MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C098 Certification Report

XPCore v1.0

File name: ISCB-3-RPT-C098-CR-v1
Version: v1
Date of document: 15 July 2019
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726630-U)
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999

Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C098 Certification Report

XPCore v1.0

15 July 2019

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
http://www.cybersecurity.my

DISTRIBUTION: UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 21st July 2019, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	12 July 2019	All	Initial draft
v1	15 July 2019	All	Final

Executive Summary

The Target of Evaluation (TOE) is XPCore version 1.0. XPCore is a secure cloud services platform that allows multiple software components, function modules or system to exchange data and communicate with each other through the XPCore API (Application Programming Interface). Authorized 3rd party developers will be able to integrate their own system/program with XPcore platform and utilize XPCore features

The scope of the evaluation is defined by the Security Target (Ref [6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2). This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by Securelytics SEF Lab - and the evaluation was completed on 7 July 2019.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at http://www.commoncriteriaportal.org

It is the responsibility of the user to ensure that XPCore v1.0 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE) is XPCore version 1.0. XPCore is a platform that allows multiple software components, function modules or system to exchange data and communicate with each other through the XPCore API (Application Programming Interface).

2 The TOE can be accessible by user via a web browser and can be deploy either in a cloud environment (hosted by MicroEngine Networks) or in the customer's premises/data center (hosted by the customers). Refer to Section 1.5.1 for more detail explanations. Authorized 3rd party developers will be able to integrate their own system/program with XPcore platform and utilize XPCore features.

3 XPCore features include managing either third party or MicroEngine's:

- Alarm Monitoring System
- CCTV Monitoring System
- Door Access Control Management System
- Time Attendance Management System
- System User Authentication
- And many more

4 The major security features of the TOE include:

a) Security Audit

b) Identification and Authentication

c) Security Management

d) Secure Communication

1.2 TOE Identification

5 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C098
TOE Name	XPCore
TOE Version	v1.0
Security Target Title	XPCore Security Target
Security Target Version	v1.0
Security Target Date	17 June 2019
Assurance Level	EAL2
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL2
Sponsor	MicroEngine Networks Sdn Bhd No.29, Jalan 19/4A, 47600 Subang Jaya, Selangor.
Developer	MicroEngine Networks Sdn Bhd No.29, Jalan 19/4A, 47600 Subang Jaya, Selangor.
Evaluation Facility	Securelytics SEF A-19-06, Tower A ATRIA SOFO SUITES, Jalan SS 22/23, Damansara Utama, 47400 Petaling Jaya, Selangor

1.3 Security Policy

6 No organisational security policies have been defined regarding the use of the TOE.

1.4 TOE Architecture

7 The TOE includes both physical and logical boundaries which are described in Section 1.5 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

8 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

a) Security Audit
The TOE generates audit records for security events. The Administrator has the ability to view the audit logs. Types of audit logs are:

- User Login Success/Fail Event
- Event type, date & time, user role and access origin

Only Administrator has the capability to review these audit records via the web interface.

b) Identification and Authentication
All users (Administrator and Authorised User) are required to perform identification and authentication with the TOE before any information flows are permitted. These users must be authenticated prior to performing any TOE functions by entering a username and password.

c) Security Management
The TOE contains various management functions to ensure efficient and secure management of the TOE. The TOE maintains role-based access control mechanisms to ensure that functions are restricted to those who have the privilege to access them. The Administrator has the ability to manage user and configure the TOE.

d) Secure Communication

The TOE provides a secure SSL channel between the TOE User and the TOE.

1.4.2 Physical Boundaries

9 The TOE is XPCore version 1.0 and it provides security functionality such as Security Audit, Identification and Authentication, Security Management and Secure Communication. The TOE can be categorised as Other Devices and Systems in

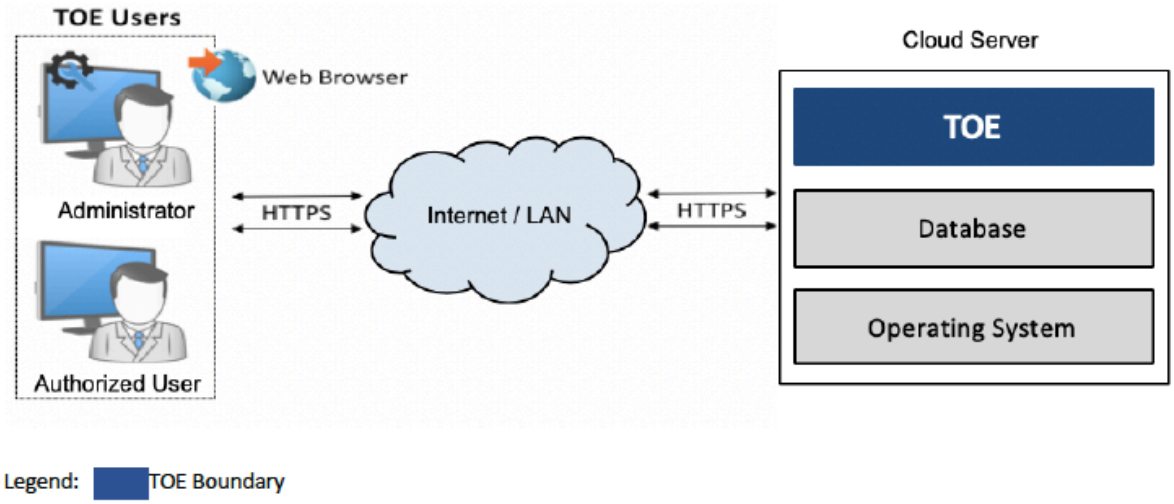
accordance with the categories identified on the Common Criteria Portal (www.commoncriteriaportal.org) that lists all the certified products.

10 The XPCore comprise the following components:

Component	Descriptions
TOE	XPCore is a secure cloud services platform that allows multiple software components, function modules or system to exchange data and communicate with each other through the XPCore API (Application Programming Interface).
TOE Users	There are two types of TOE users; Administrator and User.
Web Browser	A web browser is a software program that allows a user to locate, access, and display web pages. TOE Users interact with the TOE via a supported web browser stated in Section 1.4.3 of Security Target.
Database	A database is an electronic system that allows data to be easily accessed, manipulated and updated. a database is used as a method of storing, managing and retrieving data.
Operating System	Operating System is a software program that enables the computer hardware to communicate and operate with the computer software. The TOE requires an operating system to function. Refer to Section 1.4.3 of Security Target for minimum system requirement for operating system.

11 Refer Figure 1 for TOE physical boundary

Figure 1: TOE physical boundary



1.5 Clarification of Scope

12 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

13 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

14 Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

15 This section summarizes the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand their own IT environment and requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

1.6.1 Environmental assumptions

16 Assumptions for the TOE environment are as described in Section 3.4 of the Security Target (Ref [6]):

Identifier	Assumption Statement

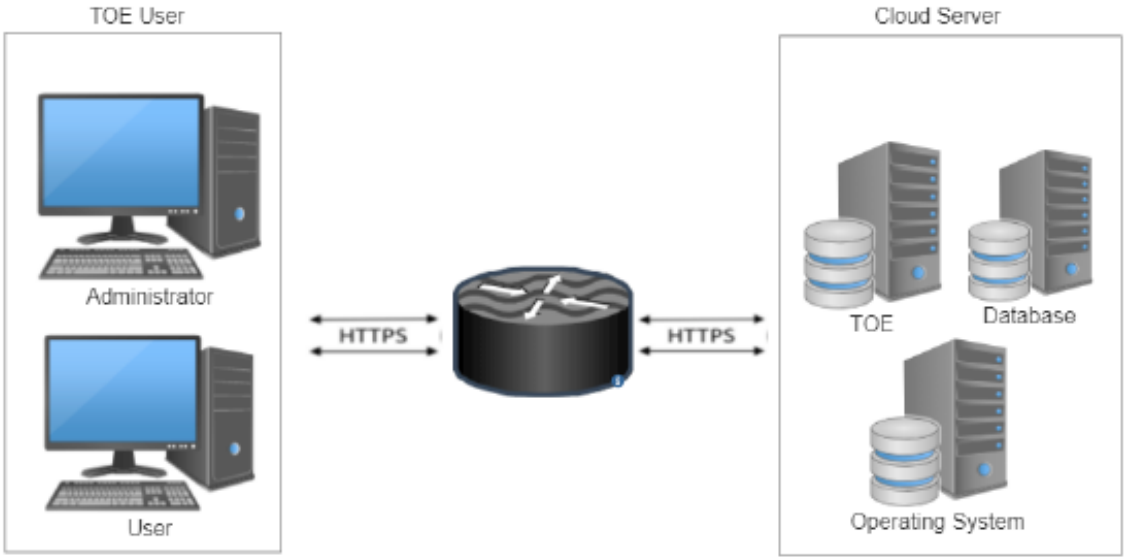
A.PLATFORM	The TOE relies upon a trustworthy platform and local network from which it provides administrative capabilities. The TOE relies on this platform to provide logon services via a local or network directory service, and to provide basic audit log management functions. The platform is expected to be configured specifically to provide TOE services, employing features
A.ADMIN	One or more competent, trusted personnel who are not careless, wilfully negligent, or hostile, are assigned and authorized as the Administrator, and do so using and abiding by guidance documentation.
A.USER	Users are not wilfully negligent or hostile and use the device within compliance of a reasonable enterprise security policy.
A.TIMESTAMP	The platforms on which the TOE operate shall be able to provide reliable time stamps.
A.PHYSICAL	It is assumed that the appliance hosting the operating system and database are in a secure operating facility with restricted physical access and non-shared hardware.

1.7 Evaluated Configuration

17 The TOE was evaluated with below Supporting hardware, software and/or firmware.

18 The evaluated configuration of the TOE, shown in Figure 2 is a combination of hardware and software application suite that provides the evaluated configuration.

Figure 2 : Evaluated Deployment Configuration of the TOE



1.8 Delivery Procedures

19 The evaluators examined the delivery procedure, in which provide guidance for the developer to initiate delivery process of the TOE and its components to the intended recipient(s). It also provides direction on the methods used to deliver the TOE to consumers and users of the product.

20 The delivery starts from manufacturing until the TOE is delivered to customer for installation and use as below in Lifecycle Documentation:

- Receiving Customer Order
- Evaluate Customer's Order
- Planning Stock Delivery
- Product Requisition
- Product Delivery Arrangement
- Product Delivery
- Invoicing
- End

2 Evaluation

21 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the ISCB Product Certification Schemes Policy (Product_SP) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

22 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

23 The evaluators checked that the TOE provided for evaluation is labelled with its reference.

24 The evaluators checked that the TOE references used are consistent.

25 The evaluators examined the method of identifying configuration items to determine that it describes how configuration items are uniquely identified.

26 The evaluators examined the configuration items to determine that they are identified in a way that is consistent with the CM documentation.

27 The evaluators checked that the configuration list includes the

28 a) the TOE itself;

29 b) the parts that comprise the TOE;

30 c) the evaluation evidence required by the SARs in the ST

31 The evaluators examined the configuration list to determine that it uniquely identifies each configuration item.

32 The evaluators checked that the configuration list indicates the developer of each TSF relevant configuration item.

33 The evaluators examined the delivery documentation to determine that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

34 The evaluators examined aspects of the delivery process to determine that the delivery procedures are used.

2.1.2 TOE Delivery

35 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

2.1.3 Development

36 The evaluators examined the security architecture description and determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

37 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

38 The evaluators examined the functional specification and determined that the TSF is fully represented, it states the purpose of each TSF interface and method of use for each TSFI is given.

39 The evaluators examined the presentation of the TSFI to determine that it completely identifies all parameters associated with every TSFI and completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI.

40 The evaluators examined the presentation of the TSFI to determine that it completely and accurately describes the SFR-enforcing actions associated with the SFR-enforcing TSFIs.

41 The evaluators examined that the developer supplied tracing links of the SFRs to the corresponding TSFIs.

42 The evaluators examined the TOE design to determine that the structure of the entire TOE is described in terms of subsystems and all subsystems of the TSF are identified.

43 The evaluators examined the TOE and determined that each SFR-non interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is SFR-non interfering.

44 The evaluators examined the TOE design to determine that it provides a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

45 The evaluators examined the TOE design to determine that it contains a complete and accurate high-level description of the SFR-supporting and SFR-non interfering behaviour of the SFR-enforcing subsystems. The evaluators determined that the TOE design provided a complete and accurate high-level description of the behaviour of the SFR-supporting subsystems.

46 The evaluators examined the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

47 The evaluators examined that all SFRs were covered by the TOE design and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.4 Guidance documents

48 The evaluators examined the operational user guidance and determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

49 The evaluators examined the operational user guidance to determine that it describes, for each user role, the secure use of the available interfaces provided by the TOE.

50 The evaluators examined the operational user guidance to determine that it describes, for each user role, the available security functionality and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

51 The evaluators examined the operational user guidance to determine that it describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

52 The evaluators examined the operational user guidance and other evaluation evidence to determine that the guidance identifies all possible modes of operation of the TOE

(including, if applicable, operation following failure or operational error), their consequences and implications for maintaining secure operation.

53 The evaluators examined the operational user guidance to determine that it describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

54 The evaluators examined the operational user guidance to determine that it is clear and it is reasonable.

2.1.5 IT Product Testing

55 Testing at EAL 2 consists of assessing developer tests, sufficiency test and conducting penetration tests. The TOE testing was conducted by evaluators from Securelytics SEF lab. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.5.1 Assessment of Developer Tests

56 The evaluators verified that the developer has met their testing responsibilities by repeating the developer test, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator). The results of the evaluators' tests are consistent with the developers' test results defined in their evaluation evidences submitted.

2.1.5.2 Independent Test

57 At EAL 2, independent test demonstrates the correspondence between the security functional requirements (SFRs) defined in Security Target, and the test cases that test the functions and behaviour of the TOE that meets those requirements. The evaluators have decided to perform testing based on the TOE Security Functions.

58 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests developed and performed by the evaluators to verify the functionality as follows:

Table 2: Independent Test

Test ID	Description	SFRs	Results
F001 – Identification and Authentication Security Management ADMIN Interface USER Interface	1. To test that each user to be successfully authenticated and identified before allowing any other TSF-mediated actions on behalf of that user. 2. To test that the TOE maintains the roles Admin and Normal User. 3. To test that the TOE enforces the access control SFP to restrict the ability to change default, modify and delete the security attributes Admin Account, TOE Configuration, Users Account to Admin. 4. To test that the TOE maintains the following list of security attributes belonging to individual users; Username, Password, User role, User Account 5. To test that the TOE enforce access control SFP to provide permissive default values for security attributes that are used to enforce the SFP. 6. To test that the TOE performs the following management functions: Refer to objects listed in Section 5.2.13 of the ST. 7. To test that the TOE restricts the ability to modify the User Accounts to Admin 8. To test that the TOE enforces the access control SFP on objects listed in Section 5.2.4 of the ST. 9. To test that If the Admin and Normal User are successfully authenticated accordingly, then access is granted based on privilege allocated and If the Admin and Normal User are not authenticated successfully, therefore, access permission is denied 10. To test that the TOE restricts the ability to disable, enable and modify the behaviour of the functions of TOE Configurations to Administrators	FIA_ATD.1 FIA_UID.2 FIA_UAU.2 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_MOF.1 FMT_SMF.1 FMT_SMR.1 FDP_ACC.1 FDP_ACF.1	Pass

Test ID	Description	SFRs	Results
F002 – Trusted Path SSL_API	1. To test that the TOE provides a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure 2. To test that the TOE permits remote users to initiate communication via the trusted path 3. To test that the TOE requires the use of the trusted path for initial user authentication and all further communication after authentication	FTP_TRP.1	Pass
F003 – Security Audit ADMIN Interface	1. To test that the TOE able to generate audit record of the following auditable events: a. User Login Success/Fail Event b. Event type, date & time, user role and access origin 2. To test that the TOE record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST (none). 3. To test that the TOE provides the admin with the capability to read all audit information from the audit records and provide the audit records in a manner suitable for the user to interpret the information.	FAU_GEN.1 FAU_SAR.1	Pass

59 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.5.3 Vulnerability Analysis

60 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public

domain sources and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

61 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapse time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation

2.1.5.3.1 Vulnerability testing

62 The penetration tests focused on:

a) SQL Injection

b) Cross Site Scripting

c) Cross-site Request

d) Forgery (CSRF)

e) Security misconfiguration

f) Failure to restrict URL Access

g) Information Disclosure

h) Directory Traversal

63 The results of the penetration testing demonstrate that the TOE is resistant to an attacker possessing a basic attack potential. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref [6]).

2.1.5.3.2 Testing Results

64 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all the tests conducted were PASSED as expected.

3 Result of the Evaluation

65 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of XPCore v1.0 which is performed by Securelytics SEF.

66 Securelytics SEF found that XPCore v1.0 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2.

67 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

68 EAL 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and complete interface specifications, guidance documentation and a description of the design of the TOE and the implementation to understand the security behaviour.

69 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to an attacker possessing a Basic attack potential.

70 EAL 2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

71 Securelytics SEF has made recommendation such as:

a) The users should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

b) The users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialization, start-up and operation if stored or handled outside the TOE.

c) System Auditor should review the audit trail generated and exported by the TOE periodically.

d) The users must ensure appropriate network protection is maintained, the network on which the TOE is installed must be both physically and logically protected.

72 The Malaysian Certification Body (MyCB) strongly recommended that:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

b) Potential purchasers of the TOE should ensure that the administrators responsible for the TOE are provided sufficient training and are familiar with the guidance supplements prior to configuring and administering the TOE.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] ISCB Product Certification Schemes Policy (Product_SP), v1b, CyberSecurity Malaysia, March 2018.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v1a, March 2018.

[6] XPCore Security Target, Version 1.0, 17 June 2019.

[7] Evaluation Technical Report XPCore, Version 1.0, 7 July 2019.

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target

Acronym	Expanded Term
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.

Term	Definition and Source
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---