição pode proporcionar uma estratégia sustentável e eficiente de proteção contra ameaças cibernéticas, fortalecendo a confidencialidade, integridade, disponibilidade dos dados e sistemas, além de assegurar conformidade regulatória e confiança nos serviços digitais oferecidos pelas instituições públicas.

REFERÊNCIAS

ALAZMI, Suliman, DE LEON, Daniel Conte. A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners. I*EEE Access*, [s.l.], v. 10, p. 33200-33219, 2022.

AMANKWAH, Richard, et al. An empirical comparison of commercial and open-source web vulnerability scanners. Wiley Online Library, [s. l.], v. 50, p. 1842-1857, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001 Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2022; 23p.

CENTER FOR INTERNET SECURITY. CIS Controls Version 8. CIS, 2021; 87p.

CRUZ, Dinis Barroqueiro et al. Open Source Solutions for Vulnerability Assessment: A Comparative Analysis. IEEE Access, [s. l.], v. 11, p. 100234-100255, 2023.

CTIR GOV - CENTRO DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO. ESTATÍSTICAS RESULTANTES DO TRABALHO DE DETECÇÃO, TRIAGEM, ANÁLISE E RESPOSTA A INCIDENTES CIBERNÉTICOS. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: 13 de Janeiro de 2025.

DOUPÉ, Adam et al. Enemy of the State: A State-Aware Black-Box Web Vulnerability Scanner. In: 21st USENIX Security Symposium, 21., 2012, Bellevue. Proceedings [...]. Bellevue: USENIX Association, 2012. p. 523-538.

KRITIKOS, Kyriakos et al. A survey on vulnerability assessment tools and databases for cloud-based web applications. Array, [s. l.], v. 3-4, n. 100011, p. 1-21, 2019.

LAVENS, Emma et al. A Quantitative Assessment of the Detection Performance of Web Vulnerability Scanners. In: 17th International Conference on Availability, Reliability and Security (ARES '22), 17., 2022, Vienna. Proceedings [...]. New York: Association for Computing Machinery, 2022, p. 149-159.

OWASP FOUNDATION. Vulnerability Scanning Tools. Disponível em: https://owasp.org/www-community/Vulnerability_Scanning_Tools. Acesso em: 19 de Janeiro de 2025.

SECRETARIA DE GOVERNO DIGITAL. Guia de Gerenciamento de Vulnerabilidades. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_gerenciamento_vulnerabilidades.pdf. Acesso em: 09 de Julho de 2023.

SECRETARIA DE GOVERNO DIGITAL. Guia do Framework de Privacidade e Segurança da Informação. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf. Acesso em: 13 de janeiro de 2025.

ZALEWSKI M. et al. Skipfish - Web Application Security Scanner. Disponível em: https://code.google.com/archive/p/skipfish/wikis/SkipfishDoc.wiki. Acesso em: 3 de fevereiro de 2025.

TRIBUNAL DE CONTAS DA UNIÃO. Segurança da informação e segurança cibernética. Disponível em https://sites.tcu.gov.br/listadealtorisco/seguranca_da_informacao_e_seguranca_cibernetica.html. Acesso em: 13 de Janeiro de 2025.

WORLD ECONOMIC FORUM. The Global Risks Report 2024. Cologny/Geneva : World Economic Forum, 2024, 123p.