Development Team Project: Design Document (Team A)

Introduction

Online shopping or e-commerce has increased from 14% of all global trade in 2019 to 19% in 2020, and is forecast to increase further (Hude, 2021). This growing market has led to an estimated 5-fold increase in cyber-attacks. which underscores the need for adequate security for both customers and the businesses providing the online service (Chin et al., 2020).

This design proposal will effectively articulate our plan to plan to carry out testing of your website for vulnerabilities, as well as how serious we deem the risks to be. Once security flaws are detected, we will advise you on how to mitigate the risks, which will be provided in a follow up document. We will also analyse compliance with current legislation and current security standards.

Threats

Open Web Application Security Project (OWASP) released a list of their top 10 security threats in 2017. We plan to analyse both the top 10 threats as well as specific threats to the e-commerce store. All the business specific threats are included in the OWASP top 10.

Business specific threats include:

- **Malware and ransomware** - Attackers may gain access to sensitive data and encrypt this data so that the business may not have access to it.
- **Point of sale** - Attackers may take advantage of unencrypted communications when processing payments, and therefore steal the customers personal details.
- **Compliance with industry standards** - Compliance with General Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCI-DSS). Noncompliance may lead to legal challenges.
- **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks** - Overloading of network systems prevent customers from completing transactions, as well as preventing the business from running efficiently.
- **Infrastructure** - Outdated hardware without current firmware updates may allow attackers to exploit a known vulnerability.
- **Vulnerable third-party modules** - Any third-party applications in use by the business may be a source of attack. We will analyse all these applications to ascertain the level of risk to the business and customers.

Compliance with legislation or standards

GDPR - Data privacy law enacted in 2018 across Europe (European Union, 2018).

PCI-DSS - The PCI standards Council was formed in 2006. They developed the standards and the security features to mitigate the possibility for data breaches for merchants as well as end users. All entities that store, process, or transmit cardholder data must validate PCI-DSS compliance (Global Payments Integrated, N.D.).

Investigation of threats

A virtual box is a hypervisor software. A hypervisor is computer software that creates a virtual hardware by borrowing the hardware from the host computer. This process is called virtualisation. We will use Kali Linux Operating system in a virtual machine in order to conduct most tests. All testing will be done remotely due to practicality. We will run multiple assessments from a variety of sources to determine the threats posed to the website by malicious actors. This will be done using the following tools:

1. **OWASP web application security guide** - This guide provides resources to outline the approach for testing web applications. We will use this guideline as a basis for our testing methodology, in line with industry best practices.

2. **OWASP Zed Attack Proxy (ZAP)** - This tool will be used to automatically and manually test the given website. Outcomes include the ability to detect security misconfiguration, sensitive data exposure and SQL injection vulnerabilities (Mburano and Si, 2019; Al Anhar and Suryanto, 2021).

3. **GDPR** - GDPR compliance will be assessed automatically and manually. The automatic testing will be done using Cookiebot, which analyses compliance by performing a GDPR cookie compliance test. This service will analyse cookies and trackers on the target website. The manual part of this assessment will be conducted using the GDPR checklist.

4. **The Harvester** - The harvester is an open-source tool that scans 40 public sources for emails, DNS names and subdomains belonging to an organization. This is an automated scanning tool. It allows in early phases of an attack to determine the attack surface.
   We are going to run harvester to verify that there are no sensitive data leaks, and advise as to how to mitigate these threats (theHarvester, N.D.).

5. **NMAP** - Nmap is a free and open-source utility for network discovery and security auditing. This is an automated scanning tool. It can be used for things including port scanning, service detection, and OS detection. This will allow us to see any open ports which may be vulnerable and any out-of-date software running on the network, as well as being able to view any unknown devices operating on it (NMAP, N.D.).

6. **OpenVAS** - OpenVAS is a free and open-source vulnerability scanning tool. This is an automated scanning tool. It can be used to scan a network for vulnerabilities against a feed of known security vulnerabilities, which is daily updated. As well as highlighting any vulnerabilities found, OpenVAS also gives a severity score to each one as well as providing descriptions of the vulnerability (Greenbone Vulnerability Management, N.D.).

Assumptions

- The website will be running during all hours, as well as all days of the week.
- The website will be typical of an e-commerce site, i.e., process payments, query stock levels, store users' personal information, order information (past and present).
- User to gain access to the target website based on the infrastructure scheme set out in Appendix 2.
- All tools are free and open source so that they can be audited and constantly updated.

Limitations:

- Due to the target website being an AWS educate account, there will be a limitation as to the number of hours available per month for the site to be running. As such we will liaise with the site owners to arrange testing at suitable times.
- The only access point to the web server is going to be a proxy server that is going to be publicly accessible, but that is going to restrict unallowed traffic using a whitelist mechanism.

Business impacts due to vulnerability testing:

- Some tests place a high load on the network and may slow down or cause the website to be unavailable. These tests will be done during low network usage hours, and the business will be duly informed prior to testing.

References

Al Anhar, A. and Suryanto, Y. (2021) 'Evaluation of Web Application Vulnerability Scanner for Modern Web Application', ICAICST 2021 - 2021 International Conference on Artificial Intelligence and Computer Science Technology. IEEE, pp. 200–204. doi: 10.1109/ICAICST53116.2021.9497831. [Accessed 15 September 2021]

Chin, I. E. et al. (2020) 'Cyber Attacks in the Era of Covid-19 and Possible Solution Domains', Preprints 2020, (September), pp. 1–15. doi: 10.20944/preprints202009.0630.v1. [Accessed 15 September 2021]

European Union (2018) 'General Data Protection Regulation (GDPR) – Official Legal Text', General Data Protection Regulation, pp. 1–99. Available at: https://gdpr-info.eu/ [Accessed: 17 September 2021].

Global Payments Integrated. (N.D.) PCI-DSS: The 6 Major Principles. Available from: https://www.globalpaymentsintegrated.com/en-us/blog/2019/09/17/pci-dss-the-6-major-principles [Accessed: 17 September 2021].

Greenbone Vulnerability Management (N.D.) Background. Available from: https://greenbone.github.io/docs/background.html#openvas-scanner [Accessed 15 September 2021]

Hude, J. (2021) 'SURGE IN ONLINE SHOPPING IN CORONA TIMES'.

Mburano, B. and Si, W. (2019) 'Evaluation of web vulnerability scanners based on OWASP benchmark', 26th International Conference on Systems Engineering, ICSEng 2018 - Proceedings. IEEE. doi: 10.1109/ICSENG.2018.8638176. [Accessed 15 September 2021]

NMAP (N.D.) Introduction. Available from: https://nmap.org [Accessed 15 September 2021]

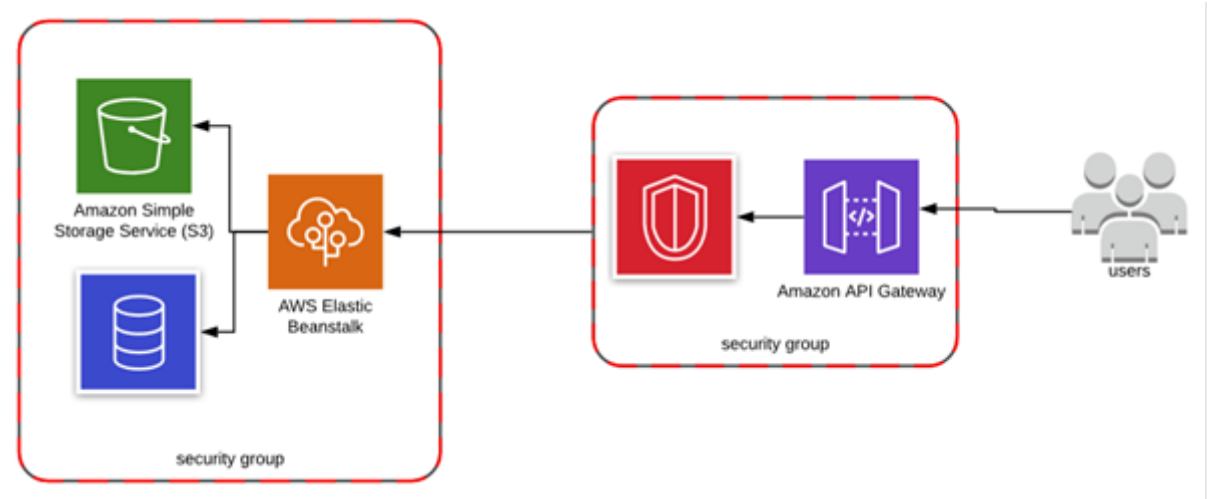
theHarvester. (N.D.) theHarvester/README.md. Available from: https://github.com/laramies/theHarvester/blob/master/README.md [Accessed: 16 September 2021].

Appendix

Appendix 1: General and business specific threats

General threats OWASP Top 10	Business specific threats
A1:2017-Injection: Attackers may use this threat to attack our database (SQL). Consequences include accessing private data or deleting private data.	Malware and ransomware
A2:2017-Broken Authentication: Attackers may compromise passwords or sessions leading to identity exploitation.	Malware and ransomware
A3:2017-Sensitive Data Exposure: Attackers may use this threat to compromise security relating to financial transactions, such as credit card fraud.	Point of sale Compliance with industry standards
A4:2017-XML External Entities (XXE): Attackers may use this threat to perform denial of service attacks, thus leading to compromised services on the site.	DoS and DDoS Attacks
A5:2017-Broken Access Control: Attackers may use this threat to compromise clients user accounts, view credit card and personal information or access unauthorized business functionalities.	Malware and ransomware Compliance with industry standards
A6:2017-Security Misconfiguration: Attackers may use this threat to intercept unencrypted communication, and steal customers or the business private information.	Compliance with industry standards
A7:2017-Cross-Site Scripting XSS: Attackers may hijack users sessions or redirect them to potentially malicious sites.	Infrastructure
A8:2017-Insecure Deserialization: Attackers may perform injection or replay attacks, or elevate their privileges to gain access to private information	Malware and ransomware
A9:2017-Using Components with Known Vulnerabilities: Attackers may take over the businesses server which will impact on the businesses functionality and customers usage.	Vulnerable third-party modules-
A10:2017-Insufficient Logging & Monitoring: Attackers may use the businesses lack of logging and monitoring as a basis for an attack, testing multiple facets of the sites security over a period in order to execute an attack.	DoS and DDoS Attacks

Appendix 2: Infrastructure scheme



Appendix 3: GANNT chart showing the timeline for expected completion