Company X Penetration Test

by Name Surname

Start of testing: February 13, 2019

End of testing: February 20, 2019

Contents

1 Executive Summary

In this penetration test the Company X was examined for security-relevant weaknesses. The kind of testing was black-box, this is the kind where no specific information about the internals of the system is given. The scope of the assessment was as follows:

- Dedicated Web Server: 127.0.0.1
  - Domain: https://example.com
    - Subdomains: all subdomains

Table 1.1 contains the overview of examined systems during the penetration test.

Web Site	**Hostname**
Domain 1	https://example.com/
Subdomain 1	https://1.example.com/
Subdomain 2	https://2.example.com/

Table 1.1: Web sites examined during the penetration test

As a result, several vulnerabilities have been found among the assets of the organization, some of them pose a significant risk. Figure 1.1 summarizes all issues by their type across all the assets of Company X. Solutions to remedy the discovered vulnerabilities are provided together with detailed descriptions and reproduction steps.

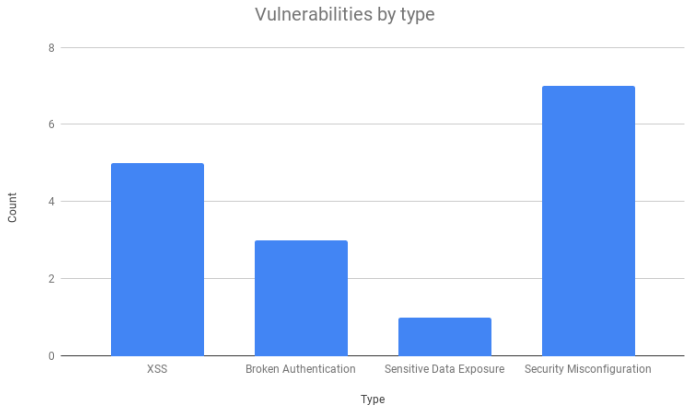

Figure 1.1: Vulnerabilities by Type

In this part add a short summary of all vulnerabilities in non-technical terms.
It's also good to mention an estimation of efforts required to resolve the issues.

2 Vulnerability overview

Table 2.1 depicts all vulnerabilities found during the penetration test. They are categorized by their risk and potential and are differentiated in the categories low, medium, high and critical.

Here describe what severities are and what do they mean in context of your report. It's better to keep the color code across all the report.

Figure 2.1 shows the overview of vulnerabilities grouped by target.

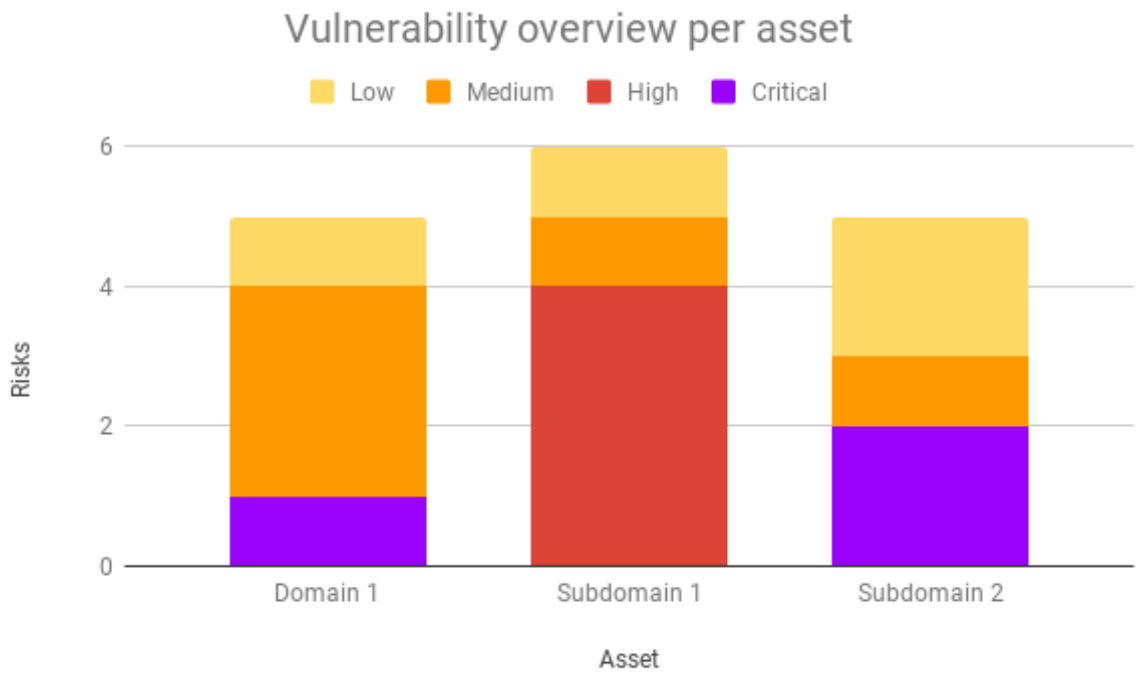

Figure 2.1: Vulnerability overview

Risk	Asset	Vulnerability	Section	Page
Critical	Domain 1	Unauthenticated SQL Injection	3.1.1	3
High	Domain 1	Stored XSS	3.1.2	5
Medium	Subdomain 1	Balance manipulation during order confirmation	3.2.1	6
Low	Subdomain 2	Mail server misconfiguration	3.3.1	7
…	…	…	…	…

Table 2.1: Vulnerability overview

3 Results

In this chapter, the vulnerabilities found during the penetration test are presented. All the issues are grouped by target and contain the following information:

- Brief description.
- CVSS Base Score – see here for details.
- Exploitability – describes the likelihood of an issue being used against customer's infrastructure.
- Business impact.
- References to classifications: WASC, OWASP, CWE.
- Steps to reproduce.
- Etc…

Also the remediation recommendations are given for each issue found during the penetration test. Both "quick win" and long term solutions are presented as well as some code examples.

3.1 Domain 1

System description goes here.
Hostname: `https://example.com`
Server IP address: 127.0.01

3.1.1 Unauthenticated SQL Injection

General vulnerability description goes here.

Basic information about this issue is presented in Table 3.1.

3.1.1.1 Minimal proof of concept

Steps to reproduce the issue go here. Screenshots are welcome.

Description	Description goes here.
CVSS Base Score	8.0
Exploitablity	High
Business impact	Business impact goes here.
References to classifications	WASC
	OWASP
Affected input	Affected input goes here
Affected output	• output 1. • output 2.

Table 3.1: Issue #1: description of the issue

3.1.1.2 Proposed solutions

Proposed solution to the issue goes here.

3.1.2 Stored XSS

General information about Persistent XSS attacks goes here.
Basic information about this issue is presented in Table 3.2.

Description	Description goes here.
CVSS Base Score	8.0
Exploitablity	High
Business impact	Business impact goes here.
References to classifications	WASC
	OWASP
Affected input	Input.
Affected output	• Output 1. • Output 2.

Table 3.2: Issue #2: description of the issue

3.1.2.1 Minimal proof of concept

Steps to reproduce the issue go here. Screenshots are welcome.

3.1.2.2 Proposed solutions

Proposed solution to the issue goes here.

3.2 Subdomain 1

System description goes here.
Hostname: `https://1.example.com`
Server IP address: 127.0.01

3.2.1 Balance manipulation during order confirmation

General vulnerability description goes here.

Basic information about this issue is presented in Table 3.3.

Description	Description goes here.
CVSS Base Score	8.0
Exploitablity	High
Business impact	Business impact goes here.
References to classifications	WASC
	OWASP
Affected input	Affected input goes here
Affected output	• output 1. • output 2.

Table 3.3: Issue #3: description of the issue

3.2.1.1 Minimal proof of concept

Steps to reproduce the issue go here. Screenshots are welcome.

3.2.1.2 Proposed solutions

Proposed solution to the issue goes here.

3.3 Subdomain 2

System description goes here.
Hostname: `https://2.example.com`
Server IP address: 127.0.01

3.3.1 Unauthenticated SQL Injection

General vulnerability description goes here.

Basic information about this issue is presented in Table 3.4.

Description	Description goes here.
CVSS Base Score	8.0
Exploitablity	High
Business impact	Business impact goes here.
References to classifications	WASC
	OWASP
Affected input	Affected input goes here
Affected output	• output 1. • output 2.

Table 3.4: Issue #4: description of the issue

3.3.1.1 Minimal proof of concept

Steps to reproduce the issue go here. Screenshots are welcome.

3.3.1.2 Proposed solutions

Proposed solution to the issue goes here.

4 Appendices

4.1 Appendix #1

Appendix 1.

4.2 Appendix #2

Appendix 2.