Essay Grader AI: security audit report

Created on 01 October 2025 @ 16:29

Essay Grader AI wants to build trust by giving you insight in how it builds software in a secure manner. The report details how software development at Essay Grader AI is being monitored and safeguarded from the developer's computer all the way to the infrastructure used for delivery.

This security report has been generated by Aikido Security based on real-time monitoring of Essay Grader AI code and infrastructure.

NIST 800-53 compliance

A brief overview of the NIST directive and any measures taken for these.

Title	Taken measures
1.2.4 Account Management | Disable Accounts	✓ Has IAM users without any assigned permissions
1.2.5 Account Management | Automated Audit Actions	✓ Has notifications for changes in IAM configurations (roles, users, policies)
1.2.8 Account Management | Privileged User Accounts	✓ Has identified over-privileged users, roles, or service accounts
1.2.13 Account Management | Account Monitoring for Atypical Usage	✓ Detect risky behaviors like IAM configuration tampering ✓ Has IAM users without any assigned permissions
1.3.8 Access Enforcement | Role-based access control	✓ Ensure custom roles are assigned appropriate permissions for resource management ✓ Detect and mitigate privilege escalation permissions in roles or users
1.4.22 Information Flow Enforcement | Physical or Logical Separation of Information Flows	✓ Encrypts data at rest ✓ Enforces safe SSL protocol usage ✓ Enforces HTTPS traffic to cloud instances ✓ Enforces latest TLS version ✓ Prevents abuse of cookies ✓ Uses up to date cryptography libraries ✓ Ensure no unrestricted access to critical infrastructure or services
1.6.2 Least Privilege | Authorize Access to Security Functions	✓ Encrypts data at rest ✓ Ensure only privileged roles are used for accessing sensitive security configurations ✓ Enforces safe SSL protocol usage ✓ Enforces latest TLS version
1.17.2 Remote Access | Monitoring and Control	✓ Ensure secure remote access protocols (e.g., RDP, SSH) are in use. ✓ Monitor and log all remote access activities for security analysis. ✓ Disable or limit access from insecure or unknown networks.

1.17.6 Remote Access | Monitoring for Unauthorized Connections	✓ Generate alerts for brute force attacks on remote access points.
1.23.1 Data Mining Protection	✓ Analyze and monitor data access patterns for unusual activity. ✓ Restrict excessive or unauthorized data mining queries. ✓ Identify and block attempts to exfiltrate sensitive information.
3.6.2 Audit Record Review, Analysis, and Reporting | Automated Process Integration	✓ Has deletion protection for cloud resources ✓ Track and analyze user activity to detect potential insider threats. ✓ Limit access to sensitive data based on user roles and responsibilities. ✓ Use Data Loss Prevention (DLP) solutions to prevent unauthorized data exfiltration.
3.9.4 Protection of Audit Information | Cryptographic Protection	✓ Encrypts data at rest ✓ Enforces latest TLS version ✓ Enforces safe SSL protocol usage ✓ Prevents abuse of cookies ✓ Enforces HTTPS traffic to cloud instances
3.9.5 Protection of Audit Information | Access by Subset of Privileged Users	✓ Has identified over-privileged users, roles, or service accounts
3.11.2 Audit Record Retention | Long-term Retrieval Capability	✓ Logging Enabled
3.12.2 Audit Record Generation | System-wide and Time-correlated Audit Trail	✓ Has file storage access security enabled
4.7.7 Continuous Monitoring | Automation Support for Monitoring	✓ Logging Enabled
5.5.2 Access Restrictions for Change | Automated Access Enforcement and Audit Records	✓ Encrypts data at rest ✓ Ensure only privileged roles are used for accessing sensitive security configurations ✓ Enforces safe SSL protocol usage ✓ Enforces latest TLS version ✓ Has file storage access security enabled

5.7.9 Least Functionality | Binary or Machine Executable Code	✓ Proper Access Management to Resources ✓ Runtimes are up to date ✓ Has proper access controls for cloud resources
6.9.6 System Backup | Transfer to Alternate Storage Site	✓ Has backups for cloud resources
7.2.2 Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	✓ Has identified over-privileged users, roles, or service accounts
7.2.3 Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	✓ Has identified over-privileged users, roles, or service accounts
7.5.2 Authenticator Management | Password-based Authentication	✓ Proper Access Management for Resources ✓ Proper Access Management to Resources ✓ Enforces multi-factor authentication (MFA)
7.5.7 Authenticator Management | Protection of Authenticators	✓ Proper Access Management for Resources ✓ Proper Access Management to Resources ✓ Enforces multi-factor authentication (MFA)
7.10.1 Adaptive Authentication	✓ Proper Access Management for Resources ✓ Proper Access Management to Resources ✓ Enforces multi-factor authentication (MFA) ✓ Detect risky behaviors like IAM configuration tampering
8.5.2 Incident Monitoring | Automated Tracking, Data Collection, and Analysis	✓ Logging Enabled ✓ Identify and block attempts to exfiltrate sensitive information.
13.12.1 Insider Threat Program	✓ Encrypts data at rest ✓ Ensure only privileged roles are used for accessing sensitive security configurations ✓ Enforces safe SSL protocol usage ✓ Enforces latest TLS version ✓ Has file storage access security enabled

16.10.1 Threat Hunting	✓ Has file storage access security enabled
17.3.2 System Development Life Cycle | Manage Preproduction Environment	✓ Encrypts data at rest ✓ Enforces safe SSL protocol usage ✓ Enforces HTTPS traffic to cloud instances ✓ Prevents abuse of cookies ✓ Uses up to date cryptography libraries ✓ Enforce network policies to separate information flows physically or logically.
18.5.2 Denial-of-service Protection | Restrict Ability to Attack Other Systems	✓ Restricts ability to attack other systems
18.5.3 Denial-of-service Protection | Capacity, Bandwidth, and Redundancy	✓ Enforces safe SSL protocol usage ✓ Has budgeting alerts set up ✓ Has deletion protection for cloud resources
18.7.6 Boundary Protection | Deny by Default Allow by Exception	✓ Encrypts data at rest ✓ Enforces latest TLS version ✓ Enforces safe SSL protocol usage ✓ Prevents abuse of cookies ✓ Enforces HTTPS traffic to cloud instances ✓ Has file storage access security enabled
18.7.8 Boundary Protection | Split Tunneling for Remote Devices	✓ Disable or limit access from insecure or unknown networks.
18.7.11 Boundary Protection | Prevent Exfiltration	✓ Analyze and monitor data access patterns for unusual activity. ✓ Restrict excessive or unauthorized data mining queries. ✓ Disable or limit access from insecure or unknown networks. ✓ Identify and block attempts to exfiltrate sensitive information. ✓ Enforces safe SSL protocol usage
18.7.16 Boundary Protection | Networked Privileged Accesses	✓ Proper Access Management for Resources ✓ Proper Access Management to Resources ✓ Has file storage access security enabled

18.12.2 Cryptographic Key Establishment and Management | Availability	✓ Encrypts data at rest ✓ Enforces latest TLS version ✓ Enforces safe SSL protocol usage ✓ Enforces HTTPS traffic to cloud instances
18.16.3 Transmission of Security and Privacy Attributes | Anti-spoofing Mechanisms	✓ Has ANI Spoofing Protection Enabled
18.16.4 Transmission of Security and Privacy Attributes | Cryptographic Binding	✓ Encrypts data at rest ✓ Enforces latest TLS version ✓ Enforces safe SSL protocol usage ✓ Enforces HTTPS traffic to cloud instances
18.20.3 Secure Name/address Resolution Service (authoritative Source) | Data Origin and Integrity	✓ Has file storage access security enabled ✓ Uses DNSSEC extensions
18.21.2 Secure Name/address Resolution Service (recursive or Caching Resolver) | Data Origin and Integrity	✓ Has file storage access security enabled ✓ Uses DNSSEC extensions
18.22.1 Architecture and Provisioning for Name/address Resolution Service	✓ Logging Enabled
18.23.4 Session Authenticity | Unique System-generated Session Identifiers	✓ Has brute force protection enabled
18.24.1 Fail in Known State	✓ Use Data Loss Prevention (DLP) solutions to prevent unauthorized data exfiltration.
18.28.2 Protection of Information at Rest | Cryptographic Protection	✓ Encrypts data at rest ✓ Enforces latest TLS version ✓ Enforces safe SSL protocol usage ✓ Prevents abuse of cookies ✓ Enforces HTTPS traffic to cloud instances
18.34.2 Non-modifiable Executable Programs | No Writable Storage	✓ Has file storage access security enabled