VULNERABILITY AUDIT AND ASSESSMENT- BASELINE ANALYSIS AND PLAN

NETWORK SECURITY

13th February, 2023

UNIVERSITY OF ESSEX

**Assessment of the website**:

This assessment encompassed of the thorough inspection of the given website (https://buymenow.org.uk), identifying the key security aspect and eliminating out-of-date practices by recognising vulnerabilities, analysis of the website to look for security breaches, risk assessment to aid in the mitigation plan and propose solutions. (Wilson, 2020)

**Security Challenges, tools and justification**:

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Tools** | **Justification** |
| Malware | A malware scans such UpGuard web scan, Snort, Malcare and Unmask Parasite etc. can help in identifying malwares. (Peter, 2022) | These tools use variety of methods such as signature based detection, sandboxing and emulation to detect malware. |
| Phishing | Network scanning tools such as Avanan, Barracuda Sentinel etc. serves as anti-phishing software. (Tim, 2022) | These tools uses URL analysis, Web content analysis and email analysis to detect phishing attacks. |
| SQL injection | A SQL injection scanner such as NS lookup, OWASP ZAP and SQLmap etc. can help look for potential attacks. (Samantha, 2021) | These tools offer variety of scanning methods. Example input validation, code analysis, database fingerprinting and exploitation to detect vulnerabilities. |
| Cross-site scripting | The tools used to detect XSS attacks are NSLookup, Acunetix and Invicti and many more to carry in-depth scanning of the vulnerabilities. (Software testing help, 2023) | These tools also work on the above scanning method for SQL injection like input validation, code analysis, exploitation and vulnerability reporting. |
| Cookie poisoning | Invicti and Acunetix can detect cookie poisoning and XSS together with OWASP and Burpsuite. (Zbigniew, 2021) | These tools uses the same method as above for SQL injection and cross site scripting in addition to session management analysis. |
| Denial of service | Web application firewalls, Wireshark, TCPdump Hping3, Hulk and Goldeneye etc. are some of the tools to scan DDOS attacks. (Redlegg, 2019) | These tools provide scanning for DDOS attacks by analysing the traffic, data packets, signature detection and behaviour analysis. |

**Standards for scanning vulnerabilities:**

|  |  |
| --- | --- |
| **Standard** | **Justification** |
| PCI DSS (Payment card industry data security standard 11.2) | The two types of scans i.e. internal and external, scan for configuration of the device, scans IP addresses, ports and services to check for vulnerability. (Surkay, 2020) |
| GDPR (General data protection regulation, article 32) | This articles implies the use of vulnerability assessment in compliance with GDPR standard. (Breachlock, 2020) |

**Methodology:**

Undertaking the vulnerability assessment would involve several steps:

1. Identifying the assets, risks and importance of the device, policies and impacts on business analysis.
2. Gather baseline system information.
3. Carrying out the vulnerability scans by use of appropriate tools.
4. Report creation, evaluation of the results, adding mitigation plans and recommendations. (Kenneth, 2018)

**Business impact on use of scanning tools:**

The impact that could be created by running the vulnerability scan would include the business activity as some scans might affect the services provided by the website and can also cause pseudo DOS attack so informing the staff members and also the service users would be essential.

Also, some scans need to be carried out during the operational hours to identify the key vulnerabilities but would disrupt the service, hence it is essential to avoid the peak hours from the user’s perspective and where possible, schedule scans in the out of hours.

**Completion of the task:**

The completion of the task depends on number of factor:

1. The threshold of the company to accept, adapt to the risks and disruptions in the services.
2. To speed up the completion, prioritizing the risks as per the harm it can cause.
3. To bring compensatory controls such as IDS, IPS and firewalls while keeping the operations running and reducing the risks.
4. Also, incorporating more automated scanners to expedite the process as well using manual testing to further reduce the risk. (Craig, 2021)

**Limitations:**

1. Not all vulnerabilities would be identified. It is recommended to use multiple scanning tools.
2. It can false positive results
3. To use the scanning tools to its fullest potential and carry additional risks by experts. (ValueSec, 2023)

**References:**

Wilson, H. (2020). How to Perform a Website Security Audit. Available from: https://www.vodien.com/learn/website-security-audit/ [Accessed 13 February 2023].

BIGCOMMERCE (n.d.). What You Need to Know About Securing Your Ecommerce Site Against Cyber Threats. Available from: https://www.bigcommerce.com/articles/ecommerce/ecommerce-website-security/ [Accessed 13 February 2023].

Peter, B. (2020). 10 Tools to Scan Website for Malware. Available from: https://www.malwarefox.com/tools-to-scan-website-for-malware/ [Accessed 13 February 2023].

Tim, F. (2022). 10 Top Anti-Phishing Tools and Services. Available from: https://www.csoonline.com/article/3575080/9-top-anti-phishing-tools-and-services.html [Accessed 13 February 2023].

Samantha, B. (2021). 3 Free Pentesting Tools for Finding SQL Injection Vulnerabilities. Available from: https://www.technotification.com/2019/11/3-free-pentesting-tools-for-finding-sql-injection-vulnerabilities.html [Accessed 13 February 2023].

Software testing help. (2023). Cross Site Scripting (XSS) Attack Tutorial with Examples, Types and Prevention. Available from: https://www.softwaretestinghelp.com/cross-site-scripting-xss-attack-test/ [Accessed 13 February 2023].

Zbigniew, B. (2021). Understanding Cookie Poisoning Attacks. Available from: https://www.invicti.com/blog/web-security/understanding-cookie-poisoning-attacks/ [Accessed 13 February 2023].

Surkay, B. (2020). What are the Requirement for PCI DSS vulnerability Scanning? Available from: https://www.pcidssguide.com/pci-vulnerability-scan-requirements/ [Accessed 13 February 2023].

Breachlock. (2020). Penetration testing and Vulnerability Scanning for GDPR. Available from: https://www.breachlock.com/resources/blog/penetration-testing-and-vulnerability-scanning-for-gdpr/ [Accessed 13 February 2023].

Kenneth, G. (2018). A Step-By-Step Guide to Vulnerability Assessment. Available from: https://securityintelligence.com/a-step-by-step-guide-to-vulnerability-assessment/ [Accessed 13 February 2023].

Craig, L. (2021). Setting Practical Time Frames to Remedy Security Vulnerabilities. Available from: https://www.techradar.com/news/setting-practical-time-frames-to-remedy-security-vulnerabilities [Accessed 13 February 2023].

ValueSec. (2023). 3 Limitations of Vulnerability Scanning You Should Be Aware of. Available from: https://www.valuesec.in/3-limitations-to-vulnerability-scanning/ [Accessed 13 February 2023].