The Journal of Information Technology and Digital Solutions (JITDS)

Volume 1, Number 4, 2025

Web Application Security: Common Risks and Protection Strategies

DEMO / THEME CONTENT

Authors

[Author Full Name 1] — [Institution Name], Pakistan — author1@example.com

[Author Full Name 2] — [Institution Name], Pakistan — author2@example.com

Abstract

Web applications are exposed to security threats because they operate through publicly accessible networks. This paper reviews common web application security risks and defensive strategies including authentication, authorization, input validation, encryption, session management, and security testing.

Keywords

Web Security; Cybersecurity; Secure Development; Authentication; Authorization

Main Content

1. Web applications frequently process sensitive information, making security an essential development concern.

2. Secure development requires validation, access control, secure session handling, dependency management, testing, monitoring, and timely updates.

3. Security should be integrated throughout the software development lifecycle rather than added only after completion.

References

1. OWASP Foundation. (2021). OWASP Top 10: The Ten Most Critical Web Application Security Risks.

2. Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice. Pearson.

3. Anderson, R. (2020). Security Engineering. Wiley.

Sample content created only for demonstrating the JITDS OJS theme and publishing workflow. It is not a genuine research publication.