Week 1 – Security Assessment Report

Target Application: Damn Vulnerable Web Application (DVWA)
Environment: Kali Linux with OWASP ZAP and manual browser testing
Security Level: Low

1. Issues Found

- Reflected XSS on multiple input forms using script payloads
- SQL Injection on login and ID fields allowing authentication bypass
- Command Injection via OS command execution in the ping form
- File Upload allows PHP shell upload bypassing extension checks
- CSRF vulnerability in forms due to missing tokens
- Insecure CAPTCHA implementation can be bypassed
- Missing input validation across forms
- No rate limiting on login, enabling brute force attacks

2. Suggested Fixes

- Sanitize all user inputs using server-side validation
- Use prepared statements to prevent SQL injection
- Escape shell commands or avoid executing user input in the shell
- Restrict file upload types and validate MIME types and file content
- Implement CSRF tokens for all state-changing operations
- Secure CAPTCHA with server-side checks and time limits
- Add input validation on both client and server side
- Implement rate limiting and account lockout on login attempts

3. Tools Used

- OWASP ZAP for vulnerability scanning and request interception
- Chrome DevTools for manual testing and payload injection

Assessed by:Nabira Khan
Week: 1
Internship Task: Web Security Testing – DVWA