# Vulnerability Assessment Plan

**Website to be assessed:** **https://buymenow.org.uk**

## 1. Security Challenges

The assessment team identified following potential security challenges for the website that will be assessed:

| Priority | General | Industry-specific (e-commerce) |
|---|---|---|
| **High** | Broken authentication & session<br>Cross-Site Scripting (XSS)<br>SQL Injection<br>Cross-Site Request Forgery (CSRF) | Online payment fraud<br>E-skimming |
| **Medium** | Bad bots and Distributed Denial of Service (DDoS)<br>Insufficient transport layer protection<br>Sensitive data exposure | |
| **Low** | Insecure direct object references<br>Unvalidated redirects and forwards | |

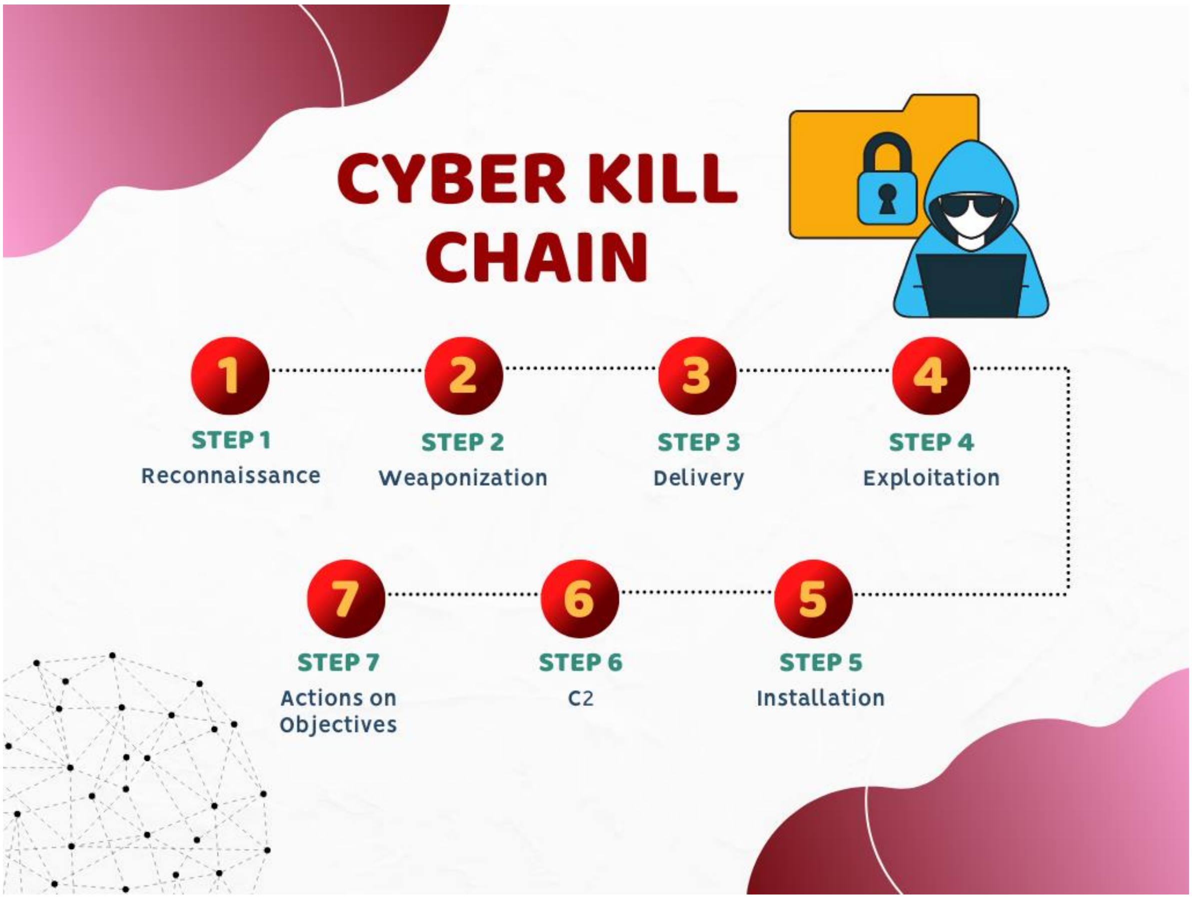
## 2. Methodology

### a. Scan method:

It is believed that the remote scan mimics the behaviour of potential attackers best. So, the scans will be carried out remotely. The assessment team will mostly rely on the automated tools for the optimal outcome. However, manual scan may be used if required.

### b. Analysis model:

The website will be assessed for cybersecurity risks using Cyber Kill Chain model suggested by Hutchins et al. (2011). It is a widely adopted, industry-recognized model that helps to assess potential vulnerabilities of a system from the perception of an attacker, which makes it the ideal model for a remote vulnerability assessment.



As a result of the analysis, mitigations to the risks identified will be suggested in six categories for each step of the Cyber Kill Chain:

| Phase | Detect | Deny | Disrupt | Degrade | Deceive | Destroy |
|---|---|---|---|---|---|---|
| **Reconnaissance** | | | | | | |
| **Weaponization** | | | | | | |
| **Delivery** | | | | | | |
| **Exploitation** | | | | | | |
| **Installation** | | | | | | |
| **C2** | | | | | | |
| **Actions on Objectives** | | | | | | |

### c. Standards and regulations:

The website will also be checked against the following industry standards to ensure the maximum compatibility with the regulations and best practices:

- PCI DSS
- DPA
- UK-GDPR
- PECR
- NIS

## 3. Tools

The following tools will be used for the purposes described in the table:

| Intended purpose | Tools |
|---|---|
| Check and identify publicly available information about the website | Maltego, whois |
| Find out more information about the host and configuration | ping, traceroute, whatweb, MTR, dig |
| Scan and detect open ports | Nmap |
| Scan for known vulnerabilities | Burp Suite, Nikto |
| Check and identify IDS, IPS, WAF and load balancers | firewalk, wafw00f, lbd |
| Check the configuration of SSL | thc-ssl-dos |
| Stress testing | slowhttptest, thc-ssl-dos |
| Detect the likelihood of social engineering | Social Engineering Toolkit (SET), Metasploit |

## 4. Business Impact

It is assessed that the scan and the tests may create a significant overhead on the system and may also lead the existing security tools to block incoming traffic or cause the website to behave unexpectedly. This may lead system to slow down, reject customer requests and disrupt business operations. Especially DDoS identification and stress testing tools (e.g., slowhttptest, thc-ssl-dos) are expected to disrupt the normal operation of the website. In order to mitigate this risk, the scans will be carried out during off-peak hours. The exact timeframe when the scans will be carried out will be decided upon consultation with the business operations team.

## 5. Limitations and Assumptions

Since the website uses a shared hosting model, some tools (e.g., nmap) will scan all services hosted on the same host and may produce erroneous reports. The assessment team is aware of this limitation and will consider this fact when using these tools or will use tools that allows to scan at higher levels of the network when applicable.

As mentioned before, the scans may trigger IPS/IDS systems in place or may seem like a DoS attack. The assessment team will take this opportunity to test the efficiency of such detection and prevention tools but will seek internal help to turn these tools off temporarily if necessary.

## 6. Timeline

The assessment process will be completed in 10 days.

All the scans and tests will be carried out in one week. This timeframe will also allow the assessment team to assess the impact of the traffic pattern throughout the week. Once the scans are complete, the results will be evaluated, and an assessment report will be prepared in three days which will be followed by a briefing to the stakeholders.

**References:**

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(1): 1-14.