# Development Team Project: Executive Summary

# Introduction

This summary provides an overview of the systematic evaluation of the target host. Below you will find the approach taken to reveal the host’s vulnerabilities followed by mapping the vulnerabilities to the GDPR and PCI DSS directives and providing a concise overview of the controls, compliance and mitigation actions required to reach the minimum baseline regarding the compliance with the directives. Please see the previously submitted design document for a detailed explanation of the tools used. Additionally, see the Appendixes for detailed scan results.

# Methodology

## Threat Landscape

The term "Threat Landscape" refers to a collection of threats and vulnerabilities found in a particular environment or field, such as sensitive credentials, assets, threats, hazards, and discovered trends (EISA, 2014).

Once evaluating the target host, threats specific to the e-commerce domain were identified on the following landscapes:

### Human Resources

#### The Harvester

The harvester was used to determine whether the host revealed sensitive human resource data such as personally identifiable information (See Appendix A).

### Network & Server Infrastructure

To assess layers 3 - 7 (OSI model), a series of scans with the following tools were performed:

#### Nmap

Nmap was used to scan all ports on the host to identify services running on each port (See Appendix B). The second scan determines whether the host is susceptible to known SSL/TLS vulnerabilities (See Appendix C).

#### TestSSL

To further evaluate whether the host has implemented SSL/TLS TestSSL was utilised. The results (see Appendix G) indicate that SSL/TLS is not offered when accessing the host.

#### OpenVas

OpenVas revealed that SSH was running on port 22 along with the vulnerability “NVT: SSH Weak Encryption Algorithms Supported” (www.securityspace.com, 2016).

### Web Application

#### OWASP ZAP

The absence of X-Frame Options HTTP headers might lead to the ClickJacking Attacks by OWASP ZAP OWASP ZAP (see appendix D).

#### OpenVas

OpenVas has identified the “MacOS X Finder '.DS\_Store' Information Disclosure” vulnerability that may result in personal identifying information being disclosed (See Appendix E).

#### SqlMap

To detect if SQL flaws were injected into the server, SqlMap was used. There were, however, no findings (Refer to Appendix F).

#### TestSSL

We have implemented TestSSL to check certificate installation in the web application. No web-based certificates (including SSL/TLS services) are deployed, as shown in Appendix (G).

### OWASP Web Application Security Guide

Section 4.1 of the website application safety guide explains the processes for information collection in the scope of this report (OWASP, 2021). This guideline has thus been adopted to compare the industry's best practices with our methodology. Additionally, we have selected the above methodology instead of STRIDE and DREAD, as OWASP provides a highly detailed technical approach.

# Compliance & Controls

## GDPR

### Introduction

The General Data Protection Regulation consists of compulsory laws regarding the processing of types of personal data in an ethical manner. Personal data is defined as any information that, directly or indirectly, may be utilised to identify a person (GDPR.EU, 2016).

### Types of Personal Data Processed

To perform the compliance assessment regarding the GDPR directive, it was necessary to define the categories of the data subject, the nature of personal data we process and the types of processing data. In the following table, we present an overview of our findings regarding the data processed as an e-commerce site providing payment services and consulting to commercial website operators (GDPR.EU, 2019).

|  | **Customers** | **Visitors** | **Employees** | **Contractors** | **Applicants** | **Third Parties** |
| --- | --- | --- | --- | --- | --- | --- |
| **Identification data** | ✔ | ✔ | ✔ | ✔ |  | ✔ |
| **Behavioural data** |  |  |  |  |  |  |
| **Banking data** |  |  |  |  |  |  |
| **Personal data** | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| **Judicial data** |  |  |  |  |  |  |
| **Geolocation data** |  |  |  |  |  |  |
| **Employee contract data** |  |  |  |  |  |  |
| **Cookies** | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |

#### Controls

The controls below have been identified as mandatory regarding the technical measures an organisation shall implement to be compliant with GDPR. The list below is not exhaustive and only applies to the purposes of the domain.

##### Authentication

People in charge of processing shall be authorised, via electronic means, to process personal data.

##### Antivirus

Protect personal data against the risk of intrusion and the effects of malicious programmes by implementing suitable electronic means to be updated at least every six months.

##### IPS/IDS

Protect against the risk of intrusion and the effects of malicious programmes by implementing suitable electronic means to be updated at least every six months.

##### Business continuity/disaster recovery

In case of damage, either data or electronic means, appropriate steps should be taken to ensure that the information access is restored within a certain time limit, Which shall be compatible with the data subject’s rights and not exceed the seven-day recovery time.

##### Retention periods and disposal mechanisms for personal data processed for marketing and profiling purposes

Mechanisms regarding retention and disposal for personal data processed for marketing purposes so as to retain such data for 24 months and profiling purposes to retain such data for 12 months, and provide for their erasure at the end of the period.

##### Vulnerability Management

Vulnerability assessments are performed periodically to test, verify, and evaluate system vulnerabilities, guaranteeing the processing is secure and mitigating the risks on data.

##### Hardening

The system is hardened based on the state of the art of technology and the costs, nature, purposes and scope of personal data processing.

##### Anonymisation

Personal data is anonymised at the end of the processing or before being transmitted to the test environment.

##### Pseudo-anonymisation

Personal data is pseudo-anonymized (e.g. via cryptography, hashing or tokenisation).

##### Secure coding

Secure coding practises are implemented to implement new applications.

##### Change management

Change Management procedures are adopted for managing system evolutions.

##### Application Security Testing

Perform testing to assess the security measures taken during the development of applications and identify weaknesses, vulnerabilities, and appropriate remedial actions.

### Vulnerabilities & Compliance

| **Control** | **Compliance Status** | **Vulnerability** | **Mitigation Action** |
| --- | --- | --- | --- |
| Business continuity/disaster recovery | Partially Compliant | Natural disasters/ cloud provider related issues | AWS has established a Business Continuity Plan for its clients. However, a local Business Continuity Plan should be implemented for issues unrelated to the cloud provider. |
| Hardening | Not compliant | ICMP enabled -  Denial of Service/ Distributed Denial of Service available to attackers. | Disable ICMP. Additionally, AWS provides the “Shield” service against denial of service attacks. |
| Change management | Not compliant | No change management policy, leading to misconfiguration of IT assets. | Establishment of a change management policy. |
| Hardening  Change management | Not compliant | Privilege escalation through enabled SSH service.  Access to hidden files through the creation of “.DS\_Store\_” with MacOS X | Change the default configuration (disable SSH) through a hardening process and establish a secure channel for remote connections. Additionally, every system alteration shall receive approval through the change management policy. |
| Authentication  Anonymisation  Pseudo-anonymisation | Not compliant | Vulnerable to list of exploits/attacks based on lack of SSL/TLS implemented services.  Additionally, the host lacks a basic authentication procedure. | SSL/TLS should be implemented.  Enable an authentication procedure (including a Multi-Factor Authentication). |
| Application Security Testing  Secure Coding | Not compliant | Vulnerable to ClickJacking attacks.  Possible session-hijacking via malicious use of CSRF token. | Implement an application security testing environment to review every alteration/ update on the software without affecting the live environment.  Additionally, implement a secure coding policy based on the best practices (e.g. OWASP, SANS). |
| IPS/IDS | Not compliant | Intrusion Detection/ Prevention System was not enabled to protect the infrastructure. | AWS provides a Trend Micro service, which enables IPS/IDS security features. |
| Antivirus | Not compliant | Antivirus software is not enabled. | AWS provides the Cloud Storage Security antivirus for their clients. |
| Retention periods and disposal mechanisms for personal data processed for marketing and profiling purposes | Not compliant | A disposal period is not set for any kind of data, especially for marketing and profiling purposes. | Establish a retention and disposal period for every type of processed data. |

## PCI DSS

### Introduction

As the domain of the target host provides payment services where cardholder information is processed, the organisation is encouraged to comply with the PCI DSS security standards (PCI Security Standards Council, 2018).

PCI DSS outlines a “baseline of technical and operational requirements designed to protect account data”. The security standards provide a security assessment tool in 12 PCI DSS requirements that organisations should follow to achieve compliance.

Below we explore the 12 requirements/domains that provide a best practice approach in preparation for a PCI DSS assessment (aws.amazon.com, 2020).

### PCI-DSS Domains

#### High-Level Overview

| **Build and Maintain a Secure**  **Network and Systems** | 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| --- | --- |
| **Protect Cardholder Data** | 1. Protect stored cardholder data 2. Encrypt transmission of cardholder data across open, public networks |
| **Maintain a Vulnerability**  **Management Program** | 1. Protect all systems against malware and regularly update anti-virus software or programs 2. Develop and maintain secure systems and applications |
| **Implement Strong Access**  **Control Measures** | 1. Restrict access to cardholder data by business need to know 2. Identify and authenticate access to system components 3. Restrict physical access to cardholder data |
| **Regularly Monitor and Test**  **Networks** | 1. Track and monitor all access to network resources and cardholder data 2. Regularly test security systems and processes |
| **Maintain an Information**  **Security Policy** | 1. Maintain a policy that addresses information security for all personnel |

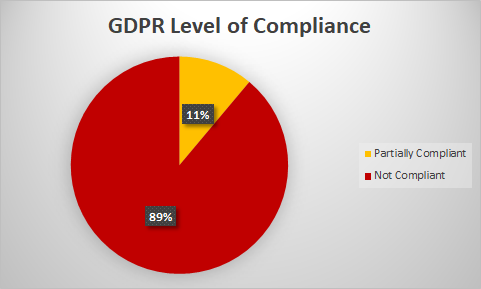
Figure 1: (PCI Security Standards Council, 2018)

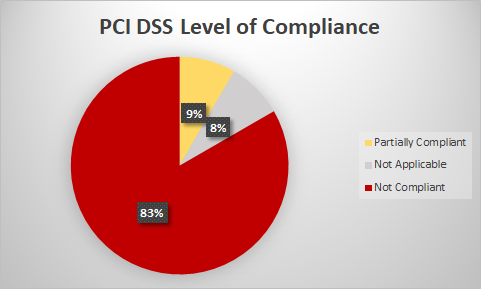
### Compliance Assessment

| **Control** | **Compliance Status** | **Vulnerability** | **Mitigation Action** |
| --- | --- | --- | --- |
| 1. Install and maintain a firewall configuration to protect cardholder data | Not compliant | Lack of configuration of the firewall provided service. | Enable and configure the AWS Firewall Manager, including the rest of the network infrastructure (e.g. routers). |
| 2. Do not use vendor-supplied defaults for system passwords and other security parameters | Partially compliant | The default MYSQL password was changed; however, the use of the root (administrative) user is not recommended. | Setup a non-root user with a strong password. Grant the user access only to tables that are required for the operation of the web application. |
| 3. Protect stored cardholder data | Not compliant | Privacy by design and by default not implemented. Retention and disposal policies and procedures not implemented. | The principles of privacy by design and by default have to be implemented, in order to store the minimum amount of cardholder data. Additionally, retention and disposal policies and procedures shall be implemented. |
| 4. Encrypt transmission of cardholder data across open, public networks | Not compliant | SSL/ TLS not implemented. Cryptography policies and procedures not implemented.  Vulnerable to list of exploits/attacks based on lack of SSL/TLS implemented services. | SSL/ TLS shall be implemented. AWS provides the AWS SDK service to assure strong cryptographic measures are in place. Additionally, cryptography policies and procedures shall be implemented. |
| 5. Protect all systems against malware and regularly update anti-virus software or programs | Partially compliant | Antivirus and antimalware solutions are already implemented on Amazon services. However, our instance does not have any type of the solution above. | Antivirus and antimalware shall be implemented on our private Amazon instance. |
| 6. Develop and maintain secure systems and applications | Not compliant | A Process to identify security vulnerabilities is not implemented.  Software is not protected from known vulnerabilities.  Custom code is not reviewed prior to release.  Change management policy is not implemented.  A Testing environment is not implemented.  A Software Development Life Cycle process is not implemented, either training to the developers.  Vulnerable to ClickJacking attacks.  Possible session-hijacking via malicious use of CSRF token.  Privilege escalation through enabled SSH service.  Access to hidden files through the creation of “.DS\_Store\_” with MacOS X | A Software Development Life Cycle process shall be implemented and communicated properly to the developers. Additionally, Amazon provides the AWS WAF service as a security measure to protect the application. |
| 7. Restrict access to cardholder data by business need to know | Not compliant | Access management policy and procedures not implemented. | An authentication portal should be implemented, including an access management policy. Staff members should process data according to their job descriptions. |
| 8. Identify and authenticate access to system components | Not compliant | Identity and Access Management (IAM) policy and procedures not implemented. | Identity and Access Management (IAM) policy and procedures should be implemented. Additionally, Amazon provides AWS Directory Service to support the management of staff personnel. |
| 9. Restrict physical access to cardholder data | Not applicable | Data not physically accessible.  No devices provided to customers. | Not applicable |
| 10. Track and monitor all access to network resources and cardholder data | Not compliant | Services to support audit trails, and system and network logging are not enabled. | Amazon provides a number of services to support their customers to meet the requirements for PCI DSS Section 10. |
| 11. Regularly test security systems and processes | Not compliant | Business continuity plans are not implemented (including disaster recovery tests). | A Business Continuity Management System framework should be implemented (www.iso.org, 2019). |
| 12. Maintain a policy that addresses information security for all personnel | Not compliant | Security policy regarding the personnel is not implemented.  A policy of Acceptable Use is not implemented.  Training and awareness activities are not implemented. | An information security policy regarding the personnel should be implemented. Additionally, after the completion, it can be communicated through a training activity where a breach simulation can take place to educate the personnel regarding the risks the organisation is facing. |

# Summary of Compliance Assessment

Following the performed assessment, the level of compliance was analysed and is presented below:





# Conclusion

A compliance assessment was performed to discover the issues the application faces against the major directives (e.g. GDPR, PCI DSS) of the selected domain. Each vulnerability was linked to a control based on each directive, following a mitigation action. Due to limitations, other directives such as the California Consumer Privacy Act, and the Privacy Shield could not be included within the assessment.

# References

aws.amazon.com (2020) *Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 on AWS*. Available at:<https://d1.awsstatic.com/whitepapers/compliance/pci-dss-compliance-on-aws.pdf> (Accessed: 17 July 2021 2021).

EISA (2014). *ENISA Threat Landscape 2014*. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2014/at_download/fullReport> [Accessed 13 June 2021].

GDPR.EU (2016) *General Data Protection Regulation*. Available at:<https://gdpr.eu/tag/gdpr/> (Accessed: 17 July 2021).

GDPR.EU (2019) *What is considered personal data under the EU GDPR?* Available at:<https://gdpr.eu/eu-gdpr-personal-data/> (Accessed: 17 July 2021).

OWASP (2021) *4.1 Information Gathering*. Available at:<https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/README.html> (Accessed: 17 July 2021).

www.iso.org (2019) *ISO 22301:2019*: @isostandards. Available at:<https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/51/75106.html> (Accessed: 13 July 2021).

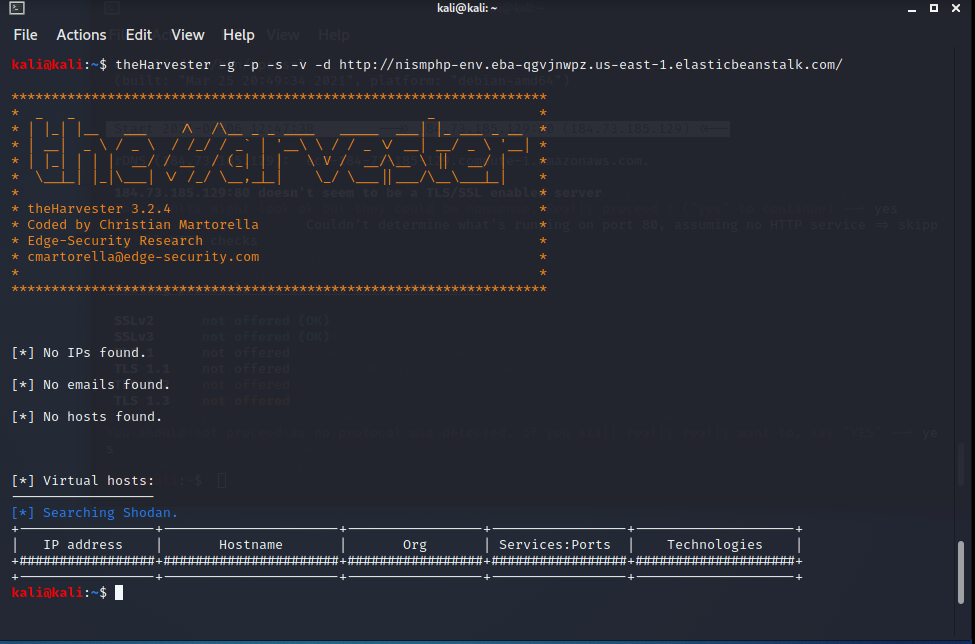
www.securityspace.com (2016) *SSH Weak Encryption Algorithms Supported*. Available at: <https://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.105611> (Accessed: 17 July 2021).

PCI Security Standards Council (2018)*: Payment Card Industry (PCI) Data Security Standard*. Available at:<https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf> (Accessed: 11 July 2021).

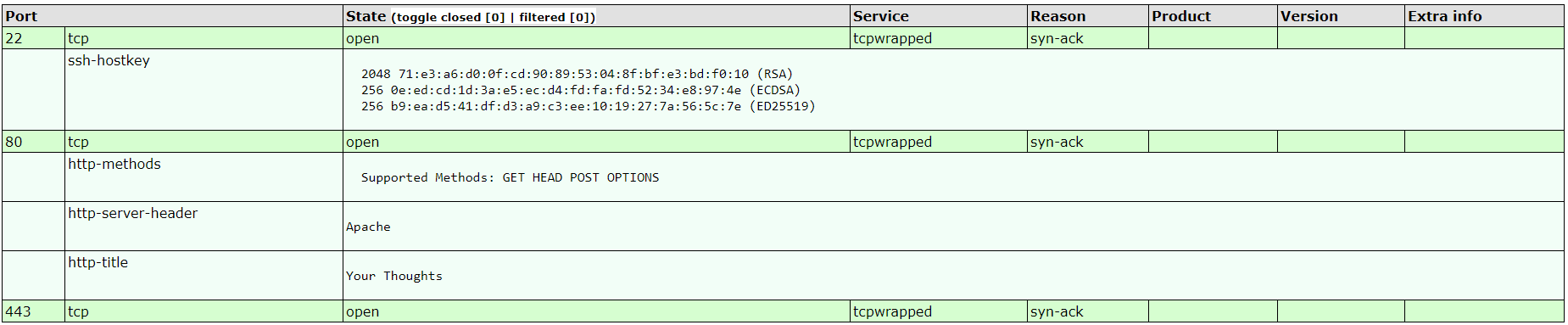
www.pcisecuritystandards.org *PCI SECURITY*. Available at:<https://www.pcisecuritystandards.org/pci_security/> (Accessed: 11 July 2021).

# Appendixes

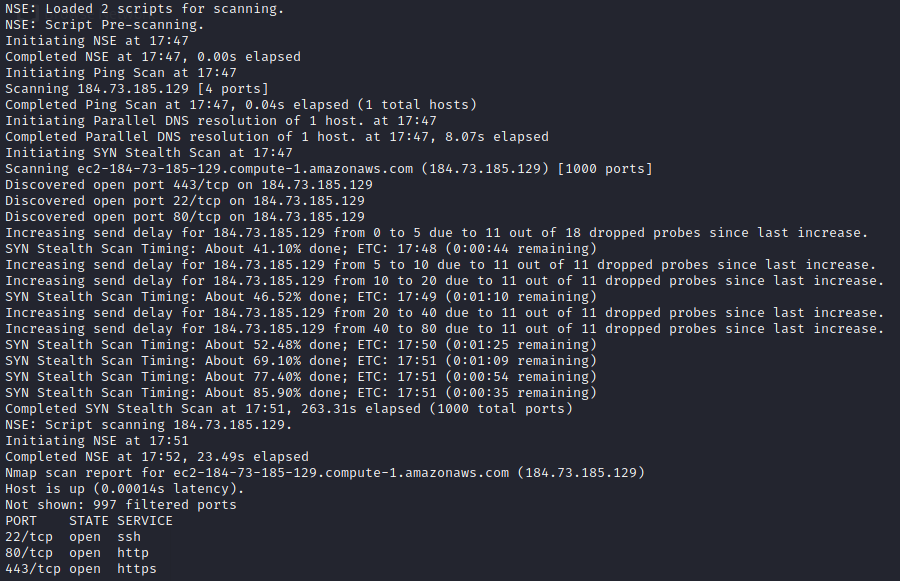
## Appendix A



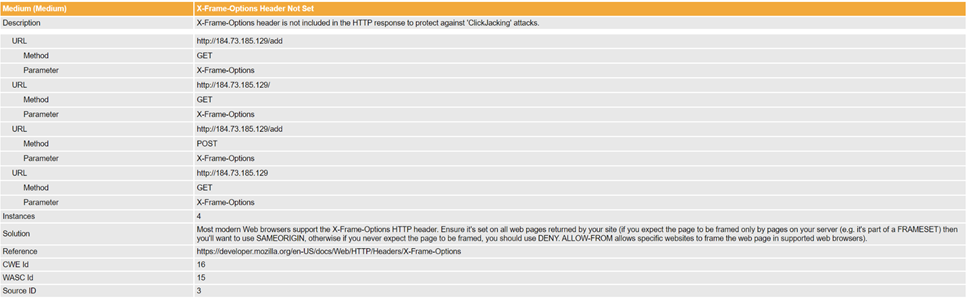
## Appendix B



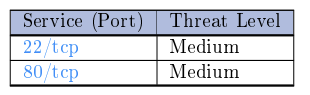
## Appendix C

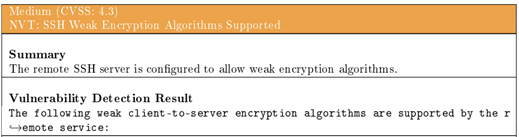


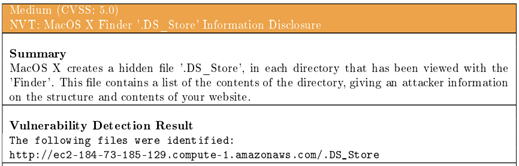
## Appendix D



## Appendix E







## Appendix F



## Appendix G

