Web Application Security Testing – Task 1

1. Introduction

This report presents the results of a web application security assessment performed as part of the Future Interns Cyber Security Internship. The objective was to identify common vulnerabilities using OWASP ZAP.

2. Target Application

URL: http://testphp.vulnweb.com
Type: Vulnerable Test Application

3. Tools Used

- OWASP ZAP
- Web Browser
- Windows OS

4. Vulnerability Findings

4.1 SQL Injection (High Risk)

SQL Injection vulnerabilities were identified in URL parameters. Error-based and time-based SQL injection issues were detected, allowing attackers to manipulate database queries.

Impact:

- Data leakage
- Unauthorized database access
- Possible system compromise

4.2 Security Misconfigurations

- Absence of Anti-CSRF Tokens
- Missing CSP Header
- Missing Anti-Clickjacking Header
- Server Information Disclosure

5. Risk Analysis

SQL Injection is a critical vulnerability that can lead to complete system compromise if exploited.

6. Recommendations

- Use parameterized queries
- Validate and sanitize user input
- Implement security headers
- Disable server information disclosure

7. Conclusion

The assessment successfully identified critical vulnerabilities. Immediate remediation is recommended to improve application security.