**Term Assignment**

**Assignment Title**: Application Security Assessment & Suggestion for Remediation.

**Instructions**:

In this section, you will apply your knowledge of ethical hacking by conducting a simulated penetration test on a vulnerable web application. You will use the OWASP WebGoat project as your target. Follow these steps:

1. **Setup Environment (20%)**:
   * Download and install OWASP WebGoat: [WebGoat Installation](https://github.com/WebGoat/WebGoat/releases).
   * Install a suitable penetration testing tool (e.g., OWASP ZAP, Burp Suite).
2. **Scanning and Enumeration (20%)**:
   * Identify the IP address of your WebGoat instance.
   * Use your chosen tool to scan and enumerate vulnerabilities in the WebGoat application.
3. **Exploitation (30%)**:
   * Choose one vulnerability you discovered and attempt to exploit it (e.g., SQL injection, XSS).
   * Document the steps you took to exploit the vulnerability.
4. **Reporting (30%)**:
   * Create a professional penetration test report that includes:
     + Executive summary.
     + Vulnerability assessment.
     + Exploitation details.
     + Recommendations for mitigating the identified vulnerabilities.

**Submission Requirements**:

1. Submit a written report (in PDF format) containing your responses to Part 1 and Part 2.
2. Include screenshots, code snippets, and logs as necessary to support your findings in Part 2.
3. Include a reference list for any external sources you used.
4. Each team has to present report to the class.

**Resources**:

1. OWASP WebGoat: [WebGoat GitHub](https://github.com/WebGoat/WebGoat)
2. OWASP ZAP: [OWASP ZAP Project](https://www.zaproxy.org/)
3. Burp Suite: [Burp Suite](https://portswigger.net/burp)