BIBLIOGRAPHY

Symantec. (2003). Internet Security Threat Report. Broadcom Inc. https://docs.broadcom.com/doc/istr-03-jan-en

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical guide to information security testing and assessment (NIST Special Publication 800-115). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-115

Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.

Rahman, M. R., Mahdavi-Hezaveh, R., & Williams, L. (2021). What are the attackers doing now? Automating cyberthreat intelligence extraction from text on pace with the changing threat landscape: A survey. ACM Computing Surveys. https://arxiv.org/pdf/2109.06808

Riadi, I., Yudhana, A., & Yunanri, W. (2020). Analisis keamanan website Open Journal System menggunakan metode vulnerability assessment. Jurnal Teknologi Informasi dan Ilmu Komputer, 7(4), 853–860. https://doi.org/10.25126/jtiik.2020701928

Ramadhan, N., & Wijaya, N. P. N. (2021). The effect of work life balance on motivation in implementing WFH policies during the COVID-19 pandemic. *Faculty of Economics and Business, Widyatama University*. https://www.researchgate.net/publication/356714902

ENISA. (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

FIRST. (2023). Common Vulnerability Scoring System v4.0. Forum of Incident Response and Security Teams. https://www.first.org/cvss/v4.0/specification-document

Darojat, E. Z., Sediyono, E., & Sembiring, I. (2022). Vulnerability assessment website e-government dengan NIST SP 800-115 dan OWASP menggunakan web vulnerability scanner. Jurnal Sistem Informasi Bisnis, 12(1), 36–44. https://doi.org/10.21456/vol12iss1pp36-44

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber security threats, vulnerabilities, and security solutions models in banking. American Journal of Computer Science and Technology. https://doi.org/10.22541/au.166385206.63311335/v1

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105.

Kim, D., & Solomon, M. G. (2023). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

Laudon, K. C., & Laudon, J. P. (2014). Management information systems: Managing the digital firm (13th global ed.). Pearson Education Limited.

Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

CISA. (2013). *DNS Amplification Attacks (TA13-088A)*. https://www.cisa.gov/news-events/alerts/2013/03/29/dns-amplification-attacks

OWASP. (2025). Review Webserver Metafiles for Information Leakage (WSTG-INFO-03). OWASP Web Security Testing Guide. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/03-Review_Webserver_Metafiles_for_Information_Leakage

NIST. (2019). CVE-2015-9481. National Vulnerability Database. https://nvd.nist.gov/vuln/detail/CVE-2015-9481

Cisco. (2023). *DNS Best Practices for Security and Performance*. Cisco Secure. https://sec.cloudapps.cisco.com/security/center/resources/dns_best_practices

NCSC Ireland. (2023). *DNS Open Resolver – Vulnerabilities and Threats*. National Cyber Security Centre Ireland. https://www.ncsc.gov.ie/emailsfrom/Shadowserver/DoS/DNS/

Tenable. (2023). *Plugin ID 10539 - DNS Recursive Query Cache Poisoning Weakness*. Nessus Plugins. https://www.tenable.com/plugins/nessus/10539

Hodges, J., Jackson, C., & Barth, A. (2012). HTTP Strict Transport Security (HSTS). RFC 6797. Internet Engineering Task Force (IETF). https://datatracker.ietf.org/doc/html/rfc6797

curl.se. (2024). HTTP Scripting with curl. https://curl.se/docs/httpscripting.html

WPScan. (2025). Elementor Pro < 3.29.1 – Contributor+ Stored XSS. https://wpscan.com/vulnerability/e6f51ff0-a6de-4124-b753-a932f7f5e5f0

WPScan. (2024). Elementor Website Builder ≤ 3.29.0 – Contributor+ Stored XSS. https://wpscan.com/vulnerability/fc8e4264-fa78-44d2-8b6d-6c4305cd2280

WordPress.org. (2024). *Roles and Capabilities*. https://wordpress.org/support/article/roles-and-capabilities/

OWASP Foundation. (2023). *Testing for Content Security Policy (WSTG-CONF-12)*. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/12-Test_for_Content_Security_Policy

PortSwigger Ltd. (2025). *HTTP History*. Burp Suite Documentation. https://portswigger.net/burp/documentation/desktop/tools/proxy/history

OWASP. (2023). *OWASP Secure Headers Project*. Retrieved from: https://owasp.org/www-project-secure-headers

Mozilla Developer Network. (n.d.). *ETag - HTTP Headers*. Retrieved July 29, 2025, from https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/ETag

Cisco Systems. (2025). A Cisco Guide to Defending Against Distributed Denial of Service. Retrieved July 29, 2025, from https://sec.cloudapps.cisco.com/security/center/resources/guide_ddos_defense.html

Cybersecurity and Infrastructure Security Agency (CISA). (2013, March 29). DNS Amplification Attacks. Retrieved July 29, 2025, from https://www.cisa.gov/news-events/alerts/2013/03/29/dns-amplification-attacks

OWASP. (2025). Review old backup and unreferenced files for sensitive information (WSTG-CONF-04). Retrieved July 29, 2025, from https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/04-Review_Old_Backup_and_Unreferenced_Files_for_Sensitive_Information

SSL.com. (2024). Apa itu HTTP Strict Transport Security (HSTS)?. Retrieved July 29, 2025, from https://www.ssl.com/id/artikel/apa-itu-http-strict-transport-security-hsts/

Patchstack. (2025). WordPress Tutor LMS Plugin ≤ 3.4.0 – HTML Injection Vulnerability (CVE-2025-32230). Retrieved July 29, 2025, from https://patchstack.com/database/wordpress/plugin/tutor/vulnerability/wordpress-tutor-lms-plugin-3-4-0-html-injection-vulnerability

Patchstack. (2025). WordPress Elementor Website Builder Plugin ≤ 3.29.0 – Authenticated (Contributor+) Stored Cross-Site Scripting Vulnerability. Retrieved July 29, 2025, from https://patchstack.com/database/wordpress/plugin/elementor/vulnerability/wordpress-elementor-website-builder-plugin-3-29-0-cross-site-scripting-xss-vulnerability?_a_id=431

WPScan. (2025). Elementor < 3.29.1 – Contributor+ Stored XSS. Retrieved July 29, 2025, from https://wpscan.com/plugin/elementor

Content Security Policy. (2025). Examples using .htaccess. Retrieved July 29, 2025, from https://content-security-policy.com/examples/htaccess/

MDN Web Docs. (2025). *Apache Configuration (.htaccess)*. Mozilla Developer Network. Retrieved July 29, 2025, from https://developer.mozilla.org/en-US/docs/Learn_web_development/Extensions/Server-side/Apache_Configuration_htaccess

htaccessbook.com. (2024). *How to disable ETags in .htaccess*. Retrieved from https://htaccessbook.com/disable-etags/

htaccessbook.com. (2025). *Increase security with X-Security Headers*. Retrieved from https://htaccessbook.com/increase-security-x-security-headers/

Cloudflare. (2023). *Cloudflare's Free DDoS alerts for everyone*. Retrieved from https://blog.cloudflare.com/free-ddos-alerts/