

**Assessment Performed by TAC Security****Application Name:** [Pabau](#)**Certification ID:** 265835be**Assessment Type:** AL1 ([Lab Tested - Lab Verified](#))**Issue Date:** 8/6/2026 10:25:36 AM**Assessment Status:** Complete**Expiration Date:** 8/7/2027**Statement of Validation**

The purpose of this report is to provide users verification that [Hambrand Technology](#) has successfully completed a Cloud Application Security Assessment (CASA), validating [Pabau](#) **has satisfied ADA-CASA application security requirements**. In meeting these assessment requirements, Pabau is **verified** to meet the ADA-CASA **AL1** requirements.

The assessment was conducted by [TAC Security](#) an independent third party lab, authorized by the App Defence Alliance to conduct CASA security assessments.

About CASA

CASA is based on the industry-recognized Open Web Application Security Project ([OWASP](#)) Application Security Verification Standard ([ASVS](#)) to provide third-party (3P) application developers with:

- A basis for testing technical application security controls
- A consistent set of requirements for secure application development
- A homogenized coverage and assurance levels for providing security verification using industry-aligned frameworks and open security standards.

More information on CASA can be found on the [App Defence Alliance Site](#). A complete list of App Defense Alliance CASA requirements is detailed on the App Defense Alliance [GitHub page](#).

Assessment Scope

The assessment was conducted using [CASA requirements](#). Please note that not all requirements apply to every application. Additionally, some applications may be validated for specific requirements based on pre-existing certifications that have been mapped to the CASA requirements by the assessing lab.

Authentication		Verdict
1.1	Implement strong password security measures	PASS
1.2	Disable any default accounts for public application access interfaces	PASS
1.3	Out of band verifiers shall be random and not reused	PASS

Session Management		Verdict
2.1	URLs shall not expose authentication material	PASS
2.2	Implement session invalidation on logout, user request, and password change	PASS
2.3	Implement and secure application session tokens	PASS
2.4	Protect sensitive account modifications	PASS
Access Control		Verdict
3.1	Implement access control mechanisms to protect data and APIs	PASS
3.2	Implement secure OAuth integrations to protect user data and prevent unauthorized access	PASS
3.3	Application exposed administrative interfaces shall use appropriate multi-factor authentication	PASS
Communications		Verdict
4.1	Protect data through strong cryptography	PASS
Data Validation and Sanitization		Verdict
5.1	Implement validation & input sanitation	PASS
5.2	Securely Handle Untrusted Files	PASS
Configuration		Verdict
6.1	Keep all components up to date	PASS
6.2	Disable debug modes in production environments	PASS
6.3	The origin header shall not be used for authentication of access control decisions	PASS
6.4	Protect Application from Subdomain Takeover	PASS
6.5	Do not log credentials or payment details	PASS
6.6	Securely clear client storage during logout	PASS
6.7	Securely store server-side secrets	PASS

Assurance Levels

Level	Description
AL1	The developer provides evidence and statements of compliance to each audit test case. The ADA approved lab reviews the evidence against the requirements or performs the necessary testing when applicable.
AL2	The ADA approved lab evaluates each audit test case directly against the application. In some cases, the developer may need to provide limited information or code snippets.