Pentest Report

Threat Modeling approach

|  |  |
| --- | --- |
| Author:  Data: xx/xx/xxxx |  |
|  |  |

**Summary**

[Version Control](#_heading=h.gjdgxs) 4

[Contracts and Issues Legals](#_heading=h.2fbirjm9la9) 4

[1.](#_heading=h.30j0zll) Goal 6

[2.](#_heading=h.1fob9te) Scope 6

[3.](#_heading=h.3znysh7) Methodology 6

[4. Architecture Information](#_heading=h.eft9yye75nt3) 8

6[. Executive Report](#_heading=h.y53vmlw2dlo4) 9

6[.](#_heading=h.mm7ye4w77dax) Technical Report 10

6[.1.](#_heading=h.hnpzrbyxj1i) Identified Vulnerabilities 10

7[. Risk](#_heading=h.2bn6wsx) Classification 11

8[.](#_heading=h.8isxaxd6pnzc) Remediation report 12

9[.](#_heading=h.8isxaxd6pnzc) Conclusions 13

# Version Control

| **Version** | **Author** | **Date** | **Changes** |
| --- | --- | --- | --- |
| 1.0 |  | xx/xx/xxxx |  |
| 1.1 |  | xx/xx/xxxx |  |

# Contracts and Issues Legals

**CLAUSE ONE - OBJECTIVE**

The purpose of this term is the protection of CONFIDENTIAL INFORMATION made available by the COMPANY, due to the employment relationship developed by the parties.

**CLAUSE TWO - DEFINITIONS**

All technical information obtained through the employment relationship with the COMPANY and related to the project, specification, operation, organization or performance of said company will be considered CONFIDENTIAL.

SOLE PARAGRAPH: For the purposes of this term, any and all information, whether patented or not, of a technical, operational, commercial, legal nature, know-how, inventions, processes, formulas and designs, whether patentable or not, production systems, logistics and layouts, business plans, accounting methods, techniques and accumulated experiences, documents, contracts, papers, studies, opinions and research to which the employee has access:.

a) by any physical means (e.g. express documents, manuscripts, facsimile, electronic messages (e-mail), photographs etc;

b) by any form recorded in electronic media (tapes, cd's, dvd's, floppy disks etc);

c) orally.

**THIRD CLAUSE - RESPONSIBILITY**

The employee undertakes to maintain secrecy by not using such confidential information for his own benefit or that of others.

PARAGRAPH ONE: Confidential information entrusted to employees may only be opened to third parties with the prior written consent of the company, or in case of a court order, in which case the employee must immediately inform the company in writing so that it can seek prevent and remove the obligation to disclose the information.

**CLAUSE FOUR - NON-CONFIDENTIAL INFORMATION**

Those are not confidential information:

a) already available to the general public through no fault of the employee;

b) that were already known to the employee before joining the company and that were not acquired directly or indirectly from the company;

c) that are no longer treated as confidential by the company.

**FIFTH CLAUSE - STORAGE OF INFORMATION**

All confidentiality and secrecy information provided for in this term will be valid throughout the term of this instrument, while the employment relationship lasts and, also, for a minimum period of 01 (one) year after the employee's relationship with the company is broken. During penetration testing, you will find and produce a considerable amount of data. These data must be properly deleted later to avoid leaking them.

Examples of data:

Correspondence (email, letters…);

Graphs, papers, electronic documents;

Logins, passwords, IP addresses, personal data…;

Proof of concepts, exploits code and vulnerabilities;

Screenshots;

Reports and deliverables Tools logs.

**CLAUSE SIX - OBLIGATIONS**

The employee must:

I) use such information only for the good and faithful purpose of fulfilling the purposes of the company;

II) maintain the confidentiality of confidential information and reveal it only to employees who need to know about it;

III) protect confidential information disclosed to you, using the same degree of care used to protect your own confidential information;

IV) maintain adequate administrative procedures to prevent the loss or loss of any documents or confidential information, and must immediately notify the company of the occurrence of incidents of this nature, which will not exclude its responsibility.

PARAGRAPH ONE: The employee is hereby prohibited from producing copies or backups, by any means or form, of any of the documents provided to him or documents that have come to his attention as a result of the employment relationship.

PARAGRAPH TWO: The employee must return, in full and in full, all documents provided to him, including any necessary copies, on the date stipulated by the company for delivery, or when it is no longer necessary to maintain confidential information, pledging not to retain any reproductions, copies or duplicates, under penalty of incurring the responsibilities provided for in this instrument.

THIRD PARAGRAPH: The employee must destroy any and all documents produced by him that contain confidential information of the company, when it is no longer necessary to maintain such confidential information, pledging not to retain any reproductions, under penalty of incurring the responsibilities provided for in this instrument.

**CLAUSE SEVEN - SPECIAL PROVISIONS**

By signing this instrument, the employee expresses his/her agreement in the following sense:

I) all conditions, terms and obligations set forth herein shall be governed by this Term, as well as by the relevant Brazilian legislation and regulations;

II) this term may only be amended by entering into a new, subsequent and additive term;

III) changes in the number, nature and quantity of confidential information made available by the company will not alter or reduce the commitment or obligations agreed in this Confidentiality and Confidentiality Agreement, which will remain valid and with all its legal effects in any of the situations typified in this instrument ;

IV) the addition, complementation, substitution or clarification of any of the confidential information made available to the employee, due to the present purpose, will be incorporated into this Term, becoming an integral part of it, for all purposes and effects, also receiving the same protection described for the initial information made available, not being necessary, in these cases, the signature or formalization of an amendment.

**CLAUSE EIGHT - VALIDITY**

This term will become valid from the date of its effective signature by the parties.

Sole Paragraph: The provisions of this instrument shall, however, be applied retroactively to any confidential information that may have already been disclosed, before the date of its signature.

**CLAUSE NINE - PENALTIES**

Failure to comply with any of the confidentiality provisions established in this instrument will subject the offending employee, as well as the causative agent or facilitator, by action or omission of any of those listed in this Term, to the payment, or recomposition, of all losses and damages proven by the company, as well

as the respective civil and criminal liability, which will be determined in a regular judicial or administrative process.

# Goal

# The Pentest with Threat Modeling approach aims to implement a more comprehensive threat analysis strategy adding greater executive value by defining specific risks for the business, and also adds value to Pentest execution, since with more information provided about the application architecture, the pentest will be performed with better efficiency.

# Scope

The information obtained for this analysis was provided by the architecture teams of the development squads responsible for the application.

It is a Pentest white box where access to the application's source code and internal information about the architecture was provided.

# Methodology

# The use of Threat Modeling in a phase prior to vulnerability analysis, adds knowledge about possible attack vectors for the pentester, so the methodologies used were as follows:

# Threat Identification

It is necessary to use a model to identify the threats that can compromise each component of the application architecture, using the STRIDE methodology developed by Microsoft.

* 1. **Identification of Threat Profiles**

It is important during Threat Modeling to have a clear understanding of threat profiles, ie the profiles of attackers that can exploit certain threats.

* 1. **Risk Classification**

It is necessary to use a Risk Classification Methodologies in the elaboration of Threat Modeling, which will serve as a basis for prioritization, giving a focal point to the greatest risks for the corporation.

Vulnerabilities are classified according to the use of the OWASP Risk Rating framework, which aims to classify according to the impact that the vulnerability will have on the business and the probability that it will occur.

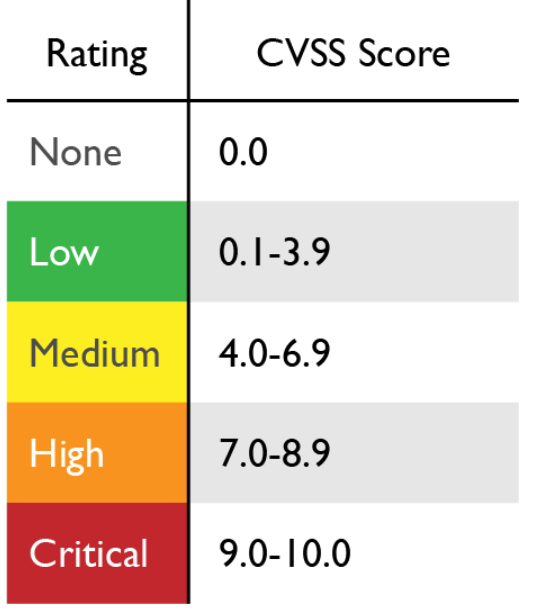
For this classification, several questions are listed about the risk context of vulnerabilities present for the organization, taking into account factors such as customer reach, non-compliance with legislation, difficulty of exploitability and others.

| **Levels** | |
| --- | --- |
| 0 à <3 | BAIXO |
| 3 à <6 | MÉDIO |
| 6 à 9 | ALTO |

The overall risk severity is equal to the probability x impact, below is an image that is used for the final classification using the OWASP methodology:

| **Risk = Probability x Impact** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Impact** | **High** | **Medium** | **High** | **Critical** |  |
| **Medium** | **Low** | **Medium** | **High** |  |
| **Low** | **Info** | **Low** | **Medium** |  |
|  | **Low** | **Medium** | **High** |  |
|  | **Probability** | | | |  |

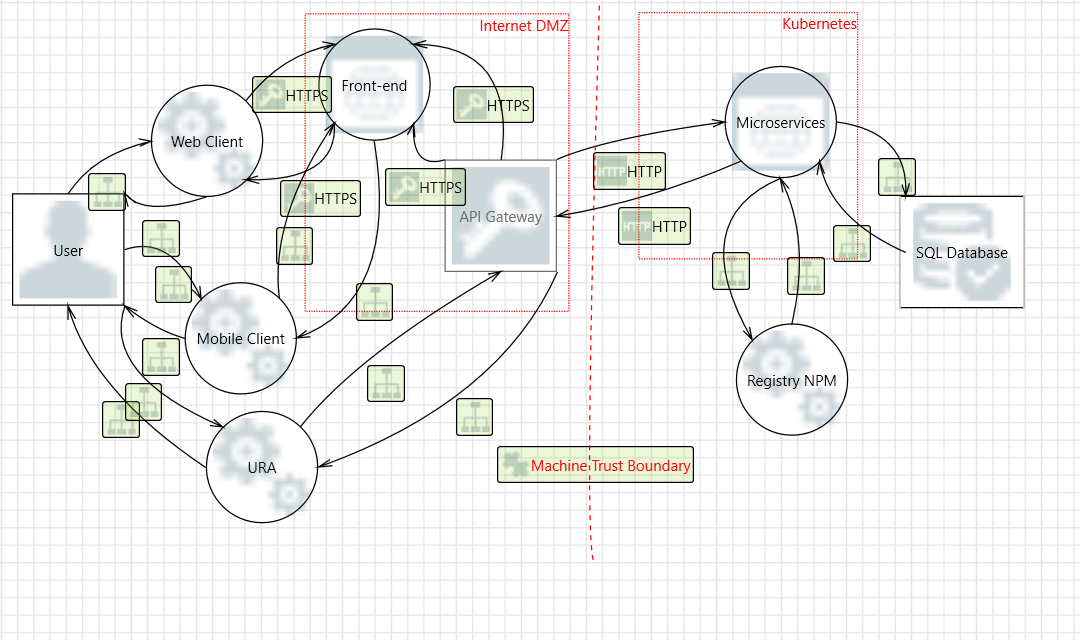
The vulnerability classification is merged with CVSS, giving a view focused on business risks and another more technical view, below is an image of the vulnerability classification provided by CVSS:



# Architecture Information

In this topic, a drawing made by Pentester with Microsoft's Threat Modeling Tool is shown on the architecture of the application that is in the scope of pentesting.

**e.g.**

****

# Executive Report

This topic aims to briefly demonstrate an executive view of the impact that the vulnerabilities found reflect on the risks to your business. Also presenting a deadline policy for fixing vulnerabilities. If you already have a remediation policy at your company, ignore it, but it's a good standard to follow in the long run.

**SLA policy suggestion for fixing vulnerabilities:**

* **Critical**: In less than **30** days
* Vulnerability 1
* **High**: in less than **60** days
* Vulnerability 2
* Vulnerability 3
* **Medium**: in less than **90** days
* Vulnerability 4
* **Low**: in less than **120** days
* Vulnerability 5
* Vulnerability 6

# Technical Report

# 

# 6.1 Identified Vulnerabilities

# 6.2 Example 1: SQL Injection (Critical)

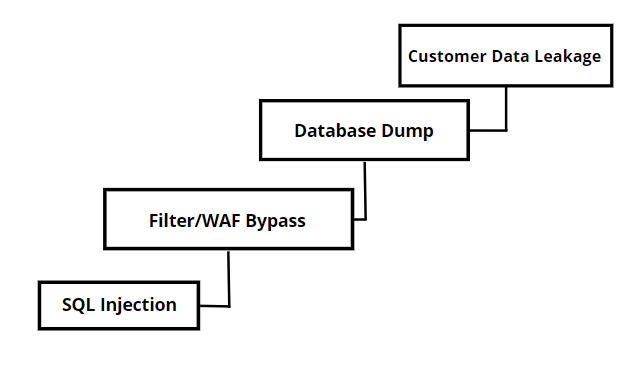
**OWASP TOP 10:** [**Injection**](https://owasp.org/Top10/A03_2021-Injection/)

**CWE:** [**89**](https://cwe.mitre.org/data/definitions/89.html)

**CVSS:** [**8.8**](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

Technical description of how the vulnerability was found and exploited here.

**Threat tree for the attack vector:**



# Risk Classification

# This topic lists the vulnerabilities classified according to the risk and established criteria.

| **Name** | **Impact** | **Probably** | **Risco** | **CVSS** | **STRIDE** | **Threat Profile** |
| --- | --- | --- | --- | --- | --- | --- |
| Example 1: SQL Injection | **High** | **High** | **Critical** | **High**  **8.8** | **Tampering** | **Hacker** |

# Remediation Report

This topic will address ways to fix the vulnerabilities detected in sequential order according to their criticality.



# Example 1: SQL Injection (Critical)



**Correction**

1. Conclusion

Conclusion of the Pentest analysis and highlighting important observations.

References

**STRIDE**

(<https://learn.microsoft.com/pt-br/azure/security/develop/threat-modeling-tool-threats>)

**OWASP Risk Rating**

(<https://owasp.org/www-community/OWASP_Risk_Rating_Methodology>)

**Threat Modeling**

(<https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling>)