

An Executive Summary for the Penetration Testing of a Customer Management System

Network and Information Security Management

MSc Cyber Security

Group Three

Beran Necat

University of Essex

23 May 2022

Table of Contents

INTRODUCTION.....	3
METHODOLOGY.....	4
SUMMARY FINDINGS.....	5
DISCUSSION	11
RECOMMENDATIONS.....	13
CONCLUSION	15
REFERENCES.....	16
APPENDICES	20

Introduction

Team three's Design Document (Ahmed et. al., 2022) which included the website's appropriate governing bodies and associated regulations such as General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI-DSS) and ISO 27000 was created prior to this Executive Summary. This document also addressed some of the possible vulnerabilities the website had, and a list of recommendations for mitigating those vulnerabilities.

As mentioned in the Design Document, businesses do benefit from Customer Relationship Management platforms (CRM), especially small ones (McNeice, 2021), as it helps boost sales and profits (DAAS Suite, 2022). However, within the virtual world, everything is followed by possible vulnerabilities and potential threats, and so a step further had to be made for keeping the website secure and safe from potential threats.

Upon the completion of the design document on the customer relationship management (CRM) website, www.customersrus.co.uk, penetration testing was conducted using relevant Kali Linux and online tools. This Executive Summary outlines the scope of the agreed penetration test, addresses the vulnerabilities found, includes recommendations and suggestions for the vulnerabilities' mitigation and compares the results from the design document, which were based on assumptions on the results of this executive summary and consequently discovered by penetration testing. The summary will also discuss why expected vulnerabilities were not detected when testing.

Methodology

To scan for vulnerabilities, the OWASP web security testing guide (2022a) outlined penetration testing methodologies such as the Penetration Testing Execution Standard (PTES) as featured in Table 1.

For quantitative purposes, this assessment uses two vulnerability grading systems: OWASP ZAP and Risk Rating Calculator. The OWASP ZAP shows a standardised level according to severity of the vulnerability, and the OWASP Risk Rating Calculator presents a score in relation to the risk for the business's website. For example, the level of impact a vulnerability would have on a CRM website: reputational loss. According to OWASP (2022b), the risk rating calculator allows for the organisation to customise the framework to suit their security needs against the vulnerabilities from the OWASP ZAP scan.

Penetration Testing Execution Standard
Pre-engagement activities
Intelligence gathering
Threat Modelling
Vulnerability Analysis
Exploitation
Post-Exploitation
Reporting

Table 1: OWASP penetration testing framework.

Summary Findings

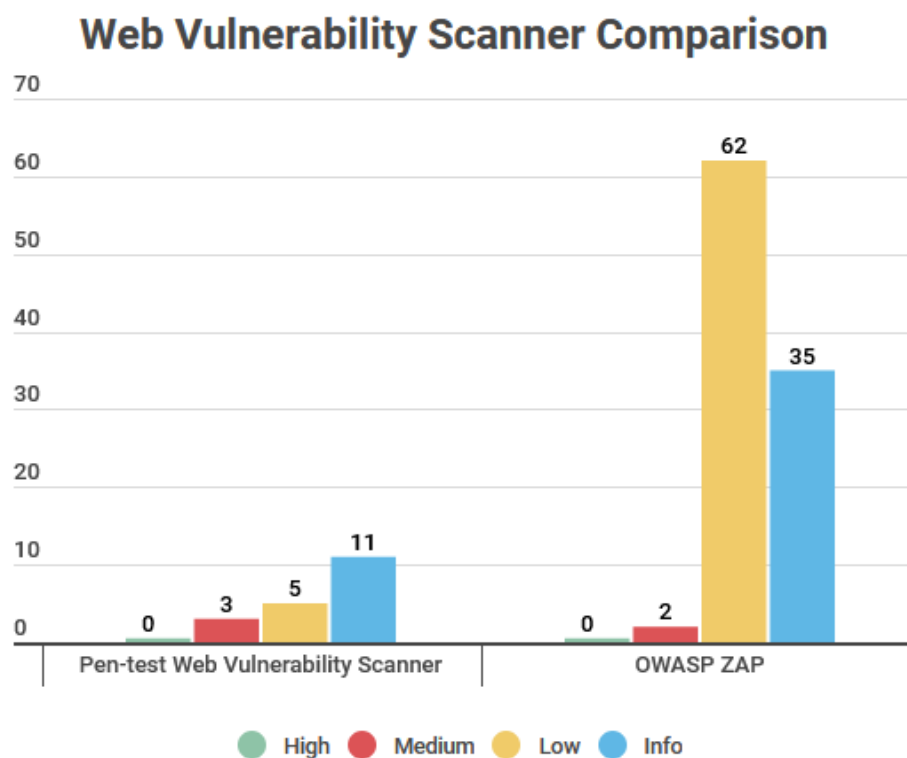
This section examines the results from the various vulnerability scanning tools via online websites and Kali Linux (see Table 2). The tools were selected for user-friendliness, ease-of-use, and availability, technical ability; security concerns, and licensing issues namely Nessus and OpenVAS which require a purchase for a feature-rich product (Amankwah et al, 2020; OWASP, 2022c). Each tool has strengths and weaknesses, and it is hoped that they will complement each other due to their different algorithms and processes (OWASP, 2022c).

Tool	Online	Kali Linux
Nmap		X
CMS Scanner	X	
OWASP ZAP		X
DNS Checker	X	
OpenVAS (light)	X	
Pen-test tools network vulnerability scanner (light)	X	
Pen-test tools SSL/TLS vulnerability scanner (light)	X	
Pen-test tools website vulnerability scanner	X	
Shodan	X	
Waf00f		X
Nikto		X

Table 2: Tools and platforms.

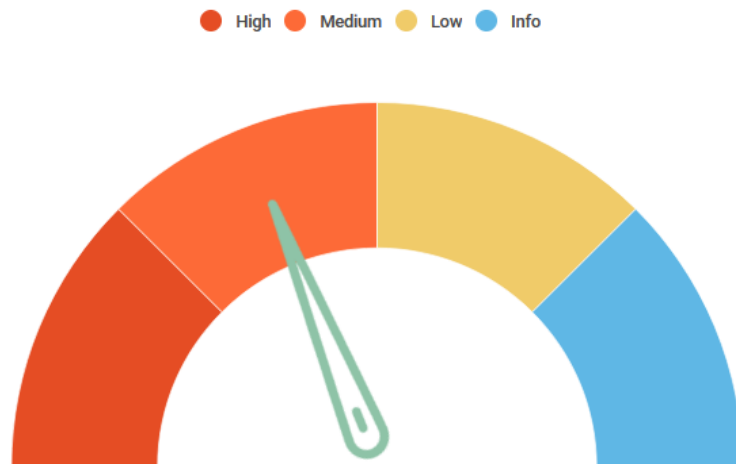
Two website vulnerability scanners were used to compare results; OWASP ZAP was used on Kali Linux and the online vulnerability scanner was used on the Pen-test website. It is worth noting ZAP produced a more in-depth assessment of the website than Pen-test. This can be attributed to the free light version on the Pen-test website which was used in this project. Nevertheless, the results discovered the same vulnerabilities with similar assessed risk; however, ZAP produced more low and informational results (see Graph 1 and Appendix A).

The main issues found were outdated software, privilege abuse, and information leakage culminating in an overall risk assessment of Medium (see Graph 2).



Graph 1: A comparison of two website vulnerability scanners.

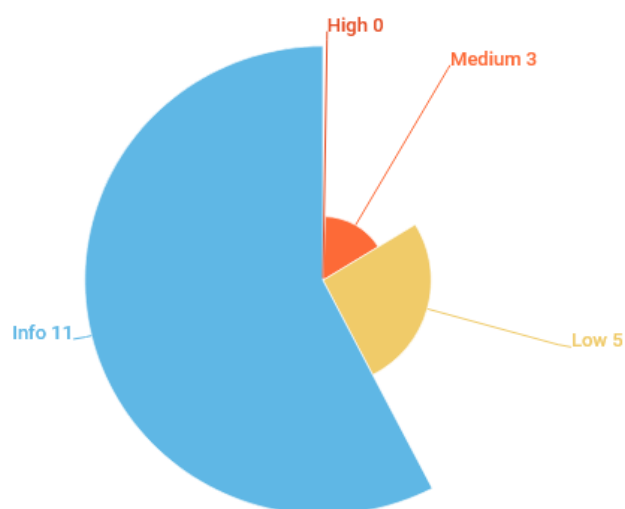
Overall Vulnerability Risk Assessment



Graph 2: Overall risk assessment summary for the website.

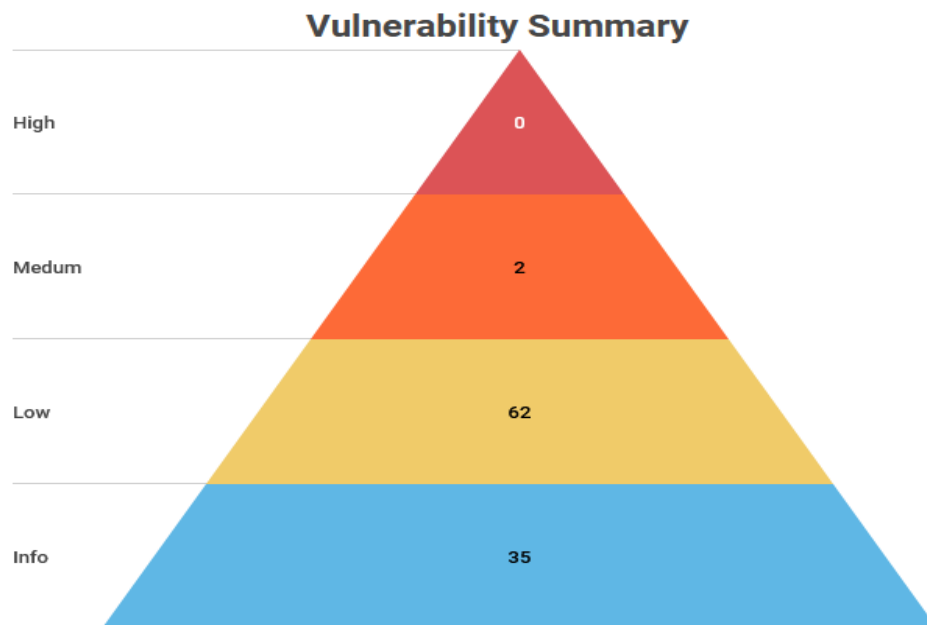
Pen-test website scanner found three medium and five low risk vulnerabilities (see Graph 3).

Vulnerability Summary



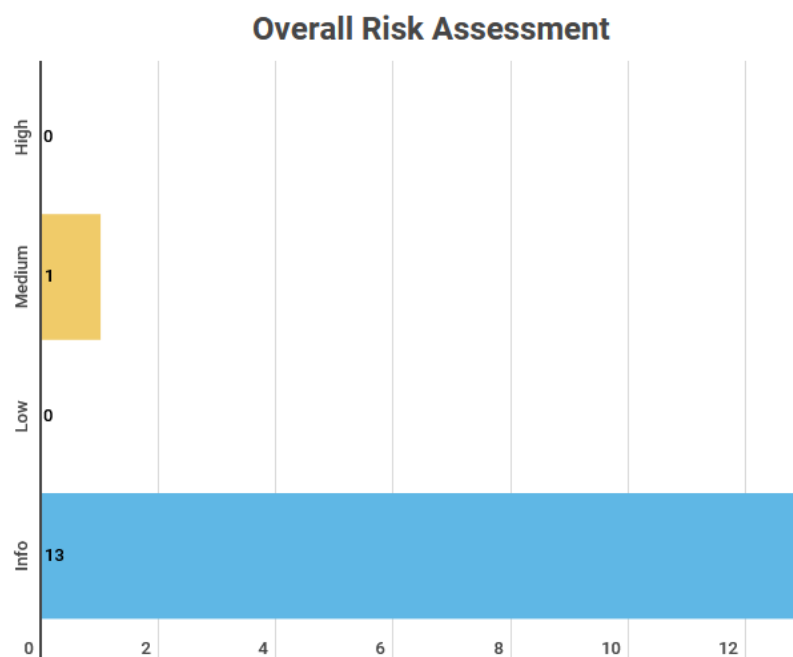
Graph 3: Pen-test website vulnerability scan results.

Graph 4 shows two medium and sixty-two low risk vulnerabilities by ZAPProxy web vulnerability scanner.



Graph 4: OWASP ZAP website vulnerability scan results.

Pen-test network vulnerability scanner found one medium risk network vulnerability which can be divided into ten associated risks (see Graph 5 and Appendix B).



Graph 5: Pen-test network vulnerability scan results.

Table 3 lists vulnerabilities by rank according to two assessments of the website. The risk column shows the level according to severity of the vulnerability, and the Business Critical column presents a grade in relation to the risk for the business.

Rank	Vulnerability	Risk	Business Critical
1	Vulnerable JS Library	Medium	6.25/ High
2	Vulnerable ISC BIND 9.11.4-p2 (port 53/tcp)	Medium	6.23/ High
3	Absence of Anti-CSRF Tokens	Low	5.75/ Medium
4	Cookie No HTTP Flag	Low	5.75/ Medium
5	Cookie Without Secure Flag	Low	5.75/ Medium
6	Cookie without SameSite Attribute	Low	5.75/ Medium
7	Incomplete or No Cache-control Header Set	Low	4.25/ Medium
8	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	2.75/ Low
9	Timestamp Disclosure - Unix	Low	2.75/ Low

10	Robots.txt File Found	Low	2/ Low
-----------	------------------------------	------------	-------------------

Table 3: Vulnerabilities ranked according to risk and business critical severity.

In Table 4, it seems all the associated software for the CRM website is outdated with the biggest vulnerability being jQuery which was released in 2011 according to their changelog (Methvin, 2011).

Software	Outdated Version	Current Version
PHP	7.3.33	8.0.18
YUI	2.9.0	3.18.1 (deprecated 2014)
jQuery UI	1.8.16	1.13.1
jQuery	1.7.1	3.6.0

Table 4: Website's outdated and current software versions.

Both Shodan and Nmap found multiple ports open; however, Table 5 highlights a *light* Pen-test web-based SSL/TLS vulnerability scan which returned no issues on port 443/HTTPS (see Appendix E, F, G). A more robust scan is needed to explore potential port vulnerabilities.

Port	State	Service	Vulnerability
443/tcp	Open	HTTPS	None

Table 5: Port 443 SSL/TLS vulnerability scan.

Nikto and Wafw00f scans both returned results indicating Web Application Firewall (WAF): Immunify360-webshield, which helps protect against CCSF, XSS, and SQL injection (see Appendices H and I).

Discussion

The Design Document (Ahmad et. al, 2022) mentioned five theoretical vulnerabilities namely an outdated jQuery, a discontinued SugarCRM edition, a shared hosting platform, possible use of weak passwords due to the uncertainties around the Cpanel, and an issue with exposed links before login. Table 3 represents the vulnerabilities found from the scans.

The two most risky vulnerabilities are the outdated jQuery and the ISC BIND 9.11.4-p2. The website uses an outdated version, while the current one is v1.7.1. There is potential for exploitation of Cross-site scripting (XSS) as vulnerable versions use the '<' symbol which can be anywhere in the HTML string. This could cause leakage of personal and financial data. ISC BIND 9.11.4-p2 and port 53 has ten vulnerabilities: a uniquely crafted packet can cause named memory to leak unlimited simultaneous tcp clients (CyberSecurityHelp, 2022).

Lower risk vulnerabilities such as the absence of Anti-CSRF tokens were found. This forces the victim to send HTTP requests to a target destination and their credentials being used without their knowledge (OWASP, 2022d). The threat of further information disclosure is amplified if the site is vulnerable to XSS (OWASP, 2021a). Incomplete or no cache-control header set vulnerability allows proxies and browsers to cache content, while the vulnerability of the server leaking information can allow attackers to identify web application vulnerabilities (PortSwigger, 2022a).

Vulnerabilities such as Timestamp Disclosure could be used to retrieve sensitive information involved in password authentication and encryption tokens (eCyLabs,

2022), whereas a robots.txt file could be used to find hidden websites (PortSwigger, 2022b). Three vulnerabilities on cookies were also found.

Cookies with no HTTP Flag can cause a user's session cookie to be vulnerable to modification or theft by a malicious script, whereas cookies without secure flag and SameSite attribute could be accessed by unencrypted connections, and the cookie is susceptible to CSRF, cross-site script (XSS) inclusion, and timing attacks, respectively (CWE, 2022).

There is no cookie or consent notification when accessing the customersrus.co.uk website (see Appendix C) which according to the Information Commissioner's Office (2019) contravenes the UK GDPR Standard of Consent and the Data Protection Act 2018 (DPA) Legal Basis and Consent (2022). See Appendix D for a comparison example of another CRM website, Salesforce.com, showing a cookie notification (Salesforce, 2022). Below is an abridged outline of the aforementioned regulations related to cookie notifications.

GDPR:

- Update your consent if they do not meet the UK GDPR standard.
- Consent requires a positive opt-in.
- Be clear, concise, and specific.

(ICO, 2019)

DPA:

- Businesses must identify and publish their legal basis for processing data or consent in a legal and valid manner (ICO, 2022).

Some theoretical vulnerabilities from the design document (Ahmad et. al., 2022) were not detected. This could be due to using the light versions of some tools instead of the paid versions, meaning there were less features available for scanning. An example is the password auditor provided by the pentest tools, which is only available when purchasing a licence (Pentest Tools, 2022). Exposed links such as Employees and About were an observation rather than a result of a vulnerability scanner, and it is recommended to be available upon logging in.

Recommendations

Based on the vulnerability findings (see Table 2), recommendations were researched to mitigate potential and future threats. Addressing the medium risk vulnerabilities first, it is initially recommended for JS libraries to be kept up-to-date and to use the latest version for patches on previous ones. External library servers are not recommended but copying JS libraries to website's servers that need them is. This ensures identical availability and reliability of the JS libraries to those of the website, and independence from third parties (Internet Security Scan, 2022). In addition, the ISC BIND 9.11.4-p2 version introduced multiple vulnerabilities. To guarantee previous vulnerabilities are patched, it is suggested that the ISC BIND is also kept up-to-date regularly (CyberSecurityHelp, 2022).

For the lower risk vulnerabilities, mitigating CSRF attacks requires mechanisms which verify a requester's identity and authority. Therefore, if the website's framework includes built-in CSRF protection, it is strongly recommended that one

properly configures it (OWASP, 2021a). Another practice is sending separate confirmation requests when identifying a user's complex operation (CWE, 2022). The theft of session cookies is targeted by most XSS attacks. Setting up the HttpOnly flag on a cookie a server creates, should prevent it from being accessible to the user (OWASP, 2022d). Although some cookies are available to the user, Secure Flag ensures that these are only accessible over secure SSL/TLS channels, which is important, security-wise, to set it for session cookies if possible (Acunetix, 2022). To prevent CSRF, XSS inclusion, and timing attacks, it is suggested SameSite attribute is set to 'lax' or 'strict' ideally for all cookies, since without it there is a chance of a cookie being sent due to a cross-site request (IBM, 2022; ZAPProxy, 2022a).

Websites are bound to use restrictive cache directives for all web traffic HTTP and HTTPS exchanges, one of them being Cache-Control header. Even though a session has been closed, exchanged private/sensitive data can still be accessible within that session through cache (OWASP, 2021b). In addition, the access to leaking information may help attackers identify other vulnerabilities. To prevent the site from leaking information, web and application servers, load balancer, etcetera must be configured to suppress "X-Powered-By" headers (ZAPProxy, 2022b).

Timestamp disclosure can be used for retrieving information such as salt or token during authentication or encryption. One way of mitigating this is manual evaluation and confirmation of the timestamp data not being sensitive and that it cannot be aggregated to reveal vulnerable patterns (eCyLabs, 2022; ZAPProxy, 2022c). Lastly, having a robots.txt file does not necessarily raise a vulnerability unless it is used incorrectly. However, it is often used for identifying a site's contents in restricted/private areas. Although a correct use of robots.txt file may represent good practice, attackers will not honour the file's instructions and will search for identified

locations in the file. It is recommended to not rely on these files for security protection (PortSwigger, 2022b).

Conclusion

This Executive Summary investigates the www.customersrus.co.uk website to ascertain for any vulnerabilities which could be exploited on a web and network level by threat actors. The OWASP Penetration Testing Execution Standard was used as a framework to guide the vulnerability testing using Kali Linux and free-to-use website tools namely OWASP ZAP.

The scanning results show there are multiple low and medium risk vulnerabilities; however, consideration should be given to the recommendations outlined to secure the website. Although this testing did not exploit any of the vulnerabilities in the form of personal and/or financial data, regular checks for software updates are strongly recommended, as the current versions offer patches on vulnerabilities found in former and outdated versions. For complete GDPR, ISO 27000 and PCI-DSS compliance, implementation of a cookie notification should be considered.

Consistency with appropriate governing bodies and regulations applying to a CRM website carries the same weight of importance as investing in strong cybersecurity systems, as lacking both could lead to reputational and financial damage (Taylor, 2022).

References

- Acunetix. (2022) Cookies without Secure flag set. Available from:
<https://www.acunetix.com/vulnerabilities/web/cookies-without-secure-flag-set/>
[Accessed 3 May 2022].
- Ahmed, A., Ashmore, J., Klacar, A., Pal, A. & Sodaba, T. V. (2022) Team three's Design Document, 18 April 2022.
- Amankwah, R., Chen, J., Kudjo, P.K. and Towey, D. (2020) An empirical comparison of commercial and open-source web vulnerability scanners. *Software: Practice and experience*, 50(9), pp.1842–1857. doi:10.1002/spe.2870.
- Common Weakness Enumeration (CWE). (2022) Cross-Site Request Forgery (CSRF). Available from: <http://cwe.mitre.org/data/definitions/352.html> [Accessed 3 May 2022].
- CyberSecurityHelp. (2022) Multiple Vulnerabilities in ISC BIND. Available from:
<https://www.cybersecurity-help.cz/vdb/SB2022031701> [Accessed 3 May 2022].
- DAAS Suite. (2022) 5 Major Reasons to Invest in CRM. Available from:
<https://daassuite.com/blog/en/reasons-invest-crm/> [Accessed 9 May 2022].
- eCyLabs. (2022) What Happens If Timestamp Gets Disclosed?. Available from:
<https://ecylabs.com/blog/2021/06/21/what-happens-if-timestamp-gets-disclosed/>
[Accessed 3 May 2022].
- GitHub. (2021) wstg/document at master · OWASP/wstg. Available from:
<https://github.com/OWASP/wstg/tree/master/document> [Accessed 16 May 2022].

IBM. (2022) Vulnerability: Cookie without SameSite attribute. Available from: <https://www.ibm.com/docs/en/cdfsp/7.6.1.x?topic=checklist-vulnerability-cookie-without-samesite-attribute> [Accessed 3 May 2022].

Information Commissioner's Office (ICO). (2019) Consent. Available from: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/> [Accessed 9 May 2022].

Information Commissioner's Office (ICO). (2022) When is consent appropriate? Available from: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/> [Accessed 9 May 2022].

Internet Security Scan. (2022) 5 tips for a secure use of JavaScript libraries. Available from: <https://internet-security-scan.com/vulnerability-scan/5-tips-for-a-secure-use-of-javascript-libraries.php> [Accessed 3 May 2022].

McNeice, K. (2021) Is CRM Software Worth the Investment for Small Businesses?. Available from: <https://www.accelo.com/resources/blog/is-crm-software-worth-theinvestment-for-small-businesses/> [Accessed 9 May 2022].

Methvin. D. (2011) jQuery 1.7.1 Released | Official jQuery Blog. Available from: <https://blog.jquery.com/2011/11/21/jquery-1-7-1-released/?msclkid=911375e5ced611ecae6b38902dbc6039> [Accessed 8 May 2022].

OWASP. (2021a) Cross-Site Request Forgery Prevention Cheat Sheet. Available from: https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html [Accessed 3 May 2022].

OWASP. (2021b) Session Management Cheat Sheet. Available from:
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching [Accessed 3 May 2022].

OWASP. (2022a) OWASP Web Security Testing Guide. Available from:
<https://owasp.org/www-project-web-security-testing-guide/> [Accessed 16 May 2022].

OWASP. (2022b) OWASP RISK RATING CALCULATOR. Available from:
<https://www.owasp-risk-rating.com/?msclkid=d0975c83cecf11ecaed65e7b7f8f9eda>
[Accessed 8 May 2022].

OWASP. (2022c) Vulnerability Scanning Tools. Available from:
https://owasp.org/www-community/Vulnerability_Scanning_Tools [Accessed 14 May 2022].

OWASP. (2022d) HttpOnly. Available from: <https://owasp.org/www-community/HttpOnly> [Accessed 3 May 2022].

Pentest Tools. (2022) Password Auditor. Available from: <https://pentest-tools.com/network-vulnerability-scanning/password-auditor> [Accessed 17 May 2022].

PortSwigger. (2022a) Cacheable HTTPS response. Available at:
https://portswigger.net/kb/issues/00700100_cacheable-https-response [Accessed 15 May 2022].

PortSwigger. (2022b) Robots.txt file. Available from:
https://portswigger.net/kb/issues/00600600_robots-txt-file#:~:text=Description%3A%20Robots.txt%20file%20The%20file%20robots.txt%20is%20used [Accessed 14 May 2022].

Salesforce. (2022) Salesforce UK: We Bring Companies and Customers Together.

Available from:

<https://www.salesforce.com/uk/?ir=1&msclkid=1ae1d7b7cf9411ecb3762e57c7761760&bc=HA> [Accessed 9 May 2022].

Taylor, T. (2022) How Reputational Damage from a Data Breach Affects Consumer Perception. Available from: <https://www.securelink.com/blog/reputation-risks-how-cyberattacks-affect-consumer-perception/> [Accessed 19 May 2022].

ZAPProxy. (2022a) Cookie without SameSite Attribute. Available from:

<https://www.zaproxy.org/docs/alerts/10054/> [Accessed 3 May 2022].

ZAPProxy. (2022b) Server Leaks Information via 'X-Powered-By' HTTP Response Header Field(s). Available from: <https://www.zaproxy.org/docs/alerts/10037/> [Accessed 3 May 2022].

ZAPProxy. (2022c) Timestamp Disclosure. Available from:

<https://www.zaproxy.org/docs/alerts/10096/> [Accessed 3 May 2022].

Appendices

Appendix A

OWASP ZAP website scan summary

Alert type	Risk	Count
Vulnerable JS Library	Medium	2 (2.0%)
Absence of Anti-CSRF Tokens	Low	10 (10.1%)
Cookie No HttpOnly Flag	Low	8 (8.1%)
Cookie Without Secure Flag	Low	8 (8.1%)
Cookie without SameSite Attribute	Low	8 (8.1%)
Incomplete or No Cache-control Header Set	Low	2 (2.0%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	12 (12.1%)
Timestamp Disclosure - Unix	Low	14 (14.1%)
Information Disclosure - Suspicious Comments	Informational	35 (35.4%)
Total		99

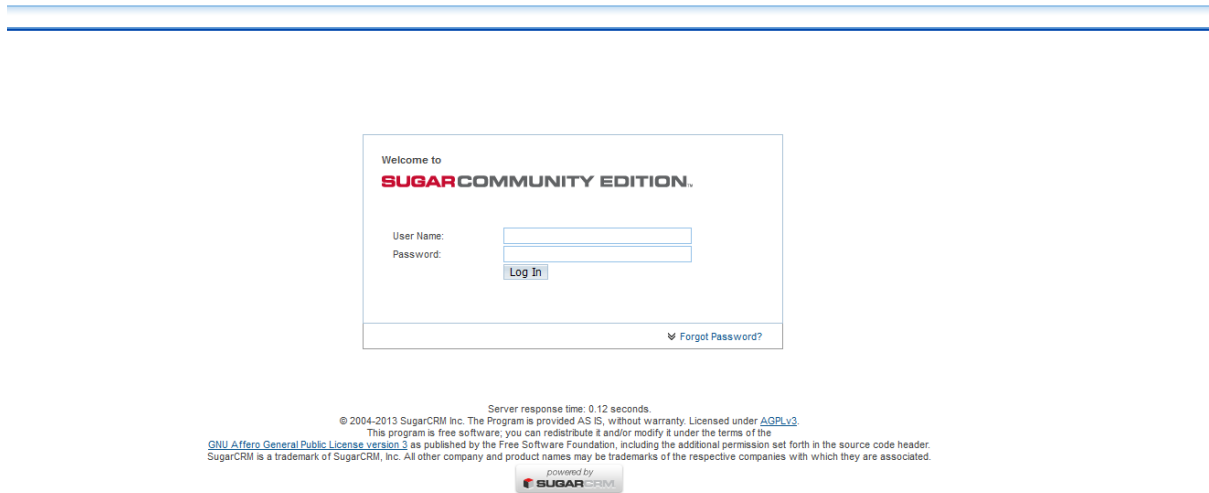
Appendix B

Pen-test network scan summary

●	5	CVE-2018-5740	"deny-answer-aliases" is a little-used feature intended to help recursive server operators protect end users against DNS rebinding attacks, a potential method of circumventing the security model used by client browsers. However, a defect in this feature makes it easy, when the feature is in use, to experience an assertion failure in name.c. Affects BIND 9.7.0->9.8.8, 9.9.0->9.9.13, 9.10.0->9.10.8, 9.11.0->9.11.4, 9.12.0->9.12.2, 9.13.0->9.13.2.	N/A
●	5	CVE-2018-5744	A failure to free memory can occur when processing messages having a specific combination of EDNS options. Versions affected are: BIND 9.10.7 -> 9.10.8-P1, 9.11.3 -> 9.11.5-P1, 9.12.0 -> 9.12.3-P1, and versions 9.10.7-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected.	N/A
●	5	CVE-2019-6470	There had existed in one of the ISC BIND libraries a bug in a function that was used by dhcpcd when operating in DHCPv6 mode. There was also a bug in dhcpcd relating to the use of this function per its documentation, but the bug in the library function prevented this from causing any harm. All releases of dhcpcd from ISC contain copies of this, and other, BIND libraries in combinations that have been tested prior to release and are known to not present issues like this. Some third-party packagers of ISC software have modified the dhcpcd source, BIND source, or version matchup in ways that create the crash potential. Based on reports available to ISC, the crash probability is large and no analysis has been done on how, or even if, the probability can be manipulated by an attacker. Affects: Builds of dhcpcd versions prior to version 4.4.1 when using BIND versions 9.11.2 or later, or BIND versions with specific bug fixes backported to them. ISC does not have access to comprehensive version lists for all repackagings of dhcpcd that are vulnerable. In particular, builds from other vendors may also be affected. Operators are advised to consult their vendor documentation.	N/A
●	5	CVE-2020-8616	A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals, cause a recursing server to issue a very large number of fetches in an attempt to process the referral. This has at least two potential effects: The performance of the recursing server can potentially be degraded by the additional work required to perform these fetches, and The attacker can exploit this behavior to use the recursing server as a reflector in a reflection attack with a high amplification factor.	N/A
●	5	CVE-2020-8617	Using a specially-crafted message, an attacker may potentially cause a BIND server to reach an inconsistent state if the attacker knows (or successfully guesses) the name of a TSIG key used by the server. Since BIND, by default, configures a local session key even on servers whose configuration does not otherwise make use of it, almost all current BIND servers are vulnerable. In releases of BIND dating from March 2018 and after, an assertion check in tsig.c detects this inconsistent state and deliberately exits. Prior to the introduction of the check the server would continue operating in an inconsistent state, with potentially harmful results.	N/A
●	4.3	CVE-2018-5743	By design, BIND is intended to limit the number of TCP clients that can be connected at any given time. The number of allowed connections is a tunable parameter which, if unset, defaults to a conservative value for most servers. Unfortunately, the code which was intended to limit the number of simultaneous connections contained an error which could be exploited to grow the number of simultaneous connections beyond this limit. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.6, 9.12.0 -> 9.12.4, 9.14.0. BIND 9 Supported Preview Edition versions 9.9.3-S1 -> 9.11.5-S3, and 9.11.5-S5. Versions 9.13.0 -> 9.13.7 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2018-5743.	N/A
●	4.3	CVE-2019-6465	Controls for zone transfers may not be properly applied to Dynamically Loadable Zones (DLZs) if the zones are writable. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.5-P2, 9.12.0 -> 9.12.3-P2, and versions 9.9.3-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2019-6465.	N/A
●	4.3	CVE-2019-6471	A race condition which may occur when discarding malformed packets can result in BIND exiting due to a REQUIRE assertion failure in dispatch.c. Versions affected: BIND 9.11.0 -> 9.11.7, 9.12.0 -> 9.12.4-P1, 9.14.0 -> 9.14.2. Also all releases of the BIND 9.13 development branch and version 9.15.0 of the BIND 9.15 development branch and BIND Supported Preview Edition versions 9.11.3-S1 -> 9.11.7-S1.	N/A

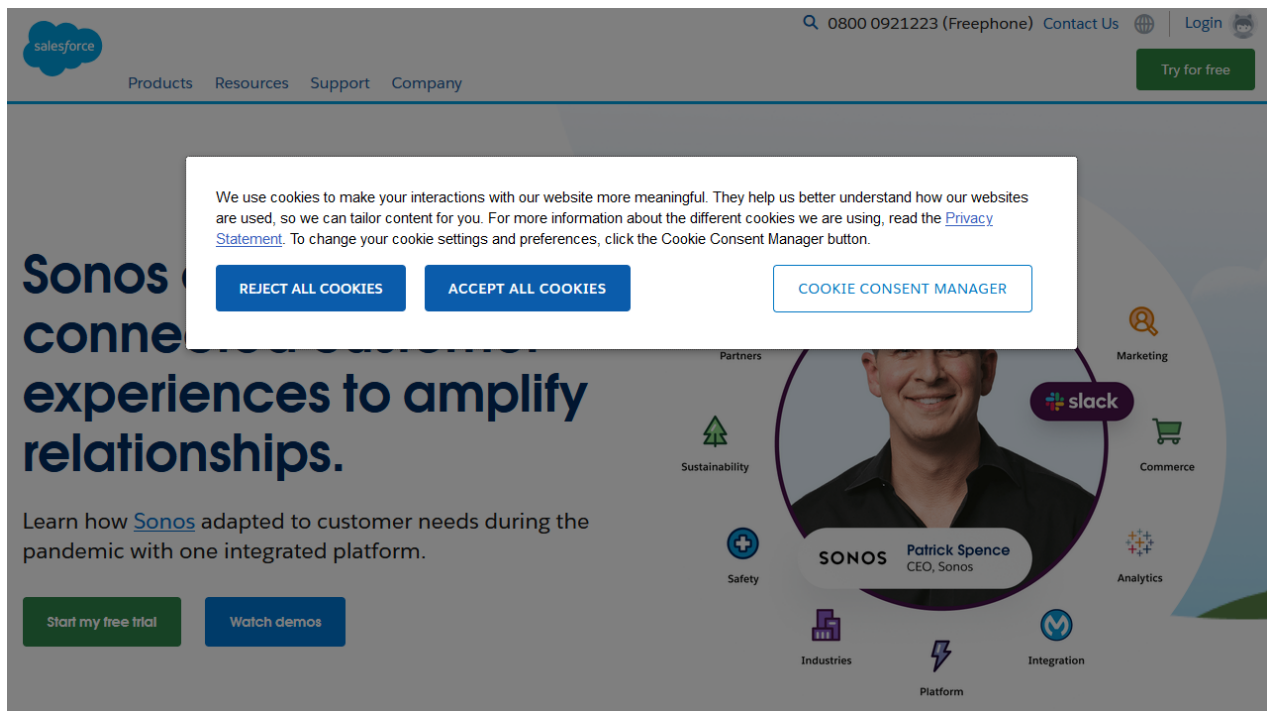
Appendix C

The website, customersrus.co.uk, not showing a cookie notification.



Appendix D

The website, Salesforce.com, shows a cookie notification.



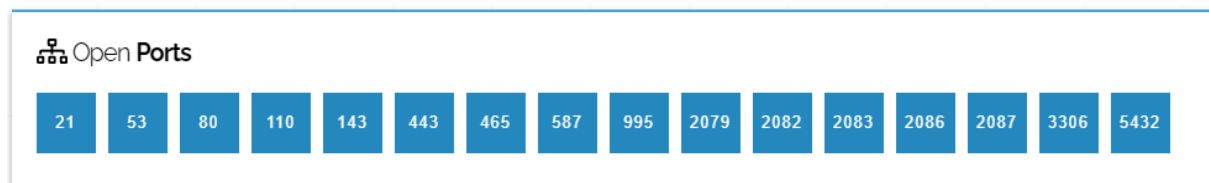
Appendix E

Nmap scan showing open ports

```
(kali㉿kali)-[~]
└─$ sudo nmap -O -v customersrus.co.uk
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-24 11:09 UTC
Initiating Ping Scan at 11:09
Scanning customersrus.co.uk (68.66.247.187) [4 ports]
Completed Ping Scan at 11:09, 0.30s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:09
Completed Parallel DNS resolution of 1 host. at 11:09, 0.49s elapsed
Initiating SYN Stealth Scan at 11:09
Scanning customersrus.co.uk (68.66.247.187) [1000 ports]
Discovered open port 993/tcp on 68.66.247.187
Discovered open port 3306/tcp on 68.66.247.187
Discovered open port 80/tcp on 68.66.247.187
Discovered open port 143/tcp on 68.66.247.187
Discovered open port 995/tcp on 68.66.247.187
Discovered open port 25/tcp on 68.66.247.187
Discovered open port 53/tcp on 68.66.247.187
Discovered open port 587/tcp on 68.66.247.187
Discovered open port 443/tcp on 68.66.247.187
Discovered open port 21/tcp on 68.66.247.187
Discovered open port 110/tcp on 68.66.247.187
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 5.25% done; ETC: 11:09 (0:00:36 remaining)
Discovered open port 5432/tcp on 68.66.247.187
Discovered open port 2525/tcp on 68.66.247.187
Discovered open port 465/tcp on 68.66.247.187
Completed SYN Stealth Scan at 11:09, 8.96s elapsed (1000 total ports)
Initiating OS detection (try #1) against customersrus.co.uk (68.66.247.187)
Retrying OS detection (try #2) against customersrus.co.uk (68.66.247.187)
Nmap scan report for customersrus.co.uk (68.66.247.187)
Host is up (0.26s latency).
rDNS record for 68.66.247.187: 68.66.247.187.static.a2webhosting.com
Not shown: 904 filtered tcp ports (no-response), 13 filtered tcp ports (port-unreach), 69 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
2525/tcp  open  ms-v-worlds
3306/tcp  open  mysql
5432/tcp  open  postgresql
Aggressive OS guesses: Linux 3.10 - 3.12 (95%), Linux 4.4 (95%), Linux 4.9 (93%), Linux 4.0 (92%), Linux 3.10 - 3.16 (92%), Linux 3.11 - 4.1 (91%), Linux 2.6.32 (91%), Linux 2.6.39 (91%), Linux 3.4 (91%), Linux 3.5 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 1.424 days (since Sat Apr 23 00:58:36 2022)
Network Distance: 16 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
```

Appendix F

Shodan scan showing open ports




Appendix G

Pen-test web-based SSL/TLS vulnerability scan



SSL/TLS Vulnerability Scanner Report (Light)



Unlock the full capabilities of this scanner

See what the **FULL** scanner can do

Perform full SSL/TLS scans with more powerful options.

Options	Light scan	Full scan
Target type	Single host	Multiple hosts
IP range scan	✗	✓
Target SSL port	443	Any port
Target service	HTTPS	<ul style="list-style-type: none">• HTTPS• SMTPs• IMAPs• FTPs• and more
SSL port specification	Manual	Auto discovery

Appendix H

Nikta scan showing WAF

```
- Nikto v2.1.6
-----
+ Target IP: 68.66.247.187
+ Target Hostname: 68.66.247.187
+ Target Port: 80
+ Start Time: 2022-04-23 19:20:17 (GMT-7)
-----
+ Server: Apache
+ Retrieved x-powered-by header: W3 Total Cache/0.9.4.6.4
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-redirect-by' found, with contents: WordPress
+ Root page / redirects to: https://tech-sourcery.co.uk/
+ Server banner has changed from 'Apache' to 'imunify360-webshield/1.18' which may suggest a WAF, load balancer or proxy is in place
+ Scan terminated: 19 error(s) and 3 item(s) reported on remote host
+ End Time: 2022-04-23 19:30:14 (GMT-7) (597 seconds)
-----
+ 1 host(s) tested
```

Appendix I

WafW00f scan showing WAF

```
(kali㉿kali)-[~]
$ sudo wafw00f https://customersrus.co.uk

      ( Woof! )

    ( / \ )
   ( / \ )
  ( / \ )
 ( / \ )
( / \ )

  ~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://customersrus.co.uk
[+] Generic Detection results:
[*] The site https://customersrus.co.uk seems to be behind a WAF or some sort
of security solution
[-] Reason: The server returns a different response code when an attack string
is used.
Normal response code is "200", while the response code to a SQL injection att
ack is "403"
[-] Number of requests: 7

(kali㉿kali)-[~]
$ sudo wafw00f http://customersrus.co.uk

      ( Woof! )

    ( / \ )
   ( / \ )
  ( / \ )
 ( / \ )
( / \ )

  ~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://customersrus.co.uk
[+] The site http://customersrus.co.uk is behind Imunify360 (CloudLinux) WAF.
[-] Number of requests: 2
```