Network and Information Security Management

Team 3 **Executive Summary**

15 February 2022

Team Members

Name	ePortfolio
Andrey Smirnov	https://soundmaven.github.io/e-portfolio/
Michael Justus	https://micjustus.github.io/essex-eport2/
Taylor Edgell	https://tedgell.github.io/MSc-ComputerScience/
Grace Clarke	https://gclarke95.github.io/University/

Document Version History

Version	Date	Author	Details
0.1	07/01/22	Grace Clarke	Document creation
0.2	25/01/22	Taylor Edgell	Restructure and initial scan input
0.3	28/01/22	Taylor Edgell	Arachni and Wapiti scanning information
0.4	30/01/22	Andrey Smirnov	Skipfish and TLSSLed scanning information
0.5	30/01/22	Michael Justus	Nmap scanning information
0.6	01/02/22	Andrey Smirnov	SQLmap scanning information
0.7	02/02/22	Grace Clarke	OWASP Zap information
0.8	05/02/22	Taylor Edgell	Restructure
0.9	08/02/2022	Michael Justus	Review, content updates, CWE links
0.10	09/02/2022	Michael Justus	Additional content update, review and recommendations
0.11	10/02/2022	Taylor Edgell	Additions to vulnerabilities
0.12	10/02/2022	Grace Clarke	Reformatting information; update of vulnerabilities
0.13	11/02/2022	Andrey Smirnov	More additions to vulnerabilities; review
0.14	11/02/2022	Michael Justus	Review, content updates
0.15	11/02/2022	Andrey Smirnov	Proper referencing of materials

1.0	13/02/22	All	The document agreed and signed off for publication to the client

Definitions and Abbreviations

Acronym	Description
CSP	Content Security Policy
DAST	Dynamic Application Security Testing
SQL	Structured Query Language
SSL	Secure Sockets Layer cryptographic protocol
TLS	Transport Layer Security (successor of SSL)
WAVSEP	Web Application Vulnerability Scanner Evaluation Project
XSS	Cross-Site Scripting

Word Count (Excluding titles and captions): 2021

Contents

1. Overview

As mentioned within the Design Document, the analysed website is www.staffmatters.co.uk, which contains an HR management solution called OrangeHRM.

1.1 Threat Analysis Framework – OWASP TOP 10

Figure 1 OWASP Top 10 (2021)

The framework used for analysing OrangeHRM is the OWASP Top 10, a highly regarded framework that helps safeguard against software security vulnerabilities. The Top 10 list is a standardised security awareness document used by the software development industry and several organisations (Sϕhoel et al., 2018). It provides an ordered list of the ten most common and critical security risks applicable to web applications.

2. Considerations

- Individual websites using name-based hosting can only be scanned by tools that allow scans utilising the website's name. This is because all websites share a common hosting system. Tools that monitor by IP address cannot reliably scan our assigned website, for example, Metasploit.
- Tools have primarily been implemented through the installation of Kali Linux. The analysis will not be made into Kali Linux. It is an operating system and not a standalone penetration testing tool.
- The attack surface area of the website is significantly increased compared to private network deployment, given that it is exposed over the public internet.
- The original design document references the 2017 version of the OWASP Top Ten framework, while this executive summary references the 2021 version. The 2017 version is only used for comparison to original theoretical vulnerabilities.

3. Scanning Tools

Name	Overview	Justification	Scope of scan
Arachni – Web application security framework	An opensource automated black-box web application security scanner	• Scans for common vulnerabilities. • Benchmarks very well in comparison of DAST tools (Chen, 2017) • Used in many recent studies (Idrissi et al., 2017).	Scans vulnerabilities such as: • SQL Injection • XSS • Security misconfiguration
Wapiti	An opensource black-box web application scanner	• Noted on OWASP website (OWASP, n.d) • Benchmarks well in comparison of DAST tools (Chen, 2017) • Included within Kali Linux • Easy to use • Considered a recommended tool (Khalil, 2018)	Scans vulnerabilities such as: • SQL injection • XSS • HTTP Security Headers • File disclosure • Bypass of weak “htcaccess” configs
OWASP Zap	An opensource black-box web application scanner	• World’s most widely used web app scanner • Easy to use • Benchmarks well in comparison of DAST tools (Chen, 2017)	Scans vulnerabilities such as: • SQL injection • XSS • Broken Authentication • Sensitive data exposure • Broken Access control • Security misconfiguration • Insecure Deserialisation • Components with known vulnerabilities • Missing security headers
Skipfish	Active web application security reconnaissance tool.	• Respected tool by security researchers (Najera-Gutierrez & Ansari, 2018) • Easy to use	Identifies the following vulnerabilities: • XSS • SQL injection

Name	Overview	Justification	Scope of scan
		• Well documented (Google LLC, N.D.)	• Command injection • XML/XPath injection • Directory traversal and file inclusions • Directory listing
TLSSLed	Linux shell script used for evaluating SSL/TLS implementation	• Specialises in checking HTTPS web server security • Provides comprehensive reports	The tool evaluates: • Support for SSLv2 • NULL cyphers • Weak cyphers • MD5 signatures in digital certificates • Renegotiation capabilities
Nmap	An open-source Linux command-line tool used to scan network IP addresses and ports to detect installed applications.	• Specialises in ports reconnaissance; useful in penetration testing (Shah et al., 2019) • Uses raw IP packets to determine services offered by hosts, operating system info and firewalls.	• Scans for SSL and website certificates • Firewall information • Open ports
SQLmap	An open-source automatic SQL injection and database takeover penetration testing tool	• Effectively finds non-obvious SQL injection vulnerabilities (Ojagbule et al., 2018)	• SQL injection

4. Vulnerabilities

4.1 Overview

Our analysis examined website vulnerabilities according to the 2021 version of the OWASP Top Ten.

4.2 Theoretical Vulnerabilities Comparison

Table 1 Theoretical vulnerabilities for analysis

OWASP 2017 Category	Theoretical Vulnerabilities	Scanned Vulnerabilities
A01 – Injection	• Lack of input validation.	• Buffer overflow
A02 – Broken Authentication	• Weak authentication mechanisms.	• Brute force attacks
A03 – Sensitive Data Exposure	• Insufficient database security. • Poor data backup strategy.	• TLS/SSL vulnerabilities
*A04 – XML External entities**		
A05 – Broken Access Control	• Inadequate access controls that allow access to restricted data by unauthorised users	• Bypass password-protected resources
A06 – Security Misconfiguration	• Lack of proper environmental controls.	• Mixed Content Secure Pages • Vulnerable software
*A07 – Cross-Site Scripting XSS**		
*A08 – Insecure Deserialization**		
A09 – Using components with known vulnerabilities	• Irregular vulnerability upgrades in the hosted environment.	• Vulnerable software

OWASP 2017 Category	Theoretical Vulnerabilities	Scanned Vulnerabilities
*A10 – Insufficient logging and monitoring**		

**Outside scope of the assignment brief*

The noted vulnerabilities cover a wide range from our investigation and use of scanning tools. They are not localised to a particular type, as seen from Figure 2.

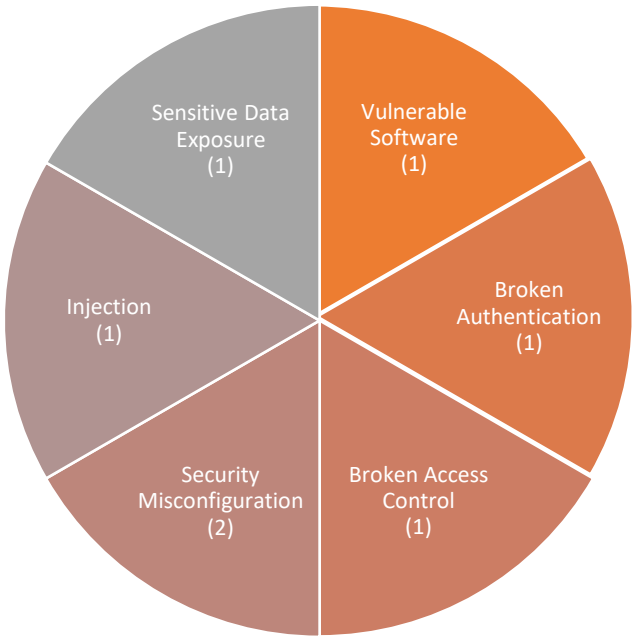

Figure 2 Total count of scanned vulnerabilities

4.3 Broken Access Control

Access control enforces a data access policy to restrict users from acting beyond their assigned permissions. Failures in this regard permit unauthorised disclosure of information and unintended data modifications.

4.3.1 Bypass access controls

The website is protected against unrestricted access since attempts to bypass password-protected resources failed, as discovered by Nmap.

4.3.2 Cross site request forgery (CSRF) (CWE-352)

The website includes checks for CSRF during the login process by having a CSRF token in the login request.

4.3.3 Spoofing attacks (CWE-290)

Archini identified that authentication could be bypassed by spoofing the originating IP address within the HTTP request header.

When scanning software alters (spoofs) its IP address to that of the local host's IP (127.0.01), it receives a positive response to the request, which permits access. The web server believes the request originated from an authorised IP (i.e., localhost), allowing the tool to bypass authentication and access unauthorised information (shown in **Error! Reference source not found.**).

Since this is a surface-level scan, gaining access to private information has not been thoroughly tested.

The authors recommend further testing to confirm this vulnerability's full scope and potential impact.

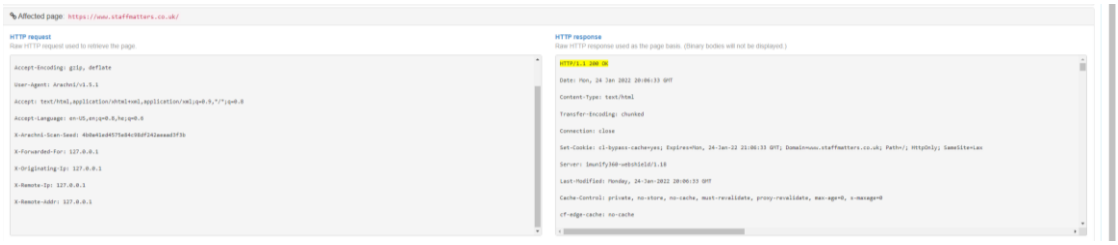

Figure 3 Spoofed response

4.4 Cryptographic Failures

Cryptographic failures relate to the protection of data in transit and at rest. These protections are fundamental in the context of the EU's GDPR.

4.4.1 HTTP redirection to HTTPS

The website redirects standard HTTP requests to secure HTTPS requests by including HSTS headers as found by TLSSLed.

4.4.2 Security certificate

The security certificate is valid and provided by Sectigo (formerly known as COMODO RSA Certification Authority).

4.4.3 Clear text data (CWE-319)

The website uses TLS encryption to secure user data and keep it safe from interception.

4.4.4 Security renegotiation (CVE-2009-3555)

The web server does not support secure renegotiation in the SSL/TLS connections, as reported by TLSSLed.

4.5 Injection

Injection vulnerabilities occur when user-provided information is neither checked nor sanitised, allowing an attacker to relay malicious code to the underlying system. Hostile data can be potentially used to gain unrestricted access to data held by the website.

This is highly important regarding GDPR implications and includes XSS and SQL injection.

4.5.1 SQL injection (CWE-20; CWE-89)

No SQL injection vulnerabilities were uncovered by SQLMap.

4.5.2 External untrusted embedded content

Skipfish found external content embedded in the Symfony PHP web application framework using the HTTP scheme.

4.5.3 Buffer overflow (CWE-119; CWE-680)

Two instances of buffer overflow were found by OWASP ZAP, and a single example was found by Wapiti. All cases related to POST requests (Figure 4) to “openIdCredentials” closed the connection and threw a 500 Internal Server Error. A buffer overflow for credentials could indicate that the website expects a username and password input of a determined length. If input increases in size, the program may write excess data beyond the buffer boundary (Lhee and Chapin, 2003).

This weakness may enable an attacker to insert attack code into the memory space used by the database or the operating system and compromise either or both (Andress, 2011). This raises GDPR concerns, given the wealth of PII stored on the website.

Request

```
POST https://staffmatters.co.uk/symfony/web/index.php/openidauth/openIdCredentials HTTP/1.1
Host: staffmatters.co.uk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Referer: https://staffmatters.co.uk/symfony/web/index.php/auth/login
Content-Length: 2128
Cookie: orangehrm=0193b563fb972e0811368e63fd9c05d4
```

Response

```
HTTP/1.1 500 Internal Server Error
Date: Sun, 23 Jan 2022 13:37:47 GMT
Server: Apache
X-Powered-By: PHP/7.3.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Strict-Transport-Security: max-age=63072000; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

Figure 4 Buffer overflow issues

4.6 Insecure Design

Website analysis was limited to using a black-box approach. Potential vulnerabilities cannot be determined with current scanning tools and visual analysis at this time.

4.7 Security Misconfiguration

This is a broad encompassing vulnerability related to all security configurations of the website and if they are set correctly according to the site's requirements. It should be noted that "we use misconfiguration as the covering term for such (human) errors in the operation of systems" (Dietrich et al., 2018)

4.7.1 No CSP configuration (CWE-300)

Wapiti and OWASP ZAP identified Content Security Policy (CSP) configurations that are currently not set within the website's configuration.

CSP configurations add additional security in HTTP response headers and allow web servers to restrict how resources are loaded by web browsers. It is predominantly adept at preventing cross-site scripting (XSS) attacks.

4.8 Vulnerable and outdated components

Using outdated and unpatched software and components with known vulnerabilities creates exploitable vulnerabilities that can be easily utilised by a malicious party.

4.8.1 Outdated software versions (CWE-1035)

The website was running outdated JQuery components, which was indicated using OWASP ZAP.

The use of third-party JavaScript libraries is commonplace because it allows developers to access functions that otherwise would take time and effort to set up themselves (Elizalde Zapata et al., 2018). A GET request identified that the library jQuery (version 3.4.1) is vulnerable.

Request

```
GET https://staffmatters.co.uk/symfony/web/webres_6051af48107ce6.31500353/js/jquery/jquery-3.4.1.min.js HTTP/1.1
Host: staffmatters.co.uk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Pragma: no-cache
Cache-Control: no-cache
Referer: https://staffmatters.co.uk/symfony/web/index.php/auth/login
Cookie: orangehrm=0193b563fb972e0811368e63fd9c05d4
```

Response

```
HTTP/1.1 200 OK
Date: Sun, 23 Jan 2022 12:03:36 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Last-Modified: Wed, 17 Mar 2021 17:57:16 GMT
ETag: "4950752-15851-5bdbf3699b700"
Accept-Ranges: bytes
Content-Length: 88145
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: max-age=604800, public
Content-Type: application/javascript
```

Figure 5 Request/Resposnse for outdated software issues

4.9 Identification and Authentication Failures

These vulnerabilities refer to insufficient or weak measures to authenticate users and confirm their identity to access resources and, if permitted, whether specific actions can be performed.

4.9.1 Permits brute force attacks (CWE-307)

The website permits an unlimited number of password attempts which leaves it susceptible to automated and brute force attacks.

4.9.2 Does not have multi-factor authentication (CWE-308)

The website does not support multi-factor authentication, leaving brute force attacks the main weak point to gain entry.

4.9.3 Password rules (CWE-521)

The website has implemented rules to limit a new password that can be set. This prevents easily guessable passwords from becoming a weak point of the website.

Examples of password rules that have been selected are the requirement on length, capital letters, numbers and symbols. One disadvantage is a non-specific message regarding password input requirements. Although not a vulnerability, it is detrimental to a user's experience.

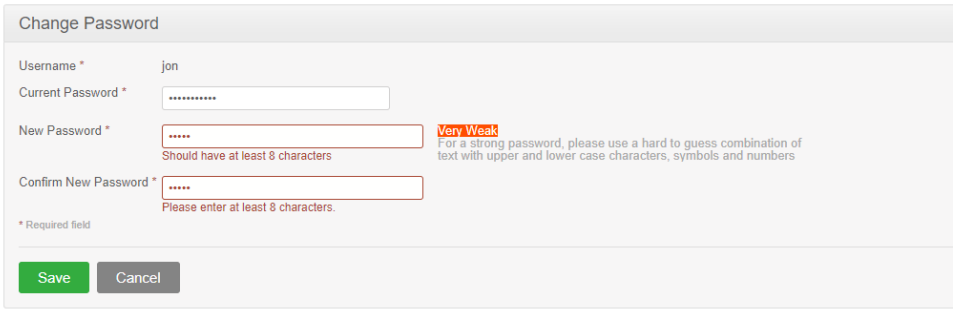

Figure 6 Create a new password

4.10 Software and Data Integrity Failures

Software and data integrity failures can be based around an application's use of plugins, libraries, or modules from untrusted sources and repositories.

It is difficult to confirm the scope of related issues through the methodology and limitations set out within this document. An in-depth look at the undelaying system and its dependencies is required to correctly define associated vulnerabilities.

Known vulnerabilities of the current version of OrangeHRM seem to be minimal (CVE Details, ND).

4.11 Security Logging and Monitoring Failures

Detecting and rectifying security errors and vulnerabilities is critical to all applications. Therefore, monitoring and logging such instance increases the visibility of issues and prevents the reoccurrence of future problems. Logging also helps maintain accountability for security.

Potential vulnerabilities regarding logging cannot be determined with external scanning tools or visual analysis at this time. Analysis of the system's internals is required.

4.12 Server-side Request Forgery

These vulnerabilities occur "where the vulnerable web application redirects the attacker's requests to the internal network and exposes local services to the remote attacker" (Jabiyev et al., 2021). This happens as the user-supplied is not validated.

4.12.1 Firewall settings

Analysis of the firewall used by OrangeHRM, namely Imunify360, indicates that a "Deny by Default" policy is in place. This policy permits only required traffic to the site.

4.12.2 SSL certificate hostname mismatch (CWE-295; CWE-297)

Skipfish uncovered an SSL certificate hostname mismatch problem when analysing the host. This is a common error due to incorrect server settings or wrong information provided when purchasing an SSL certificate.

4.13 Interesting Findings

4.13.1 Uncommon security codes

Arachni indicated a unique security code in response to an HTTP TRACE request due to further investigation.

Examining the response code 405 (Not allowed) indicates that TRACE responses have been disabled by the webserver. This is standard security practice and was not indicative of any error.

4.13.2 POODLE and QualSys TLS

1. Since the website supports TLS version 1.2 and 1.3, it is not vulnerable to the Padding Oracle on Downgraded Legacy Encryption (POODLE) vulnerability which targets the older SSL 3.0 protocol (Möller et al., 2014).
2. The cyphers are rated “A”, which follows the QualSys SSL Rating Guide (QualSys, 2021) and provides a simple guide that all cyphers are good.

5. Conclusion, Recommendations, Mitigations

5.1 Recommendations to Vulnerabilities

All vulnerabilities are listed in order of business priority.

Table 2 Summarised vulnerabilities found

Priority	Vulnerability	Recommendation
1	Lack of multi-factor authentication	• Follow best practice to combine multiple sources of authentication (Jensen et al., 2021)
2	Weak password policy	• Enact limit on number of password and username attempts
3	Outdated components	• Update Symfony to the latest stable version (6.0.4) • Update jQuery to the latest stable version (3.6.0)
4	Buffer overflow	• Enforce checks on input lengths. • Utilise libraries that implement safe, bounds-checked buffers (Kothari, 2005).
5	IP Spoofing	• Validate the client's user-agent and IP combination on each page load. • Renew session ID tokens at regular intervals to minimise hijacking.
6	Incorrect content security policy	• Correctly set all CSP configurations, such as "`Content-Security-Policy: policy`"
7	Unsupported secure renegotiation	• Update Apache web server configuration to enable SSL/TLS secure renegotiation.
8	Mixed content pages	• Embed external content via the HTTPS scheme.

5.2 GDPR Considerations

There are various aspects of the area applicable to GDPR, and should be noted:

- Strict internal document management policies must be in place to complement digital protections (Pearlgood, 2014; Ojediran, 2015).

- As the website handles confidential data, all vulnerabilities must be addressed to protect personnel data.
- Only relevant data should be obtained, and all information outside the scope of requirements must be discarded.
- Recommend utilising the ICO checklist to ensure GDPR is upheld (ICO, 2020).

5.3 Conclusion

Overall, the website is secure, with only minor or negligible vulnerabilities detected throughout our inspection. The recommendations provided will further increase website security to enable the HRM system to better adhere to GDPR and HR data security regulations.

Word Count (Excluding titles and captions): 2021

References

Andress, J. (2011). *The Basics of Information Security*: *Understanding the Fundamentals of InfoSec in Theory and Practice.* 2nd ed. Syngress.

Chen, S. (2017) Evaluation of Web Application Vulnerability Scanners in Modern Pentest/SSDLC Usage Scenarios. Available from: https://www.ukessays.com/essays/computer-science/evaluation-of-web-vulnerability-scanners-based-on-owasp-benchmark.php [Accessed 11 February 2022].

CVE Details (N.D.) OrangeHRM. Available from: https://www.cvedetails.com/vulnerability-list/vendor_id-6180/Orangehrm.html [Accessed 10 February 2022].

Decan, A., Mens, T. & Constantinou, E. (2018) 'On the impact of security vulnerabilities in the npm package dependency network', *2018 IEEE/ACM 15th International Conference on Mining Software Repositories (MSR)*. Gothenburg, 27 May-3 June. New York: IEEE. 181-191.

Dietrich, C., Krombholz, K., Borgolte, K. & Fiebig, T. (2018) 'Investigating system operators' perspective on security misconfigurations', *CCS ACM Conference on Computer and Communications Security*. Toronto, 15-19 October. New York: ACM. 1272-1289.

Google LLC (N.D.) skipfish - web application security scanner. Available from: https://code.google.com/archive/p/skipfish/wikis/SkipfishDoc.wiki [Accessed 30th January 2022].

ICO (2020) Guide to the General Data Protection Regulation (GDPR).

Idrissi, S., Berbiche, N., Guerouate, F. & Shibi, M. (2017) Performance evaluation of web application security scanners for prevention and protection against vulnerabilities. *International Journal of Applied Engineering Research* 12(21): 11068-11076.

Jabiyev, B., Mirzaei, O., Kharraz, A. & Kirda, E. (2021) 'Preventing server-side request forgery attacks', *36th Annual ACM Symposium on Applied Computing*. Virtual, 25-29 April. New York: ACM. 1626-1635.

Jackson, C. & Barth, A. (2008) 'Forcehttps: protecting high-security web sites from network attacks', *17th international conference on World Wide Web*. Beijing, 21-25 April. New York: ACM. 525-534.

Jensen, K., Tazi, F. & Das, S. (2021) 'Multi-Factor Authentication Application Assessment: Risk Assessment of Expert-Recommended MFA Mobile Applications', *Who Are You?! Adventures in Authentication Workshop (WAY)*. Virtual. Available from: https://ssrn.com/abstract=3878387 [Accessed 11 February 2022].

Khalil, R. (2018) Why Johnny Still Can't Pentest: A Comparative Analysis of Open-source Black-box Web Vulnerability Scanners. Available from: https://ruor.uottawa.ca/handle/10393/38595 [Accessed 11 February 2022].

Kothari, J., (2005) Network Security and Cryptography Summer 2005 Buffer/Stack Overflow: Mechanisms and Prevention Methods.

Lhee, K. & Chapin, S (2003) Buffer overflow and format string overflow vulnerabilities. *Software: Practice and Experience* 33(5): 423-460.

Makino, Y. & Klyuev, V. (2015) 'Evaluation of web vulnerability scanners', *8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*: 399-402. DOI: 10.1109/IDAACS.2015.7340766.

Möller, B., Duong, T. & Kotowicz, K. (2014) This POODLE bites: exploiting the SSL 3.0 fallback. *Security Advisory* (21): 34-58.

Najera-Gutierrez, G. & Ansari, J. (2018) Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux. 3rd Ed. Packt Publishing.

Ojagbule, O., Wimmer, H. & Haddad, R. (2018) 'Vulnerability Analysis of Content Management Systems to SQL Injection Using SQLMAP', *SoutheastCon 2018*. St. Petersburg, 19-22 April. New York: IEEE. 1-7.

Ojediran, S. (2015). Confidential Waste Service: A business case. Available from https://committee.nottinghamcity.gov.uk/documents/s49886/Business%20Case%20-%20CW.pdf [Accessed 13 Feb. 2021]

OWASP Foundation (N.D.) Automated Audit using WAPITI. Available from: https://owasp.org/www-community/Automated_Audit_using_WAPITI [Accessed 25 January 2022].

OWASP Foundation (N.D.) Buffer Overflow Attack. Available from: https://owasp.org/www-community/attacks/Buffer_overflow_attack [Accessed 11 February 2022].

Pearlgood, A. (2014). Document protection–whatever the weather. Computer Fraud & Security, 2014(6):19-20.

QualSys Inc. (2021) SSL Rating Guide. Available from: https://www.ssllabs.com/projects/rating-guide/ [Accessed 30 January 2022].

Sϕhoel, H., Jaatun, M. & Boyd, C. (2018) 'OWASP Top 10-Do Startups Care?', *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. Glasgow, 11-12 June. New York: IEEE. 1-8.

Shah, M., Ahmed, S., Saeed, K., Junaid, M. & Khan, H. (2019). 'Penetration testing active reconnaissance phase–optimised port scanning with nmap tool', *2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*. Sukkur, 30-31 January. New York: IEEE. 1-6.

Zapata, E., Kula, R., Chinthanet, R., Ishio, B., Matsumoto, T. & Ihara, A. (2018) 'Towards Smoother Library Migrations: A Look at Vulnerable Dependency Migrations at Function Level for npm JavaScript Packages', *2018 IEEE International Conference on Software Maintenance and Evolution (ICSME)*. Madrid, 23-29 September. New York: IEEE. 559-563.