MICROLINKS
A Technology Power House

Microlinks Source Code Review Report

Date: 14/10/2024

ILYAS SAEED & CO.
CHARTERED ACCOUNTANTS
Suit # 301, Techno City Office Tower,
Hasrat Mohani Road,
Karachi, Pakistan.

A member of
mgiworldwide

Classification: Private

Contents

1. Introduction

1.1. Background

The purpose of the activity was to identify and prioritize the potential areas of security vulnerability. The engagement began on **27/09/2024** including testing, analysis and documentation. This document summarizes the analysis, findings and recommendations for the assessment carried out by Information Security Team.

1.2. Objective

The purpose of this assessment was to identify technical as well as logical vulnerabilities in the application and provide recommendations for risk mitigation that may arise on exploiting these vulnerabilities. The idea behind this testing was to discover whether an attacker can leverage flaws in the application to compromise the confidentiality, integrity and availability of the information.

To determine whether adequate information security controls have been built into the application.

1.2.1. User Access Controls

a) Unique user IDs should be used to enable users to be linked to and held responsible for their actions.

b) The application identifiers should not be displayed until the log-on process has been successfully completed.

c) Help message should not be provided during the log-on procedure to avoid aiding an unauthorized user.

d) The log-on information should only be validated upon completion of all input data. If an error condition arises, application should not indicate which part of the data is correct or incorrect.

e) The log-on procedure should protect against brute force log-on attempts, such as via restrictions on the number of consecutive incorrect log-in attempts for username and password based authentication.

f) Inactive sessions should be locked/terminated after 30 minutes of inactivity, and the session lock should be retained until the user re-establishes access using the established identification and authentication procedure.

g) The application should force the user to change the password at the time of first login.

h) All access must be provided on a need-to-know basis, i.e., a user should only be granted access to the information they need to perform their job responsibilities/tasks/role, to limit the exposure to user related risks.

1.2.2. Password Management

The application should provide capability to enforce password control including complexity, expiration, account lockout and re-use time.

a) Users shall be authenticated to application using a minimum of user ID and password combination.

b) The following password controls shall be enforced at a minimum.

i. Access to systems shall not be allowed until a password has been authenticated with a unique username.
ii. A system based confirmation procedure shall be in place to allow for input errors at the time of password selection.
iii. Passwords shall be at least 8 characters in length.
iv. Passwords shall include a mixture of at least three of the following,

Uppercase characters (A, B, C …);
Lowercase characters (a, b, c …);
Numbers (0, 1, 2 …); and
Special Characters (!, @, # …).

User passwords shall be changed at least every 120 days.

Passwords shall be changed at least 3 times before re-use.

- After 5 failed login attempts the account should be locked out temporarily and the user should be required to contact the Administrator to reset the password or the account may automatically unlock after 30 mins.
- Initial passwords provided to users upon registration will be set to a unique value per user. The user shall be forced to change this initial password at the time of first login.
- Passwords shall not be displayed on the screen in clear text, be printed in clear text or be cached.
- Passwords shall be transmitted encrypted over a network, to avoid being captured by a network 'sniffer' program.
- Passwords shall not be stored in clear text on systems, storage devices, configuration files, logs or similar files accessible by system administrators and/or developers. Memory used for deciphering and checking passwords shall be cleared once processing is complete.

1.2.3. Encryption Requirements

a) Data shall be stored encrypted at all times. This is an all-encompassing requirement that applies to data stored in any medium, through any mechanism, in any format.
b) Data shall be transmitted encrypted at all times. This is an all-encompassing requirement that applies to data transmitted between any two nodes on the wire, through any mechanism, and in any format.

1.2.4. Algorithm Requirements

a) The encryption should be achieved using secure algorithms, such as AES, 3DES, RSA or comparable algorithm.
b) The minimum cryptographic key length should be 128 bits.
c) Self-signed Digital Certificates, if required, shall be created by applying recognized standards (e.g., X.509v3) and shall at least,
   - Identify the issuing certificate authority;
   - Identify its subscriber;
   - Provide the subscriber's public key;
   - Identify its operational period; and
   - Be digitally signed by the issuing certificate authority.
   - Logging

1.2.5. General Controls

a) Application shall maintain log of every activity performed within the application.
b) Successful and failed logins with user ID, date, timestamp, source & destination IP addresses, and other relevant elements shall be logged.
c) The log shall contain sufficient details, for example, date & time, user ID, event ID, concise description of activity etc., to track an activity.
d) The logging facilities and log information shall only be accessible as and when needed by authorized personnel.
e) Logging system time shall be synchronized (e.g., via NTP service etc.) to maintain consistent timestamps.

1.2.6. Application Administration

a) Log entries shall be created for user access provision, modification in user roles / profiles and user revocation by administrator.
b) Application shall generate record in log file whenever user password is reset or account unlocked by administrator.
c) Log data shall not record any sensitive information, including authentication or market sensitive data. Any encryption keys must also not be logged.

1.2.7. Maintaining Log Data Security and Integrity

a) The logging facilities and log information should be protected against, tampering/unauthorized changes to log information, including unauthorized log deletion;
b) The application should also restrict administrator to modify, erase or de-activate logs of their own activities;
c) Application shall store logs within database and maintain provision to make logs available as and when needed in structured human readable format.

1.3. Scope of Engagement

1) Scope includes Black Box security assessment of **Microlinks SEAMS (Equity Brokerage Back-Office System)**

Known details:

2) SEAMS (Equity Brokerage Back-Office System)

1.4. Disclaimer

Recommendations given hereunder do not constitute an audit or a review made in accordance with International Standards on Auditing or International Standards on Review Engagements and consequently, no assurance is expressed.

1.5. Contact Person

Ilyas Saeed & Co. Chartered Accountants

Name: Taha Zuberi

Designation: IT Consultant

Email: taha@ilyassaeed.org

2. Key Findings

Source Code Review Checklist

S.No.	Test Perform	Result
1	User Access Controls	Passed
2	Encryption	Passed
3	Algorithm	Passed
4	File Handling	Passed
5	General Controls	Passed
6	Error Handling	Passed
7	Application Administration	Passed
8	Session Management	Passed
9	Maintaining Log Data Security and Integrity	Passed
10	Sensitive Information Exposure	Passed
11	Using Components with Known Vulnerabilities	Passed
12	Injection	Passed
13	Security Misconfiguration	Passed
14	Insufficient Logging & Monitoring	Passed
15	Broken Access Control	Passed

Vulnerabilities Status

The following table highlights vulnerabilities that were revalidate during the revalidation exercise.

Total Risks	High	Medium	Low	First Assessment	Final Assessment
01	0	01	0	01	0

S. No.	Vulnerabilities	Severity Status at First Assessment	Severity Status at Final Assessment
1.	Hard Code Username	Medium	Fixed

3. Technical Report

3.1 Section A: Source Code Review

Following is the detailed technical report with evidence.

3.1.2. Hard Code Username

Score	Impact: Confidentiality, Integrity & Reputation | Severity: Medium | Exploitability: Medium
Description	During the security code review, it was observed that the username "SIEMS" was hard coded in the application code.
Impact	An Attacker can use this information to log in the application
Recommendation after First Assessment	Remove the hard coded username in the application code.
Status after Final Assessment	Fixed

3.2. Security Reassessment Findings

During reassessment, it is found that Microlinks has fixed all vulnerabilities found in initial assessment.

4. Conclusion

Based on the OWASP methodology, this analysis addresses Source Code Review for a SEAMS (Equity Brokerage Back-Office System) application, focusing on known threats as of the report date. Although no critical vulnerabilities were discovered during the final reassessment, it is advised to address all identified threats, regardless of severity, to enhance system security. Regular security assessments are recommended to mitigate evolving threats effectively.

We appreciate the opportunity provided to us to conduct the assessment and testing services for Microlinks (Private) Limited.

Ilyas Saeed & Co.

Hina Usmani
Partner
Ilyas Saeed & Co.
Chartered Accountants