

Company logo

Assessment Report

Mobile Application Penetration Testing



Prepared For



<CN> (<SHORT-CN>)

V 1.0

09-07-2023

Document Control Record

v

|  |  |
| --- | --- |
| **Document Owner** | Secneural LLC |
| **Client** | <CN> (<SHORT-CN>) |
| **Submitted To** |  |
| **Document Name** | Mobile Application Penetration Testing Report |
| **Project Reference No.** | 2023/07/07/<SHORT-CN>/1 |
| **Version No.** | 1.0 |
| **Effective Date** |  |
| **Total number of Pages** | 84 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Revision Control** | | | |
| **Author** | **Effective Date** | **Change Description** | **DCR no.** |
| Penetration Tester | 6th July 2023 | Initial Draft | 1.0 |
| Technical Manager | 9th July 2023 | Final | 1.2 |

****

# 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 **<CN>** or facilitate attacks against **<CN>**. hereinafter referred as **<SHORT-CN>.**

**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 **<CN>’s** environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

Table of Contents

v

[Confidentiality Notice 2](#_Toc141783439)

[Disclaimer 2](#_Toc141783440)

[Executive Summary 4](#_Toc141783441)

[High Level Assessment Overview 6](#_Toc141783442)

[Observed Security Strengths 6](#_Toc141783443)

[Area of Improvement 6](#_Toc141783444)

[Scope of Service 7](#_Toc141783445)

[Asset List 7](#_Toc141783446)

[Provided Credentials 7](#_Toc141783447)

[Methodology and Approach 8](#_Toc141783448)

[Mobile Application Penetration Testing 8](#_Toc141783449)

[Penetration Testing and Auditing Tools 11](#_Toc141783450)

[Standards and Frameworks followed 12](#_Toc141783451)

[Assessment Findings 13](#_Toc141783452)

[Detailed Findings 14](#_Toc141783453)

[Authentication Bypass 14](#_Toc141783454)

[Appendix 1 – Classification Definitions 16](#_Toc141783455)

[A. Risk Classification 16](#_Toc141783456)

[B. Exploitation Likelihood Classification 17](#_Toc141783457)

[C. Business Impact Classifications 17](#_Toc141783458)

[D. Remediation Difficulty Classifications 18](#_Toc141783459)

[Appendix 2 – Client Information 19](#_Toc141783460)

[Appendix 3 – About Us 20](#_Toc141783461)

[Secneural LLC - Cyber Security Consulting Company 20](#_Toc141783462)

[Our Mission 20](#_Toc141783463)

[Our Vision 20](#_Toc141783464)

[Contact Details 20](#_Toc141783465)

# ExecutiveSummary

v

**Secneural LLC** performed a Mobile Application Penetration Testing assessment on the \_\_\_\_\_ applications provided as part of the scope of work by **<SHORT-CN>**. The penetration test simulated an attack from an external threat actor or a rouge user attempting to compromise the security and integrity of the **<SHORT-CN>** \_\_\_\_\_ application services and servers. The purpose of this assessment was to discover and identify vulnerabilities in **<SHORT-CN>**’s \_\_\_\_\_\_\_ mobile applications and suggest methods to remediate the vulnerabilities.

The assessment was performed during the following timeline

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. No | Activity | Start Date | End Date |
| 1 | Mobile Application Penetration Testing | 21st June 2023 | 6th July 2023 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sr. No | Application Name | Package ID | Platform | Application Hash |
| 1 |  |  | Android |  |
| 2 |  |  | iOS |  |

During the assessment, a total of 21 vulnerabilities were identified within the scope of the engagement which are broken down by severity in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| CRITICAL | HIGH | MEDIUM | LOW |
| 2 | 6 | 11 | 2 |

The highest severity vulnerabilities give potential attackers the opportunity to exploit the authentication bypass due to which the consultants were able to compromise the accounts and gain access on "\_\_\_\_\_\_application" impersonating the victim account. In order to ensure data confidentiality, integrity, and availability, security remediation should be implemented as described in the security assessment findings. 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.

The table below summarizes the findings for OWASP top 10 list of [Mobile application vulnerabilities](https://owasp.org/www-project-mobile-top-10/) and [API Vulnerabilities](https://owasp.org/www-project-api-security/). The OWASP Top 10 is a standard awareness document for developers and mobile/API security. It represents a broad consensus about the most critical security risks to mobile application and API.

|  |  |
| --- | --- |
| Mobile Top10 Category | Discovered |
| M1: Improper Platform Usage | Yes |
| [M2: Insecure Data Storage](https://owasp.org/www-project-mobile-top-10/2016-risks/m2-insecure-data-storage) | Yes |
| [M3: Insecure Communication](https://owasp.org/www-project-mobile-top-10/2016-risks/m3-insecure-communication) | Yes |
| [M4: Insecure Authentication](https://owasp.org/www-project-mobile-top-10/2016-risks/m4-insecure-authentication) | Yes |
| [M5: Insufficient Cryptography](https://owasp.org/www-project-mobile-top-10/2016-risks/m5-insufficient-cryptography) | Yes |
| [M6: Insecure Authorization](https://owasp.org/www-project-mobile-top-10/2016-risks/m6-insecure-authorization) | Yes |
| [M7: Client Code Quality](https://owasp.org/www-project-mobile-top-10/2016-risks/m7-client-code-quality) | Yes |
| [M8: Code Tampering](https://owasp.org/www-project-mobile-top-10/2016-risks/m8-code-tampering) | No |
| [M9: Reverse Engineering](https://owasp.org/www-project-mobile-top-10/2016-risks/m9-reverse-engineering) | Yes |
| [M10: Extraneous Functionality](https://owasp.org/www-project-mobile-top-10/2016-risks/m10-extraneous-functionality) | No |

| API Top10 Category | Discovered |
| --- | --- |
| API1:2019 Broken Object Level Authorization | No |
| API2:2019 Broken User Authentication | Yes |
| API3:2019 Excessive Data Exposure | Yes |
| API4:2019 Lack of Resources & Rate Limiting | Yes |
| API5:2019 Broken Function Level Authorization | Yes |
| API6:2019 Mass Assignment | No |
| API7:2019 Security Misconfiguration | Yes |
| API8:2019 Injection | No |
| API9:2019 Improper Assets Management | Yes |
| API10:2019 Insufficient Logging & Monitoring | Yes |

# High Level Assessment Overview

v

## Observed Security Strengths

Secneural identified the following strengths in <SHORT-CN>’s mobile application which greatly increases the security of the mobile application. <SHORT-CN> should continue to monitor these controls to ensure they remain effective.

* It was observed that the \_\_\_\_\_ mobile application have baseline controls such as root detection, emulator detection, and SSL pinning implemented to the application.

## Area of Improvement

Secneural recommends <SHORT-CN> takes the following actions to improve the security of the applications. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack <SHORT-CN>’s information systems and/or reduce the impact of a successful attack.

* Implement stronger session management to avoid any response tampering at the application level.
* Implement proper rate limiting on OTP code validations.
* Restrict android application from logging sensitive data such as session tokens in the application logs and debug logs.
* Implement proper account lockout policy for failed authentication attempts.

# Scope of Service

v

All testing was based on the scope as defined from <SHORT-CN> and official written communications. The items in scope are listed below.

## Asset List

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. no | Name | Platform | Assets |
| 1 |  | Android |  |
| 2 |  | iOS |  |

## Provided Credentials

The Mobile Application Penetration Testing assessment was conducted with a grey box approach where the consultants were given non-admin privileged accounts. The below credentials were provided for commencing the assessment :

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. No | User (Phone number) | OTP | Description |
| 1 |  |  |  |
| 2 |  |  |  |

# Methodology and Approach

v

## Mobile Application Penetration Testing

Secneural’s Mobile application penetration test combines the results from industry-leading scanning tools with manual testing to enumerate and validate vulnerabilities, configuration errors, and business logic flaws. In-depth manual application testing enables us to find business logic vulnerabilities and vulnerabilities which are often missed by automated testing tools. Using this approach, Secneural’s comprehensive Mobile Application Penetration Test covers the classes of vulnerabilities outlined in the Open Mobile Application Security Project (OWASP) Top 10 and beyond-

Graphical user interface, text, application

Description automatically generated

**Initial Planning**

Identifying the specific area of the organization’s Mobile application and how the applications are deployed either Google Playstore, Apple app store or private app store service.

**Application Mapping**

1. Map the application for possible security vectors
2. What is the application genre? (Game, business, productivity etc)
3. Does the application connect to backend web services?
4. Is the application purely native or incorporates readymade frameworks?
5. Does the application store data on the device?
6. What all features of the device are used by the application? (Camera, gyroscope, contacts etc)

**Information Gathering**

1. Observe application behaviour
2. Determine the application’s data states (at rest, in transit or on display) and sensitivity
3. Identify access methods
4. Identify what frameworks are in use
5. Identify server-side APIs that are in use
6. Identify what protocols are in use
7. Identify other applications or services with which the application interacts
8. Get information about what functions, classes and methods are referenced in the application and in the dynamically loaded libraries.
9. List the dynamic dependencies.

**Application Traffic Analysis**

1. Analyze error messages
2. Analyze cacheable information
3. Transport layer security (TLS version; NSURLRequest object)
4. Attack XML processors
5. SQL injection
6. Privacy issues (sensitive information disclosure)
7. Improper session handling
8. Decisions via untrusted inputs
9. Broken cryptography
10. Unmanaged code
11. URL Schemes
12. Push notifications
13. Authentication
14. Authorization
15. Session management
16. Data storage
17. Data validation (input, output)
18. Transport Layer protection – are the certificates validated, does the application implement Certificate Pinning
19. Denial of service
20. Business logic
21. UDID or MAC ID usage (privacy concerns)

**Reporting**

Document all the identified security vulnerabilities and remediation to fix glitches by introducing product updates or system upgrades.

With addition to the penetration testing cycle an integral part of the approach is on the industries best standard approach for testing Mobile application. Secneural’s mobile application penetration testing assessment follows OWASP standardized approach for the same.

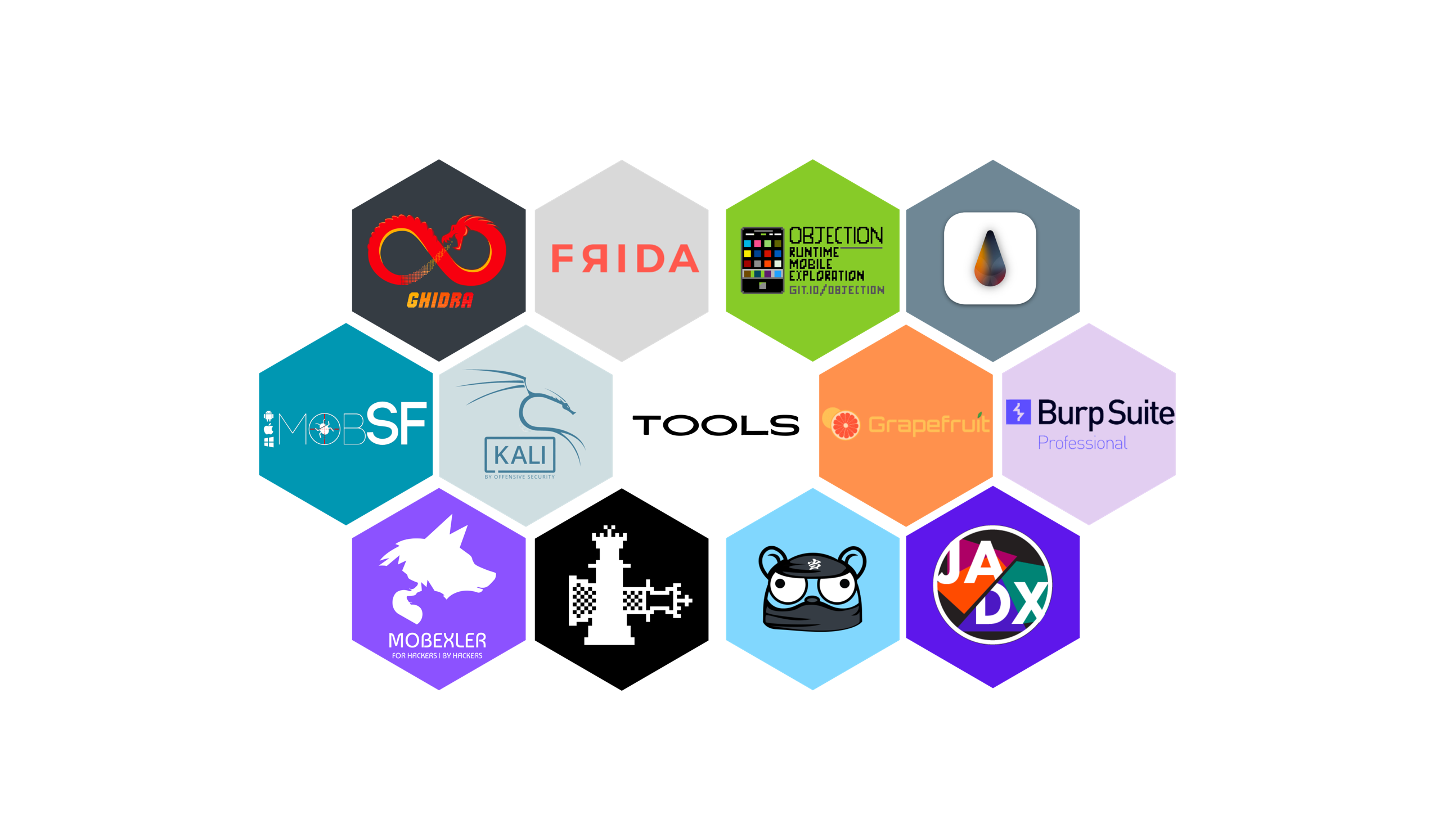
**OWASP Step-by-step Approach**

* M1 - Weak Server-side controls
* M2 - Insecure Data storage
* M3 - Insufficient Transport Layer Protection
* M4 - Unintended Data Leakage
* M5 - Poor Authorization and Authentication
* M6 - Broken Cryptography
* M7 - Client-Side Injection
* M8 - Security Decisions via untrusted inputs
* M9 - Improper Session Handling
* M10 - Lack of Binary Protection

# Penetration Testing and Auditing Tools

v

|  |  |  |
| --- | --- | --- |
| Sr.no | Tool | Version |
| 1 | Burp Suite Pro | 2023.6.2 |
| 2 | Drozer | 2.50 |
| 3 | Mobsf | 3.6.2 |
| 4 | Kali Linux OS | 2023.2 |
| 5 | Jadx | 1.4.7 |
| 6 | Objection | 1.11.0 |
| 7 | Frida | 16.1.0 |
| 8 | Application Debugger | - |



# Standards and Frameworks followed



v

# Assessment Findings

v

The below mentioned are the list of vulnerabilities identified during the application security assessment.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sr. No. | Vulnerability ID | Finding | Platform | Risk Score | Risk |
| 1 | <SHORT-CN>- QD-MAPT-01 | Authentication Bypass | Web API | 9.1 | **Critical** |

# Detailed Findings

v

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

# Authentication Bypass

|  |  |
| --- | --- |
| **Vulnerability - <SHORT-CN>-<APPLICATION NAME> -MAPT-01** | |
| Vulnerability Name | **Authentication Bypass** |
| Affected Endpoint(s) |  |
| Platform | Web API |
| Risk Rating | **CRITICAL (9.1/10)** |
| CVSS Vector | **CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N** |
| Exploitation Likelihood | **Possible** |
| Business Impact | **Major** |
| Remediation Difficulty | **Easy** |

1. **Description**

An OTP (One-Time Password) bypass vulnerability refers to a security flaw or weakness that allows an attacker to bypass the OTP authentication mechanism and gain unauthorized access to a system or account. This vulnerability can pose a significant risk to the security and privacy of users' sensitive information.

However, if there is a vulnerability in the implementation or configuration of the OTP system, an attacker may find a way to bypass the OTP check altogether. This could be achieved through various means, such as exploiting flaws in the code, intercepting OTP messages, or manipulating the authentication flow.

Once an attacker successfully bypasses the OTP, they can gain unauthorized access to the targeted account or system without the legitimate user's knowledge or permission. This can lead to various consequences, depending on the nature of the compromised account, including unauthorized data access, financial fraud, identity theft, and more.

1. **Severity**

The severity of an OTP bypass vulnerability leading to authentication bypass can be considered high.

Thus, bypassing the OTP, an attacker can gain unauthorized access to an account or system without having to provide the valid and time-limited code that is supposed to verify their identity. This allows the attacker to masquerade as a legitimate user and potentially perform malicious activities.

The impact of an authentication bypass vulnerability depends on the nature of the compromised account or system. It can range from unauthorized access to personal or sensitive information to the ability to perform unauthorized actions, such as initiating financial transactions, modifying account settings, or gaining administrative control.

1. **Proof of Concept**

During the assessment, the consultant logged into the application with the credential provided for the user account **“+97431111**”and intercepted the request into the burp suite.

Figure 1.1: Initial Login Request

After collecting the valid **“sessionToken”** the user account is logged out using the application logout ………

1. **Remediations**

* It is recommended to manage the ***sessionToken*** expiry at the web API to validate the ***sessionToken*** is not being reused once the user attempts to logout.
* It is recommended to use auto-session expiry to the idle ***sessionToken(s)*** to validate that the session is only valid for a certain period of time.

1. **References**

* https://cheatsheetseries.owasp.org/cheatsheets/Session\_Management\_Cheat\_Sheet.html#session-id-life-cycle

# Appendix 1 – Classification Definitions

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. |

## 

# Appendix 2 – Client Information

v

|  |  |
| --- | --- |
| Client Information | |
| Client | **<CN>** |
| Primary Contact | Mr. |
| Approvers | The following people are authorized to change the scope of engagement and modify the terms of the engagement.   * Mr. Praveen Kumar Nair |

# Appendix 3 – 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

|  |  |
| --- | --- |
| 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 |



**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.**

