Development Team Project: Executive Summary

1. Introduction

This document provides a summary of the evaluation of the e-commerce site carried out using the STRIDE framework (Johnstone, 2010; Khan *et al.*, 2017). A description of the framework and the tools used are available in section 2. Evaluations of the site's compliance with GDPR (European Union, 2018) and PCI DSS (PCISSC, 2018) are available in sections 4.3 and 4.5 respectively. The evaluations found a number of vulnerabilities and compliance issues. Recommended actions are provided in section 6 to ensure that the site meets the minimum requirements set by these regulations.

2. Methodology

2.1 Threat modelling

We conducted a thorough examination and testing of the site using the STRIDE framework for vulnerability assessment (Hernan *et al.*, 2006; Johnstone, 2010; Khan *et al.*, 2017).

Threat	**Security Property Violated**	**Description**	**Test**
Spoofing	Authentication	Confirmation of identity. Assurance that both the host and user are trusted parties.	OWASP ZAP OpenVas

Tampering	Integrity	Tampering includes modification of the source code. This is accomplished by a malicious actor inside the organization, or by gaining access via a physical access point.	sqlmap Physical access controls cannot be tested remotely. Mitigation strategies are explained in section 6.
Repudiation	Non-repudiation	Ensuring communications are received, and the receipt may be digitally verified.	This cannot be physically tested. Measures include digital signatures, time stamping and adequate log maintenance.
Information disclosure	Confidentiality	Ensuring that confidential information is hidden and not easily accessible so as to allow for malicious actors to take advantage of.	The Harvester Google Dorking sqlmap
Denial of service (DoS)	Availability	Overloading site resources, preventing customers access and normal business functionality.	slowHTTPtest sqlmap
Elevation of privilege	Authorization	Gain access to confidential business and user information.	Nmap OpenVAS

3. Security Testing

3.1 Testing Tools

Our team carried out security testing using the tools listed below:

Tool	Usage
Nmap	Free and open-source utility for network discovery and security auditing (Bhingardeve and Franklin, 2018; Rahalkar, 2019a)).
theHarvester	Open source tool that scans 40 public sources for emails, DNS names and subdomains belonging to an organization (Patel, 2019).
sqlmap	Open source tool that automates the process of detecting SQL injection flaws (Bin Ibrahim and Kant, 2018).
OpenVAS	Free and open-source vulnerability scanning tool (Fashoto, SG; Ogunleye, GO; Adabara, 2018; Rahalkar, 2019b).
OWASP ZAP	Free and open source web app security scanner backed by the Open Web Application Security Project (OWASP) (Makino and Klyuev, 2015).
Google Dorking	Using a search engine with appropriate filters to identify hidden information or vulnerabilities (Exposing the Invisible, 2020).
slowHTTPtest	A tool that simulates Application Layer DoS attacks.

3.2 Security Vulnerabilities

N.	Vulnerability	Tool	Risk Level	Risk Factors
1	Port 443 was found to be closed.	Nmap	High Risk	HTTP requests and responses are unencrypted and can be read by an attacker. This can lead to the exposure of sensitive data such as user payment information (Cloudflare (a), N.D.).

2	".DS_Store" files found.	OpenVAS	Medium Risk	Attackers can glean valuable information such as the internal structure and contents of a website from these files (File.org, N.D.).
3	X-Frame-Options header was not set.	OWASP ZAP	Medium Risk	Click-jacking attacks can be performed to steal login credentials or other personal information from users (Mozilla, August 2021).
4	No Anti-CSRF tokens were found.	OWASP ZAP	Low Risk	Cross Site Request Forgery attacks (CSRF) can be used to gain access to an active authenticated user session. This can lead to sensitive data exposure or fraudulent purchases being made through an account (OWASP, N.D.).
5	Cross-domain JavaScript source file inclusion.	OWASP ZAP	Low Risk	The use of third party JavaScript can lead to security vulnerabilities if the source file is not trusted, or is accessible by an end user (Mozilla, N.D.).
6	X-Content-Type-Options header was not set.	OWASP ZAP	Low Risk	MIME-sniffing attacks can be performed. These can lead to cross site scripting (XSS) attacks (Mozilla, N.D.).
7	Potential information disclosure made in a file's comments.	OWASP ZAP	Low Risk	Code comments can disclose known issues, or other relevant information, to an attacker (CWE, July 2021).
8	Potential DDOS attack	slowHTTPtest	Medium Risk	DoS and Distributed DoS (DDoS) attacks can be executed against the site. This can leave the site inaccessible to users (Cloudflare (b), N.D.).

4. Regulatory Compliance

4.1 Assumptions

The following assumptions were made when performing the compliance assessments on the e-commerce site:

- Hosted using Amazon Web Services (AWS).
- Available 24/7.
- Stores personal customer information such as names, email addresses, and payment information.
- Directly processes payments when completing transactions.
- Processes under 1 million transactions per year (PCI DSS level 3).

4.2 General Data Protection Regulation (GDPR)

An e-commerce business is a complex entity composed of a website and internal departments, which interacts with external entities. In order to serve customers residing in the European Union (EU), the e-commerce site must be GDPR compliant (European Union, 2018; ICO, 2018).

Customer data should be processed using the following guidelines:

- Users personal data is entered by the users at the time of registration.
- Consent is rightfully requested during registration; checkboxes are not preselected and the purpose and privacy policy are clear.
- Customers' right of access and right to erase can be exercised from the user control panel.
- Terms and conditions define the lawful reason and necessity for storing and using data.
- Shopping history is recorded based on the user activity on the website. Users may opt out of such information gathering and usage.

- User data will be stored as long as the user is registered on the platform.

4.3 GDPR Compliance Checklist

The assessment was performed using the following checklist adapted from the GDPR guidelines (*GDPR compliance checklist - GDPR.eu*, 2021). Recommendations are available in section 6.

1.	**Lawful basis and transparency**	
a.	Conduct an information audit and determine what information you process and who has access to it	✔
b.	Have a legal justification for your data processing activities	✔
c.	Provide clear information about your data processing and legal justification in your privacy policy	✘
2.	**Data security**	
a.	Create an internal security policy for your team members, and build awareness about data protection	✘
b.	Know when to conduct a data protection impact assessment, and have a process in place to carry it out	✘
c.	Have a process in place to notify the authorities and your data subjects in the event of a data breach	✘
3.	**Accountability and governance**	
a.	Designate someone responsible for ensuring GDPR compliance across your organization	✘
b.	Sign a data processing agreement between your organization and any third parties that process personal data on your behalf	✘

c.	If your organization is outside the EU, appoint a representative within one of the EU member states	X
d.	Appoint a Data Protection Officer	X
4.	**Privacy rights**	
a.	It's easy for your customers to request and receive all the information you have about them	X
b.	It's easy for your customers to ask you to stop processing their data	X
c.	It's easy for your customers to receive a copy of their personal data in a format that can be easily transferred to another company.	X
d.	It's easy for your customers to object to you processing their data	X
e.	If you make decisions about people based on automated processes, you have a procedure to protect their rights	X

4.4 Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is a security standard designed for companies that acquire, store, and process payment data. Compliance is not required but in the case of a data breach, the company can face more severe fines if it is found to be non-compliant. PCI DSS is divided into levels, a merchant is placed in a level based on the total number of transactions run each year (PCISSC, 2018).

The requirements for level 3 organisations are: annual self-assessment questionnaire, attestation of compliance form, and quarterly network scans. We are limited by not having physical access to the organisation.

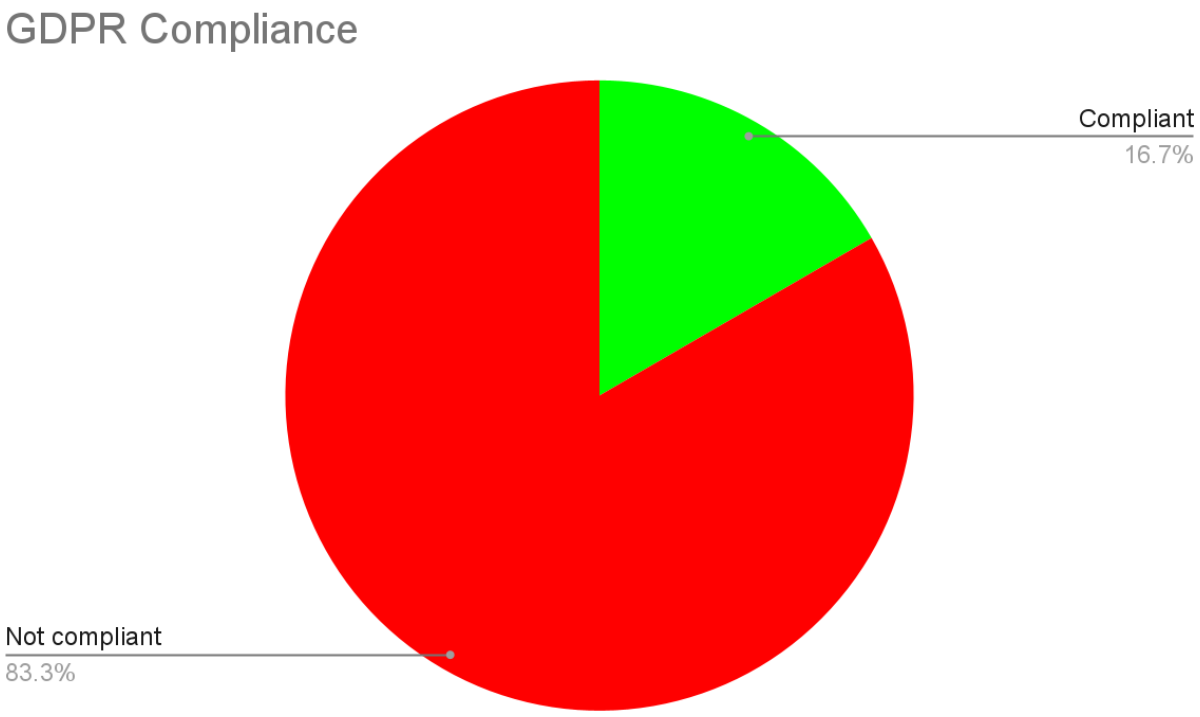
4.5 PCI DSS Compliance Assessment

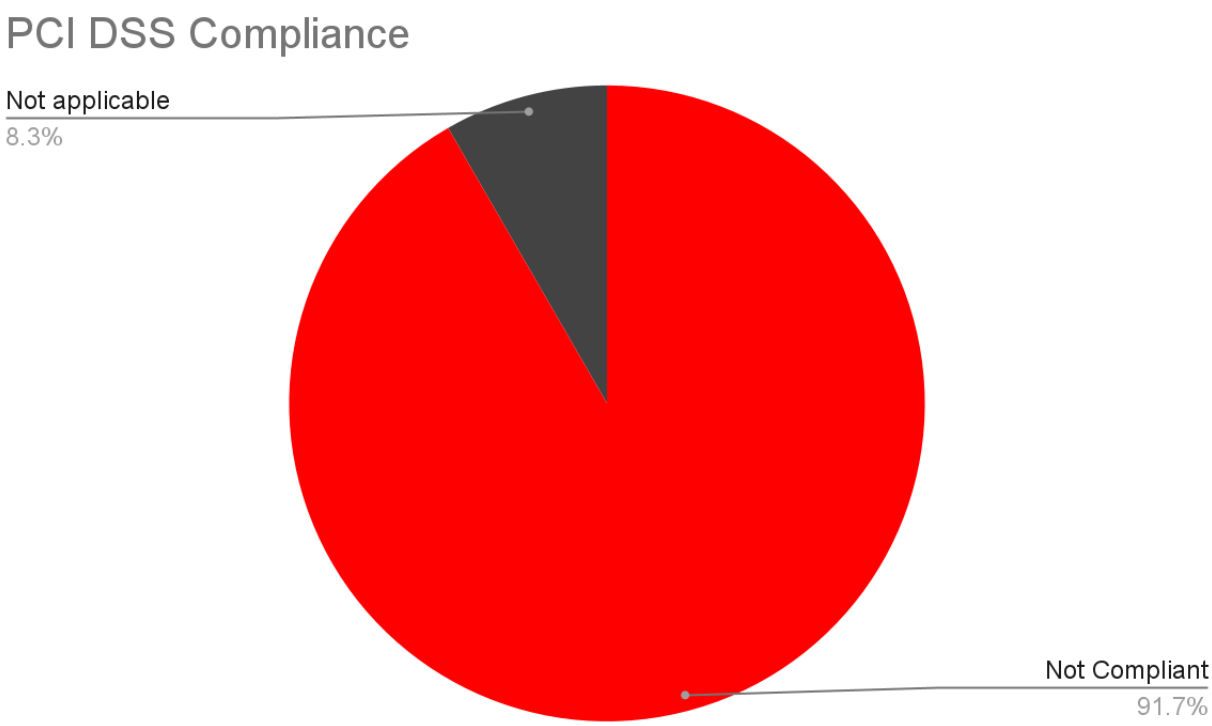
For this assessment we followed the PCI Remote Assessment Guideline (PCI Security Standards Council (a), N.D.; PCI Security Standards Council (b), N.D.). Recommendations are available in section 6.

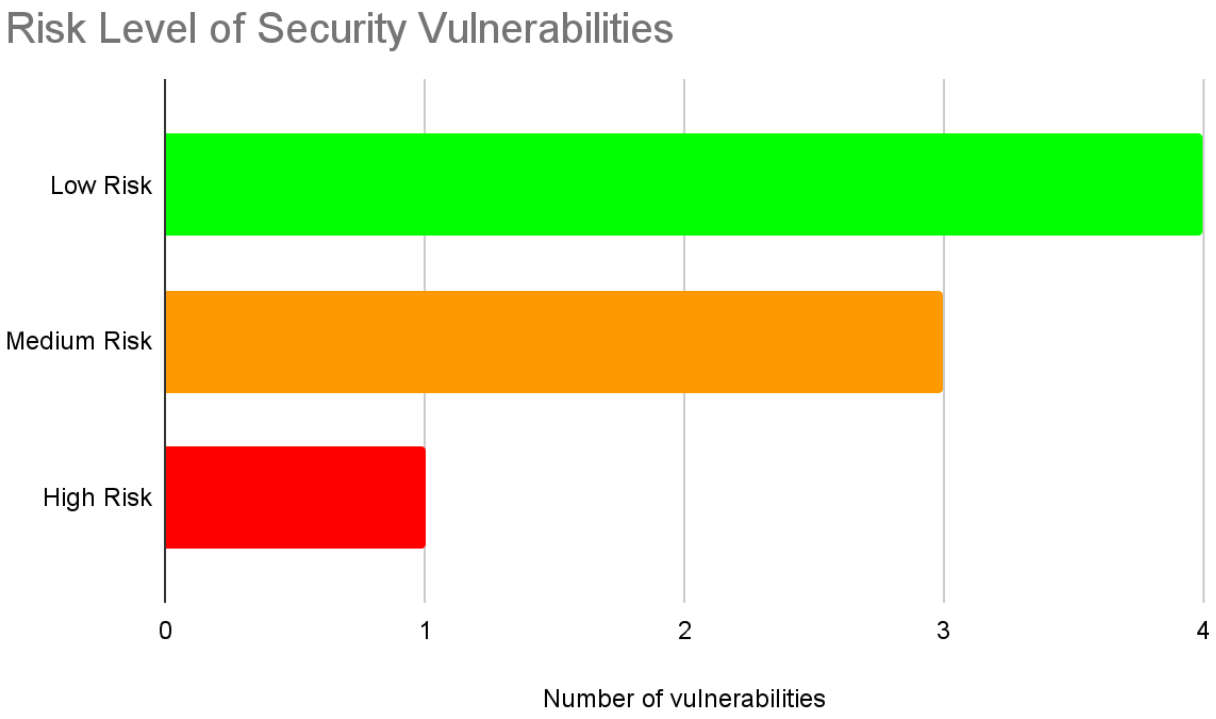
N.	Requirement	Compliance	Explanation
1	Install and maintain a firewall configuration to protect cardholder data.	Not compliant	No firewall configuration has been performed.
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	Not compliant	No non-root users were created. The unnecessary use of root user privileges is not recommended.
3	Protect stored cardholder data.	Not compliant	No systems are implemented to protect stored cardholder data.
4	Encrypt transmission of cardholder data across open, public networks.	Not compliant	Port 443 is closed and TLS is not in use. No cryptographic policies are currently in place.
5	Use and regularly update anti-virus software or programs.	Not compliant	Amazon takes responsibility for some AWS security. No specific antivirus software currently in use by the site.
6	Develop and maintain secure systems and applications.	Not compliant	No processes currently in place to identify or address potential security vulnerabilities. Vulnerabilities were identified in section 3.2.
7	Restrict access to cardholder data by business need to know.	Not compliant	No access management is currently implemented.

8	Assign a unique I.D. to each person with computer access.	Not compliant	Identity and Access Management (IAM) not in place.
9	Restrict physical access to cardholder data.	N/A	Data is stored remotely on AWS servers. Not physically accessible.
10	Track and monitor all access to network resources and cardholder data.	Not compliant	No logging is enabled.
11	Regularly test security systems and processes.	Not compliant	No policy in place regarding security testing.
12	Maintain a policy that addresses information security (IS) for all personnel.	Not compliant	No IS policies regarding staff are implemented. No IS training is available to personnel.

5. Data Summary







6. Recommendations

N.	Recommended Action	Addressed Issues
1	Implement HTTPS using Transport Layer Security (TLS) for all connections. Produce cryptography policies.	Security vulnerability 1 PCI DSS requirement 4
2	Block access to hidden files in the server's configuration. Delay creation of ".DS_Store" files when viewing network drives on macOS.	Security vulnerability 2
3	Set the X-Frame-Options header to "DENY".	Security vulnerability 3
4	System and network logging should be enabled.Rate limiting can be introduced to help mitigate against DoS and DDoS attacks. Amazon provides services such as AWS CloudTrail which can be used to help meet this requirement.	Security vulnerability 8 PCI DSS requirement 10

5	The OWASP has multiple vetted libraries and frameworks available to mitigate against CSRF attacks, including the OWASP CSRFGuard library.	Security vulnerability 4
6	Only load JavaScript from a trusted source which cannot be controlled by an end user.	Security vulnerability 5
7	Setting the X-Content-Type-Options header to “nosniff” will avoid MIME-sniffing in older browsers. Users should also be encouraged to use a modern web browser which does not perform MIME-sniffing.	Security vulnerability 6
8	Issues highlighted by code comments should be addressed, and the comments removed, before being used in production. A Software Development Life Cycle should be implemented, allowing any vulnerabilities to be dealt with appropriately.	Security Vulnerability 7 PCI DSS requirement 6
9	Create a comprehensive privacy policy. Privacy by design and by default should be implemented to protect cardholder data. Only the minimum required amount of cardholder data should be stored.	PCI DSS requirement 3 GDPR requirement 1
10	Implement an easy way for users to request and receive any data which has been collected about them. Provide an easy way for customers to object to having their information processed, or opt out of any unnecessary data collection.	GDPR requirement 4
11	A policy of regular systems and security testing should be implemented. A Business Continuity Management System (BCMS) encompasses this, along with procedures for responding to any data breaches.	PCI DSS requirement 11 GDPR requirement 2
12	An IS policy should be implemented throughout the organisation. This should include regular training for personnel.	PCI DSS requirement 12 GDPR requirement 2

13	Appoint a Data Protection Officer, along with someone responsible for GDPR across the organisation. Appoint an EU representative if the organisation is based outside of the EU.	GDPR requirement 3
14	A firewall should be configured and enabled. This can be achieved using AWS services such as the Firewall Manager.	PCI DSS requirement 1
15	Set up non-root users using the principle of least privilege.	PCI DSS requirement 2
16	Sensitive user data should only be accessible after authentication by employees. The principle of least privilege ensures that employees only have access to information necessary to their roles.	PCI DSS requirement 7
17	Antivirus software should be run on the AWS instance hosting the site.	PCI DSS requirement 5
18	An IAM policy should be implemented. AWS has built in IAM support, along with other staff management tools.	PCI DSS requirement 8

7. Conclusion

An assessment has been carried out on the e-commerce site in order to highlight any issues found with security or compliance with the GDPR and PCI DSS regulations. An explanation on each vulnerability or compliance failure has been provided, along with recommendations on how to address each issue. Due to limitations, assumptions were made in cases where information could not be verified. We strongly urge the organisation to address the mentioned vulnerabilities in order to ensure adequate security and compliance with the relevant regulatory authorities.

Word count: 2190

References

Bhingardeve, N. and Franklin, S. (2018) 'A Comparison Study of Open Source Penetration Testing Tools', *International Journal of Trend in Scientific Research and Development*, Volume-2(Issue-4), pp. 2595–2597. doi: 10.31142/ijtsrd15662.

Bin Ibrahim, A. and Kant, S. (2018) 'Penetration Testing Using SQL Injection to Recognize the Vulnerable Point on Web Pages', *International Journal of Applied Engineering Research*, 13(8), pp. 5935–5942. Available at: http://www.ripublication.com.

Cloudflare (a). (N.D.) Why is HTTP not secure? | HTTP vs. HTTPS. Available from: https://www.cloudflare.com/en-gb/learning/ssl/why-is-http-not-secure/ [Accessed 19th October 2021]

Cloudflare (b). (N.D.) What is a DDoS attack? Available from: https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/ [Accessed 23rd October 2021]

CWE. (July 2021) CWE-615: Inclusion of Sensitive Information in Source Code Comments. Available from: https://cwe.mitre.org/data/definitions/615.html [Accessed 19th October 2021]

European Union (2018) 'General Data Protection Regulation (GDPR) – Official Legal Text', *General Data Protection Regulation*, pp. 1–99. Available at: https://gdpr-info.eu/ (Accessed: 17 September 2021).

Exposing the Invisible (2020) 'Smart Searching with GoogleDorking'. Available at: https://exposingtheinvisible.org/en/guides/google-dorking/ (Accessed: 23 October 2021).

Fashoto, SG; Ogunleye, GO; Adabara, I. (2018) 'Evaluation Of Network And Systems Security Using Penetration Testing In A Simulation Environment', *GESJ: Computer Science and Telecommunications*, 2(2), pp. 91–99.

File.org. (N.D.) Having problems opening a DS_STORE file? Available from: https://file.org/extension/ds_store [Accessed 19th October 2021]

GDPR compliance checklist - GDPR.eu (2021) *General Data Protection Regulation*. Available at: https://gdpr.eu/checklist/ (Accessed: 20 October 2021).

Hernan, S. *et al.* (2006) 'Threat modeling-uncover security design flaws using the stride approach', *MSDN Magazine*, November, pp. 68–75.

ICO. (2018) Guide to the general data protection regulation GDPR. [ONLINE] Available from:https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/. [Accessed 19 October 2021]

Johnstone, M. N. (2010) 'Threat modelling with STRIDE and UML', *Proceedings of the 8th Australian Information Security Management Conference*, (November), pp. 18–27. doi: 10.4225/75/57b670493477c.

Khan, R. *et al.* (2017) 'STRIDE-based threat modeling for cyber-physical systems', *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT-Europe 2017 - Proceedings*, 2018-January(September), pp. 1–6. doi: 10.1109/ISGTEurope.2017.8260283.

Makino, Y. and Klyuev, V. (2015) 'Evaluation of web vulnerability scanners', Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2015, 1(September), pp. 399–402. doi: 10.1109/IDAACS.2015.7340766.

Mozilla. (August 2021) X-Frame-Options. Available from: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options [Accessed 19th October 2021]

Mozilla. (N.D.) Same-origin policy. Available from: https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy [Accessed 19th October 2021]

Mozilla. (N.D.) X-Content-Type-Options. Available from: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options [Accessed 19th October 2021]

OWASP. (N.D.) Cross Site Request Forgery (CSRF). Available from: https://owasp.org/www-community/attacks/csrf [Accessed 19th October 2021]

Patel, K. (2019) 'A Survey on Vulnerability Assessment & Penetration Testing for Secure Communication', in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, pp. 320–325.

PCISSC (2018) *Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards*, *PCI Security Standards Council*. Available at: https://www.pcisecuritystandards.org/ (Accessed: 23 October 2021).

PCI Security standards Council (a). (N.D.) Assessing the security of your cardholder data. [ONLINE] Available from: https://www.pcisecuritystandards.org/pci_security/completing_self_assessment. [Accessed 18 October 2021].

PCI Security standards Council (b). (N.D.) Remote Assessment. [ONLINE] Available from: https://www.pcisecuritystandards.org/documents/PCI-SSC-Remote-Assessment-Guidelines-Procedures-v1_0.pdf [Accessed 20 October 2021]

Rahalkar, S. (2019a) 'Introduction to NMAP BT - Quick Start Guide to Penetration Testing: With NMAP, OpenVAS and Metasploit', in Rahalkar, S. (ed.). Berkeley, CA: Apress, pp. 1–45. doi: 10.1007/978-1-4842-4270-4_1.

Rahalkar, S. (2019b) ‘OpenVAS’, in *Quick Start Guide to Penetration Testing: With NMAP, OpenVAS and Metasploit*. Berkeley, CA: Apress, pp. 47–71. doi: 10.1007/978-1-4842-4270-4_2