Summary of Findings

In performing a detailed penetration testing study against team one’s NISMPHP web application portal, team four identified several issues of concern. This report provides brief descriptions of each testing category and offers more details where findings were negative.

The Open Web Application Security Project (OWASP) was used to identify vulnerabilities and complicated logic flaws. While this methodology outlines a series of privacy and applications security risks, it is not a compliance methodology with General Data Protection Regulation(GPDR). We used the Common Vulnerability Scoring System (CVSS) framework to measure quantitive scores to reflect the severity of the discovered vulnerabilities. The scores were translated into a qualitative representation (such as low, medium, high, and critical) to assess and prioritise the vulnerability management process.

Below is the table showing details of the identified vulnerabilities established on category and severity of the risk. Following the table below is a detailed breakdown outlining each testing category.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SECURITY RISK** | **COUNT** | **VULNERABILITY SEVERITY/SECURITY RISK** | | |
| **HIGH** | **MEDIUM** | **LOW** |
| A1. Injections | 2 |  | X |  |
| A2. Broken Authentication |  |  |  |  |
| A3. Cross-Site Scripting (XSS) | 2 |  | X |  |
| A4. Sensitive Data Exposure | 1 | X |  |  |
| A5. Insecure Deserialization |  |  |  |  |
| A6. Broken Access Control |  |  |  |  |
| A7. Insufficient Logging & Monitoring |  |  |  |  |
| A8. Server-Side Request Forgery (SSRF) |  |  |  |  |
| A9. Known Vulnerabilities | 3 |  | X |  |
| A10. Security Misconfiguration | 64 |  |  | X |

Table 1: Vulnerability and Security Risk

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SECURITY RISK** | **COUNT** | **VULNERABILITY SEVERITY/SECURITY RISK** | | |
| **HIGH** | **MEDIUM** | **LOW** |
| A1. Injections |  |  |  |  |
| A2. Broken Authentication |  |  |  |  |
| A3. Sensitive Data Exposure | 1 | X |  |  |
| A4. Insufficient Logging & Monitoring |  |  |  |  |
| A5. Insecure Deserialization |  |  |  |  |
| A6. Security Misconfiguration | 64 |  |  | X |
| A7. Cross-Site Scripting (XSS) | 2 |  | X |  |
| A8. Server-Side Request Forgery (SSRF) |  |  |  |  |
| A9. Known Vulnerabilities | 3 |  | X |  |
| A10. Broken Access Control |  |  |  |  |

Sensitive Data Exposure

The web application uses an insecure web protocol that transmits data in plain text without encryption. Confidentiality, One of the tenets of the CIA(Confidentiality, Integrity, Availability) triad is a set of rules designed to ensure that information access is limited to the authorised subjects. The impact on an individual or an entity resulting from unauthorised access to sensitive information usually determines the risk rating of the data to vary (Wesley Chai, 2021).

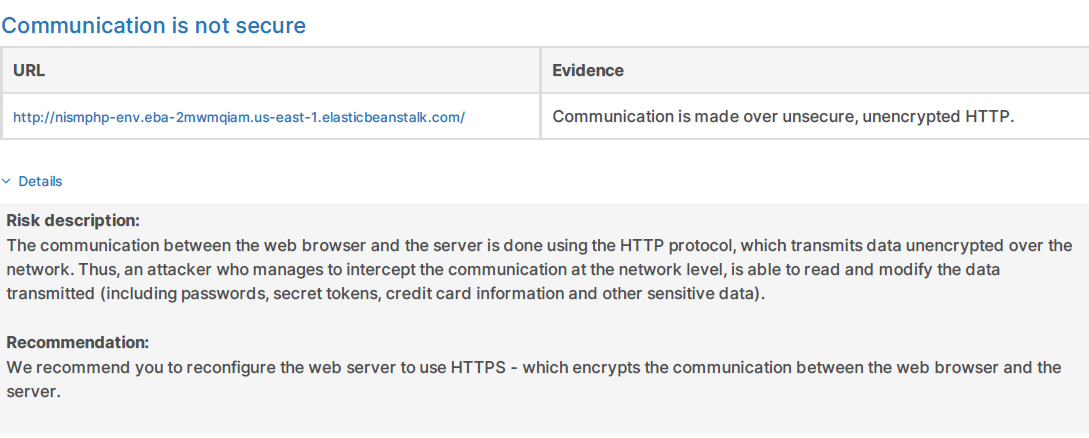


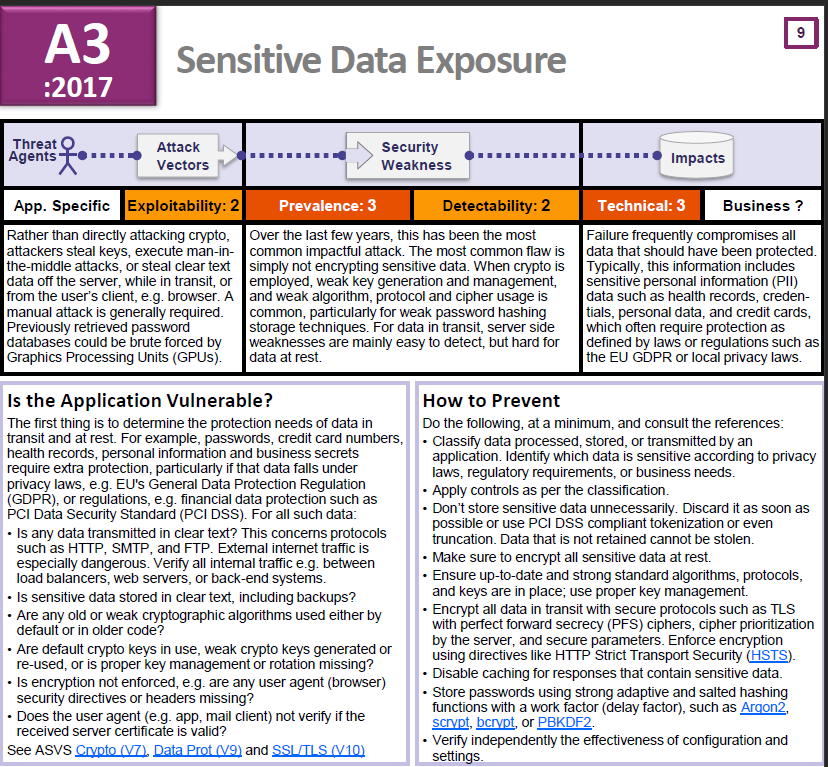
Figure 1 expands on the finding further to assist with the understanding concerning compliance with standards and regulations.

Figure 1: OWASP A3 Sensitive Data Exposure (Adapted from (Dehalwar et al., 2018))

Cross-Site Scripting (XSS)

Failing of restricting the sources that are allowed to input data into the web application leads to malicious data from the victim’s web browser included with dynamic content of the browser delivered to the web application. Thus, a cross-site scripting attack is successful. The usage of such attacks at other times results in defaced websites (Rosencrance, 2018).

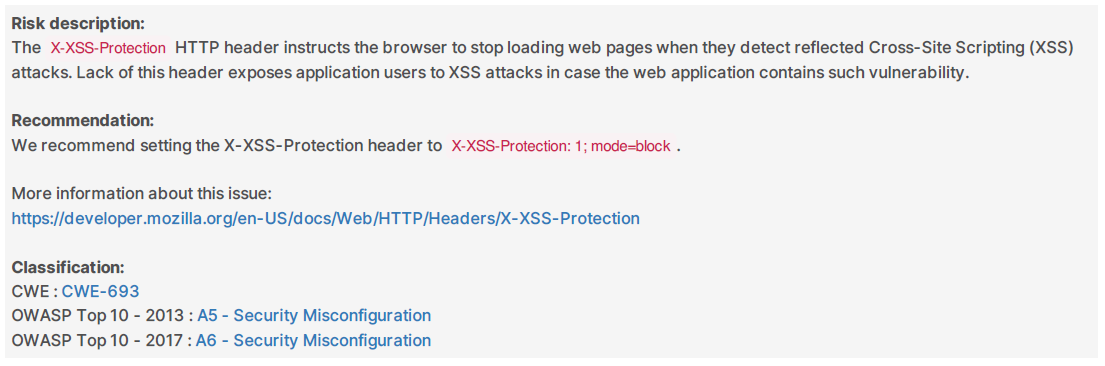
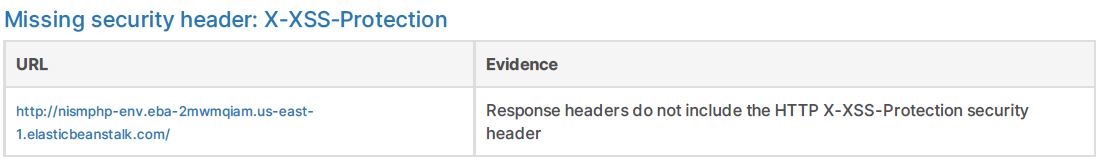


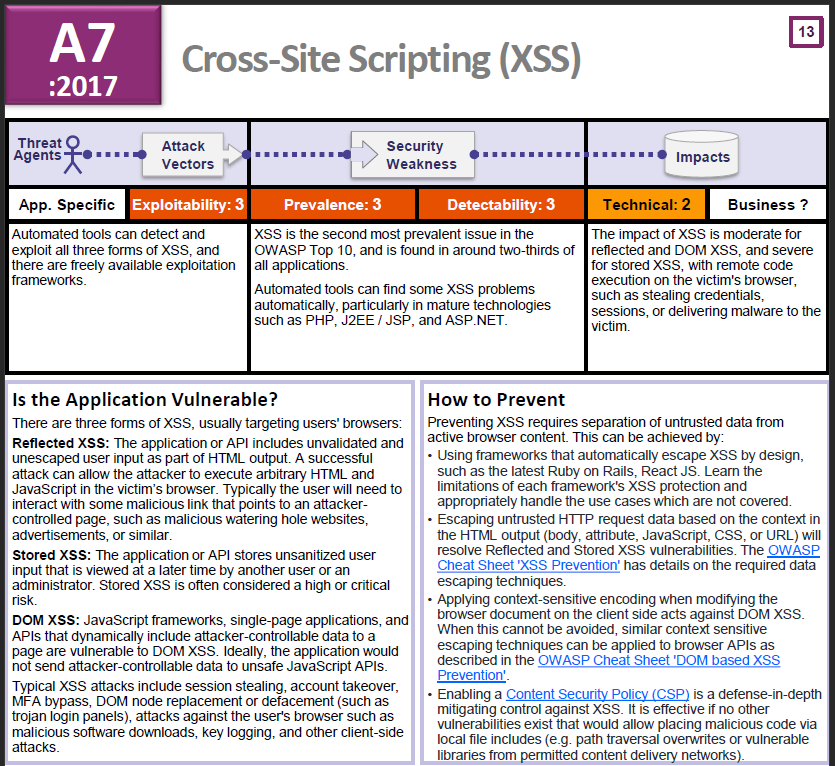
Figure 2 illustrates and details methods that malicious actors can exploit Cross-Site Scripting vulnerabilities.

Figure 2: OWASP A7 Cross-Site Scripting (XSS) (Adapted from (Dehalwar et al., 2018))

Security Misconfiguration

This can include a default account, unpatched or unmaintained server code, references to old versions of services, and so on. Attackers can exploit any security misconfiguration to gain access, elevate privileges, or violate the confidentiality or integrity of the data.

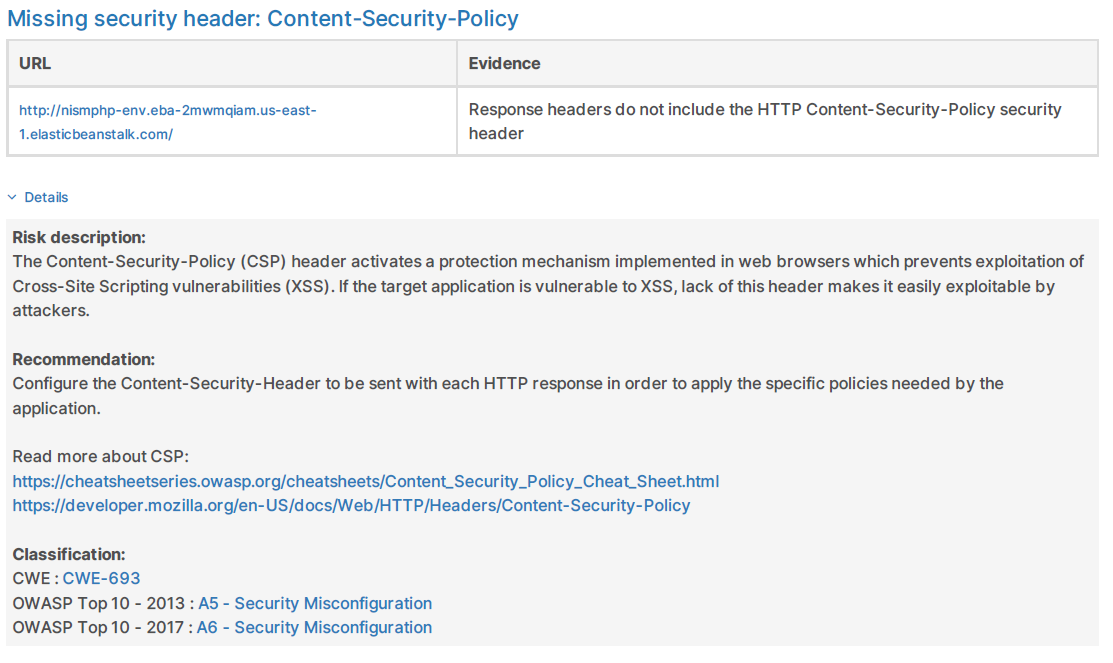


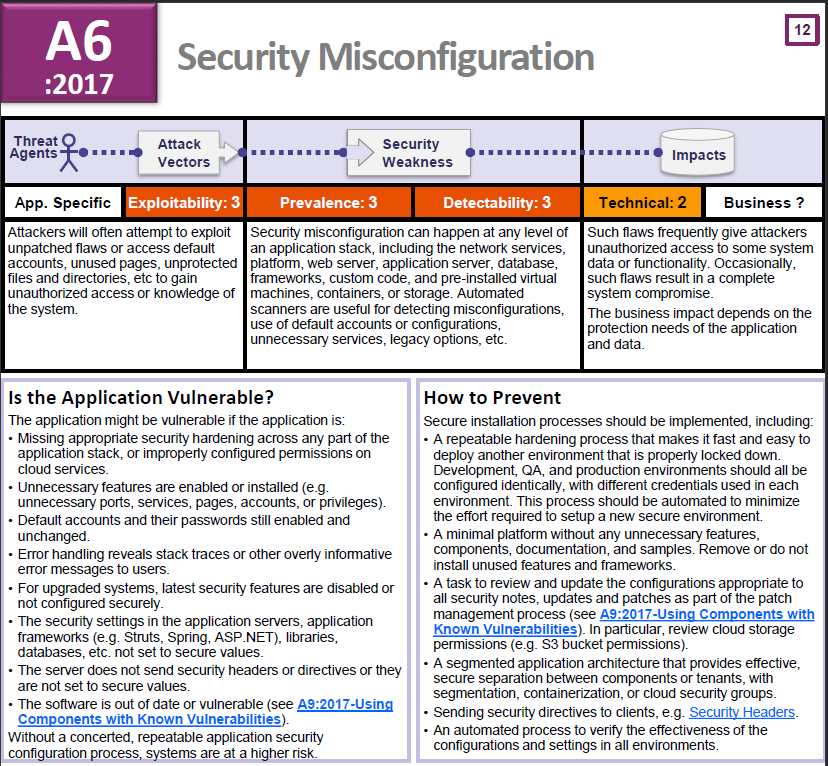
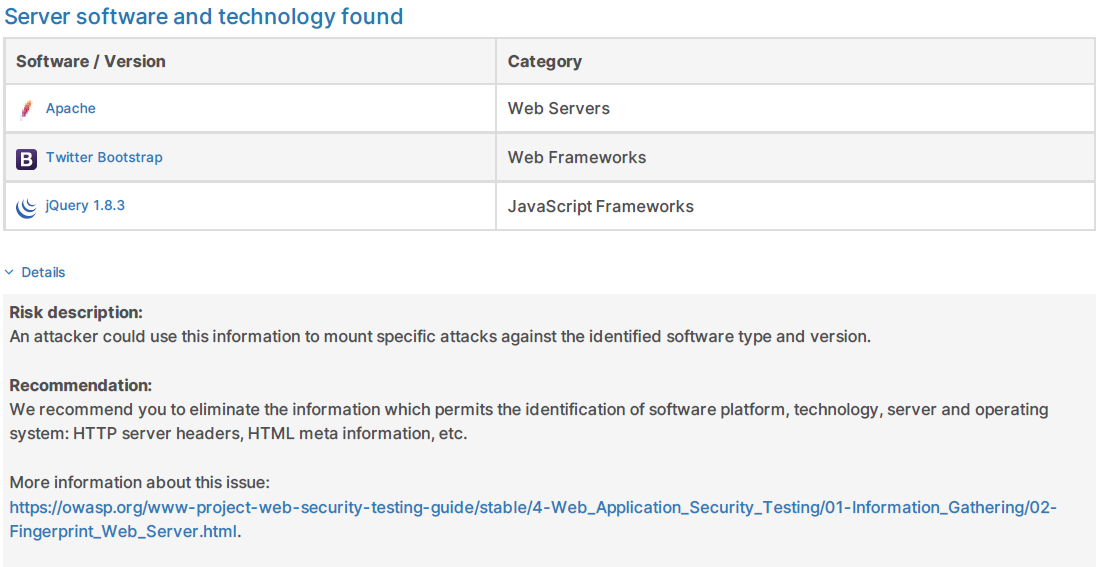
Figure 3 shows some of the causes of security misconfiguration.

Figure 3: OWASP A6 Security Misconfiguration (Adapted from (Dehalwar et al., 2018))

Using Components with Known Vulnerabilities

(ISC) 2, (2006) states that components, such as libraries, frameworks and other software modules, almost run with full privileges. If a vulnerable component is exploited, such an attack can facilitate severe data loss or server takeover. Applications vising components with known vulnerabilities may undermine application defences and enable a range of possible attacks and impacts.



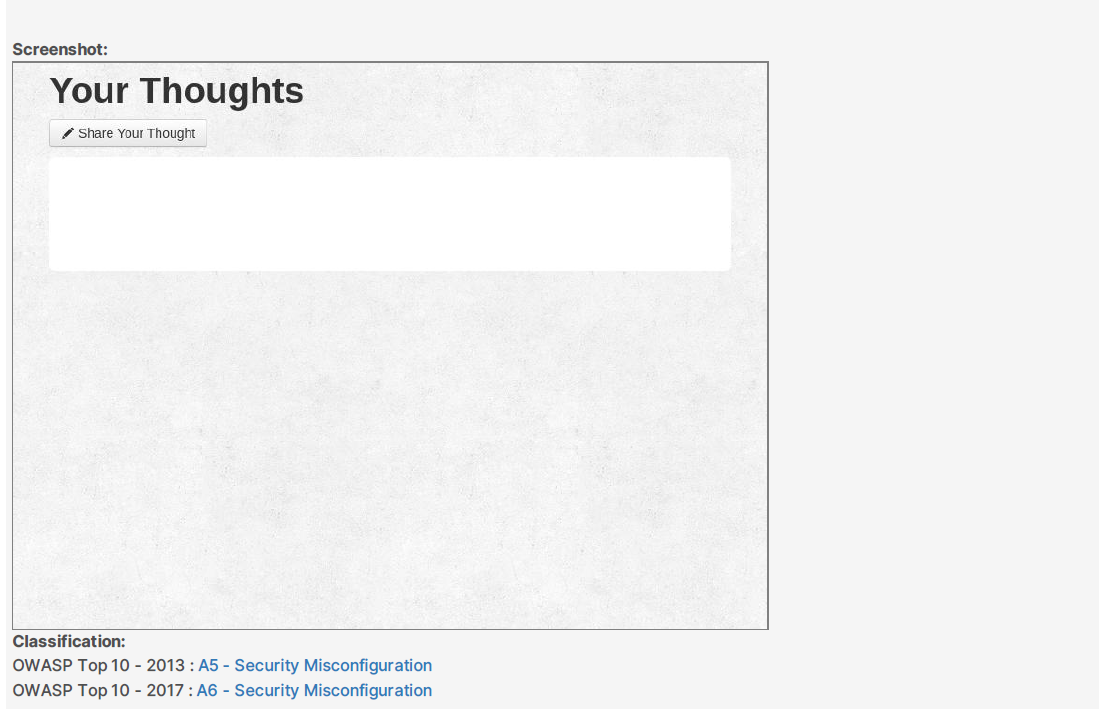


Figure 4 illustrates the need for developers to establish a secure coding framework.

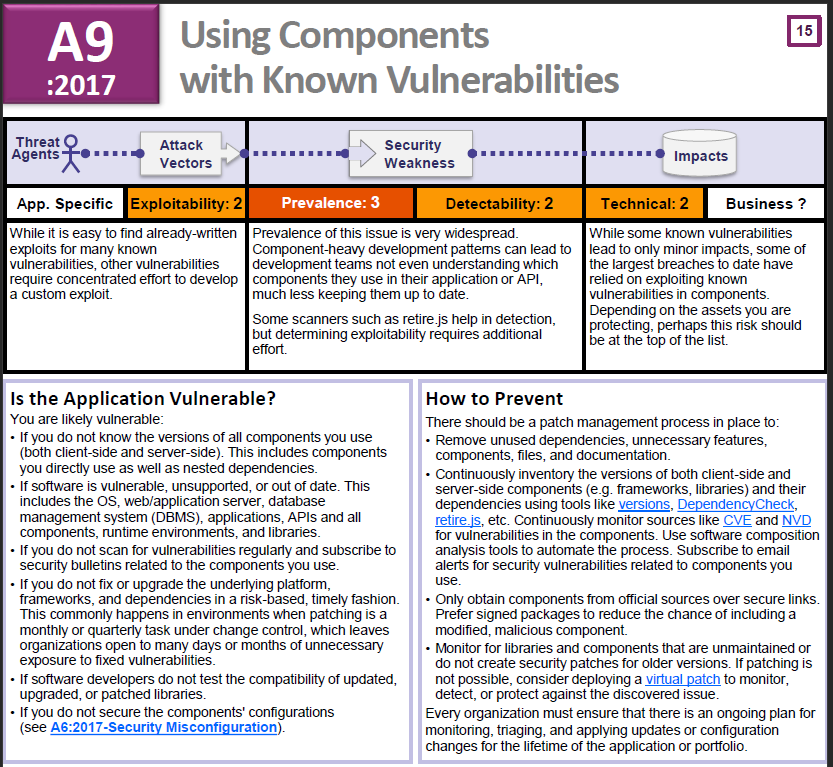


Figure 4: OWASP A9 Using Components with Known Vulnerabilities. ( Adapted from (Dehalwar et al., 2018))

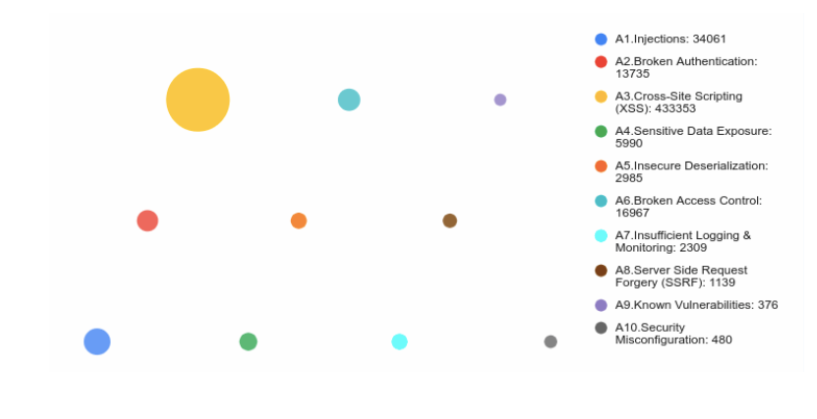
Figure 5 shows the distribution of these categories by amount of security reports, mean bulletins, bug bounties, exploits, altogether:

Figure 5: Distribution of OWAS categories. ( Adapted from (Wallarm, 2021))

**References :**

(ISC) 2 (2006) *What is OWASP Top Ten? - Definition from WhatIs.com*. Available at: https://searchsoftwarequality.techtarget.com/definition/OWASP-Top-Ten [Accessed: 15 July 2021].

Dehalwar, V. *et al.* (2018) ‘Review of web-based information security threats in smart grid’, *2017 7th International Conference on Power Systems, ICPS 2017*, pp. 849–853. doi: 10.1109/ICPES.2017.8387407.

Rosencrance, L. (2018) *What is cross-site scripting (XSS)? - Definition from WhatIs.com*. Available at: https://searchsecurity.techtarget.com/definition/cross-site-scripting [Accessed: 15 July 2021].

Wallarm, I. (2021) *Statistics-Based OWASP Top 10 2021 Proposal - DZone Security*. Available at: https://dzone.com/articles/statistics-based-owasp-top-10-2021-proposal [Accessed: 15 July 2021].

Wesley Chai (2021) *What is the CIA Triad? Definition, Explanation and Examples*. Available at: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA [Accessed: 28 March 2021].