Vulnerability Assessment Report

Executive Summary

1. Summary of the assessment process

The Assessment Team carried out a vulnerability assessment of https://www.buymenow.org.uk website. The purpose of the assessment was to identify the potential vulnerabilities of the website and suggest actions to mitigate the risks posed by the vulnerabilities identified.

The Assessment Team tried to mimic the tactics of an attacker by adopting a remote testing approach. Thanks to this approach, it was possible to realistically assess the potential impact of outsider attacks as well as to identify any preventive measures in place.

A total of 14 automated tools that were selected based on the STRIDE (Microsoft, 2022) threat modelling framework were used to scan the website against known vulnerabilities and 13 vulnerabilities were identified in total. Detailed breakdown of the vulnerabilities identified can be seen in the Findings section.

The assessment process took 7 days and the Assessment Team avoided performing scans during peak times to minimise the business impact.

2. Findings

The Assessment Team identified a total of 13 vulnerabilities on the website by using automated tools. The breakdown according to the CWE risk level is as follows:

Risk	High	Medium	Low	Informational
Count	0	3	4	6

While no high-risk vulnerabilities could be found, it should be noted that the scan results were limited due to the capabilities of the scanning tools and therefore, there might be other, possibly high-risk vulnerabilities that couldn't be identified by the Assessment Team.

When tried to apply active scanning techniques, the Assessment Team was blocked by Imunify360 (N.D.) – a comprehensive security suite which brings together an antivirus, a firewall, a WAF and a PHP security layer. While this is a good indication that the website is secured against such attacks, it doesn't mean that sophisticated attackers may not find their way around the security system to exploit potential vulnerabilities that they might identify.

The password policy of the website has been assessed weak. The Assessment Team was able to create an account with the password 'aaaa' and there are no complexity requirements or password strength meters in place.

3. Security Standards

Based on the findings above, the website has been evaluated against two security standards: UK GDPR which applies to all organisations operating within the UK and PCI DSS which is particularly applicable to the e-commerce websites.

3.1 Data Protection Act (UK GDPR)

As per Data Protection Act (2018), the website was checked according to the criteria below:

Criteria	**Assessment**
Privacy Policy	The website lacks a proper Privacy Policy.
Consent for collecting data	User's consent for collecting data is not sought. Likewise, no option is offered to the users to withdraw their consent.
Knowledge of data that's collected	No information is available.
Data subject's rights	The users are not informed about their rights concerning their data. No procedures

	are in place for users to exercise their right to access, rectification or erasure.
Lawful basis requirements	No problems identified.
Data Protection Policy	No Data Protection Policy is in place.

A detailed discussion of UK GDPR compliance of the website is included in the appropriate section of the report.

3.2. PCI DSS

The website was also evaluated against PCI DSS based on the requirements (PCI SSC, 2022) below:

Requirement	**Assessment**
Install and maintain network security controls	Imunify360 web server security suite is used. It successfully blocks intrusion attempts.
Protect all systems and networks from malicious software	
Protect stored account data	Detailed information not available. A better password policy may help to better protect the account data.
Protect cardholder data with strong cryptography during transmission over open, public networks	No problems identified.
Develop and maintain secure systems and software	The website is vulnerable to the common vulnerabilities identified which include CSRF, XSS or SQL injection.
Apply secure configurations to all system components	
Restrict access to cardholder data by business need-to-know	No information available.
Identify users and authenticate access to system components	No information available.
Restrict physical access to cardholder data	No information available.
Log and monitor all access to system components and cardholder data	No logs were identified by the Assessment Team, even though it doesn't necessarily indicate to nonexistence of logs.
Test security of systems and networks regularly	Regular vulnerability assessments are performed. No pen tests have been carried out so far.
Support information security with organizational policies and programs	No privacy policy or similar policies or programs are in place.

4. Conclusions

The potential security issues are enumerated using STRIDE framework as follows:

STRIDE	Security Challenges	Number of vulnerabilities identified	Risk
Spoofing	Cross-Site Request Forgery (CSRF)	2	High
	Unvalidated redirects and forwards	-	Low
Tampering	Clickjacking	1	Medium
	Cross-Site Scripting (XSS)	6	High
	SQL Injection	1	High
	E-skimming	1	High
Repudiation	N/A	-	N/A
Information Disclosure	Insufficient transport layer protection	1	Medium
	Sensitive data exposure	3	Medium
	Insecure direct object references	-	Low
Denial of Service	Bad bots and Distributed Denial of Service (DDoS)	1	Medium
Elevation of Privilege	Broken authentication & session	3	High

As can be seen above, out of the 11 potential security challenges identified in the baseline analysis, no vulnerabilities were found to confirm the existence of 4 of them. Aside from these, during the analysis phase, the Assessment Team decided to add one more challenge - “Clickjacking”.

Besides the known vulnerabilities, the Assessment Team also found that the website was not compliant with the two important security standards that it was evaluated against:

- **UK GDPR**: The website fails to meet the requirements set out by the Data Protection Act, and this might lead to severe legal and ethical implications. Most notably, Privacy Policy is an essential component of any website seeking to operate within the borders of the United Kingdom.

- **PCI DSS**: The website's PCI DSS compliance is questionable. Apart from the identified known vulnerabilities, it was not possible to gather enough information to identify if the website meets some of the requirements due to the Assessment Team not having visibility into some of the system components. Since payment fraud is one of the most common security issues facing e-commerce websites, it poses a great risk to customer protection and business reputation and therefore, a detailed in-house examination should be carried out to determine the level of compliance.

5. Recommendations

The Assessment Team recommends following actions to be taken in order to mitigate potential caused by the vulnerabilities identified:

a. Comply with the UK GDPR by (1) drafting a Privacy Policy which includes the procedures for data subject's rights to access, rectify or erase their data, (2) disclosing information about cookies (i.e., cookie notification) and seeking user consent, and (3) preparing and publishing a Data Protection Policy.
b. Act on the identified common vulnerabilities, either via in-house or outsourced teams of developers.
c. Even though NCSC (2018) doesn't recommend the use of password complexity, the Assessment Team recommends introducing a minimal password policy to help the users to set a strong password. It is also advised that, following NCSC guidance, the reliance of the website on passwords is reduced by using technologies such as SSO and, MFA should be used to further secure customer accounts.
d. A full penetration testing should follow this vulnerability assessment to gain full visibility into potential security issues.

References:

Data Protection Act 2018, United Kingdom. Available from: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [Accessed 25 February 2023].

Hutchins, E. M., Cloppert, M. J. & Amin, R. M. (2011) Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Leading Issues in Information Warfare & Security Research* 1: 78-104.

Imunify360 (N.D.) Imunify360: Security Solution with Linux Malware Scanner for Servers. Available from: https://www.imunify360.com/imunify360/ [Accessed 26 February 2023].

Microsoft (2022) Microsoft Threat Modeling Tool. Available from: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats#stride-model [Accessed 1 March 2023].

NCSC (2018) Password policy: updating your approach. Available from: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach [Accessed 1 March 2023].

PCI Security Standards Council (2022) PCI DSS v4.0 Quick Reference Guide. Available from: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf [Accessed 25 February 2023].