Client Final Report

Web Application Vulnerability Project

[redacted]

V 1.0

July 2024

Designed to deliver the final project outcome information about an organization's web application/s vulnerabilities.

Table of Contents

1.0 Vulnerability Report

1.1 Introduction

This report details the findings from an unauthenticated external vulnerability assessment, targeting our client's publicly accessible web applications. The assessment simulates the perspective of an external actor with no prior access to internal networks, aiming to pinpoint exploitable vulnerabilities that could be leveraged in a cyber-attack.

1.2 Objective

This assessment aims to identify and evaluate security vulnerabilities from an external standpoint, focusing on internet-facing assets. The intent is to uncover risks an attacker could exploit to gain unauthorized access or disrupt services, thus providing actionable intelligence to bolster the client's defensive perimeter.

2.0 High-Level Summary

I was commissioned to conduct an external black box vulnerability assessment against the client's digital web application/s. An external black box vulnerability assessment is a rigorous evaluation of the systems exposed to the internet without internal network access or prior knowledge. The primary aim of this assessment was to simulate an adversary's approach to compromise the client's externally accessible systems and to infiltrate the organization's external defense mechanisms. Our fundamental goal was to scrutinize the network, catalog externally accessible systems meticulously, exploit vulnerabilities and document our findings to the client.

I discovered several critical vulnerabilities within the client's network during the assessment. Our approach allowed us to emulate the actions of a potential attacker, and we could infiltrate the client's systems predominantly due to unpatched software and suboptimal security configurations. Throughout the assessment, we achieved administrative-level access to several systems, all of which were successfully compromised, thus demonstrating the need for immediate remedial action. The implicated systems, along with a succinct synopsis of the exploitation methods, are itemized as follows:

Summary	Risk Rating	Comments
SWEET32	7.5	This vulnerability exploits the weakness of 64-bit block ciphers, which become susceptible to birthday attacks due to their relatively small block size.
TLS Version 1	6.5	TLS 1.0 lacks several security improvements in later versions of the protocol, such as stronger encryption algorithms and better resistance to various attacks.
TLS Version 1.1	6.5	TLS 1.1 lacked advanced security features and optimizations in later protocol versions, such as TLS 1.2 and TLS 1.3.
Unprotected Transport of Credentials	Medium	The application transmits authentication credentials over a channel that does not provide sufficient protection against interception or tampering.

2.1 Recommendations

I recommend patching the vulnerabilities identified during the testing to ensure that attackers cannot exploit these systems in the future. Remember that these systems require frequent patching and should remain on a regular patch program once patched to protect against additional vulnerabilities that are discovered later.

3.0 Methodologies

We utilized a widely adopted approach to performing the vulnerability assessment that effectively tests how well the clients' environments are secured.

3.1 Information Gathering

The information-gathering portion of a vulnerability assessment focuses on identifying the scope of the vulnerability assessment. The specific web applications were:

Web Application:

- **https://demo-compliance.[redacted]**

3.2 Web Application Vulnerability Assessment

Service Enumeration: The service enumeration portion of a vulnerability assessment focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors in a system. Understanding what applications are running on the system gives an attacker the required information before performing the penetration test. In some cases, some ports may not be listed.

Note:

- All identified vulnerabilities (including those classified as Low) will be included in this section.
- Informational scan results will be included in the appendix at the end of this document.

Underlying Web Application URL:demo-compliance.[redacted]

Service Enumeration

Server IP Address	Ports Open	Observations
104.[redacted]	TCP: 104.[redacted]	
	UDP: N/A	
172.[redacted]	TCP: 172.[redacted]	
	UDP: N/A	

Vulnerability: SSL Medium Strength Cipher Supported (SWEET32)

Description:

Evidence (if applicable): The remote host supports using SSL ciphers with medium-strength encryption. Nessus regards medium strength as any encryption that uses key lengths of at least 64 bits and less than 112 bits or uses the 3DES encryption suite.

CVE: 2016-2183

Risk Rating:7.5

Likelihood: Medium Risk

Consequence: Data exposure, Man-in-the-Middle Attacks, and Loss of confidentiality and Integrity

Impact: Compliance Issues, Decrease Trust, and Operational Impacts.

Recommendation: Disable 64-bit Block Ciphers, Use Stronger Ciphers, Keep Systems Updated, and Audit and Test Configurations.

Vulnerability: TLS Version 1 Protocol Detection

Description: The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has several cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS, like 1.2 and 1.3, are designed against these flaws and should be used whenever possible.

Evidence (if applicable): N/A

CVE: N/A

Risk Rating: 6.5

Likelihood: Medium Risk

Consequence: Weak Encryption can allow attackers to decrypt data transmitted between a client and server.

Impact: Can be exposed to Beast Attacks, Poodle Attacks, and Downgrade Attacks.

Recommendation: Disable TLS 1.0 Reconfiguration Servers, update all software, conduct regular audits, and educate and train staff.

Vulnerability: TLS Version 1.1 Deprecated Protocol

Description: The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation and authenticated encryption modes such as GCM cannot be used with TLS 1.1.

Evidence (if applicable): N/A

CVE: N/A

Risk Rating: 6.5

Likelihood: Medium Risk

Consequence: Weak Encryption can allow attackers to decrypt data transmitted between a client and server.

Impact: This causes compliance issues and will have operational implications.

Recommendation: Disable TLS 1.1, Update software, educate and train staff, and implement stronger protocols.

Vulnerability: Linux Kernel's /Proc Filesystem

Description: Local users could exploit a vulnerability in the Linux kernel's /proc filesystem to cause a denial of service. The issue was due to an improper handling of certain sequences of commands, which could trigger a system crash.

Evidence (if applicable): N/A

CVE: 2005-3299

Risk Rating:

Likelihood: Medium Risk

Consequence: Local users could exploit this vulnerability.

Impact: Denial of Service (DoS)

Recommendation: This vulnerability was patched in later versions of the Linux kernel. As always, keeping systems updated to mitigate such risks is essential.

Appendix: Informational Vulnerability Assessments

- Http (Multiple Issues)
- IETF Md5 (Multiple Issues)
- Services Detection
- Nessus SYN Scanner
- SSL Certificate Chain Contains Certificates Expiring Soon
- Common Platform Enumeration (CPE)
- Device Type
- Nessus Scan Information
- OS Identification
- TCP/IP Timestamp Supported
- Traceroute Information
- Cookie Scoped to Parent Domain
- Email Address Disclosed
- Credit Card Numbers Disclosed