Using the website(s) assigned to you in Unit 1, carry out the following exercise and answer the questions listed below.

1.0 Instructions

Carry out a literature search/audit on software sites and the national vulnerabilities database to create a baseline audit on potential vulnerabilities with websites.

1.1 Learning Outcomes

- Identify and analyse security threats and vulnerabilities in network systems and determine appropriate methodologies, tools and techniques to manage and/or solve them.
- Design and critically appraise computer programs and systems to produce solutions that help manage and audit risk and security issues.
- Gather and synthesise information from multiple sources (including internet security alerts and warning sites) to aid in the systematic analysis of security breaches and issues.

1.2 Reflection

Reflect on this activity by answering the following questions:

- Did you have any issues or challenges with the literature search/audit on software sites and the national vulnerabilities database?
- How did you overcome them?
- How will they affect your final report?

2.0 Introduction

I am conducting an audit on the website https://loadedwithstuff.co.uk/ that sells electronic devices and personal care stuff to customers. It has visible telephone number, a visible email address and at the bottom of the page a link the company's official Facebook account. It allows users to create accounts and login. Without knowing for certain, I assume the login is to make the shopping experience smoother and for the company to know their customers.

2.1 Ocular investigation of the website

Upon initial investigation of the website, I have two immediate concerns: the email is public which can make it a target for spear-phishing attacks whilst the public telephone number makes the company vulnerable to Smishing attacks. Business e-email compromise (BEC) targes businesses where social engineering techniques are used to gain access to the organisations email to initiate bank transfers (ENISA report, 2021). Spam messages can be sent via email, text messages, SMS and to the company's Facebook account (ENISA report, 2021). The customer login feature does not utilise two step authentication which may put the customer base at risk with hacked accounts, stolen credit card details or fraudulent orders.

Without knowing the architecture and design of the system in details, I can only make general assumptions. The web application is built using Softaculos scripts, and any understanding and assumptions is general based secondary sources.

3.0 Reconnaissance

3.1 Secure Sockets Layer

Any website should utilise SSL encryption across the board as it creates safe tunnels for data passage and is de facto standard for e-commerce.

3.2 Cookies

It can be assumed the website application users' cookies to store data about its customers and to allow users to save their login details. An attacker can exploit this cookie by introducing malware to utilise cross-site scripting to impersonate a customer (Tunggal, 2021).

3.3 Anti-malware software

Malware is an umbrella term that covers any software, firmware or code intended to perform a malicious unauthorised process that will have vast consequence on confidentiality, integrity or the availability of a system. (ENISA report, 2021). Anti-malware software can automatically detect, remove, and prevent standardised threats. Does loadedwith.stuff.co.uk/ have appropriate safety guards in the auto-malware software? If not, what can be recommended?

3.4 Two step authentication

A potential vulnerability is the weak single login system. Once an attacker has gained access to login details, the path forward is straightforward for illicit purposes.

3.5 Company policies and procedure documents

What are the company policies in place to manage people and what procedures are in place?

3.6 Adequately trained staff

Are the employees at loadedwithstuff.co.uk/ trained on security behaviours to a satisfactory standard? ENISA reported that most breaches relating to data were errors caused by employees (ENISA, 2021) and such risk could be mitigated by training staff to company frameworks.

3.7 GDPR compliance

Any organisation or business are required to comply with the UK General Data Protection Regulation (UK GDPR) operating within the UK. Because loadedwithstuff.co.uk target UK customers and operates on the UK market, the UK GDPR applies in conjunction with the Data Protection Act 2018 and must be adhered to by loadedwithstuff.co.uk (ISO, 2022).

4.0 Solutions

4.1 Secure Sockets Layer

As loadedwithstuff.co.uk/ uses Softaculos scripts are created by development company, and publicly accessible from the internet, it must be assumed SSL are configured (NCSC, 2021). Another factor speaking to the configuration of SSL are the padlock visible next to the URL in the address bar of the internet browser.

4.2 Cookies

HTTPsOnly is a configuration setting that prevents scripts from accessing the cookie. When malware access the cookie, it returns blank login details. If HttpsOnly is not set, it returns the login credentials and the attacker have access to an account.

Secure – This is a flag that ensures cookies are passed though secure SSL tunnels. Cookies can be read in transit if the flag is not activated, which makes it vulnerable to snooping and failure to use this flag means that data are passed between secure and unsecure connections. (Up guard, 2021).

4.3 Anti-malware software

Anti-malware software provides (sometimes) automated protection against malicious code, but can also be used to disinfect infected programs or clean malicious software from the system (Koret and Bachaalany, 2015). Anti-malware software protects against known malicious code, behaviours and patterns and not new types of attacks (Koret and Bachaalany, 2015). By configuring a malware program on the companies' devices, the attack surface is reduced if the program is continuously updated, automated security scans are set up and prevent connections to malicious websites (NCSC, 2021).

4.4 Multi factor Authentication

Multi factor Authentication adds an additional layer of security for accounts and reduces the attack surface for illicit actors (NIST, 2022). Attackers would have to steal both login credentials and the second authentication device, which can be either a mobile phone, an app or a randomised line of numbers decreasing the risk of an attack by increasing the work burden for the attacker to steal data (NCSC, 2022).

4.5 Company policies, procedures, and action plan

Company policies to train staff in password security, digital behaviour to avoid phishing attacks, spear-phishing attacks, social engineering attacks and a company procedure how to tackle potential insider threat and how to proceed if attacks occur.

4.6 GDPR compliance

Without the specific details about loadedwithstuff.co.uk data handing, the Information Commissioners Office (ICO) provides a checklist for small business of legal requirements of how and when data is processed in the UK (ICO, 2022). Any employee or owner of loadedwithstuff.co.uk must be trained and educated on dataprotection handling and the legal

obligations imposed on the organisation to permit the customer base to exercise their rights under Chapter 3, Articles 12–22 and other obligations (UK GDPR, 2022).

4.7 Adequately trained workforce

A good line of defence is to keep employees trained in digital behaviours, what to be cautious about whilst online, educate staff of phishing, spoofs, and untrusted sources. Social engineering techniques are getting sophisticated where the attackers gain access to credentials which are used to further attack employees.

One example of this is the SendGrid attack, where malicious actors used credentials of executives to further attack employees and saying that payment should be send to the attackers account instead (Chen et al, 2020). To mitigate such risk, training should be provided on attacks and combined with a company policy reduces the attack surface.

5.0 Reflections

The challenge with this literature review lied in my complete lack of subject-knowledge, lack of understanding and not knowing how to approach the subject or where to start. I overcame these challenges by starting to research the topics and subject, where I consumed vast amounts of YouTube videos, articles, and books on google scholar and the library database. In the end, I think the literature review and potential threats regarding web application security covers the many factors associated with network security. I look forward to gain more in-depth- knowledge in my future learning.

References

ENISA (2021). *ENISA THREAT LANDSCAPE 2021 April 2020 to mid-July 2021*. [online] European Union Agency for Cybersecurity (ENISA), 2021, pp.1–116. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 [Accessed 23 Jun. 2022].

Tyas, Tunggal, A. www.upguard.com. (2021). *How does Amazon handle cybersecurity?* [online] Available at: https://www.upguard.com/blog/prime-day-how-amazon-handles-cybersecurity.

Rigopoulos, K. (2016). *Back to Basics: What's multi-factor authentication - and why should I care?* [online] NIST. Available at: https://www.nist.gov/blogs/cybersecurity-insights/back-basics-whats-multi-factor-authentication-and-why-should-i-care.

Ncsc.gov.uk. *Small businessguide* (2019). [online] Available at: https://www.ncsc.gov.uk/collection/small-business-guide.

Trend Micro. (2020). *Water Nue Phishing Targets Execs Office 365 Accounts*. [online] Available at: https://www.trendmicro.com/en_us/research/20/h/water-nue-phishing-targets-execs-office-365-accounts.html [Accessed 23 Jun. 2022].

Information Commissioner's Office (2019). *Guide to the General Data Protection Regulation (GDPR)*. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

ico.org.uk. (2021). *How well do you comply with data protection law: an assessment for small business owners and sole traders*. [online] Available at: https://ico.org.uk/for-organisations/sme-web-hub/checklists/assessment-for-small-business-owners-and-sole-traders/.

Anon, (n.d.). *UK General Data Protection Regulation - UK GDPR*. [online] Available at: https://uk-gdpr.org/.

Koret, & Bachaalany, E. (2015). *The Antivirus hacker's handbook* (First edition.). John Wiley and Sons.