VULNERBILITY AUDIT AND ASSESSMENT – BASELINE ANALYSIS AND PLAN

Date July 1st 2022

OVERVIEW

1. Background

ℹ *This document will detail the possible security vulnerabilities for the website **https://allthegear.org.uk**. This document will also include appropriate standards for the ecommerce business.*

Black box security testing is performed by businesses to ensure that they are in compliance with regulatory requirements, that they are protecting confidential and proprietary information, and that they are protecting the organization's brand and reputation. (Ken, 2013)

2. Project Scope

ℹ *The purpose of this proposed project is to outline LUMA's ecommerce web application security evaluations. Web application evaluations are conducted to discover possible or actual vulnerabilities resulting from unintended misconfiguration, insufficient authentication, poor error handling, sensitive data leakage, etc.*

In Scope:

- *Penetration testing from internet (External facing website) – Black box testing*
- *Vulnerability assessment for the top 10 OWSAP threats*
- *A detailed report*

3. Regulatory Compliance

ℹ *The scope of the web application is ecommerce, The testing and final executive report will include guidance for regulatory compliance*

- ***GDPR*** *(General Data Protection Regulation): It is a law of the European Union that gives people in the EU more protection, rights, and control over how their personal information is used online.*
- ***PCI DSS*** *(Payment card Industry – Data Security Standard):*
- ***ISO 27001*** *(Information security management ISMS 27000:2018)*

4. Methodology

An information security assessment is the process of finding out how well a host, system, network, procedure, or person (which is called the assessment object) meets certain security goals. Tests, exams, and interviews are all viable options for this. As the name implies, black box testing is adversarial in nature, as it is carried out without any prior knowledge of the application itself, but with the ***full acknowledgement and approval.***

Our testing methodology follows the ***NIST 800-115*** *Penetration testing standards. The four-stage testing methodology as showed in Figure 1 – Stages of Penetration Testing (Scarfone, 2008)*

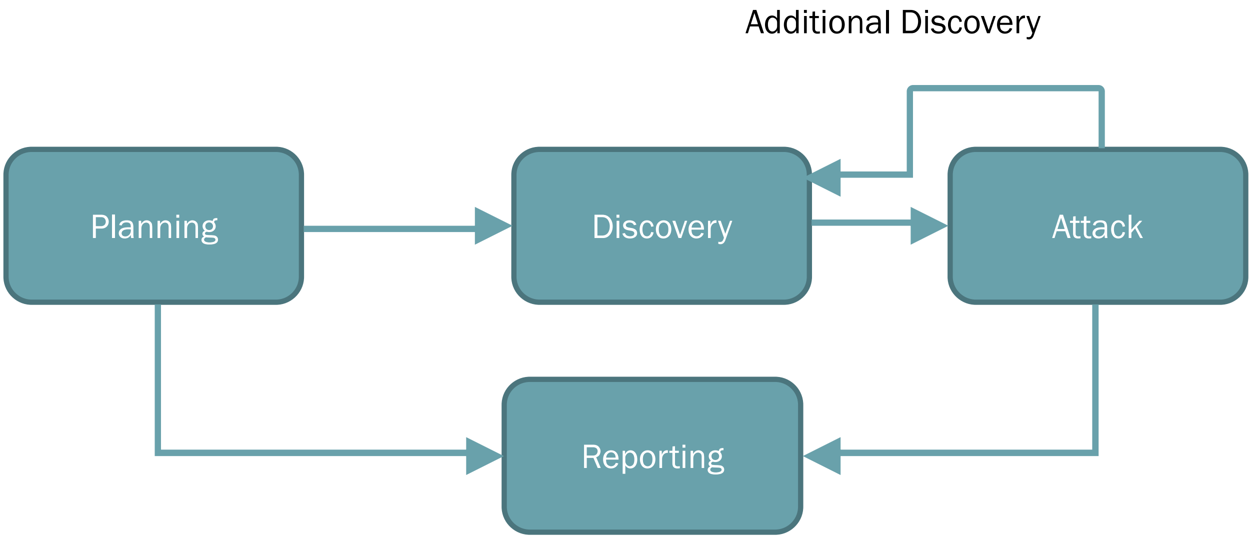


Figure 1 - Stages of Penetration Testing (Scarfone, 2008)

Planning: During the planning phase resources are identified, required approval are secured. Planning might also start with earlier penetration testing reports.

1. Application name & address

2. Contact information
3. Written approval
4. Testing window approval

Discover: During the discovery phase, we perform vulnerability analysis against the vulnerability standard database.

1. Misconfiguration
2. Kernel flaws
3. Buffer overflow
4. Incorrect permissions
5. Direct object references etc.
6. OWASP top ten vulnerabilities

Attack: During the attack phase, application will undergo the Penetration test scenarios. This includes all worst-case scenarios that simulates an outside attack.

1. Open sources tools will be used for penetration testing (Table 1 Security tools)

Reporting: During the reporting phase, a detailed vulnerability reports and recommendation for the web application will be summitted

1. Executive summary - Brief high-level summary and major findings
2. Detail scan results of each vulnerability
3. Clean / scrub up data (if any)

5. Tools and Purpose

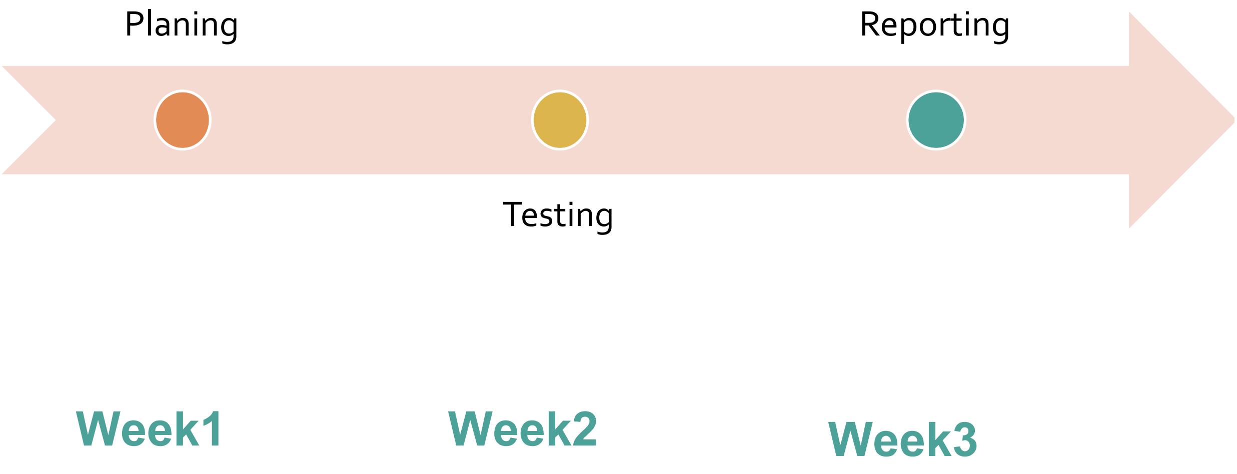
> *We will be utilizing the list of open-source free tools for this project as listed in Table 1. (CISA.gov , OWASP.org)*

Table 1 Security tools

Security Testing Technique	Security Testing tool
Network and Port scanner	NMAP (Nmap is a utility for network exploration or security auditing) Whois, Ping, Nslookup
Scan web server for known vulnerabilities	Nikto (Kali linux – Kali.org)
SQL injection	W3af (w3af.org)
Intercepting proxy server for security testing of web applications	Burp community Edition
Integrated penetration testing tool for finding vulnerabilities in web applications	OWSAP ZAP
SAAS based - vulnerability scanning platform	https://appcheck-ng.com

6. Project Timeline

High level Project timeline - Figure 2



Arkin, N.D (garymcgraw.com)

Figure 2 Project Timeline

7. Impacts on the application performance and availability

i *Because of the nature of penetration testing, it may disturb business activities during normal hours. Attempts to avoid disruption may increase testing time, resources, and complexity. To speed up testing, a separate production-like environment highly recommended for testing. In absence of the production-like environment, its highly recommended to schedule the testing* ***outside the business hours****. (C.C, 2005)*

Due to the existence of certain vulnerabilities, there is the potential for an accidental disclosure of data. (Baker 2022)

8. Limitations and Assumptions

i

- *A written project approval and authorization for penetration testing outside the business hours*
- *Because open-source tools have their own significant drawbacks, the scan results might not be comprehensive*
- *Proposed project will perform a single penetration testing, it will not be sufficient to remediate the all vulnerabilities.*

REFERENCE:

1. Anon, N.D, Guide to the General data protection Available from : GDPR https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ [Accessed 30 June 2022]
2. PCI DSS : https://listings.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf [Accessed 30 June 2022]
3. OWSAP Organization, (2021) Available from: https://owasp.org/www-project-top-ten/ [Accessed 01 July 2022]
4. Karen, S, et all. Technical guide to information security Testing and Assessment Available from: NIST 800-115 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf [Accessed 01 July 2022]
5. C.C, et all. Black Box Security Testing tools Available from: https://www.cisa.gov/uscert/bsi/articles/tools/black-box-testing/black-box-security-testing-tools
6. Brian, A, et all. Software Penetration Testing Available from: https://www.garymcgraw.com/wp-content/uploads/2015/11/bsi6-pentest.pdf [Accessed 29 June 2022]
7. Alice. B, (March 2022) Pros and cons of Penetration testing Available From: https://www.itgovernance.eu/blog/en/pros-and-cons-of-penetration-testing [Accessed June 29 2022]