Introduction

The client Financial institution engaged security consultants to do a vulnerability assessment on its public facing website hosting financial web applications and sensitive data.

According to a 2021 Verizon's Data Breach Investigations Report (DBIR), the leading data type compromised within the financial services industry is personal - 83%, followed by bank data - 33% (Verizon, 2021). The financial services industry is heavily dependent on customer's personal data and payment card data. In addition, security breaches and data loss can cause reputational damage to the company, hence security is a priority for any company offering financial services. Since the financial sector relies heavily on the implicit trust between itself and the customers, it is especially susceptible to loss of confidence due to cyber-attacks.

Majority of the cyber-attacks are targeted towards banks (91 percent of the attacks) followed by insurance companies (7 percent). Among the banking lines of business, retail banking is attacked 39 percent of the time and credit card services are targeted 25 percent of the time.

Financial institutions are bound by governance directives such as GDPR (general data protection regulation) and PCI DSS (payment card industry data security standard). By complying with PCI DSS, an entity can ensure that they have met the minimum requirements to protect payment card data. Similarly, by complying with GDPR, an organization can confirm the minimum requirements to secure the customer's personal data.

Scope and Methodology

The scope of the assessment only includes the financial website hosted in AWS cloud with the following URL **http://ec2-184-73-185-129.compute-1.amazonaws.com**

The assessment is based on both static analysis and dynamic analysis methods

Static Analysis

- Implementation of user identification, authentication, authorization, and access control systems was assessed against general financial industry business requirements and web application best practices
- Data confidentiality and integrity by checking against current encryption standards and implementations
- Source based analysis of program code, scripts, html files, configuration files, directory lists allowing identification vulnerabilities not covered by protocol based dynamic testing approaches
- Security policies and procedures

Dynamic Analysis

- Systematic scan of ports, network protocols, web server OS and services
- Vulnerability patterns based on protocols such as network or HTTP, SSL/TLS etc.
- Validate security configuration settings, software versions and security shortcomings.

Summary of Findings

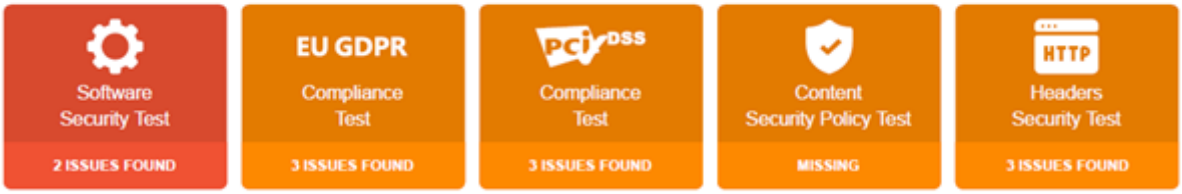

Figure 1 – Summary of findings

Web Server Security Test Results

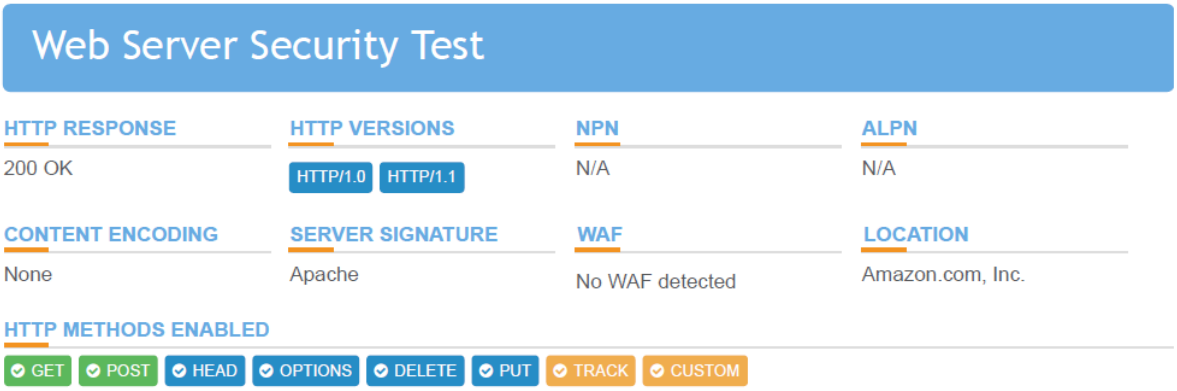

Figure 2 – Web Server Security Test

GDPR Compliance Test Results

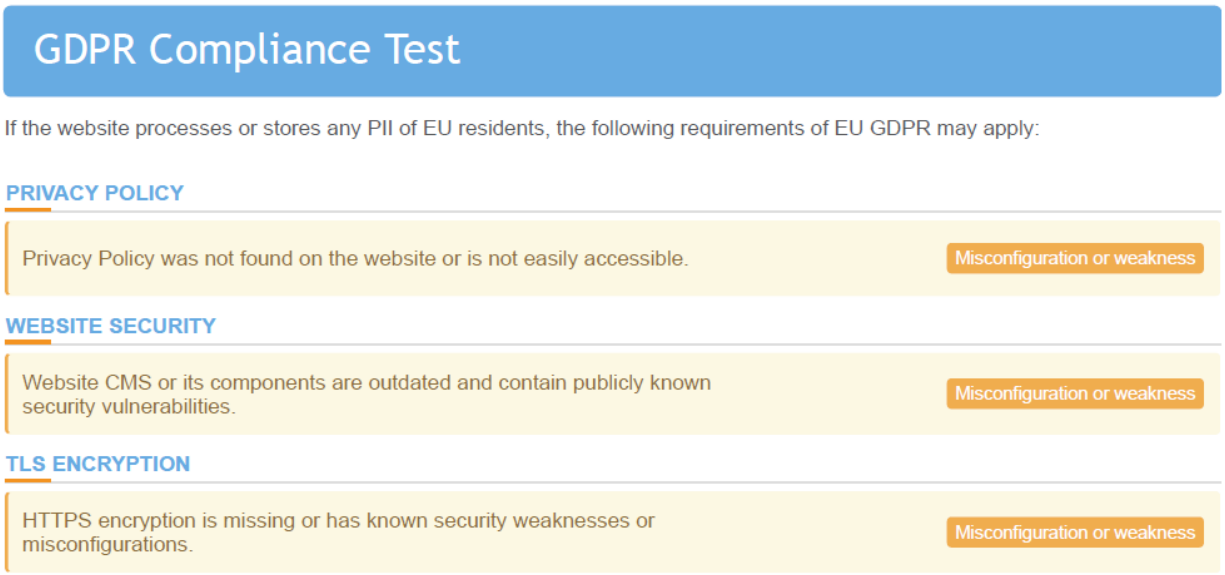

Figure 3 – GDPR Compliance Test

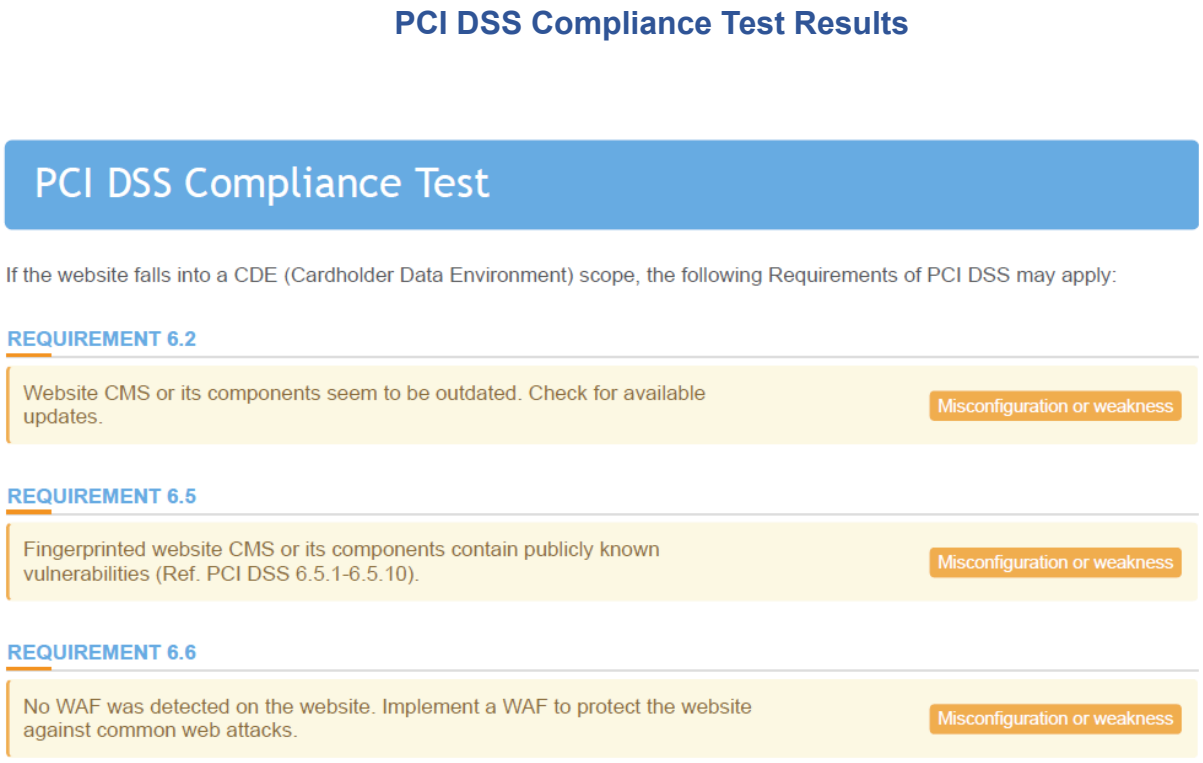

Figure 4 – PCI DSS Compliance Test

Figure 5 – HTTP Headers Security

Software Security Test Results

FINGERPRINTED CMS & VULNERABILITIES

No CMS were fingerprinted on the website. Information

FINGERPRINTED CMS COMPONENTS & VULNERABILITIES

jQuery 1.8.3

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **3.6.0**.

CVSSv3.0 Score	Vulnerability CVE-IDCVE	Vulnerability TypeType
5.5 Medium	CVE-2020-7656	CWE-79 — Cross-site scripting
5.5 Medium	CVE-2020-11022	CWE-79 — Cross-site scripting
5.5 Medium	CVE-2012-6708	CWE-79 — Cross-site scripting
5.3 Medium	CVE-2015-9251	CWE-79 — Cross-site scripting
4.8 Medium	CVE-2019-11358	CWE-400 — Prototype pollution
4.2 Medium	CVE-2020-11023	CWE-79 — Cross-site scripting

Bootstrap 2.2.2

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **5.0.2**.

CVSSv3.0 Score	Vulnerability CVE-IDCVE	Vulnerability TypeType
5.5 Medium	CVE-2018-14040	CWE-79 — Cross-site scripting
5.5 Medium	CVE-2018-14042	CWE-79 — Cross-site scripting
5.5 Medium	CVE-2018-14041	CWE-79 — Cross-site scripting
5.3 Medium	CVE-2018-20677	CWE-79 — Cross-site scripting
5.3 Medium	CVE-2018-20676	CWE-79 — Cross-site scripting

Figure 6 – Software Security - CMS and WEB Vulnerabilities.

Recommendations

Following assessment, our recommendations for the vulnerabilities found throughout scanning follows the Open Web Application Security Project (OWASP) methodology. OWASP is a nonprofit foundation that builds a framework for vulnerability assessment using community-driven, open-source software projects to better define web-based vulnerabilities to direct the development of secure website design and web software (owasp.org, nd).

OWASP releases the OWASP top ten (A1-A10) to broadly categorize the top ten vulnerability categories. Vulnerability severity ratings are decided based on the OWASP Risk Rating Methodology seen in the table below; ranking areas such as technical impacts or exploitability on a three-tier scale, 3 being the most severe. While this list is not exhaustive and does not include all vulnerabilities assessed, it does represent the most urgent vulnerabilities to resolve.

Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
Application Specific	Easy: 3	Widespread: 3	Easy: 3	Severe: 3	Business Specific
	Average: 2	Common: 2	Average: 2	Moderate: 2	
	Difficult: 1	Uncommon: 1	Difficult: 1	Minor: 1	

Figure 7: OWASP Risk Rating Methodology Table (OWASP, 2017)

Vulnerability	Recommendation
Using HTTP provides an insecure connection between website and client browser OWASP Class: **A3** - Sensitive Data Exposure OWASP Risk Score out of **10: 7**	HTTP traffic is insecure, the standard being HTTPS using TLS encryption. Configuring the web server to use HTTPS will ensure greater security between webserver and web browser. Not only is this required to be PCI compliant, but it is also mandatory by GDPR; failure to provide encrypted traffic can result in heavy fines and penalties. See **Figure 2 – Web Server Security Test** for vulnerability details
Vulnerability	**Recommendation**

Missing Security Headers: • Content-Security-Policy (CSP) • X-XSS-Protection • X-Content-Type-Options • Mac OSX .DS Store Web Directory Listing • Anti-clickjacking X-frame-Options header OWASP Class: **A6** - Security Misconfiguration OWASP Risk Score out of **10: 6**	Security misconfigurations, such as missing security headers can be particularly damaging due to their presence up and down the application stack, from network services to server and database functions. Impact can range from unauthorized access to system data or function to complete system compromise. • While each of these reflect distinct risks their resolution is often to enable, change or configure from the default setting. • Having a repeatable configuration process for hardening new websites can ensure these services and settings don't go unchecked when designing a website. • Containerized architecture can prevent vulnerability bleed across a website in the event of compromise. • Anti-clickjacking can be resolved by configuring See **Figure 5 – HTTP Headers Security** for vulnerability details
Medium Severity Cross Site Scripting (XSS): OWASP Class: **A7** - Cross-Site Scripting OWASP Risk Score out of **10: 6**	This highly exploitable vulnerability can be easy to detect and can have moderately severe impacts if left unchecked. This is best resolved by: • understanding the capabilities and limitations of the XSS protections offered by the frameworks used (Ruby on Rails, React JS, etc). Selecting a framework that incorporates preventative XSS measures will greatly improve security by default. • Enabling a Content-Security Policy is a very effective means to harden a website, especially if code injection vulnerabilities have been identified and policy is configured to prevent local file access to vulnerable libraries. See **Figure 5 – HTTP Headers Security** for vulnerability details
Vulnerability	**Recommendation**
Out of Date Components: jQuery and Bootstrap OWASP Class: **A9** - Using Components with Known Vulnerabilities	This can be resolved through a well-defined patch tracking and management policy. • The version of jQuery used is out of date and should be brought to latest version **3.6.0**

OWASP Risk Score out of **10:** 4.7	• The version of Bootstrap is out of date and should be brought up to the latest version **5.0.2** See **Figure 6 – Software Security - CMS and WEB** for vulnerability details

Figure 8: Ranked vulnerabilities and recommended solutions (OWASP, 2017)

General Data Protection Regulation (GDPR)

By complying with GDPR, an entity can confirm the minimum requirements to secure the customer's personal data.

The data governance and compliance practices should include people, processes, and technology (Olavsrud, 2021). Therefore, evaluating the website for compliance with security standards requires a more holistic approach than just technical assessment or scanning activities. The evaluation steps should include reviewing various policies, standards, and procedures. In addition, interviewing and inquiring members from senior management, middle management, subject matter experts, and employees also should be included within the evaluation process.

GDPR unites data privacy laws across the European Union (EU). The objective of the GDPR is protecting citizen's personal data, with the interests of the individual at its core. To evaluate the financial services website against GDPR, identifying personal data and data flow within the website.

Personal information can be identified by performing data discovery scans or using Data Loss Prevention Solution (DLP). After personal data is identified within the website, GDPR related requirements can be verified.

Goals	GDPR Reference Article	Website Evaluation Against GDPR*	GDPR Evaluation Results**
Accountability Governance	5(2) 7(1) 37(5,7) 38(1-6) 39(1,2)	Onsite Assessment	N/A
Processing Principles	5(1) 6(1,2,3,4) 9(1,2) 10 24(1,2,3)	Onsite Assessment	N/A

Privacy by Design and Default	24(1): Responsibility of the controller 25(1,2): Data protection by design and by default 32(1,2,4): Security of processing	Onsite Assessment	Non-compliance: Privacy Policy was not found on the website or is not easily accessible.
Data Protection Impact Assessment	35(1,2,7,9,11) 36(1,2,3)	Onsite Assessment	N/A
Records of Processing	30(1,2,3,4,5) 31	Onsite Assessment	N/A
Data Subject Rights	15(1,2,3,4) 16 17(1,2,3) 18(1,2,3) 19 20(1,2) 21(1,2,3,4,6) 22(1,2,3,4)	Onsite Assessment	N/A
Consent and Notices	7(1,2,3) 8(1,2) 12(1,3,4,5) 13(1,2,3,4) 14(1,2,3,4,5)	Onsite Assessment	N/A
Breach Management	24(1,2,3) 32(1) 33(1,2,3,4,5) 34(1,2,3)	Onsite Assessment	N/A
Processors	24(1,2,3) 25(1) 28(1,2,3)	Onsite Assessment	N/A

Data Transfers	32(1): Security of processing 44: General principle for transfers 45(1,8): Transfers on the basis of an adequacy decision 46(1,2,3): Transfers subject to appropriate safeguards 47(1,2): Binding corporate rules	Technical Assessment: Encrypt data encryption; and Secure data transfer methods. Onsite Assessment	Non-compliance: The website is using HTTP instead of HTTPS. All requests and responses can be read by anyone who is monitoring the session. Website CMS or its components are outdated and contain publicly known security vulnerabilities.

* **Onsite Assessment** includes the review of website, policies, standards & procedure and interviews various stakeholders.

** **N/A** indicates, unable to determine due to insufficient data.

Payment Card Industry Data Security Standard (PCI DSS)

By complying with PCI DSS, an organisation can ensure that they have met the minimum requirements to protect payment card data. Identifying the payment card data and cardholder data environment (CDE) within the network is a critical step. A data flow diagram can be used to determine the in-scope systems and flows of data (Calver, 2018).

If any third-party service providers are used within the CDE environment, that is essential to ensure that the service providers comply with PCI DSS requirements (PCI Security Standards Council, 2018). This can be attained by using audit reports completed by reputed audit firms.

Amazon Web Services (AWS) compliance status can be obtained from the AWS website. According to the AWS site, AWS is certified as a PCI DSS Level 1 Service Provider.

Goals	PCI DSS Requirements	Website Evaluation Against PCI DSS	PCI Evaluation Results
Build and Maintain a Secure Network and Systems	1) Install and maintain a firewall configuration to protect cardholder data	Review the website architecture diagram Onsite Assessment	N/A

	2) Do not use vendor-supplied defaults for system passwords and other security parameters	Vulnerability Assessment; Onsite Assessment	N/A
Protect Cardholder Data	3) Protect stored cardholder data	Data Discovery Scans; Onsite Assessment	N/A
	4) Encrypt transmission of cardholder data across open, public networks	Technical Assessment: Encryption; Onsite Assessment	**Non-compliance:** The website is using HTTP instead of HTTPS. All requests and responses can be read by anyone who is monitoring the session **Note:** Because the website didn't host payment card data, this was not identified as PCI non-compliance by the PCI scan. However, as this is a financial service related website, this will result in non-compliance.
Maintain a Vulnerability Management Program	5) Protect all systems against malware and regularly update antivirus software or programs	Vulnerability Assessment; Onsite Assessment	N/A

	6) Develop and maintain secure systems and applications	Technical Assessment: Vulnerability Assessment; Application Security Assessment. Onsite Assessment	**Non-compliance:** Website CMS or its components seem to be outdated. Check for available updates. Fingerprinted website CMS or its components contain publicly known vulnerabilities (Ref. PCI DSS 6.5.1-6.5.10). No WAF was detected on the website. Implement a WAF to protect the website against common web attacks.
Implement Strong Access Control Measures	7) Restrict access to cardholder data by business need to know	Technical Assessment:Access controls related to cardholder data. Onsite Assessment	N/A
	8) Identify and authenticate access to system components	Technical Assessment: Authentication controls Onsite Assessment	N/A
	9) Restrict physical access to cardholder data	Onsite Assessment	N/A
Regularly Monitor and Test Networks	10) Track and monitor all access to network resources and cardholder data	Technical Assessment: Network access controls; Onsite Assessment	N/A

	11) Regularly test security systems and processes	Technical Assessment: Penetration testing; Vulnerability scanners; PCI Certified Assessors Onsite Assessment	N/A
Maintain an Information Security Policy	12) Maintain a policy that addresses information security for all person	Onsite Assessment	N/A

* **Onsite Assessment** includes the review of website, policies, standards & procedure and interviews various stakeholders.

** **N/A** indicates, unable to determine due to insufficient data.

Conclusion

Vulnerability assessment is essential in any system to identify security weaknesses. It is done to evaluate if the system is prone to vulnerabilities and if any remedies to mitigate the vulnerabilities can be identified. Attackers, in most cases, target websites hosting sensitive data. The most compromised data type in the financial sector is personal data containing personal information of individuals followed by bank information. This industry depends on customers' personal information and details of their payment cards.

Vulnerability assessment is based on two methods: statistical analysis and dynamic analysis. Statistical analysis targets user identification, authorization, and authentication. It tests the confidentiality and integrity of data by checking against current encryption standards and implementations. The dynamic analysis deals with systematic scanning of ports, network protocols, and web servers. It also checks the validation of security configuration settings, software versions, and security shortcomings.

Financial institutions need to be bound by General Data Protection Regulation (GDPR). This is the regulation that deals with data protection and privacy. It addresses how personal data should be transferred. It aims at enhancing individual control of rights over one’s personal data. If an organization complies with GDPR, only minimum requirements to secure the customer's data are needed.

All components in a website need to be up to date. Outdated software causes the risk to the organization. They may end up slowing down the whole network, thus making it hard for any work to be done. Outdated components like JQuery and Bootstrap on the amazon web services may lead to crashing down the site; this may eventually lead to customers' complaints as they try to access the system, resulting in loss to a couple of them. To avoid such cases, regular software updates need to be carried out.

Security headers are crucial for the security of any website. Their presence protects the site against many attacks that the site may be exposed to. They protect against code injection and many other vulnerabilities.

References

owasp.org. (n.d.). *OWASP Foundation, the Open Source Foundation for Application Security*. Available at: https://owasp.org/ [Accessed 12 Jul. 2021].

OWASP Top 10 - 2017. (2017). *OWASPFoundation, the Open Source Foundation for Application Security*, OWASP, pp.1–25. Available at: https://github.com/OWASP/Top10/raw/master/2017/OWASP%20Top%2010-2017%20(en).pdf [Accessed 12 Jul. 2021].

Olavsrud, T. (2021) What is data governance? A best practices framework for managing data assets. Available from: https://www.cio.com/article/3521011/what-is-data-governance-a-best-practices-framework-for-managing-data-assets.html [Accessed 14 July 2021].

PCI Security Standards Council (2018) PCI DSS Quick Reference Guide. Available from: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf [Accessed 14 July 2021].

Calver, N. (2018) Preparing for a PCI audit. Available from: https://www.itgovernance.co.uk/blog/preparing-for-a-pci-audit [Accessed 14 July 2021].

Intersoft Consulting. (2016) *General Data Protection Regulation.* Available from: https://gdpr-info.eu/ [Accessed 14 July 2021].