Development Team Project

An Executive Summary of a Network and Information Security Management (NISM) Assessment Project

MSc Cyber Security
Module 2, Unit 11 Submission
Words 1976

Introduction

The document below provides an Executive Summary of the Network and Information Security Management (NISM) Assessment Project, covering the scope of the assessment, recorded findings, a compliance evaluation and recommendations.

Grey box penetration testing was conducted as the client provided access to both the source code and the PHP version used. This approach was efficient with reduced testing time and delivered a more economical testing solution (Conklin et al., 2017). The test was conducted in line with the Amazon Web Services terms and conditions, including avoiding simulating damaging attack types, such as Distributed Denial of Service (DDoS) (AWS, N.D.).

Various open source and commercial tools were used to ensure a comprehensive test. A range of tools were used for initial stages of enumeration and vulnerability scanning (McNab, 2016). Based on the findings, a smaller subset of the tools were used to pursue exploitation of potential vulnerabilities and the software utilised by the application. An iterative approach was taken, revisiting the steps of the Cyber Kill Chain upon discovery of new information (Lockheed Martin, N.D.). All tools used are documented in Appendix A.

Findings

The 14 findings of the assessment have been documented in order of criticality. Throughout the assessment, outdated software, poor encryption practices, privilege escalation and inadvertent data leakage were themes seen. Please note that none of the below findings were exploited during the assessment; however, that is not to say that an exploit is not possible and all should be considered based on criticality rating.

Below are two charts to show the variation in criticality rating. The majority of findings have been classified as Medium for criticality rating.

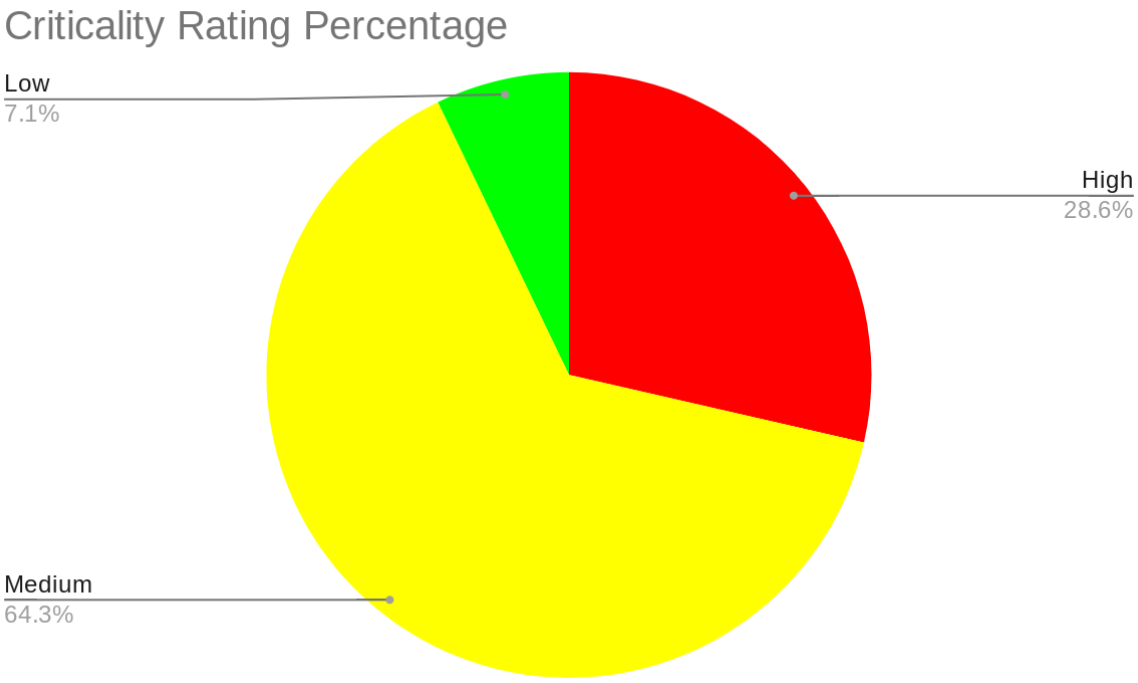

Chart 1.

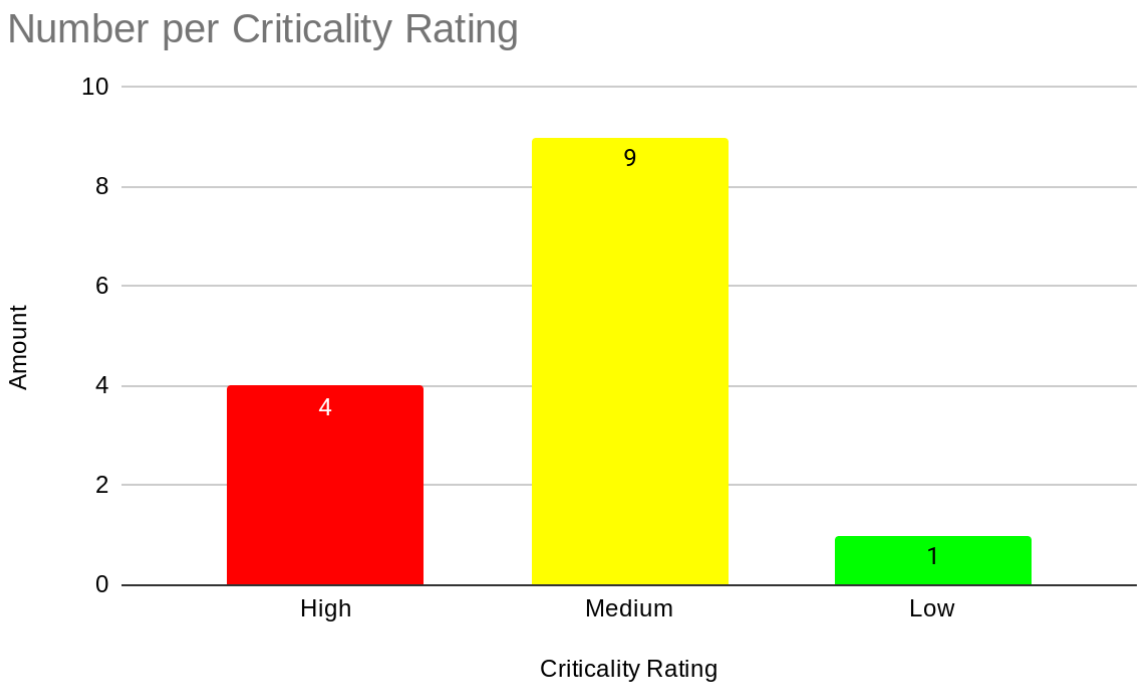

Chart 2.

No.	Finding Description	Score	Criticality Rating
1	**Unencrypted Traffic** Lack of encryption allows an attacker to view confidential information, such as personal and payment data, in clear text (OWASP, 2021). This was identified by the HTTP port 80 being open.	7.6	High
2	**Deprecated PHP version 7.3** Version 7.4 has 46 known vulnerabilities. It is also considered as end of life software with active support ceased in December 2020 and security support only available until December 2021 (PHP, 2021). If these functions are utilised, some vulnerabilities may be of concern, such as those that allow for remote code execution.	6.8	High
3	**Outdated Jquery version 1.8.3.** Version 1.8.3 has 6 known vulnerabilities. If further functionality is added to the site, these vulnerabilities may be exploited. These possible exploits can allow for Cross-Site Scripting (XSS), allowing potential leakage of credentials, personal data or payment card data.	6.3	High
4	**Outdated Bootstrap version 2.2.2** Version 2.2.2 has 5 known vulnerabilities. These possible exploits can allow for XSS, allowing potential leakage of credentials, personal data or payment card data.	6.3	High
5	**Data Residency** The application is hosted in the US which contravenes the GDPR requirement to ensure all data is held in a location subject to either EU data laws or a similar level of data protection laws.	4.9	Medium
6	**CloudWatch Alarms**	4.9	Medium

	The CloudWatch alarms that detect anomalous behavior in environments can be disabled and deleted. This will allow the attacker to remain undetected while performing malicious activities (Gietzen, N.D).		
7	**Outdated OpenSSH version 7.4 used** Version 7.4 has 12 known vulnerabilities. Some of the exploits could be used to conduct a Man-in-the-Middle attack.	4.7	Medium
8	**Subresource Integrity (SRI) Not Implemented** This feature enables browser checks to be completed for third parties and verify that resources are delivered without manipulation.	4.1	Medium
9	**Outdated TWIG version 2.0 used** Version 2.0 has 2 known vulnerabilities. Although not currently exploitable, it is recommended to patch to the most recent version.	4	Medium
10	**Mac OS X Find-By-Content .DS_Store Web Directory Listing** This contains a vulnerability that may lead to an unauthorized information disclosure, such as files containing web directory information.	3.9	Medium
11	**SSH Server CBC Mode Ciphers Enabled** This could result in data being accessed in plaintext via a SSH session.	3.8	Medium
12	**Missing X-Frame-Options Header** Without this, the site could be subject to Clickjacking or UI redress attacks and users could perform fraudulent transactions unknowingly.	3.8	Medium
13	**Missing X-XSS-Protection Header** This could leave the site vulnerable to a Cross-Site Scripting attack.	3.8	Medium
14	**ICMP Timestamp Request Remote Date Disclosure** The availability of an ICMP timestamp response could enable time-based authentication protocols to be exploited.	2.6	Low

Using OWASP's risk rating methodology, the security findings have been scored and prioritised (OWASP, N.D.). This methodology is designed for web applications and allows the scores to be tailored to the e-commerce business whilst considering the CVE data available in the NVD. Overall, the scoring is more flexible and meaningful to the business than only using CVSS scoring as it considers the various impacts, such as reputational damage. Thresholds have been defined to assign repeatable impact ratings of Low (0 to <3), Medium (3 to <6) and High (6 to 9) to the findings based on the average risk score (Ramadlan, 2019). These allow the business to easily understand and prioritise the findings in order to ameliorate the security posture of the application.

The scoring and resulting ratings in this report have been assigned on the basis of the site employing genuine e-commerce functionality, such as user authentication and payment forms. It is recommended that the business triages and ratifies the ratings given based on internal information available, such as the business impact analysis (BIA) of the target application (Tang, 2014).

Security Compliance Evaluation

Several regulations and standards applicable to the target site share common requirements that are considered best practice for protecting data assets (Swift, 2010). Whilst the GDPR carries serious consequences for poor data security practices, it only gives examples of security controls in Article 32, not containing detailed security guidance (IT Governance, N.D.). Best practice can instead be sought from security standards with more prescriptive

recommendations, such as ISO27001 for general practice and PCI DSS for the security of payment card data.

Under the GDPR, all personal data must be sufficiently protected using encryption, including in transit (EUR-Lex, 2016). The PCI DSS goes further and recommends that only strong cryptographic algorithms are utilised to authenticate and encrypt communications containing sensitive data (PCI SSC, 2018). Therefore, the use of HTTP connections and CBC to encrypt SSH traffic is not compliant against these standards.

In addition, PCI DSS standards state that end of life software, such as PHP 7.3, should be avoided as they may not offer the required level of security. This also applies to older versions of software, of which there are multiple examples utilised in this application. Further to this, PCI DSS places a lot of emphasis on secure coding practices for preventing certain attacks, such as XSS.

Overall, the site is not currently in line with GDPR or PCI DSS regulations. If further development of the site continues, it is advised that a project to become GDPR and PCI DSS compliant is initiated alongside any development. This will help to avoid any unnecessary fines in the future, as well as improving security controls and reputation of the business.

Recommendations

Technical, procedural and people controls have been recommended and prioritised to directly address the findings of the test (Campbell, 2016). A holistic approach to security controls will ensure a much stronger security posture that will create benefit for the target application and the wider business. The below recommendations have been prioritised based on cost vs benefits, impact on compliance and number of related findings addressed. This is a suggested order of priority and can be utilised in whichever way the business deems best.

Priority	Recommendation	Cost of Implementation	Benefits of Implementation	Related Finding(s)
1	HTTPS should be enabled and encrypted using known strong ciphers, i.e. TLS 1.2 and above.	**Low** A SSL certificate for the server needs to be purchased.	**High** Without encryption, the site will be insecure and customers may not wish to use it as the likelihood is high that data could be compromised, leading to potential fines and reputational damage.	1
2	Update to most current PHP, jQuery, Bootstrap & TWIG versions.	**Low** Regression testing verifying that the applied patches do not have negative effects will be cost effective	**High** Patching of software prevents vulnerability exploits from impacting the site.	2, 3, 4, 7, 9
3	Implement patching policy and process	**Low** Ensures software remains supported (Campbell, 2016)	**High** Alignment of PCI DSS 6.2	2, 3, 4, 7, 9

4	Close port 22 (SSH) if not business critical, otherwise update SSH version	**Low** AWS is already utilised, only a setting change	**High** Unnecessary entry point closed and vulnerabilities of older versions patched.	7, 11
5	Migrate to a GDPR-compliant hosting solution, such as AWS data center(s) in the EEA.	**Low** Migration to EU hosting should not cost much since the site is already AWS hosted.	**High** GDPR compliant.	5
6	Disable ICMP timestamp responses by blocking ICMP on the affected host or/and block it at a firewall	**Low**	**High** ICMP timestamp request will not be answered	14
7	Configure Apache to send X-Frame-Options and X-XSS-Protection Headers to all pages	**Low**	**Medium**	12, 13
8	Configure Apache to disregard .DS_Store file.	**Low** Activate the Apache feature.	**Medium** Potential leakage closed	10
9	Implement Admin access controls and process, along with access log review	**Low**	**Medium**	6
10	Implement SRI (Subresource Integrity)	**Low** Activate feature	**Medium** Provides a check integrity of resources hosted by third parties	8

Additional Recommendations

Throughout the assessment, additional recommendations have been identified. These collectively help to improve the security controls of the site and also improve compliance of GDPR, PCI DSS and ISO27001. These have not been prioritised as they are additional to the above recommendations.

1. Implement a scalable, cloud-based Web Application Firewall (WAF) - to protect against multiple threats including DDoS.
2. Improve encryption of the database and backups (currently non-existent).
3. Close Common Gateway Interfaces (CGI) that are not in use to reduce attack surface.
4. Create a security training programme, including technical skills training and general awareness.
5. Implement a robust third party security schedule with Cloud Service Provider, if not already in place.
6. Implement a Content Security Policy to protect against Cross Site Scripting attacks.

AWS (2021) states that all customers get free protection from typical network and transport layer attacks through AWS Shield Standard. However, it is recommended to implement additional technical controls to create defence in depth (Howard and LeBlanc, 2003). An appropriately tailored configuration should be set and maintained on technical solutions, such as the WAF, in order to ensure control effectiveness.

An indication of the cost to implement each recommendation is included along with the benefits in addition to reducing the proven risks outlined in this report. For some technical controls, such as the log monitoring tools, open source options are available which can reduce the cost of becoming compliant (Clark, N.D.). In addition, a number of the recommendations do not involve direct costs.

Conclusion

To conclude the assessment, it is recommended that if the site were to develop further, for example through the addition of html tags and further sub-pages, fundamentally it would be vulnerable to attack. The recommendations outlined above should be considered and prioritised prior to adding anything further and it would be necessary to follow secure software development standards.

Furthermore, as an e-commerce business, it is recommended that improvements are made in line with multiple different security standards such as PCI-DSS and ISO27001, with an overlay of security controls to meet GDPR requirements. If personal data or card payment data is required, then it is imperative that these standards are met, otherwise fines and potential blockers, for example being unable to take card payments, may occur and cause unnecessary issues for the business.

References

AWS (N.D.) Penetration Testing. Available from: https://aws.amazon.com/security/penetration-testing/ [Accessed 11 July 2021].

AWS (2021) AWS Shield. Available from: https://aws.amazon.com/shield/ [Accessed 11 July 2021].

Campbell, T. (2016) *Practical Information Security Management*. 1st ed. APRESS.

Clark, C. (N.D.) Building Wireless IDS System Using Open Source. Available from: http://sagan.quadrantsec.com/papers/wirelessids/ [Accessed 18 July 2021].

Conklin, L. et al. (2017) OWASP Code Review Guide 2.0. Available from: https://owasp.org/www-pdf-archive/OWASP_Code_Review_Guide_v2.pdf [Accessed 18 July 2021].

EUR-Lex (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434 [Accessed 18 July 2021].

Gietzen, S. (N.D) Pacu: The Open Source AWS Exploitation Framework. Available from: https://rhinosecuritylabs.com/aws/pacu-open-source-aws-exploitation-framework/ [Accessed 15 July].

Howard, M. and LeBlanc, D. (2003) *Writing secure code*. 2nd ed. Redmond, Washington: Microsoft Press.

IT Governance (N.D.) ISO27001 and the GDPR. Available from: https://www.itgovernance.co.uk/gdpr-and-iso-27001 [Accessed 11 July 2021].

Lockheed Martin (N.D.) The Cyber Kill Chain. Available from: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html [Accessed 18 July 2021].

McNab, C. (2016) *Network Security Assessment: Know Your Network*. 3rd ed. O'Reilly Media.

OWASP (N.D.) OWASP Risk Rating Calculator. Available from: https://owasp-risk-rating.com/ [Accessed 18 July 2021].

OWASP (2021) Transport Layer Protection Cheat Sheet. Available from: https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html [Accessed 18 July 2021].

PCI SSC (2018) Payment Card Industry (PCI) Data Security Standard. Available from: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1625664637522 [Accessed 11 July 2021].

PHP (2021) Supported Versions. Available from: https://www.php.net/supported-versions.php [Accessed 18 July 2021].

Ramadlan, M. (2019) Introduction and implementation: OWASP Risk Rating Management. Available from: https://owasp.org/www-pdf-archive/Riskratingmanagement-170615172835.pdf [Accessed 18 July 2021].

Swift, D. (2010) Successful SIEM and Log Management Strategies for Audit and Compliance. Available from: https://www.sans.org/white-papers/33528/ [Accessed 18 July 2021].

Tang, A. (2014) A guide to penetration testing. *Network Security* 2014(8): 8-11.

Vielberth, M. & Pernul, G. (2018) 'A Security Information and Event Management Pattern', *12th Latin American Conference on Pattern Languages of Programs (SLPLoP)*. Valparaiso, Chile, 20-23 November. 1-12.

Appendix A

Tool	Reconnaissance	Vulnerability Scanning	Exploitation of Vulnerabilities	Successful Exploitation
Pacu	X	X	X	X
Nmap & Nmap Script Engine (NSE)	X	X	X	
Nessus Professional	X	X		
Netsparker	X	X		
DIRB	X	X		
Netcat	X	X		
SQLmap		X	X	
Shhgit		X	X	
Burp Suite Community Edition		X	X	
Metasploit		X	X	
Wafw00f	X			
Dotdotpwn	X			
Firefox Developer Mode	X			
Dig	X			
Nikto		X		
XSSer			X	