Test Report #: PS-44383822

CASA Compliance Report

Serverless, Inc.

Prescient Security LLC

Identification

Product Name	Avi
Application Name	Web Application
Application Version	1.0
Application URL	https://avi.run/
Company	Serverless, Inc.
CASA Specification Version	v2.1.1
Assurance Level	AL2 - Lab Assessment
Evaluated Configuration	Default configuration
Summary	**IN COMPLIANCE — All applicable requirements of CASA v2.1.1 were satisfied for Avi (Web Application) version 1.0 (Default configuration) at AL2.**
Laboratory attestation (ASTL)	Pablo Gallegos, Manager, Enterprise Testing Attested in the ADA certification platform by KC Garza, Manager, Enterprise Testing, on 15 October 2026. The laboratory attests to its evaluation and to the contents of this report. It does not make the certification decision.
Date of Evaluation	21 September 2026
Engagement team members	Pablo Gallegos Syed Ali Abbas Ujjwal Saran
Engagement Partner	Prescient Security
Engagement Quality Control Reviewer	Jullius Jimenez

Implement strong password security measures		Verdict			
		P	F	NA	INC
1.1.1	Authentication is resistant to brute force attacks	**P**			
1.1.2	System generated initial passwords or activation codes shall be securely randomly generated and expire after a short period.	**P**			
1.1.3	Passwords shall be stored in a form that is resistant to offline attacks.	**P**			

Disable any default accounts for public application access interfaces		Verdict			
		P	F	NA	INC
1.2.1	Default credentials shall not be present on publicly exposed interfaces.	**P**			

Out of band verifiers shall be random and not reused		Verdict			
		P	F	NA	INC
1.3.1	Out of band verifier shall expire in a reasonable timeframe.	**P**			
1.3.2	Out of band verifier shall only be used once.	**P**			
1.3.3	Out of band verifier shall be securely random	**P**			
1.3.4	Out of band verifier shall be resistant to brute force attacks	**P**			

URLs shall not expose authentication material		Verdict			
		P	F	NA	INC
2.1.1	The application shall not reveal passwords or session tokens in URL parameters. In cases where the application provides an API, the application shall prevent (or give developers an option to prevent) exposing sensitive information like API keys or session tokens within the URL query strings.	**P**			

Implement Session Invalidation on Logout, User Request, and Password Change		Verdict			
		P	F	NA	INC
2.2.1	Users shall have the ability to logout of the application. Logout or session expiration shall invalidate all stateful session tokens, including refresh tokens.	**P**			
2.2.2	The application shall provide the option (or acts by default) to terminate all other active sessions, including stateful refresh tokens, after a successful password change (including change via password reset/recovery), and that this is effective across the application, federated login (if present), and any relying parties.	**P**			
2.2.3	Non-revocable stateless authentication tokens must expire within 24 hours of being issued	**P**			

Implement and secure application session tokens		Verdict			
		P	F	NA	INC
2.3.1	Cookie-based session tokens shall have the 'Secure' attribute set.			**NA**	
2.3.2	Cookie-based session tokens shall have the 'HttpOnly' attribute set.			**NA**	

2.3.3	The application shall use session tokens rather than static API secrets and keys, except with legacy implementations.	**P**			
2.3.4	Stateless session tokens shall use digital signatures, encryption, and other countermeasures to protect against tampering, enveloping, replay, null cipher, and key substitution attacks.	**P**			

Protect sensitive account modifications		Verdict			
		P	F	NA	INC
2.4.1	Verify the application ensures a full, valid login session or requires re-authentication or secondary verification before allowing any sensitive transactions or account modifications.	**P**			

Implement access control mechanisms to protect confidential data and APIs		Verdict			
		P	F	NA	INC
3.1.1	The application shall enforce least privilege access control rules on a trusted service layer.	**P**			
3.1.2	All user and data attributes and policy information used by access controls shall not be able to be manipulated by end users unless specifically authorized.	**P**			
3.1.3	Access controls shall fail securely including when an exception occurs.	**P**			
3.1.4	Sensitive resources shall be protected against Insecure Direct Object Reference (IDOR) attacks targeting creation, reading, updating and deletion of records, such as creating or updating someone else's record, viewing everyone's records, or deleting all records.	**P**			
3.1.5	The application or framework shall enforce a strong anti-CSRF mechanism to protect authenticated functionality, and effective anti-automation or anti-CSRF protects unauthenticated functionality.	**P**			
3.1.6	Directory browsing shall be disabled unless deliberately desired.	**P**			

Implement secure OAuth integrations to protect user data and prevent unauthorized access		Verdict			
		P	F	NA	INC
3.2.1	Application shall implement only secure and recommended OAuth 2.0 flows, such as the Authorization Code Flow or the Authorization Code Flow with PKCE, while avoiding the use of deprecated flows like the Implicit Flow or the Resource Owner Password Credentials Flow.	**P**			
3.2.2	Application shall securely validate the redirect_uri and state parameters during the OAuth 2.0 authorization process to prevent open redirect and CSRF vulnerabilities.	**P**			

Application exposed administrative interfaces shall use appropriate multi-factor authentication.		Verdict			
		P	F	NA	INC
3.3.1	Application administrative interfaces shall use appropriate multi-factor authentication to prevent unauthorized use.	**P**			

Protect confidential data through strong cryptography		Verdict			
		P	F	NA	INC
4.1.1	Application shall enforce the use of TLS for all connections and default to TLS 1.2+. In cases where support for legacy clients is necessary, TLS 1.0 and 1.1 may be supported if mitigations are implemented to minimize the risk of downgrade attacks and known TLS exploits. Regardless of the TLS version in use, the application shall default to secure cipher suites and reject those with known vulnerabilities.	**P**			
4.1.2	Connections to and from the server shall use trusted TLS certificates. Where internally generated or self-signed certificates are used, the server must be configured to only trust specific internal CAs and specific self-signed certificates. All others should be rejected.	**P**			
4.1.3	No instances of weak cryptography which meaningfully impact the confidentiality or integrity of data.	**P**			
4.1.4	All cryptographic modules shall fail securely, and errors are handled in a way that does not enable Padding Oracle attacks.	**P**			

Implement validation & input sanitation		Verdict			
		P	F	NA	INC
5.1.1	Protect against HTTP parameter pollution.	**P**			
5.1.2	URL redirects and forwards are limited to allowlisted URLs or a warning is displayed when redirecting to untrusted content.	**P**			
5.1.3	Avoid the use of eval() or other dynamic code execution features. When there is no alternative, any user input is sanitized and sandboxed before being executed.	**P**			
5.1.4	Protect against template injection attacks by ensuring that any user input being included is sanitized or sandboxed.	**P**			
5.1.5	Prevent Server-Side Request Forgery (SSRF)	**P**			
5.1.6	Protect against XPath or XML injection attacks	**P**			
5.1.7	Context-aware output escaping or sanitization protects against reflected, stored, and DOM based XSS.	**P**			
5.1.8	Protect against database injection attacks	**P**			
5.1.9	Protect against OS command injections	**P**			

5.1.10	Protect against local file inclusion or remote file inclusion attacks	**P**			

Securely handle untrusted files		Verdict			
		P	F	NA	INC
5.2.1	Protect against malicious file uploads by limiting uploads to expected file types and preventing direct execution of uploaded content.	**P**			

Keep all components up to date		Verdict			
		P	F	NA	INC
6.1.1	The application only uses software components without known exploitable vulnerabilities.	**P**			

Disable debug modes in production environments		Verdict			
		P	F	NA	INC
6.2.1	Disable debug modes in production environments	**P**			

The origin header shall not be used for authentication of access control decisions		Verdict			
		P	F	NA	INC
6.3.1	The origin header shall not be used for authentication of access control decisions	**P**			

Protect application from subdomain takeover		Verdict			
		P	F	NA	INC
6.4.1	The application shall not be susceptible to subdomain takeovers.	**P**			

Do not log credentials or payment details		Verdict			
		P	F	NA	INC
6.5.1	The application shall not log credentials or payment details. Session tokens shall only be stored in logs in an irreversible, hashed form.	**P**			

Securely clear client storage during logout		Verdict			
		P	F	NA	INC
6.6.1	Browser storage is securely cleared during logout	**P**			

Securely store server-side secrets	Verdict

		P	F	NA	INC
6.7.1	The application shall securely store access tokens, API keys, and other server-side secrets.	**P**			

Application and Developer Info

Application Name	Web Application
Application Version	1.0
Link to Application	https://avi.run/
Company Name	Serverless, Inc.
Company Address	522 San Anselmo Ave, San Anselmo, CA 94969
Contact name and Email	Austen Collins austen@serverless.com
Onboarding Questionnaire Filename and Hash	`8bd8a8b09b00a148afcefd3fca26d39f89b22891eed42ef8e42a59e16eb5315d` CASA AL2 Onboarding Questionnaire.xlsx

Evaluated Environment

Environment tested	https://app.avi.run
Testing window	09/01/2026 - 09/20/2026

Testing Verdicts

PASS	P
FAIL	F — blocks certification
NOT APPLICABLE	NA — requires a permitted, documented basis verified and accepted by the CB
INCONCLUSIVE	INC — blocks certification

Remarks and Comments

none.

Certification Decision

Certificate Number	10293
Decision Date	October 19, 2026
Valid From	October 19, 2026
Valid Until	October 19, 2027
Status at Issuance	Valid
Certification Body	TrustCB B.V.
Certification Body Address	Van den Berghlaan 48, 2132 AT Hoofddorp, The Netherlands
Certification Body Contact	certs@trustcb.com
Certification Body Website	https://www.trustcb.com

This Compliance Report was approved for publication by the Certification Body named above as the public summary of its certification decision. The Certification Body approves this report; it does not certify the report itself.

Generated by the ADA certification platform on 19 October 2026, 20:24 UTC for certification request #145.