eCPPTv2 Certification

COMPANY

Security Assessment Finding Report

By PENTESTER

December 10, 2022

Confidentiality Statement

This document is the property of COMPANYand PENTESTER(PENTESTER). It contains confidential and proprietary information that should not be shared or reproduced without the consent of both parties. PENTESTERmay share this document with auditors who have signed non-disclosure agreements in order to prove compliance with penetration test requirements.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.
Time-limited engagements do not allow for a full evaluation of all security controls. PENTESTER prioritized the assessment to identify the weakest security controls an attacker would exploit. PENTESTER recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

1 Contact Information

PENTESTER
Phone: 000000000
Email: random@random.com

Table of Contents

1 Contact Information 2

2 Assessment Overview 5

3 Assessment Components 6

4 Findings Severity Classification 6

5 Scope 7

6 Executive Summary 8

6.1 Most Important Findings . . . 8

6.2 Advice . . . 8

7 Remediation Report 9

7.1 Remediation on Strategic Level . . . 9

7.2 Remediation on Tactical Level . . . 9

7.3 Remediation on Operational Level . . . 9

8 Vulnerabilities by Impact 11

9 Penetration Test Findings - 12

9.1 Critical Finding (Critical 10.0) . . . 12

9.1.1 Impact . . . 12

9.1.2 Method of Exploitation . . . 12

9.1.3 Remediation . . . 12

9.1.4 References . . . 13

9.2 High Finding (High 8.0) . . . 14

9.2.1 Impact . . . 14

9.2.2 Method of Exploitation . . . 14

9.2.3 Remediation . . . 14

9.2.4 References . . . 14

9.3 Medium Finding (Medium 10.0) . . . 15

9.3.1 Impact . . . 15

9.3.2 Method of Exploitation . . . 15

9.3.3 Remediation . . . 15

9.3.4 References . . . 15

9.4 Low Finding (Low 3.1) . . . 16

9.4.1 Impact . . . 16

9.4.2 Method of Exploitation . . . 16

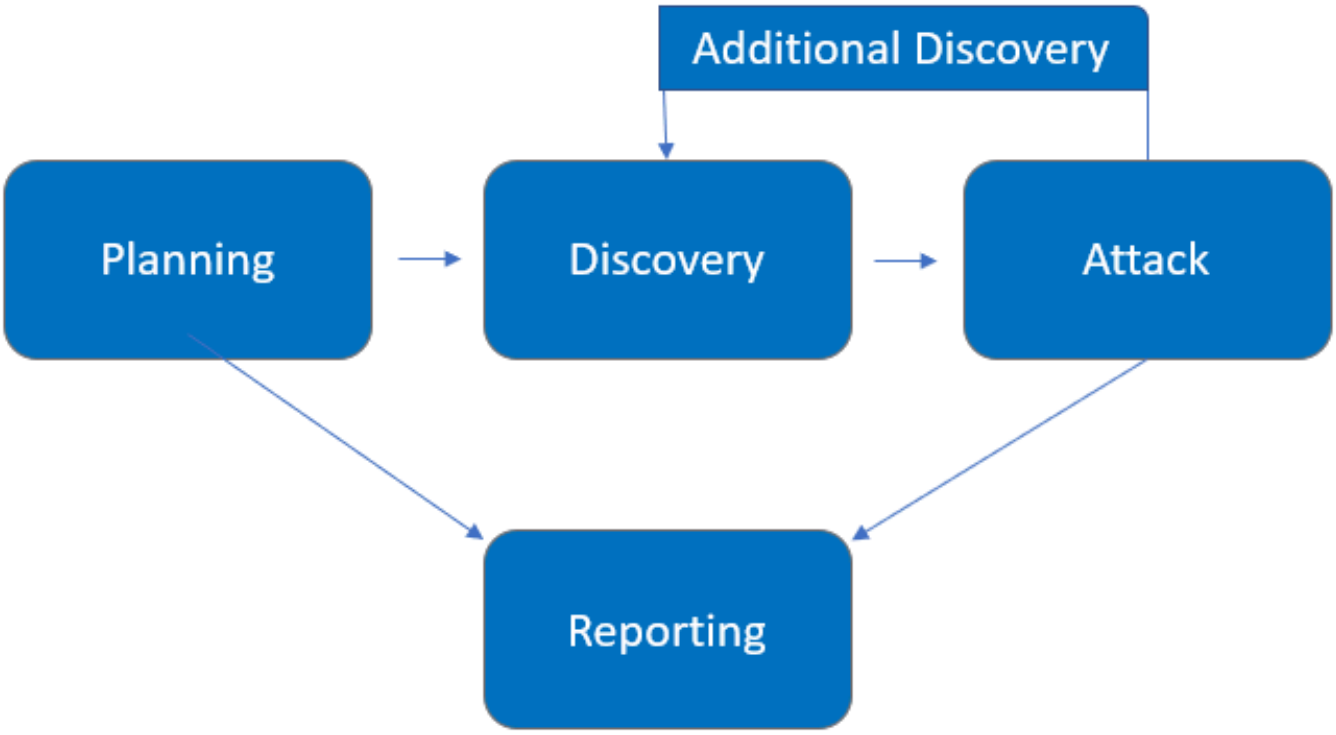
9.4.3 Remediation 16
9.4.4 References 16
9.5 Info Finding (Info 0.0) 17
9.5.1 Impact 17
9.5.2 Method of Exploitation 17
9.5.3 Remediation 17
9.5.4 References 17

10 Summary of Exploited Machines **18**

2 Assessment Overview

From December 2nd, 2022 to December 9th, 2022, PENTESTER engaged COMPANY to evaluate the security posture of its infrastructure compared to current industry best practices that included a penetration test. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks. Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



3 Assessment Components

A penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. PENTESTERattempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. PENTESTERalso performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

4 Findings Severity Classification

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Table 2: Summary of the findings severity classification used.

Severity	CVSS v3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

5 Scope

The overview of the scope of the engagement is described in Table 3.

Table 3: Scope of the engagement

Description	IP Range
Web server	10.10.10.0/24 random.com

6 Executive Summary

PENTESTER evaluated COMPANY' external security posture through an external network penetration test from December 2nd to December 9th, 2022. The test consisted of a series of attacks designed to uncover vulnerabilities in COMPANY' systems. Unfortunately, PENTESTERfound several critical vulnerabilities that could allow an attacker to gain full access to COMPANY' internal network and control of the DMZ. It is highly recommended that COMPANYaddress these vulnerabilities as soon as possible, as they are easily discovered and exploited with minimal effort. Failure to address these vulnerabilities could result in a significant security breach for COMPANY.

6.1 Most Important Findings

All findings, sorted by importance, are displayed in chapter 8 Vulnerability by Impact. The most important findings are:

- 1
- 2

6.2 Advice

All findings in chapters 9 through 11 include steps on remediation. The most important remediation steps are:

- 1
- 2

7 Remediation Report

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

7.1 Remediation on Strategic Level

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

7.2 Remediation on Tactical Level

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

- LOREM
- IPSUM

7.3 Remediation on Operational Level

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum.

- 1

- 2
- 3
- 4

8 Vulnerabilities by Impact

Impact	Finding
Critical	Lorem ipsum
High	Lorem ipsum
Medium	Lorem ipsum
Low	Lorem ipsum
Info	Lorem ipsum

9 Penetration Test Findings - 5 Findings

The following findings have been written down in chronological order.

9.1 Critical Finding (Critical 10.0) CWE 614

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.

9.1.1 Impact

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.

9.1.2 Method of Exploitation

1. 1.
2. 2
3. 3

Some random python code

```
import random

def random_useless_code():
x = random.randint(0, 100)
y = random.randint(0, 100)
z = x * y
return z

print(random_useless_code())
```

9.1.3 Remediation

The following steps should be taken to remediate

1. 1.
2. 2
3. 3

9.1.4 References

- https://clickeys.nl

9.2 High Finding (High 8.0) CWE 614

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.

9.2.1 Impact

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.

9.2.2 Method of Exploitation

1. 1.
2. 2
3. 3

9.2.3 Remediation

The following steps should be taken to remediate

1. 1.
2. 2
3. 3

9.2.4 References

- https://clickeys.nl

9.3 Medium Finding (Medium 10.0) CWE 614

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.

9.3.1 Impact

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.

9.3.2 Method of Exploitation

1. 1.
2. 2
3. 3

9.3.3 Remediation

The following steps should be taken to remediate

1. 1.
2. 2
3. 3

9.3.4 References

- https://clickeys.nl

9.4 Low Finding (Low 3.1) CWE 614

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.

9.4.1 Impact

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.

9.4.2 Method of Exploitation

1. 1.
2. 2
3. 3

9.4.3 Remediation

The following steps should be taken to remediate

1. 1.
2. 2
3. 3

9.4.4 References

- https://clickeys.nl

9.5 Info Finding (Info 0.0) CWE 614

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.

9.5.1 Impact

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.

9.5.2 Method of Exploitation

1. 1.
2. 2
3. 3

9.5.3 Remediation

The following steps should be taken to remediate

1. 1.
2. 2
3. 3

9.5.4 References

- https://clickeys.nl

10 Summary of Exploited Machines

Host	Open Ports	Services	Access	Exploited
lorem	lorem	lorem	lorem	lorem
lorem	lorem	lorem	lorem	lorem
lorem	lorem	lorem	lorem	lorem
lorem	lorem	lorem	lorem	lorem
lorem	lorem	lorem	lorem	lorem
lorem	lorem	lorem	lorem	lorem