Amarnath Kamath & Associates
Chartered Accountants

Vulnerability Assessment and Penetration Testing Report

To
The Board of Directors
Synergics Solutions Private Limited
Mumbai

Subject: Vulnerability Assessment and Penetration Testing for SEA-ERP

Report Narration
Independent Practitioner's Report providing an assurance that the ERP Product SEA-ERP has adequate security features which protects the data entered through it.

Detailed Report

1. This Report is issued in accordance with the request from the management of Synergics Solutions Private Limited
2. The Company has designed, developed and implementing at its Clients Place an ERP called SEA-ERP.
3. The Company sought our opinion whether the said Product has any vulnerability or can be penetrated in an unauthorized way.

Management's Responsibility for the Statement
The management is responsible to develop the product with required confidentiality and privacy protection features and have the necessary controls, risk assessment and risk response methods and procedures.

Practitioner's Responsibility
Our responsibility is to express an opinion on the Security Features of the product – SEA-ERP especially focusing on the vulnerability risks and penetration possibilities.

We have done Vulnerability Assessment by performing the below assessments:

Host assessment – The assessment of critical servers, which may be vulnerable to attacks if not adequately tested or not generated from a tested machine image.

Network and wireless assessment – The assessment of policies and practices to prevent unauthorized access to private or public networks and network-accessible resources.

Database assessment – The assessment of databases or big data systems for vulnerabilities and misconfigurations, identifying rogue databases or insecure dev/test environments, and classifying sensitive data across an organization's infrastructure.

Application scans – The identifying of security vulnerabilities in web applications and their source code by automated scans on the front-end or static/dynamic analysis of source code.

Amarnath Kamath & Associates
Chartered Accountants

The Vulnerability Assessment process consists of four steps: testing, analysis, assessment and remediation.

We have used the following types of tools in performing the Vulnerability Assessment
1. Web application scanners that test for and simulate known attack patterns.
2. Protocol scanners that search for vulnerable protocols, ports and network services.
3. Network scanners that help visualize networks and discover warning signals like stray IP addresses, spoofed packets and suspicious packet generation from a single IP address.

We have performed the below Penetration Testing:

1. **Black Box Penetration Testing**: This test is done to identify whether any person with hacking tools but without having any knowledge of User Company or SEA-ERP Particulars can enter the system and see, enter, delete or edit any data.
2. **White Box Penetration Testing**: This test is done to identify whether any person with hacking tools can enter, see, edit or delete any data when they have critical information like User Name, User System Credentials and like
3. **Grey Box Penetration Testing:** This test is done to identify whether any person with hacking tools can enter, see, edit or delete any data when they have partial information about the user or his system or network
4. **Web Application Testing:** This test is done to identify whether the web based application has any developmental flaws or coding flaws through which an hacker can enter, see, add, edit or delete data

We used Open Source Tools to perform Vulnerability Assessment and Automated Proprietary Tools for performing Penetration Testing in an Automated Way.

Our testing methodologies, investigative process and procedures are aligned with SANS, NIST and OWASP standards, testing guides and best practices for application / infrastructure security appraisal. These guidelines are followed to elevate the level of risk awareness to globally recognized standards.

We had no knowledge of the infrastructure used by the developer or end users. We had no person to avail the information through Social Engineering and use the same to test for Vulnerability or Penetration. Therefore, we performed all our tests as a “Test Administrative User” that is the Vulnerability Assessment and Penetration Testing is done only on a Non Production or Non Live Application

Tested Application: https://app.synergicserp.com/dnettmpl/

Opinion

We observe that the SEA-ERP is not having any dangerous vulnerability or penetration possibility if the following conditions are satisfied: -

1. User Company has a proper User Access Management Policy and a proper password policy.
2. The User Company prevents the people from accessing SEA-ERP from unauthorised devices.
3. The Internet and Networking Configuration of the user company is done in a right way.
4. The Users use VPN when using Public Free Network.

5. The users have proper internet cache clearing done on their machine.

Tests Performed:

We performed OWASP Top 10 for Web Applications & found no major observations

1. SQL Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXL)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging and Monitoring

We performed below SANS 25 Software Tests and found no major observations:

1. Improper Restriction of Operations within the Bounds of a Memory Buffer
2. Improper Neutralization of Input During Web Page Generation ('XSS')
3. Improper Input Validation
4. Information Exposure
5. Out-of-bounds Read
6. Improper Neutralization of Special Elements used in an SQL Command (SQLi)
7. Use After Free
8. Integer Overflow or Wraparound
9. Cross-Site Request Forgery (CSRF)
10. Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
11. Improper Neutralization of Special Elements used in an OS Command
12. Out-of-bounds Write
13. Improper Authentication
14. NULL Pointer Dereference
15. Incorrect Permission Assignment for Critical Resource
16. Unrestricted Upload of File with Dangerous Type
17. Improper Restriction of XML External Entity Reference
18. Improper Control of Generation of Code ('Code Injection')
19. Uncontrolled Resource Consumption
20. Missing Release of Resource after Effective Lifetime
21. Untrusted Search Path
22. Deserialization of Untrusted Data
23. Improper Certificate Validation
24. Use of Hard-coded Credentials
25. Improper Privilege Management

We have performed the various Test Cases for Windows Users and found no major issues as long as the User Machines are not having any Pirated or Cracked Application and follows basic Security Policy. The only issue we observed is that the deployment of SEA-ERP in newer machines based on Windows 11 is difficult as Microsoft SilverLight Plugins have been discontinued since October 2021.

Amarnath Kamath & Associates
Chartered Accountants

We found that the SEA-ERP does not work on iPad, iPhone or Android Devices and hence we did not do any testing for that platform.

We observed that SEA-ERP Work on Macintosh Systems but we were informed that the number of Macintosh Based Users for the ERP is insignificant and hence we did not do any testing for that.

For Amarnath Kamath & Associates
Chartered Accountants

V. Narayanan, Partner
F.R. No. 000099S | M. No. 219265
Date: Jan 31, 2023
UDIN: 23219265BGRZHH1362