

DAFTAR PUSTAKA

- “BSP Zapin.” n.d.-a. Accessed July 20, 2026. <https://bspz.co.id/id/profil/sejarah>.
- “BSP Zapin.” n.d.-b. Accessed July 20, 2026. <https://bspz.co.id/id/profil/visi-misi>.
- Buana, Komang Gede Jaya Wira, Lilik Widyawati, and Ondi Asroni. 2025. “Analisis Dan Implementasi Keamanan Authentication Menggunakan Multi Factor Authentication (MFA) Pada Aplikasi Web.” *CORISINDO* 2025 1 (September): 501–10. <https://doi.org/10.30812/corisindo.v1.5549>.
- Halil, M. Isma and Mansur. 2026. “Analysis and Improvement of an Agribusiness Web Information System Security Using Grey-Box and White-Box Testing.” *SISTEMASI* 15 (2): 628. <https://doi.org/10.32520/stmsi.v15i2.5939>.
- Hasibuan, Abdul Fattah, Tommy, and Divi Handoko. 2023. “Analisis Keretakan Website Dengan Aplikasi Owasp Zap.” *Jurnal Ilmu Komputer Dan Sistem Informasi* 2 (2): 141–54. <https://doi.org/10.70340/jirsi.v2i2.51>.
- OWASP Foundation. n.d. “Otentikasi - Seri Lembar Panduan OWASP.” Accessed July 21, 2026. https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html.
- Politeknik Negeri Bengkalis. 2025. *Panduan-Magang-2025*.
- Samsudiat, Hartanto Kurniawan, and Cahyono Nugroho. 2024. “PENGEMBANGAN SISTEM INFORMASI PENILAIAN KEAMANAN APLIKASI BERDASARKAN APPLICATION SECURITY VERIFICATION STANDARD (ASVS).” *INDEXIA* 6 (1): 62. <https://doi.org/10.30587/indexia.v6i1.7629>.
- Widyaningrum, Bajeng Nurul, Destri Maya Rani, and Lingga Kurnia Ramadhani. 2024. “Analysis of the OWASP V4.2 Method in Hospital Information System Security Testing.” *MEDIKA TRADA* 5 (2): 87–97. <https://doi.org/10.59485/jtemp.v5i2.99>.
- “WSTG - v4.2 | OWASP Foundation.” n.d.-a. Accessed July 20, 2026. <https://owasp.org/www-project-web-security-testing-guide/v42/>.
- “WSTG - v4.2 | OWASP Foundation.” n.d.-b. Accessed July 20, 2026. https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection.

“WSTG - v4.2 | OWASP Foundation.” n.d.-c. Accessed July 20, 2026.
[https://owasp.org/www-project-web-security-testing-guide/v42/4-](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/02-Testing_for_Stored_Cross_Site_Scripting)

[Web_Application_Security_Testing/07-Input_Validation_Testing/02-Testing_for_Stored_Cross_Site_Scripting](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/02-Testing_for_Stored_Cross_Site_Scripting).

“WSTG - v4.2 | OWASP Foundation.” n.d.-d. Accessed July 20, 2026.
[https://owasp.org/www-project-web-security-testing-guide/v42/4-](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery)

[Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery).

Zahra, Nabila Athifah, Farras Hafish Zidane, and Nur Racana Kuslaila. 2023. “ANALISIS KEAMANAN SISTEM INFORMASI PADA WEBSITE PT SENTRA VIDYA UTAMA (SEVIMA) MENGGUNAKAN METODE OWASP.” *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi* 3 (1): 384–93. <https://doi.org/10.33005/sitasi.v3i1.564>.

“ZAP – Big Redirect Detected (Potential Sensitive Information Leak).” n.d. Accessed July 20, 2026. <https://www.zaproxy.org/docs/alerts/10044-1/>.

“ZAP – Content Security Policy (CSP) Header Not Set.” n.d. Accessed July 20, 2026. <https://www.zaproxy.org/docs/alerts/10038-1/>.

“ZAP – Cookie No HttpOnly Flag.” n.d. Accessed July 20, 2026. <https://www.zaproxy.org/docs/alerts/10010/>.

“ZAP – Strict-Transport-Security Header Not Set.” n.d. Accessed July 20, 2026. <https://www.zaproxy.org/docs/alerts/10035-1/>.

“ZAP – Sub Resource Integrity Attribute Missing.” n.d. Accessed July 20, 2026. <https://www.zaproxy.org/docs/alerts/90003/>.

“ZAP – User Controllable HTML Element Attribute (Potential XSS).” n.d. Accessed July 20, 2026. <https://www.zaproxy.org/docs/alerts/10031/>.