# Document Control Record

|  |
| --- |
|  |
|  | v |

|  |  |
| --- | --- |
| **Document Owner** | Secneural LLC |
| **Document Name** | External Penetration Testing |
| **Project Reference No.** | svu557576454 |
| **Version No.** | 1.0 |
| **Effective Date** | 9th Jun 2024 |
| **Total number of Pages** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Revision Control** | | | |
| **Version No.** | **Author** | **Effective Date** | **Change Description** |
| 1.0 | mukesh test | 9th Jun 2024 |  |



# Confidentiality Notice

|  |
| --- |
|  |
|  | v |

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to **testo** or facilitate attacks against **testo**. hereinafter referred as **testo.**

**Secneural LLC** shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.

# Disclaimer

|  |
| --- |
|  |
|  | v |

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on **testo’s** environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

# Table of Contents

|  |
| --- |
|  |
|  | v |

[*Document Control Record*](#documentControlRecord)

[*Confidentiality Notice*](#confidentialityNotice)

[*Disclaimer*](#disclaimer)

[*Executive Summary*](#executiveSummary)

[*High Level Assessment Overview*](#highLevelAssessmentOverview)

[*1. Observed Security Strengths*](#observedSecurityStrength)

[*2. Area of Improvement*](#areaOfImprovement)

[*Scope of Service*](#scopeOfService)

[*1. Assets List*](#assetsInScope)

[*2. Provided Credentials*](#providedCredentials)

[*Methodology and Approach*](#methodologyAndApproach)

[*Penetration Testing and Auditing Tools*](#penetrationTestingAndAuditingTools)

[*Standards and Frameworks Followed*](#standardAndFrameworkFollowed)

[*Attack Surface*](#attackSurface)

[*1. Port Scanning Results*](#portScanningResults)

[*2. Breached Credentials Discovered*](#breachedCredentialsDiscovered)

[*3. Email Address Discovered*](#emailAddressDiscovered)

[*Assessment Findings*](#assessmentFindings)

[*Detailed Findings*](#detailedFindings)

[*Annexure*](#annexure)

[*1. Risk Classification*](#riskClassification)

[*2. Exploitation Likelihood Classification*](#exploitationLikelihood)

[*3. Business Impact Classifications*](#businessImpact)

[*4. Remediation Difficulty Classifications*](#remediationDifficulty)

[*5. Test Case Performed*](#testCasePerformed)

[*About Us*](#aboutUs)

[*Client Information*](#clientInformation)

# Executive Summary

|  |
| --- |
|  |
|  | v |

**Secneural LLC** performed an External Penetration Testing assessment of the external corporate network of **testo**. Secneural LLC’s penetration test simulated an attack from an external threat actor attempting to gain access to systems within the **testo** corporate network. The purpose of this assessment was to discover and identify vulnerabilities in **testo**’s infrastructure and suggest methods to remediate the vulnerabilities.

The assessment was performed during the following timeline

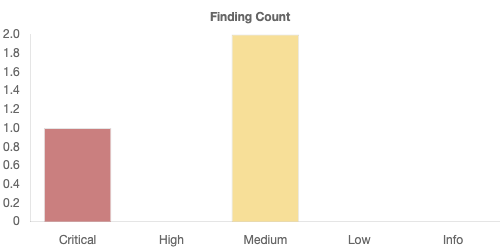
**Secneural LLC** identified a total of **3** vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

The assessment was performed during the following timeline

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. No | Activity | Start Date | End Date |
| 1 | External Penetration Testing | 24th Jan 2024 | 25th Jan 2024 |

**Secneural LLC  identified** a total of 3 vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CRITICAL | HIGH | MEDIUM | LOW | INFORMATIONAL |
| 1 | 0 | 2 | 0 | 0 |



***Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.***

# High Level Assessment Overview

|  |
| --- |
|  |
|  | v |

## Observed Security Strengths

Secneural identified the following strengths in **testo**’s network which greatly increases the security of the network. **testo** should continue to monitor these controls to ensure they remain effective.

* **testo** have all the internet exposed web services behind a web application firewall.
* **testo** have a strong patch management for the internet exposed services.

## Area of Improvement

Secneural recommends **testo** takes the following actions to improve the security of the network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack **testo**’s information systems and/or reduce the impact of a successful attack.

* It is recommended to regularly review and disable any unnecessary file system mounts to minimize potential attack surfaces.
* It is recommended to immediately change any usernames and passwords that were found in exposed configuration files. Ensure that the new credentials are strong and unique.
* Review and revise access controls and permissions within the virtual desktop environment. Limit user privileges to only what is necessary for their roles and responsibilities, reducing the likelihood of unauthorized access.
* Immediately change any LDAP usernames and passwords found in exposed configuration files. Use strong, unique passwords.
* Verify that the MFA settings are properly integrated with the Microsoft authentication services to prevent any bypass.
* It is recommended to configure policies to enforce MFA at every login attempt, especially for accessing critical applications and data.
* Mandate the use of MFA for all users, including administrators and privileged accounts, to add an extra layer of security.
* It is recommended to use long passphrases to make passwords easier to remember and more secure. Encourage users to create passwords that are complex and difficult to guess. A strong password typically includes a combination of uppercase and lowercase letters, numbers, and special characters.
* It is recommended to set up rate limiting mechanisms to restrict the number of logins attempts from a single IP address within a specific time.
* It is recommended to enforce Code Integrity Policies (CIP) to restrict the execution of binaries and scripts to only approved locations, preventing unauthorized execution of DLL files.
* It is recommended to upgrade a newer version of the operating system, such as Windows Server 2019 or 2022 and Windows 10 or 11, as Windows Server 2012 R2 and Windows 8.1 have reached their end-of-life, meaning they no longer receive security updates.
* Configure application execution policies to restrict the applications that can be run on devices. This can help to prevent scripts from being executed.
* It is recommended to configure the server to strip the **X-OWA-Version** header from all responses. This can usually be achieved through server settings or by using a web application firewall (WAF) to filter out this header.
* It is recommended to configure the web server to strip the **X-FEServer** header from all responses. This can typically be done through the server configuration files (e.g., Apache's httpd.conf, Nginx's nginx.conf) or via a web application firewall (WAF).
* It is recommended to configure account lockout policies to automatically lock user accounts after a certain number of failed login attempts.
* Regularly update WordPress to the latest version, apply security patches promptly, and maintain awareness of potential security issues affecting their WordPress installation.
* Monitor web server logs and network traffic for suspicious activity indicating attempts to enumerate user accounts via RDF files.
* Upgrade to the latest version of the jQuery library to leverage enhanced functionalities and security improvements.
* Implement a robust SSL certificate management process that includes monitoring SSL certificate expiration dates and proactively renewing SSL certificates before they expire.
* As a security measure, disable support for TLS 1.0 and TLS 1.1 to enforce stronger encryption protocols and safeguard against vulnerabilities.
* Configure the SMTP server to require authentication for sending emails which ensures that only authorized users can send emails through the server.
* Ensure that the application only accepts valid and expected Host headers and any deviation from the expected values should be rejected or sanitized.
* Ensure that internal naming conventions are not used on Exchange servers can help minimize this risk.

# Scope of Service

|  |
| --- |
|  |
|  | v |

All testing was based on the scope as defined from {{**client\_name}}** and official written communications. The items in scope are listed below.

## Assets List

|  |  |  |
| --- | --- | --- |
| Sr. No. | Name | Asset |
| 1 | 192.168.3.116 | 192.168.3.116 |
| 2 | 10.40.13.58 | 10.40.13.58 |
| 3 | 10.40.13.52 | 10.40.13.52 |
| 4 | 10.40.13.73 | 10.40.13.73 |
| 5 | 10.40.13.47 | 10.40.13.47 |
| 6 | 10.40.13.43 | 10.40.13.43 |
| 7 | 10.40.13.72 | 10.40.13.72 |
| 8 | 10.40.13.42 | 10.40.13.42 |
| 9 | 10.40.13.33 | 10.40.13.33 |
| 10 | 10.40.13.22 | 10.40.13.22 |
| 11 | 10.40.13.27 | 10.40.13.27 |
| 12 | 10.40.13.20 | 10.40.13.20 |

## Provided Credentials

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. No. | Name | Username | Password |
| 1 | 192.168.3.116 | - | - |
| 2 | 10.40.13.58 | - | - |
| 3 | 10.40.13.52 | - | - |
| 4 | 10.40.13.73 | - | - |
| 5 | 10.40.13.47 | - | - |
| 6 | 10.40.13.43 | - | - |
| 7 | 10.40.13.72 | - | - |
| 8 | 10.40.13.42 | - | - |
| 9 | 10.40.13.33 | - | - |
| 10 | 10.40.13.22 | - | - |
| 11 | 10.40.13.27 | - | - |
| 12 | 10.40.13.20 | - | - |

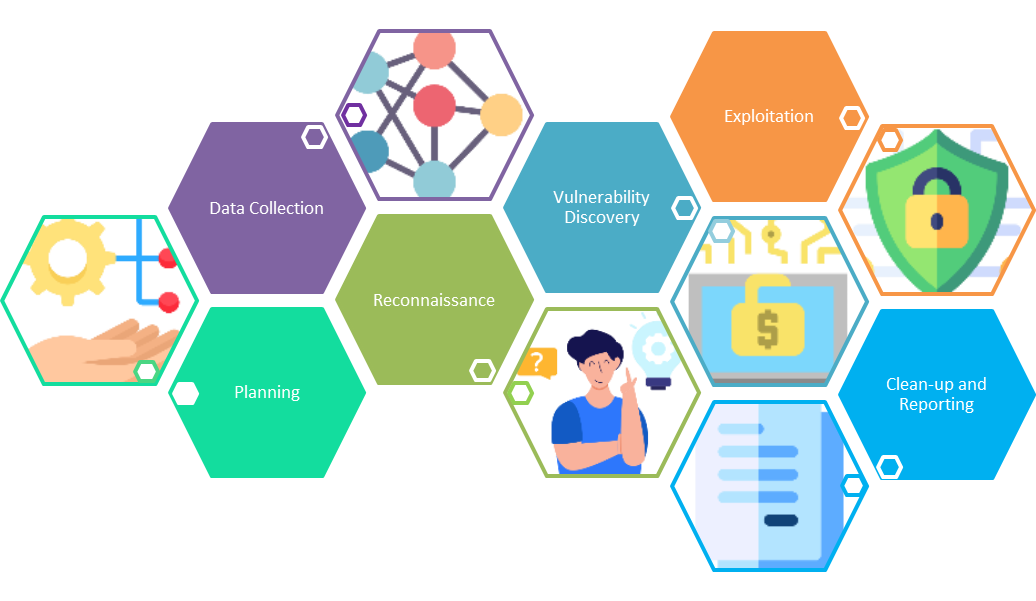
# Methodology and Approach

|  |
| --- |
|  |
|  | v |

**External Penetration Testing**

The External Penetration testing in a blackbox approach is one of the most effective assessments to provide a 360-degree visibility on the probable weaknesses that a threat actor or adversary or an organized cybercriminal/group might exploit without any on-premises access to the organizational infrastructure and minimal to zero knowledge of the organization’s IT infrastructure. This emulates a case scenario which provides the resultant with all the technical security gaps in the organization’s IT infrastructure which an external entity access or exploit such as any internet user residing in any country or imitating any cloud service etc.

During the External Penetration testing the following Phases are included:



**PLANNING**

First, the Secneural team understands the requirements for network/infrastructure assessment and defines the test scope. These can be very open or get very specific. For example, a pentest may involve a customer-facing webpage, but will not cover employee email accounts. It is vital that the team know the scope of the test going into it.

**RECONNAISSANCE**

Secneural perform both active and passive reconnaissance during the assessment. The starting phase of assessment, Secneural will perform a passive reconnaissance to find all the assets exposed over the internet for the respective organization using several different methods and sources without actively engaging with the organization’s assets. Once the asset list id prepared our team seeks a confirmation of all the assets mention in the list to be added to the scope of work from the customer. Once the mutually agreed on the scope of work the active reconnaissance is initiated to identify all network assets and security gaps that malicious actors may exploit to compromise the network. This may involve everything from public websites, VPN services etc.

**DATA COLLECTION**

This is the phase where further detailed information is collected about the target system, including databases, software versions, plugins, hardware, etc. Together, the Reconnaissance and Data Collection phases are known as “enumeration.”

**VULNERABILITY DISCOVERY**

Secneural actively look for flaws in the network, systems, and applications. This may include unpatched software, least privilege vulnerabilities, or pwned passwords.

**EXPLOITATION**

Identified flaws are actively exploited to compromise a target using an exploit kit. Secneural may use tools such as Metasploit or Netsparker, or compromised usernames and passwords may be used to log into an otherwise inaccessible network.

**REPORTING**

The Identified vulnerabilities and all weaknesses observed during the assessment will be documented along with a possible recommendation based on industry best practices.

**CLEANUP**

This last phase validate that no artifacts created/used during the assessment is left out on any of the active servers/services of the targeted IT assets.

# Penetration Testing and Auditing Tools

|  |
| --- |
|  |
|  | v |

|  |  |  |
| --- | --- | --- |
| **Sample Tools** | | |
| **S.No** | **Name** | **Type** |
| 1 | Nmap | Mobile, Web, Network |
| 2 | Metasploit | Mobile, Web, Network |
| 3 | Responder | Network |
| 4 | Bloodhound | Network |
| 5 | Ntlmrelayx | Network |
| 6 | Nessus | Web, Mobile, Network |
| 7 | Ettercap | Network |
| 8 | VoIP hopper | Network |
| 9 | Publicly available tools from GitHub | All |
| 10 | Sysinternals | Network |
| 11 | Mimikatz | Network |
| 12 | Nikto | Web, Mobile |
| 13 | GoPhish | Social Engineering |
| 14 | ApkTool | Mobile |
| 15 | Hopper | Mobile |
| 16 | Burp Suite Pro | Mobile, Web |
| 17 | Mobsf | Mobile |
| 18 | CIS Benchmarks | Network |
| 19 | Nipper | Network |
| 20 | Wireshark | Network |
| 21 | Custom Scripts | All |



# Standards and Frameworks Followed

|  |
| --- |
|  |
|  | v |



# Attack Surface

|  |
| --- |
|  |
|  | v |

## Port Scanning Results

| **Sr. No.** | **Hostnames** | **IPs** | **Ports** |
| --- | --- | --- | --- |
| 1 | <CLIENT>.com | 1xx.1x.x.x4 | 80/tcp, 443/tcp, 8880/tcp, 2083/tcp, 2096/tcp, 2053/tcp, 2095/tcp, 2086/tcp, 2052/tcp, 8443/tcp, 2087/tcp, 2082/tcp |
| 2 | autodiscover.<CLIENT>.com | 8x.xx.5x.x0 | 443/tcp |
| 3 | creeningsm.<CLIENT>.com | 2x.x1.2x.xx5 | 443/tcp |
| 4 | reporter.<CLIENT>.com | 8x.xx.57.12 | 443/tcp |
| 5 | payment.<CLIENT>.com | 2x.2x.xxx.xxx | 443/tcp |
|  |  |  |  |
| **<Redacted>** | | | |
|  |  |  |  |
| 68 | 4app.<CLIENT>.com | N/A | N/A |

## Breached Credentials Discovered

| **Sr. No.** | **Emails** |
| --- | --- |
|  | mahmoud.a@<CLIENT>.com |
|  | info@<CLIENT>.com |
|  | maly@<CLIENT>.com |
|  | aea@<CLIENT>.com |
|  | asam@<CLIENT>.com |
|  | jcyr@<CLIENT>.com |
|  | ali@<CLIENT>.com |
|  | jwan@<CLIENT>.com |
|  | salki@<CLIENT>.com |
|  | fgra@<CLIENT>.com |
|  | rlad@<CLIENT>.com |
|  |  |
| **<Redacted>** | |
| 467 | adia@<CLIENT>.com |

## Email Address Discovered

| **Sr. No.** | **Emails** |
| --- | --- |
|  | mahmoud.a@<CLIENT>.com |
|  | info@<CLIENT>.com |
|  | maly@<CLIENT>.com |
|  | aea@<CLIENT>.com |
|  | asam@<CLIENT>.com |
|  | jcyr@<CLIENT>.com |
|  | ali@<CLIENT>.com |
|  | jwan@<CLIENT>.com |
|  | salki@<CLIENT>.com |
|  | fgra@<CLIENT>.com |
|  | rlad@<CLIENT>.com |
|  |  |
| **<Redacted>** | |
| 467 | adia@<CLIENT>.com |

# Assessment Findings

|  |
| --- |
|  |
|  | v |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sr. No. | Vulnerability ID | Finding | Risk Score | Risk |
| 1 | testo-ftest-EPT-002-001 | outdated version | 9.7 | CRITICAL |
| 2 | testo-ftest-EPT-003-002 | Improper root or jailbreak detection | 6 | MEDIUM |
| 3 | testo-ftest-EPT-001-003 | clickjacking | 5.5 | MEDIUM |

# Detailed Findings

|  |
| --- |
|  |
|  | v |

Below mentioned are the detailed description, risk and remediations of each finding identified during the assessment.

**outdated version**

|  |  |
| --- | --- |
| **Vulnerability - testo-ftest-EPT-002-001** | |
| Vulnerability Name | **outdated version** |
| Affected Host | 10.40.13.47 |
| Affected Port | N/A |
| Risk Rating | **CRITICAL RISK (9.7/10)** |
| Exploitation Likelihood | **Likely** |
| Business Impact | **Major** |
| Remediation Difficulty | **Moderate** |

* **Description**

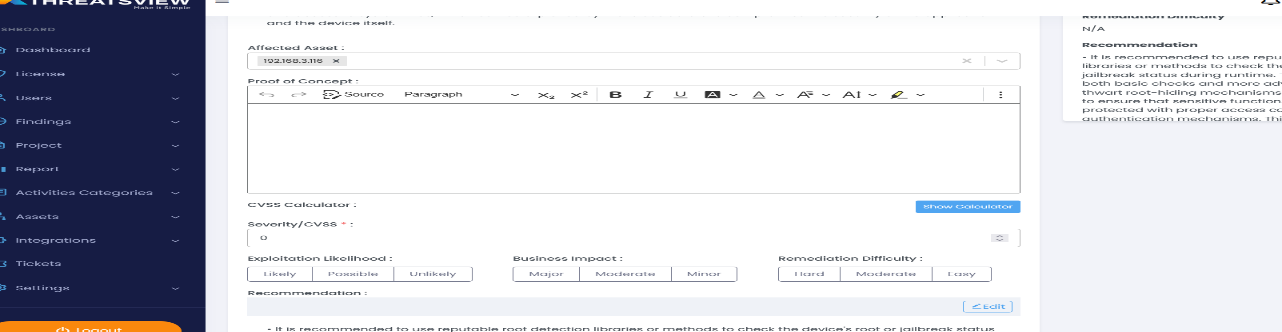
Using outdated software versions can pose significant security risks as they may contain known vulnerabilities that can be exploited by attackers. The longer a software version remains outdated, the more likely it is that security patches and updates addressing those vulnerabilities are available. Attackers can target these vulnerabilities to gain unauthorized access, compromise data, or disrupt systems.

* **Remediation**

. It is recommended to regularly monitor vendor websites and security advisories for updates and patches . It is recommended to keep software up-to-date . It is recommended to monitor and detect outdated software

* **Proof of Concept**

The risk classification is calculated using CVSS v3 standard.  The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.



* **Severity**

Hai are you fine

* **References**

https://owasp.com

**Improper root or jailbreak detection**

|  |  |
| --- | --- |
| **Vulnerability - testo-ftest-EPT-003-002** | |
| Vulnerability Name | **Improper root or jailbreak detection** |
| Affected Host | 192.168.3.116 |
| Affected Port | N/A |
| Risk Rating | **MEDIUM RISK (6/10)** |
| Exploitation Likelihood |  |
| Business Impact |  |
| Remediation Difficulty |  |

* **Description**

No Root Detection is a security vulnerability that exists in mobile applications when they fail to detect whether a device has been rooted or jailbroken. Rooting or jailbreaking a device typically provides users with elevated privileges and access to system files, which can be exploited by malicious actors to compromise the security of the application and the device itself.

* **Severity**

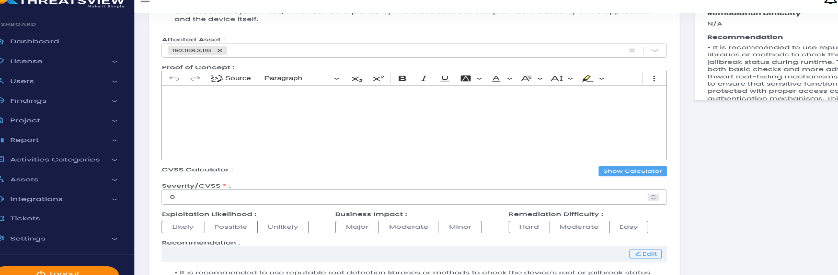
• It is recommended to use reputable root detection libraries or methods to check the device's root or jailbreak status during runtime. This should include both basic checks and more advanced techniques to thwart root-hiding mechanisms. • It is recommended to ensure that sensitive functions and data are protected with proper access controls and authentication mechanisms. This should prevent unauthorized access, even if a rooted device manages to bypass root detection. • Apply code obfuscation techniques to make it more difficult for attackers to reverse-engineer the application and find vulnerabilities related to root detection.

* **Remediation**

It is recommended to use reputable root detection libraries or methods to check the device's root or jailbreak status during runtime. This should include both basic checks and more advanced techniques to thwart root-hiding mechanisms. • It is recommended to ensure that sensitive functions and data are protected with proper access controls and authentication mechanisms. This should prevent unauthorized access, even if a rooted device manages to bypass root detection. • Apply code obfuscation techniques to make it more difficult for attackers to reverse-engineer the application and find vulnerabilities related to root detection.

* **Proof of Concept**

Secneural perform both active and passive reconnaissance during the assessment. The starting phase of assessment, Secneural will perform a passive reconnaissance to find all the assets exposed over the internet for the respective organization using several different methods and sources without actively engaging with the organization’s assets. Once the asset list id prepared our team seeks a confirmation of all the assets mention in the list to be added to the scope of work from the customer. Once the mutually agreed on the scope of work the active reconnaissance is initiated to identify all network assets and security gaps that malicious actors may exploit to compromise the network. This may involve everything from public websites, VPN services etc.



* **Severity**

jsdojsadkjsdkf oauskdaus  aosfousadofu ajsaodjfosadjf ojosadjfosdajfoi ljdsf lkjdsaf lkkjlsajdkf  jdlkfjsaldfjlksajfd

* **References**

https://owasp.org

**clickjacking**

|  |  |
| --- | --- |
| **Vulnerability - testo-ftest-EPT-001-003** | |
| Vulnerability Name | **clickjacking** |
| Affected Host | 10.40.13.47 |
| Affected Port | N/A |
| Risk Rating | **MEDIUM RISK (5.5/10)** |
| Exploitation Likelihood | **Likely** |
| Business Impact | **Minor** |
| Remediation Difficulty | **Easy** |

* **Description**

Clickjacking, also known as UI redress attack or UI/UX attack, is a type of web application vulnerability that allows an attacker to trick users into clicking on a malicious link or button by hiding it behind a legitimate and seemingly harmless element on a website. This can lead to unauthorized actions being performed by the user, such as making purchases, changing settings, or revealing sensitive information, without their knowledge or consent.

* **Remediation**

. It is recommended to implement X-Frame-Options header . It is recommended to implement Content Security Policy (CSP) . It is recommended to Use frame-busting code

* **Proof of Concept**]

Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions

# 

* **Severity**

Hello how are you

* **References**

https://owasp.in

# Annexure

|  |
| --- |
|  |
|  | v |

## Risk Classification

The risk classification is calculated using CVSS v3 standard.  The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

| **Level** | **Score** | **Description** |
| --- | --- | --- |
| **Critical** | **10** | The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed. |
| **High** | **7-9** | The vulnerability poses an urgent threat to the organization, and remediation should be prioritized. |
| **Medium** | **4-6** | Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible. |
| **Low** | **1-3** | The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible. |
| **Informational** | **0** | These findings have no clear threat to the organization but may cause business processes to function differently than desired or reveal sensitive information about the company. |

## Exploitation Likelihood Classification

The exploitation likelihood classification helps understand the actual technical ease factor of a vulnerability to be used against organizations network(s)/assets.

|  |  |
| --- | --- |
| **Likelihood** | **Description** |
| **Likely** | Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty. |
| **Possible** | Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation. |
| **Unlikely** | Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation. |

## Business Impact Classifications

This classification helps the organization to understand the business impact due to a successful exploitation of the vulnerability addressed.

|  |  |
| --- | --- |
| **Impact** | **Description** |
| **Major** | Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage. |
| **Moderate** | Successful exploitation may cause significant disruptions to non-critical business functions. |
| **Minor** | Successful exploitation may affect few users, without causing much disruption to routine business functions. |

## Remediation Difficulty Classifications

The classification helps organization to prioritize the patch management cycle and help the organization with its patch management KPI matrix to allocate the manpower and resource accordingly.

| **Difficulty** | **Description** |
| --- | --- |
| **Hard** | Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions. |
| **Moderate** | Remediation may require minor reconfigurations or additions that may be time-intensive or expensive. |
| **Easy** | Remediation can be accomplished in a short amount of time, with little difficulty. |

## Test Case Performed

|  |  |  |
| --- | --- | --- |
| Sr No | Test case | Status |
| 1 | DNS brute-forcing | Pass |
| 2 | Zone transfer Vulnerability | Pass |
| 3 | Server Version Disclosure | Pass |
| 4 | Outdated software version in use | Fail |
| 5 | Clickjacking | Fail |
| 6 | Password with auto complete enabled | Pass |
| 7 | Insecure login over HTTP | Pass |
| 8 | Username Enumeration | Pass |
| 9 | Missing Security Header | Pass |
| 10 | No Password policy | Pass |
| 11 | Information Leakage through HTTP response Header | Pass |
| 12 | Exposed Sensitive Files | Pass |
| 13 | Directory Listing | Pass |
| 14 | Missing HttpOnly Attribute | Pass |
| 15 | Missing Secure Flag Attribute | Pass |
| 16 | Default Credentials | Pass |
| 17 | Missing Account Lockout Mechanism | Pass |
| 18 | Reflected Cross Site Scripting | Pass |
| 19 | Open Redirection | Pass |
| 20 | Database credential leakage | Pass |
| 21 | Harcoded senstive information found on public repositories | Pass |
| 22 | Subdomain Takeover | Pass |
| 23 | Misconfigured cloud buckets | Pass |
| 24 | OWA password spraying | Pass |
| 25 | Information disclosure | Pass |
| 26 | Default Web page | Pass |
| 27 | Open Mail Relay | Pass |
| 28 | IKE aggressive mode | Pass |
| 29 | Unexpected Perimeter Services | Pass |
| 30 | Historical Account Compromise | Pass |
| 31 | Information disclosure in error messages | Pass |
| 32 | Security Misconfiguration | Pass |
| 33 | Insufficient traffic blocking | Pass |

# About Us

|  |
| --- |
|  |
|  | v |

     Secneural LLC - Cyber Security Consulting Company

Secneural is a one-stop trustworthy partner that ensures comprehensive protection of online assets (be it websites, mobile apps, etc.). Our team consists of handpicked cyber security professionals who come with years of substantial experience to come up with effortless and efficient cyber security solutions. We provide our services across industries such as Healthcare, Machineries, Retail, Finance, Manufacturing, and Utilities.

Our Mission

Our mission to make the world a safe and secure place by transforming the way enterprises conduct cyber security activities.

Our Vision

We envision to effectively detect, improve, mitigate, and get rid of the risk of cyber-attacks to maintain a good cyber security posture.

 Contact Details

|  |  |
| --- | --- |
|  |  |
| **Phone Number** | +974 4423 1323 |
| **Contact Email Id** | info@secneural.com |
| **Website** | www.seneural.com |
| **Office Address** | Office No.133Register09, 1st Floor, Regus Business Centre, No. 65, Doha, Qatar |

# Client Information

|  |
| --- |
|  |
|  | v |

|  |  |
| --- | --- |
|  |  |
| **Client** | testo |
| **Primary Contact** | **testo**  **testo** |
| **Approvers** | The following people are authorized to change the scope of engagement and modify the terms of the engagement.   * mukesh test |



**Thank you again for the opportunity to work with you, to help your organization, and to earn your trust. Please contact us at your convenience to discuss any aspect of our report.**

image

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | |  | |  |  | | --- | --- | |  |  | | | |  |  | | --- | --- | |  | Page | |