Executive Summary

Summary of Work Carried Out

Table 1 describes the summary of work carried out, including target, scope, duration, target assets, assessment approach, methodologies, tools, standards, and threat risk analysis methodologies.

Group	Group 2
Organisation Name	Pink Organisation e-health services
Duration	Unit 4 (August 31 2021) - Unit 11 (October 25 2021)
Assets Scanned	(First Scan) - http://ec2-18-220-182-24.us-east-2.compute.amazonaws.com - 18.220.182.24 (Second Scan) - http://ec2-3-133-205-18.us-east-2.compute.amazonaws.com - 3.133.205.18
Scope of Scan & Analysis	Web Applications, Servers, Physical Securities (analysis only)
Scanning Approach	Remote Passive/Active Information Gathering (PIG/AIG)
Testing Methodologies	Automated Vulnerability Testing, Manual Check
Assessment Tools	Tenable Nessus, OWASP Zed Attack Proxy (ZAP), Kali Linux
Standards	General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI-DSS)
Threat Risk Analysis Methodologies	STRIDE, DREAD
Assessed by	Group 3

Table 1: Summary of Work Carried Out

Scope and Timeline

Adversaries utilise multiple types of information gathering, including passive, semi-passive, and active, to develop a target profile (Sood&Enbody, 2012). To identify the attack surface, Group 3 applied the exact step. Some PIG and AIG target Social Networks or Physical Securities. However, Group 3 does not consider staff members and Physical Securities in the scope but incorporates Office Wi-Fi to provide insight on threats over vulnerabilities (See Table 2).

Attack Surface	Descriptions	Vulnerability Scanning Scope	Threat/Risk Analysis Scope	Comments
Servers	Server Configuration	In Scope	In Scope	-
Applications	Web Application Code & Behaviour	In Scope	In Scope	-
Staff Member	Social Networks, Internal Adversaries	Out of Scope	Out of Scope	-
Physical Securities	Datacenter / Office Access / Office Wi-FI	Out of Scope	Partial	Only Office Wi-Fi considered

Table 2 Attack Surface and Scope

As Group 2 changed their website URL, IP, and configuration during our exercise, Group 3 had conducted another scanning exercise, which is the reason for including analyses and recommendations against several assets in this report. Image 1 describes the timeline of information gathering, scanning, evaluation, and documentation.

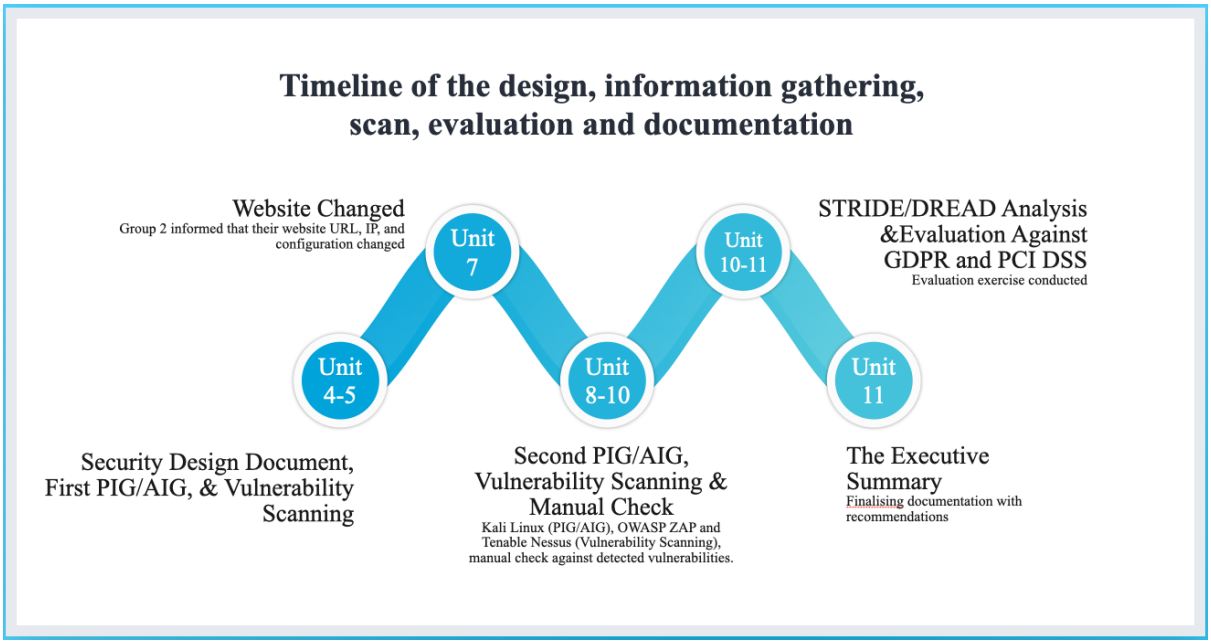


Image 1: Timeline of information gathering, scanning, evaluation, and documentation

Findings Summary

PIG and AIG

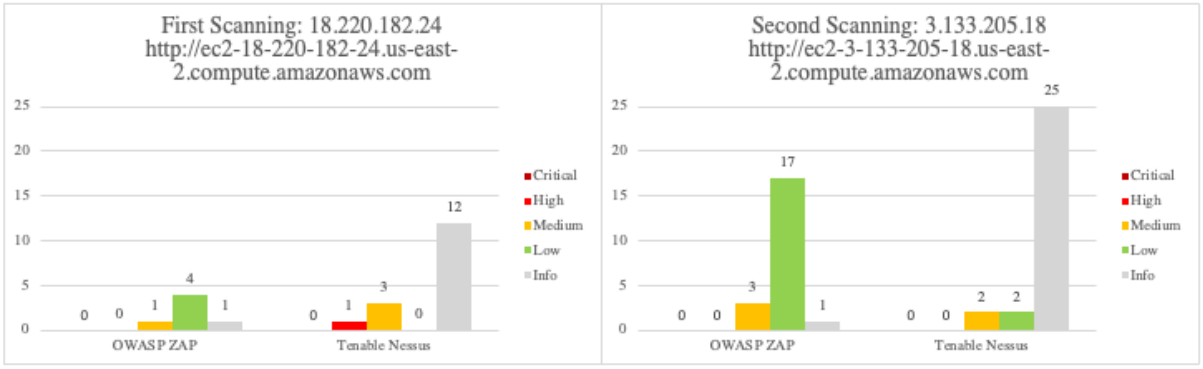
PIG safely collects information without direct communication with the target system (Thion, 2007), often before AIG. Group 3 carried out scanning using Kali Linux to the assets to identify the attack surface basic information, including open protocols and ports, configuration of Web Application Firewall (WAF), Contents Delivery Network (CDN) and operating system (OS). Table 3 shows the summary of the scanning results.

Scanning Domain	Scanning results
Open Protocols	TCP (HTTP, SSH), ICMP, UDP
Open Ports	22, 80, 111
Running Operating System	Linux 2.6.x
Running Web Server	Apache
Server Hosted	US Seattle
Protection type	Firewall
WAF / CDN / Load Balancer	Not Detected

Table 3: AIG: Kali Linux Scanning Results

Vulnerability Scanning Results

Group 3 utilised Tenable Nessus and OWASP ZAP for the vulnerability scan. Graph 1 shows the results of the two vulnerability scanning exercises on two assets.

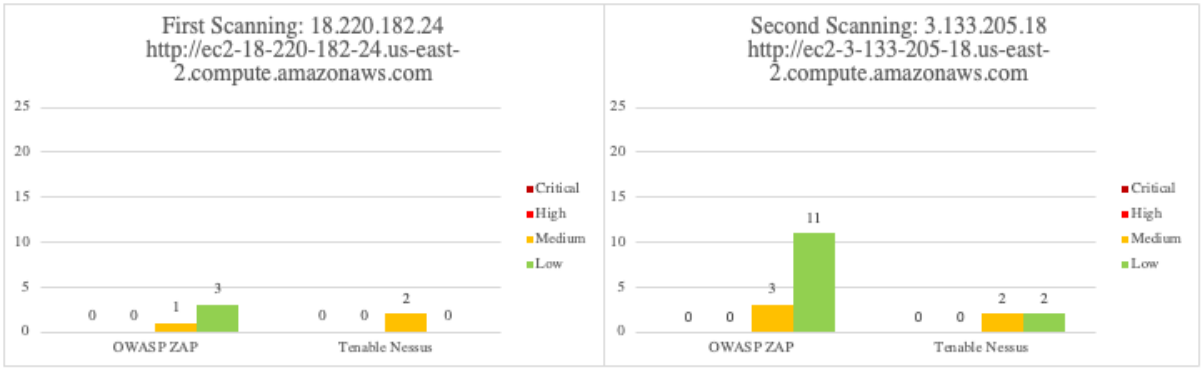


Graph 1: Results of OWASP ZAP & Tenable Nessus Scanning

List of Vulnerabilities				Total Vulnerability Found (First Scan / Second Scan)	
Name	Risk Level	Category	Status	OWASP ZAP	Tenable Nessus
CGI Generic SQL Injection	High	Applications	Closed False Positive	0	1 (1/0)
CGI Generic Path Traversal	Medium	Applications	Closed False Positive	0	1 (1/0)
Vulnerable to Clickjacking	Medium	Applications	Open	4 (1/3)	2 (1/1)
.DS_Store Web Directroy Listing	Medium	Applications	Open	0	2 (1/1)
Absense of Anti-CSRF Tokens	Low	Applications	Open	3 (1/2)	0
Cross-Domain JavaScript Source File Inclusion	Low	Applications	Closed False Positive	7 (1/6)	0
X-Content-Type-Options Header Missing	Low	Applications	Open	11 (2/9)	0
SSH Server CBC Mode Ciphers Enabled	Low	Server	Open	0	2 (1/1)
SSH Weak Key Exchange Algorithms Enabled	Low	Server	Open	0	2 (1/1)

Table 4: List of Vulnerabilities Detected

Tenable Nessus and OWASP ZAP identified five web application vulnerabilities and two server vulnerabilities (See Table 3). As Graph 1 shows the apparent gaps between the two results, Group 3 had conducted additional checks on the detected vulnerabilities. Because of the nature of the tools, checking false positives is necessary. Qasaimeh et al. (2018) examined Tenable Nessus and OWASP ZAP and observed the former scored 31 false positives out of 340 scans, while OWASP ZAP scored 281 false positives out of 1039 scans. As Table 4 shows, three types of vulnerabilities are false positives by the manual checks on the detected vulnerabilities. Graph 2 illustrates the actual vulnerabilities of the applications and servers. Tenable Nessus marked 20% false positives, while OWASP ZAP did 28% this time.



Graph 2: Results of OWASP ZAP & Tenable Nessus Scanning and Manual Check

Evaluation against GDPR and PCI DSS

Group 2 website is an e-health website that provides consultancy/advisory services to the users using medical records, expecting the use of sensitive user data and payment over the advisory services. Hence, Group 3 had assessed the website against GDPR and PCI DSS. Governments in the European Union established and maintained the GDPR framework to protect the users' data in a system as the primary goal (Butpheng et al., 2020). Table 5 describes the possible non-compliance items against GDPR and PCI DSS.

List of Vulnerabilities and Consideration Items	GDPR Article	PCI DSS Requirement
CGI Generic SQL Injection, No WAF	5, 32, 34	6.6
SSH Server CBC Mode Ciphers Enabled	32, 34	4.1, 6.5.4
SSH Weak Key Exchange Algorithms Enabled	32, 34	4.1, 6.5.4
ICMP/UDP Protocols, Port 22&111 are Open	32, 34	1.2.1, 4.1, 6.5.4
Vulnerable to Clickjacking	32, 34	N.A.
Absense of Anti-CSRF Tokens	32, 34	6.5.9
X-Content-Type-Options Header Missing	32, 34	6.5.7
No SSL	32, 34	4.1, 6.5.4
.DS_Store Web Directroy Listing	32	N.A.
No cookie agreement screen	28	N.A.

Table 5: List of Vulnerabilities Against GDPR and PCI DSS

Evaluation against GDPR

All listed items possibly contravened Art. 32 that requires "risk-appropriate and state-of-the-art security measures" (Shah et al., 2019). Hence, any possible vulnerabilities are necessary to fix promptly. In addition, code injection vulnerability may lead to contravening Art. 5 that requires assuring an adequate degree of security to protect personal data (Barrett, 2020) by keeping data accurate, complete and up to date. Although the vulnerability was false positive, the organisation should have protection because of the enormous impacts of the attack. Another possible violation item is data breach-related vulnerabilities that relate to Art. 34 "Communication of a personal data breach to the data subject" (Intersoft Consulting, N.D.). The items directly or indirectly affect the threats

which lead to a data breach. In addition to detected vulnerabilities, the website should have a GDPR data processing agreement with the visitors as required in Art. 28, "Processor". Hussain et al. (2020) recommend that the organisation establish clear policies for customer-related information, especially data protection, processing, and portability.

Evaluation against PCI DSS

Based on the scans, most vulnerabilities relate to its requirements. Req. 6.1 requires the organisation to treat these vulnerabilities per the organisation's vulnerability classification scheme (PCI Security Standard Council, 2018). The listed items do not comply with Req 1.2.1 "Restrict inbound and outbound traffic to that which is necessary", Req. 4.1 "Use strong cryptography and security protocols", Req. 6.5.4 “Insecure communications", Req. 6.5.7 "Cross-site scripting (XSS)", Req. 6.5.9 "Cross-site request forgery (CSRF)" and Req. 6.6 "Ensuring to protect applications against known attacks" (PCI Security Standard Council, 2018). The organisation should fix all items before any third party conducts the PCI DSS assessment.

Threat Risk Analysis

STRIDE Threat Analysis

STRIDE is a conventional threat methodology (Hussain et al., 2014), categorising security threats based on their nature (Jiang et al., 2010), which analyses threats against attack scenarios that adversaries may apply to imperil the whole system using vulnerabilities (Khan et al., 2017). Table 6 shows threats and possible attacks against the organisation's assets based on PIG/AIG and the detected vulnerabilities. The STRIDE security categories' description in Table 2 references Abomhara et al. (2015).

Assets	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Escalation of Privilege
Category Description (Abomhara et al., 2015)	*Gain access to a system by a false identity.*	*The unauthorized modification of data*	*Ability to deny that they performed specific actions.*	*Unwanted exposure of private data.*	*Process of making a system unavailable.*	*Gain privileged access to an asset.*
Servers	Impersonate admin user	Tamper configuration	Deleting access logs	Disclose medical information	Flood with ICMP/UDP data	Takeover Account
Potential Attack(s)	*SSH Password Cracking*	*SSH Password Cracking*	*SSH Password Cracking*	*SSH Password Cracking*	*ICMP/UDP Flood*	*SSH Password Cracking*
Applications	Impersonate a web application	Tamper data records	Deny sending data to the server	Disclose medical / payment Information	Flood with HTTP GET/POST request	Server account takeover
Potential Attack(s)	*Clickjacking CSRF Attack*	*Code Injection / CSRF Attack / Clickjacking*	*MITM*	*Code Injection / MITM / XSS Attack*	*HTTP GET/POST Flood*	*OS Injection Attack*

Table 6: STRIDE Threat Analysis With Potential Attacks

STRIDE analysis has its limitations. Microsoft (2007) criticises the fact that "STRIDE has a number of cross-correlations". One threat security category directly impacts other threat categories. For example, escalation of privilege leads to other five security categories components. Hence, almost all security categories embrace SSH Password Cracking.

DREAD Risk Analysis

DREAD is a threat risk ranking framework developed by Microsoft (Suprihanto&Mustofa, 2018) that enables the prioritisation of risks by quantifying risk values of threats (Singhal&Banati, 2011).

DREAD provides the organisation with a risk estimate against business impact by an attack (Abdulrazeg et al., 2014).

The values for the DREAD 3-point scale criteria in Table 7 stemmed from the reference Rao&Pant (2010) and Group 3 professional experience inputs.

Identification (Abbreviation)	Description (Rao&Pant, 2010).	Rating		
		1	2	3
Damage Potential (D)	The loss if the vulnerability is exploited	Nothing	Individual/employer non-sensitive user data compromised	All data compromised
Reproducibility (R)	How easy is it to reproduce the attack	Very hard, even for administrators of the system	Complex, 1-2 steps are required, requires an authorised user	Very easy through a web browser, no authentication
Exploitability (E)	How easy to attack the assets	Advanced programming, deep knowledge, networking skills	Exploit easily performed using available attacks tools	Web browser
Affected Users (A)	Average affected users in enterprise	No users affected	Some users, but not all	All users
Discoverability (D)	How easy to find out the vulnerabilities	Very hard, requires administrative access	Can figure out by guessing or analysing a system or IT data flow	Details of faults are already in public domains and can be easily discovered using a search engine

Table 7: DREAD Identification and 3-Point Scale Scoring Criteria

Risk Rating	DREAD Score	Remediation Timelines	Comments
Critical	13-15	Within 3 days	The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations. Should be considered immediately for review and resolution.
High	10-12	Within 7 days	The threat event could be expected to have a serious adverse effect on organizational operations. Should be considered for review and resolution within a short period of time.
Medium	7-9	Within 30 days	The threat event could be expected to have a limited adverse effect. Recommended to consider for review.
Low	5-6	Recommendation Only	The threat event could be expected to have a negligible effect.

Table 8: Risk Rating Matrix and Scoring Methodology Against Business Impact

Table 8 provides a risk rating matrix and DREAD scoring methodology against business impact, which indicates how each threat may impact the organisation business.

The STRIDE threat and DREAD risk models are pertinent and complementary and provide a structured analysis (Kavallieratos&Katsikas, 2020), inheriting potential attacks listed in STRIDE as threats in DREAD analysis. While STRIDE promotes qualitative threat analysis by identifying the potential threats using six security categories, DREAD produces quantitative risk estimates that emerge from the threats discovered by STRIDE (Kavallieratos&Katsikas, 2020). Table 9 describes the DREAD analysis against threats listed in the STRIDE analysis.

Threats	D	R	E	A	D	Total	Risk Rating
Code Injection	3	3	3	3	2	14	Critical
SSH Password Cracking	3	2	2	3	2	12	High
ICMP/UDP Flood	1	3	2	3	2	11	High
HTTP GET/POST Flood	1	3	2	3	2	11	High
MITM by cracking organization Wi-FI and monitor unencrypted data	2	2	2	2	2	10	High
Clickjacking	2	2	1	3	2	10	High
XSS Attack	3	1	1	3	2	10	High
CSRF Attack	3	1	1	3	2	10	High
.DS_Store Web Directory listing	1	2	1	1	2	7	Medium

Table 9: DREAD Analysis Against Threats Discovered By The STRIDE Analysis.

Deriving risk values is a must when performing cost/benefit analyses. However, people intentionally avoid deriving values or quantifying risk with attributes and numerical values since this quantification requires further involvement of subjective judgement, which organisations must thoroughly address during the entire lifecycle of the risk management process (Redmill, 2001).

DREAD-based risk scoring and STRIDE-based threat classification are subjective in threat classification and risk assessment. Risk analyses contribute to a determination of risk value, especially for DREAD-based evaluations. However, most of the process stages involve different subjectivity due to the need for judgement. Redmill (2001) stated that it leads to a more subjective and biased outcome and contributes to the dilemma between accuracy and precision. Due to this dilemma, results collected on each performed risk analysis could vary from one risk analyst to another (Redmil, 2001).

Moreover, due to the nature of the process, subjectivity is considered one of the most significant challenges and limitations, which can be further decreased with thorough consideration of environment-specific conditions.

Conclusions

In conclusion, a combination of scanning methodologies, evaluation methods, and evaluation against security standards sheds light on security challenges from different perspectives. AIG, PIG and vulnerability scan provide essential information to evaluate against security standards and address potential threats produced in STRIDE and utilised in DREAD. A threat modelling process addresses identifying the potential threats, attacks, risks and countermeasures to meet the organisation security goals and mitigate the negative business impacts against the observed risks at large (Rao&Pant, 2010). The risk score varies depending on the methodologies applied, which alerts us not to get relieved to see the low-risk group. The low-risk item potentially impacts the organisation severely.

Group 3 recommends that Pink Organisation e-health services start working on countermeasures per risk score.

Recommendation

Protecting personal data and payment data is critical as improper security measures will lead to sanctions to the company, and cardholder data breaches will directly impact user financial loss. GH.

(2019) reported that the Hague Hospital got penalised 460,000 euros for lacking organisation protection measures against patient data.
As Table 8 describes, the DREAD rating scores directly relate to a business impact. As Table 10 shows the vulnerabilities and consideration items as per DREAD score rating in descending order, Group 3 provides the countermeasure recommendations accordingly, leading to compliance with GDPR and PCI DSS.

List of Vulnerabilities and Consideration Items	Risk by Scanning Tools	Threat	DREAD Score	DREAD	Category	GDPR Article	PCI DSS Requirement	Countermeasures
No WAF	N.A.	Code Injection	14	Critical	Servers	5, 32, 34	6.6	Implement WAF
SSH Server CBC Mode Ciphers Enabled	Low	SSH Password Cracking	12	High	Servers	32, 34	4.1, 6.5.4	Disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.
SSH Weak Key Exchange Algorithms Enabled	Low	SSH Password Cracking	12	High	Servers	32, 34	4.1, 6.5.4	Disable the weak algorithms.
ICMP/UDP Protocols, Port 22&111 are Open	N.A.	ICMP/UDP Flood, SSH Password Cracking	11	High	Servers	32, 34	1.2.1, 4.1, 6.5.4	Close ICMP/UDP Protocol including Port 22 & 111
HTTP GET/POST Flood	N.A.	HTTP GET/POST Flood	11	High	Servers & Applications	32, 34	6.5.5	Monitoring and Firewall rule improvement. Proper Error handling.
Vulnerable to Clickjacking	Medium	Clickjacking	10	High	Applications	32, 34	N.A.	X-Frame-Options or Content Security Policy to be added to HTTP Header.
Absense of Anti-CSRF Tokens	Low	CSRF Attack	10	High	Applications	32, 34	6.5.9	- Add one-time token - Add SameSite=Lax or Strict
X-Content-Type-Options Header Missing	Low	XSS Attack	10	High	Applications	32, 34	6.5.7	X-Content-Type-Options header to 'nosniff' for all web pages.
No SSL	N.A.	MITM Attack	10	High	Servers	32, 34	4.1, 6.5.4	Implement SSL and force HTTPS
.DS_Store Web Directroy Listing	Medium	Directroy Listing	7	Medium	Applications	32	N.A.	Remove .DS_Store file from the server.
No Cookie agreement screen	N.A.	GDPR Sanction	N.A.	N.A.	Applications	28	N.A.	Add agreement screen

Table 10: List of Countermeasures

Critical Risk

No WAF was detected, which may not prevent known vulnerabilities, including code injection attacks. WAF enables the system to block code injection (Harefa et al., 2021). The blind SQL Injection allows the malicious actor to access the database server and perform critical actions such as adding, altering or deleting records. As a consequence of this attack, the security triad of the business is vulnerable, where confidentiality is susceptible to data exposure, and the integrity of the data is at risk due to the attacker's capability of altering existing data (Spett, 2004). Group 3 recommends implementing WAF to comply with PCI DSS Req. 6.6 "Ensuring to protect applications against known attacks", GDPR Art. 5 that requires keeping personal data accurate and up to date, Art. 32 that requires applying necessary security measures, and Art. 34 that requires implementing technical protection measures to the personal data.

High Risk

For high-risk items, server-and-application-related countermeasures are recommended, leading to complying with GDPR Art. 32 and 34. PCI DSS requires limiting only necessary inbound and outbound traffic in Req. 1.2.1, applying secure cryptography and security protocols in Req. 4.1, and avoiding insecure communications in Req. 6.5.4. Hence, for servers related items, Group 3

recommends (1) disabling CBC mode cypher encryption and weak key exchange algorithm to prevent SSH password cracking; (2) closing ICMP/UDP protocol including ports 22 and 11 to prevent ICMP/UDP Flood; (3) forcing HTTPS by implementing SSL and opening port 443 to block Man-in-the-middle (MITM); and (4) monitoring and tuning firewall to prevent HTTP-GET-POST flood. Organisations need to be careful because these attacks will lead to the threats classified in all security threat categories in STRIDE analysis shown in Table 6.

For application related items, OWASP ZAP and Tenable Nessus detected Clickjacking, CSRF, XSS vulnerabilities, which contravenes PCI DSS Req. 6.5.9 and Req. 6.5.7 respectively. Clickjacking vulnerability allows the attacker to trick the webserver user into making fraudulent actions by clicking space where unethical hackers injected malicious codes, which derives from lacking x-Frame options (Nessus, 2015).

Medium Risk, N.A. and others

For medium risk items, Group 3 recommends deleting the DS_Store file from the server. DS_Store is a file that helps locate the position of the files and directory in the webserver (Nessus, 2001). This vulnerability leads to different threats depending on the files and directories that adversaries can read.

For the N.A. item, Hussain et al. (2020) recommend that the organisation establish clear policies for customer-related information, especially data protection, processing, and portability, to comply with GDPR Art. 28 "Processor", and the website should have a GDPR data processing agreement with the visitors.

Lastly, Group 3 recommends testing systems regularly, at least once a year or when the organisation changes their systems at a large scale, to ensure that vulnerabilities do not exist and comply with PCI DSS Req. 11 and GDPR Art. 32, both of which require regular security testing.

References

Abdulrazeg, A. A., Norwawi, N. M. & Basir, N. (2014) 'Extending V-model practices to support SRE to build secure web application'. *2014 International Conference on Advanced Computer Science and Information System*. Jakarta, Indonesia, 18-19 October. Jakarta:IEEE. 213-218. DOI: 10.1109/ICACSIS.2014.7065838

Abomhara, M., Gerdes, M. & Koien, G. M. (2015) A stride-based threat model for telehealth systems. *Norsk informasjonssikkerhetskonferanse (NISK)*. *8*(1):82-96.

Barrett, C. (2020) Emerging Trends from the First Year of EU GDPR Enforcement. *Scitech Lawyer*. 16(3):22-35.

Butpheng, C. Yeh, K. Xiong, H. (2020) Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review. *Symmetry.* 12(7): 14-15.available from: https://doi.org/10.3390/sym12071191

GH., A.E.I.C. (2019) The new data protection regulation claims under GDPR. Journal of Information Systems & Operations Management 13(2): 100-115. Available from: http://web.rau.ro/websites/jisom/Vol.13%20No.2%20-%202019/JISOM-WI19-A07.pdf [Accessed 13 September 2021].

Harefa, J., Prajena, G., Alexander, A.M. Dewa, E.V.S. & Yuliandry, S. (2021) SEA WAF: The Prevention of SQL Injection Attacks on Web Applications. Available from: https://www.researchgate.net/profile/Alexander-Alexander-z4/publication/350488284_SEA_WAF_The_Prevention_of_SQL_Injection_Attacks_on_Web_Applications/links/60763b19299bf1f56d560b8e/SEA-WAF-The-Prevention- of-SQL-Injection-Attacks-on-Web-Applications.pdf [Accessed 2 July 2021].

Hussain, F., Hussain, R., Noye, B. & Sharieh, S. (2020) Enterprise API security and GDPR compliance: design and implementation perspective. *IT Professional*. 22(5):81-89.

Hussain, S., Kamal, A., Ahmad, S., Rasool, G. & Iqbal, S. (2014) Threat modelling methodologies: a survey. Sci. Int. 26(4): 1607-1609. Available from: https://www.researchgate.net/profile/Sajid-Iqbal-8/publication/307902746_THREAT_MODELLING_METHODOLOGIES_A_SURVEY/links/57d103a608ae5f03b4891979/THREAT-MODELLING-METHODOLOGIES-A- SURVEY.pdf [Accessed 30 June 2021].

Intersoft Consulting (N.D.) General Data Protection Regulation. Available from: https://gdpr-info.eu/ [Accessed 3 October 2021].

Kavallieratos, G. & Katsikas, S. (2020) Managing cyber security risks of the cyber-enabled ship. *Journal of Marine Science and Engineering*. 8(10): 768.

Khan, R., McLaughlin, K., Laverty, D. & Sezer, S. (2017) ' STRIDE-based threat modeling for cyber-physical systems'. *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-*

Europe). Turnin, Italy, 26-29 September. Trurnin: IEEE. 1-6. DOI: https://doi.org/10.1109/ISGTEurope.2017.8260283

Liu, C., Shinghal, A. & Wijesekera, D. (2020) 'Forensic Analysis of Advanced Persistent Threat Attacks in Cloud Environments', IFIP International Conference on Digital Forensics: Advances in Digital Forensics XVI. New Delhi, 6-8 January. New Delhi: Springer, Cham: 161-180.

Microsoft (2007) DREADful. Available from: https://docs.microsoft.com/en-us/archive/blogs/david_leblanc/dreadful [Accessed 24 October 2021].

Morse, E. Raval, V. (2008) PCI DSS: Payment card industry data security standards in context. Computer Law & Security Review. 24(6): 540 Available from: https://www.sciencedirect.com/science/article/pii/S0267364908000976

Nessus (2001) Nessus | Plugins. Available from: https://www.tenable.com/plugins/nessus/10756 [Accessed 22 October 2021]

Nessus (2015) Nessus | Plugins. Available from: https://www.tenable.com/plugins/nessus/85582 [Accessed 22 October 2021]

PCI Security Standards Council (2018) Payment Card Industry (PCI) Data Security Standard. Available from: https://www.commerce.uwo.ca/pdf/PCI_DSS_v3-2-1.pdf [Accessed 11 October 2021].

Qasaimesh, M., Shamlawi, A. & Khairallah, T. (2018) Black Box evaluation of web application scanners: standards mapping approach. Journal of Theoretical and Applied Information Technology 96(14): 4584-4596.

Redmill, F (2001) Subjectivity in Risk Analysis. Available from: http://www.csr.ncl.ac.uk/FELIX_Web/new_index.html [Accessed 25 October 2021].

Shah, A., Banakar, V., Shastri, S., Wasserman, M. & Chidambaram, V. (2019). 'Analyzing the impact of {GDPR} on storage systems'. *11th {USENIX} Workshop on Hot Topics in Storage and File Systems (HotStorage 19)*. the Hyatt Regency Lake Washington, Washington, 8-9 July. Renton: {USENIX} Association.

Singhal, A. & Banati, H (2013). Fuzzy logic approach for threat prioritization in agile security framework using DREAD model. *IJCSI International Journal of Computer Science Issues.* 8(4): 182-190.

Sood, A. K. & Enbody, R. J. (2012) Targeted cyberattacks: a superset of advanced persistent threats. *IEEE security & privacy*. 11(1):54-61.

Spett, K. (2004) securityDocs.com. Available from: https://web.archive.org/web/20101230192555/http://www.securitydocs.com/library/2651 [Accessed 21 October 2021].

Suprihanto, D., Wardoyo, R. & Mustofa, K. (2018) Determination of Weighting Assessment on DREAD Model using Profile Matching. *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*. 9(10):68-72.

Bibliography

Alhassan, J. K., Abba, E., Olaniyi, O. M. & Waziri, O. V. (2016) Threat modelling of electronic health systems and mitigating countermeasures. Available from: http://repository.futminna.edu.ng:8080/xmlui/handle/123456789/9522 [Accessed 24 Oct 2021].

Campbell, S. (2006) Risk and the Subjectivity of Preference. *Journal of Risk Research*. 9(3):225-242. DOI: 10.1080/13669870600603147

Venkataraman, S. & Harrison, W. (2005) Prioritization of threats using the k/m algebra. *Proceedings of Workshop on Software Security Assurance Tools, Techniques, and Metrics.* 90-95.

Zhang, L., Taal, A., Cushing, R., de Laat, C. & Grosso, P. (2021) A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces. *International Journal of Information Security*. 1-17.