## PROPOSED SOLUTION:

During this project, we conducted *manual and automated vulnerability assessments* on *DVWA (Damn Vulnerable Web Application)* to identify security flaws that could be exploited by attackers. Using *OWASP ZAP*, we scanned the application and discovered *15 critical vulnerabilities*, including *SQL Injection, Cross-Site Scripting (XSS), Remote Code Execution, CSRF, and Directory Traversal.* These findings highlighted weaknesses in *input validation, authentication mechanisms, session management, and web security configurations.*

To mitigate these security risks, we propose a *multi-layered security approach* that addresses both *application-level weaknesses and infrastructure security.*

1. **Secure Development Practices Based on Findings**
2. **Authentication and Access Control Improvements**
3. **Automated Vulnerability Scanning and Security Monitoring**
4. **Strengthening Security Headers and Web Server Configurations**
5. **Mitigation of CSRF and Session Hijacking Risks**
6. **Enhancing Web Application Firewall (WAF) & Intrusion Detection**
7. **Regular Patch Management and Security Updates**
8. **Security Awareness and Training for Users**
9. **Incident Response and Disaster Recovery Planning**