This report will evaluate buymenow.org.uk for security vulnerabilities by using available tools and frameworks. There are two types of testing: the first, Whitebox Testing, is where the tester is given details to simulate internal attacks. The second is Black Box testing, where the tester has limited or no details and simulates an attack externally [ncsc.gov.uk, 2022].

This report will perform external testing out of hours, to avoid business impact. The first instance will be manually and if there is no impact this will become an automated process. There are several steps required.

- Information Gathering
- Business and Application mapping
- Discovering Vulnerabilities - Both a manual and automated approach
- Generate report for each attack to be shared with stakeholders
- Final report

[www.tutorialspoint.com, N/A]

Several threats have been defined below. The business impact for each of these, would be loss of data or website.

Threat	Definition	Mitigation	Recommendation
Malware Attack	Malicious software executed	Antivirus software	Patching the antivirus software
Spoofing (Man in the middle)	Something is pretending to be something else and modifying the data	Using spam filters	Managing end to end connection
Traffic Analysis attack	Monitor network traffic Unused open ports	Network Scanning tools	Up to date Firewalls Intrusion Detection System Intrusion Prevention System
Injection	Sending harmful packets within the network Executing harmful OS	Network Scanner	Intrusion Detection System Intrusion Prevention System

	commands to the Operating System Executing SQL command to the database Manipulating JavaScript vulnerability		Vulnerability scanner Patching to the recent version
Software Library Zero-day /Protocol Vulnerability	Loopholes within common communication protocols Vulnerabilities exploited on the day of release of software	Vulnerability scanner	Patching to the recent version
Data protection standards	Follow the UK Data Protection standards	Review of the standards is maintained	Follow the standards when accessing the site

The mains tools can be catergorised as follows:

- Port Scanner
- Vulnerability Scanner
- Network Analyser
- Pen testing tool

The below is a list of tools that will be used

Tools	Justification	Challenges
PING	Network packets to be sent to the host	No response from DMZ and if multiple pings sent at once can cause a denial of service
Traceroute	Route of the network packet being sent from one host to another	No response from DMZ and routers may be configured to refuse requests
NSlookup	DNS to give the IP address of the default server name	No response from the server
Netstat	Provides information on active connections	Lack of output
WIRESHARK	Network protocol Analyse	Dropped packets and latency
NMap	Provides information on vulnerability and port scanning	Too much information can be provided
Nessus	Scans and remotely identifies vulnerabilities	The Free version is limited to the number of scans performed

[Unit 3: Vulnerability Assessments, Lecturecast, June 2022]

Several testing frameworks are available depending on the type of testing required. The types of tests available are Social Engineering, Web Application, Physical, Network Services and Wireless Security. [softwaretestinghelp.com , 2022].

Below are available frameworks.

- Open Web Application Security Project
- Mobile Security Testing Guide
- The Open Source Security Testing Methodology Manual
- National Institute of Standards and Technology (NIST), Cybersecurity Framework
- The Penetration Testing Execution Standard

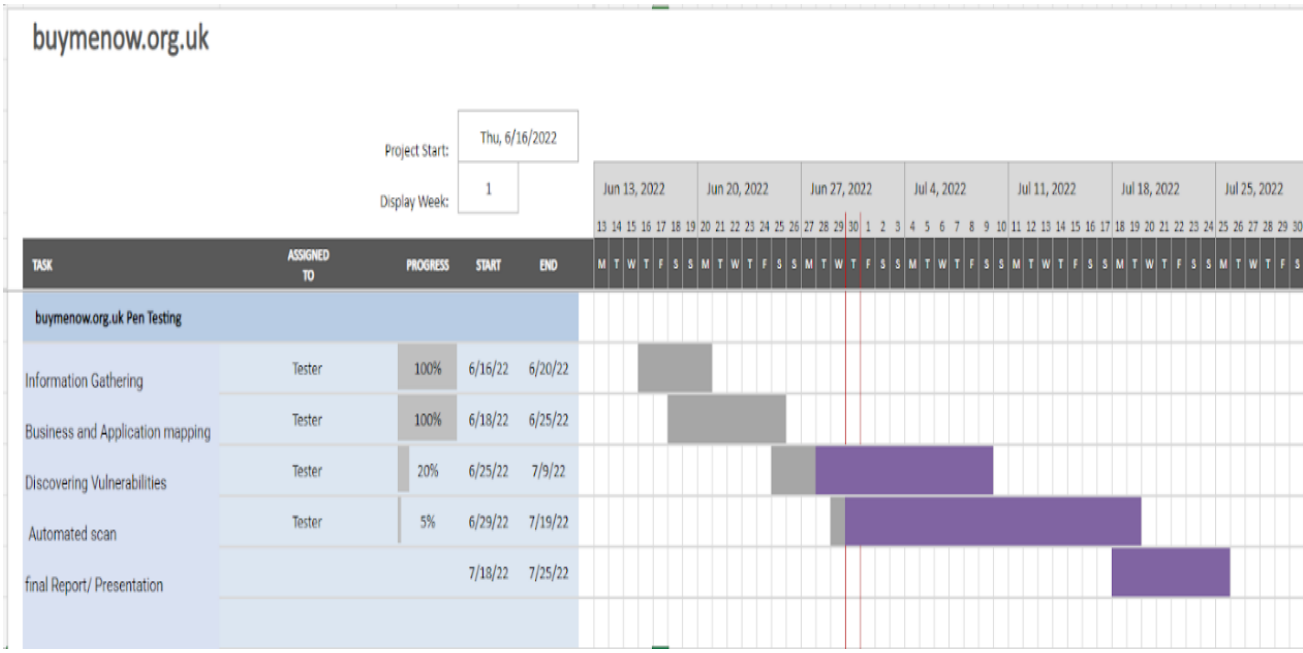
The recommendation of the report is to follow the OWASP Web Security. The below table shows each threat that was identified above categorised within the OWASP framework.

OWASP Security Risk Category	Threat
A02:2021-Cryptographic Failures	Data Theft
A03:2021-Injection	SQl Injection Command Injection Network Injection DOM injection Cross site scripting

A06:2021-Vulnerable and Outdated Components	Open Ports Protocol Vulnerability
A07:2021-Identification and Authentication Failures	Spoofing (Man in the middle)
A08:2021-Software and Data Integrity Failures	Software Library Zero day attacks Malware Attack
A09:2021-Security Logging and Monitoring Failures	Traffic Analysis attack

[owasp.org, n.a] and [Singh, 2020]

Timeline of the completion of the task



Below is a list of limitations and assumptions that we have made.

- There is no information on what Operating System is supported, if any failover is present or backend information like the database or source code
- https://buymenow.org.uk/ has no IT/Development resources or contact details
- Due to the word count limitation not, all vulnerabilities have been listed and details of the frameworks has not been added

There are many frameworks and tools available and to achieve the best results a mix and match of frameworks and tools would need to work in conjunction to reduce the risk exposure.

References

A Complete Penetration Testing Guide With Sample Test Cases

Anon(2022) A Complete Penetration Testing Guide With Sample Test Cases Available from:https://www.softwaretestinghelp.com/penetration-testing-guide/#Penetration_Testing_Types/ [Accessed 26 June 2022]

ncsc.gov.uk(2017) Penetration Testing Advice on how to get the most from penetration testing Available from: https://www.ncsc.gov.uk/pdfs/guidance/penetration-testing.pdf[Accessed 26 June 2022]

Open Source Security Testing Methodology Manual (OSSTMM): Definition & Overview

O'Nolan, C(N.D) Open Source Security Testing Methodology Manual (OSSTMM): Definition & Overview Available from: https://study.com/academy/lesson/open-source-security-testing-methodology-manual-osstmm-definition-overview.html [Accessed 26 June 2022]

OWASP Application Security Verification Standard Available from: https://owasp.org/www-project-application-security-verification-standard/ [Accessed 26 June 2022]

OWASP Top 10:2021 (2021) Available from:https://owasp.org/www-project-top-ten/ [Accessed 26 June 2022]

Singh, R(2020) OWASP Top 10 Web Application Security Risks and Vulnerabilities to Watch Out for in 2020 Available from: https://www.indusface.com/blog/owasp-top-10-web-application-security-risks-and-vulnerabilities-to-watch-out-for-in-2020/ [Accessed 26 June 2022]

tutorialspoint.com(N.D) Penetration Testing - Method Available from: https://www.tutorialspoint.com/penetration_testing/penetration_testing_method.htm[Accessed 26 June 2022]

(n.D) Unit 3: Vulnerability Assessments, Lecturecast Network Secuity NS_PCOM7E university of Essex delivered June 2022