System Proposal – E-commerce Website Pen Test

1. Introduction

Today, the operation of e-commerce websites is on the rise. In 2020, nearly thirty-six per cent of U.S. consumers were buying retail goods online, a trend projected to continue growing (Morgan, 2020). With more and more consumers performing online transactions, it is becoming vital to address privacy and security issues (Hlova, 2020). Following a 2019 global online shopping survey around seventy-six per cent of consumers consider privacy and security a very significant factor for deciding where to shop (2checkout, 2019) (See Appendix A).

2. Security Challenges Identification and Classification

Step One: Information Gathering (Reconnaissance):

We are going to perform an active reconnaissance on the web application. The information we intend to collect during the reconnaissance is as follows: **Fingerprinting**, to enable the gathering of information about the web application; such as the scripting language used, the server's operating system, the server's software and its version, open network ports and services running on the server. **DNS forward and reverse lookup**, to associate IP addresses with the fully qualified domain names (FQDN) or subdomain of the web application by utilising nslookup. **DNS Zone transfer**, to attempt the DNS transfer zone by using the "dig" command. With "dig" we will identify all external sites related to the target server and monitor all traffic exchanged. **Analyse HEAD and OPTIONS request**, to obtain information about the webserver software and its version. Analysis of the response generated from the HEAD and OPTIONS HTTP REQUEST will be performed.
We will also inspect the source code to discover other vulnerabilities, to determine the application environment and discover the application's overall functioning.

Step Two: Documentation and Investigation of gathered data:

Information and vulnerabilities discovered during the reconnaissance will be documented for classification and investigation of the discovered vulnerabilities. Additionally, the Open Web Application Security Project (OWASP), Center for Internet Security (CIS), cve.mitre.org and other scholarly research papers will be used to research and investigate identified vulnerabilities.
The probability and severity of each identified vulnerability will be factored into determining the risk rating it possesses to the web application. Classification of the identified vulnerabilities will be a derivative of the risk rating. The rating will rank from low, medium, or high.
And finally, the Network, Application and Software are the three categories in which discovered vulnerabilities will be classified.

3 Tools to be used.

-**Nmap (Network Mapper)**. This will allow us to discover basic information about the target website. Leverage the tool's scripting module can be used to detect vulnerability, backdoor and execution of exploitations, along with network information of the target web application such as open ports, ICMP request to check if the system is available and the services offered and detecting security risks.

-**OWASP ZAP Proxy**. This will help us to discover security vulnerabilities in the web application such as SQL injection, Broken Authentication, Sensitive data exposure, Sensitive data exposure, Broken Access control, Security misconfiguration, Cross-Site Scripting(XSS),

Insecure Deserialization, Components with known vulnerabilities and Missing security headers.
-**Nikto Scan** along with the capabilities of the ZAP proxy tool. Nikto performs comprehensive tests for multiple items, including one-thousand two-hundred-fifty outdated servers and version specific problems on over two-hundred-fifty servers.

We will also use automated vulnerability scanning tools such as pentest-tools.com and ImmuniWeb network security test and basic commands such as Traceroute, Pathping, nslookup, Ping and Whois.

4. Methodology

We will consult the Open Web Application Security Project (OWASP). This framework assists with identifying vulnerabilities in web and mobile applications. The updated guide of OWASP provides sixty-six controls to identify and assess vulnerabilities with numerous functionalities found in the latest applications currently. It also equips organisations with the resources to secure their applications from potential business loss.

5. Business Impacts From The Use Of The Tools.

Common impacts include (Beaver, 2018):
-Complications with Availability (DoS). Certain penetration activities, such as automated scanning, have the potential to cause disruptions, more so on legacy systems.
-Accidental Confidentiality violation such as unintended disclosure of sensitive information while conducting penetration testing activities.
-Email flooding resulting from web forms with no CAPTCHA protection. The risk of filling databases with illicit data junk data can be difficult to clean after penetration testing (Beaver, 2018).
-The need to use IT, security and development resources in ensuring the production environment remains stable during application testing impacting system performance negatively.

The majority of the tests will be performed outside of normal working hours to mitigate the impact.

6. Limitations and Assumptions.

Limitation of time: Penetration testing is an activity that is, in most cases, carried out with a defined period. The testing team has a specified period to identify threats and vulnerabilities and produce results in the form of a report. In contrast, attackers are not bound by time constraints and have ample time to identify and explore more vulnerabilities. Thus timed penetration test provides the attacker with an edge over the tester, allowing them more time to exploit the vulnerabilities (Cure, 2020).

Limitation of Access: A penetration test often has restricted access to the target environment. Such penetration tests would not reveal misconfiguration issues and potential vulnerabilities on the entire network that a white box vulnerability assessment would reveal (Cure, 2020).

Limitation of Methods: Depending on whether the production or staging environment is the testing target, conducting a penetration test is intended to exploit the system by performing transactions that the system was not intended to handle. Thus, during penetration testing, the testing team may be limited to use specific methods in order to avoid downtime. For instance, creating a denial of service flood attack may impact the production system (Cure, 2020).

Assumption of availability of the web application to be tested: The stated timeline can only be met if the web application remains available for testing.

7. Completion Timeline.

A penetration test consists of a series of steps, which include: Planning Step, execution, Data Analysis and Documentation, Final Presentation and Additional Testing.

The completion time required is also affected by various factors. These include the application size, the testing restrictions, the number of user roles, etc. In general, most penetration tests take approximately two to six weeks to be completed (Johnson, n.d).
Testing activities are expected to be finalised by the 19th of July.

References:

2checkout (2019) eCommerce Strategies Security and Compliance Trends for eCommerce in 2020. Available from: https://blog.2checkout.com/security-and-compliance-trends-for-ecommerce-in-2020/ [Accessed 09 June 2021].

Cypress Data Defense (2020) Major Limitations of Penetration Testing You Need to Know. Available from: https://www.cypressdatadefense.com/blog/limitations-of-penetration-testing/ [Accessed 09 June 2021].

Forbes.com (2020) More Customers Are Shopping Online Now Than At Height Of Pandemic, Fueling Need For Digital Transformation. Available from: https://www.forbes.com/sites/blakemorgan/2020/07/27/more-customers-are-shopping-online-now-than-at-height-of-pandemic-fueling-need-for-digital-transformation/ [Accessed 08 June 2021].

N-iX.com (2020) 6 types of security vulnerabilities in e-commerce and how to solve them. Available from: https://www.n-ix.com/6-types-security-vulnerabilities-ecommerce-solve-them/ [Accessed 07 June 2021].

Principle Logic, L. (2018) Testing applications in production vs. non-production benefits. Available from: https://searchsecurity.techtarget.com/tip/Testing-applications-in-production-vs-non-production-benefits [Accessed 08 June 2021].

Triaxiom Security (n.d) How Long Does A Web Application Penetration Test Take? Available from: https://www.triaxiomsecurity.com/how-long-does-a-web-application-penetration-test-take/ [Accessed 07 June 2021].

Appendix A

Fig 1.1 “Security with online retailers”. (Hlova, 2020)