Instructions: Based on your chosen website in Unit 1, carry out a literature search/audit on software sites and the national vulnerability database to create a baseline audit on potential vulnerabilities within websites.

Website Link: https://buymenow.org.uk/

Website Type: Online Store

Given the popularity of online stores and e-commerce platforms such as Amazon, AliExpress, Shopee and others, many much smaller businesses have also digitized to offer their products online. While many sell on platforms like Etsy and eBay, to name a few, other businesses have decided to build their own platforms. Whilst ecommerce giants like Amazon are certainly not immune to vulnerabilities, as proven by the discovery of the CVE-2024-21626 - Runc container issue on the Amazon AWS platform (Amazon, 2024) smaller businesses are just as, if not more, vulnerable, as they have less resources to build and maintain their platforms. They often rely on third-party payment providers and therefore have less control. They may also lack the expertise to build a secure platform.

At a base level, there are vulnerabilities to every platform, and there are some threats each platform is vulnerable to, as long as it is connected to the internet. Two of such threats are DoS and DDoS attacks (Kalamkar, 2017). Another common vulnerability e-commerce platforms are plagued by is the possibility of unauthorized access by a third-party (via flaws in the authentication system, or attacks such as XML scripting). As a countermeasure to such vulnerabilities, Kalamkar (2017) makes mention of the six dimensions of e-commerce security:

- Integrity
- Non-Repudiation
- Authenticity
- Confidentiality
- Privacy
- Availability

Furthermore, the author of said article recommends using firewalls, SSL protocols for encryption, using strong passwords, encrypting critical data, as well as third-party audits to uphold security.

In an article about logic errors in e-commerce applications, Fangqi et al. discuss how the complexity of online stores and the use of various third-party payment APIs give rise to such vulnerabilities. These vulnerabilities range anywhere from logic flaws and faulty code causing incorrect integration of third-party payment services, insufficient validation of the integrity and authenticity of payments on a platform, to potentially allowing a malicious third-party to tamper with critical payment status components. To mitigate and solve these problems, the authors propose a novel approach using static analysis and taint tracking (Fangqi et al., 2014).

However, vulnerabilities do not exist solely based on flaws introduced during the coding process, or because of a lack of security in a particular online store. As mentioned by Zhao et al. (2009), data available on the internet can potentially pose a threat to an organization. Focussing on Fortune500 companies, the authors argue that with publicly available information about IP addresses and network ranges, hackers can potentially gain access to a businesses systems. Whilst firewalls are commonly used to protect against such instructions, the authors argue that negotiations with internet registrars like the American Registry of Internet Numbers could help in restricting public access to sensitive information.

The authors of '*E-Commerce Security Issues*' rate consumer privacy as a major security issue, among others such as platforms being vulnerable to viruses and trojan horses, potentially leading to theft and fraud (Merchany et al., 2002).

Searching through the National Vulnerability Database with the keyword '*e-commerce*' results in a total of 156 hits, with the top four results being:

- Cross-Site Scripting (XML Scripting)
- SQL Injection
- Unrestricted File Upload
- Directory Traversal

Based on initial research conducted, Cross-Site Scripting and SQL Injection are the most common vulnerabilities discovered in e-commerce platforms, ranging in rating from medium all the way to critical (NIST, N.D.).

References

Amazon (2024) CVE-2024-21626 - Runc container issue. Available from: https://aws.amazon.com/security/security-bulletins/AWS-2024-001/ [Accessed 07 February 2024].

Fangqi, S., Liang, X. & Zhendong, S. (2014) Detecting Logic Vulnerabilities in E-Commerce Applications. *NDSS Symposium***.** Available from: https://www.cs.ucdavis.edu/~su/publications/ndss14.pdf [Accessed 07 February 2024].

Kalamkar, M. D. (2017) A Study of Ecommerce Security. *IJCTA - International Science Press* 10(9): 67-70. Available from: http://210.212.169.38/xmlui/bitstream/handle/123456789/4084/Study%20of%20Ecommerce%20Security.pdf?sequence=1&isAllowed=y [Accessed 07 February 2024].

Zhao, J.J., Truell, A.D. and Alexander, M.W., 2009. A Security Vulnerability Audit of Fortune 500 E-Commerce Network Systems. *Issues in Information Systems*. 88-94. Available from: https://doi.org/10.48009/2_iis_2009_88-94 [Accessed 07 February 2024].

Marchany, R.C. & Tront, J.G., 2002. E-Commerce Security Issues. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS-35'02)*. IEEE. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=994190 [Accessed 07 February 2024].

NIST (N.D.) National Vulnerability Database. Available from: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=e-commerce&search_type=all&isCpeNameSearch=false [Accessed 07 February 2024].