ChecklistGuro

ERP API Security Checklist

Authentication & Authorization

Verify the robustness of authentication mechanisms and access controls for ERP API endpoints.

Authentication Method

- [ ] API Keys
- [ ] OAuth 2.0
- [ ] Basic Authentication
- [ ] JWT (JSON Web Tokens)

Maximum API Request Attempts per IP Address

Enter a number...

Authorization Protocol

- [ ] Role-Based Access Control (RBAC)
- [ ] Attribute-Based Access Control (ABAC)
- [ ] Access Control Lists (ACLs)

Last Password/API Key Rotation Date

Enter date...

Authentication Factors Required

- [ ] Password
- [ ] MFA (Multi-Factor Authentication)
- [ ] Biometrics

Input Validation & Sanitization

Ensure proper validation and sanitization of all input data to prevent injection attacks.

Order Quantity

Enter a number...

Customer Name

Write something...

Product Description

Write something...

Invoice Amount

Enter a number...

Delivery Date

Enter date...

Currency Type

- [ ] USD
- [ ] EUR
- [ ] GBP

Rate Limiting & Throttling

Implement rate limiting and throttling to prevent abuse and denial-of-service attacks.

Maximum API Requests per Minute (Global)

Enter a number...

Maximum API Requests per Minute (Per User)

Enter a number...

Burst Limit (Requests per Second)

Enter a number...

Rate Limiting Enforcement Point

- [ ] API Gateway
- [ ] Application Server
- [ ] Database
- [ ] Custom Logic

Response Code on Rate Limit Exceeded

- [ ] 429 - Too Many Requests
- [ ] 503 - Service Unavailable
- [ ] Custom

Custom Rate Limit Exceeded Response Message (if applicable)

Write something...

Date of Last Rate Limit Policy Review

Enter date...

Encryption & Data Protection

Confirm encryption of data in transit and at rest, adhering to relevant standards.

Encryption Protocol in Use (e.g., TLS 1.3)

- [ ] TLS 1.0
- [ ] TLS 1.1
- [ ] TLS 1.2
- [ ] TLS 1.3

Encryption Key Length (bits)

Enter a number...

Encryption at Rest Method

- [ ] Full Disk Encryption
- [ ] Database Encryption
- [ ] File-Level Encryption

Description of Key Management System

Write something...

Data Masking Implementation

- [ ] None
- [ ] Static
- [ ] Dynamic

Last Key Rotation Date

Enter date...

API Key Management

Review processes for secure generation, storage, rotation, and revocation of API keys.

Number of Active API Keys

Enter a number...

Last API Key Rotation Date

Enter date...

API Key Generation Method

- [ ] Automated
- [ ] Manual

Average API Key Lifespan (Days)

Enter a number...

API Key Security Policy Description

Write something...

Key Storage Location

- [ ] Vault
- [ ] Database
- [ ] Cloud Storage

Next Scheduled Key Rotation Date

Enter date...

Logging & Monitoring

Establish comprehensive logging and monitoring to detect and respond to suspicious activity.

Average API Request Rate (Requests/Minute)

Enter a number...

Failed Authentication Attempts Threshold (per hour)

Enter a number...

Description of Current Logging System (e.g., SIEM Integration)

Write something...

Last Review of Log Retention Policy

Enter date...

Types of Events Currently Logged (Select all that apply)

- [ ] Authentication Success
- [ ] Authentication Failure
- [ ] Data Access
- [ ] Error Events
- [ ] API Usage
- [ ] System Events

Log Storage Location

- [ ] On-Premise Server
- [ ] Cloud Storage (AWS, Azure, GCP)
- [ ] Hybrid Environment

Description of Alerting System & Thresholds

Write something...

Vulnerability Scanning & Penetration Testing

Schedule regular vulnerability scans and penetration tests to identify and remediate security flaws.

Last Vulnerability Scan Date

Enter date...

Vulnerability Scan Frequency (Days)

Enter a number...

Scanning Tool Used

- [ ] Nessus
- [ ] Qualys
- [ ] OpenVAS
- [ ] Manual
- [ ] Other

Summary of Last Scan Findings

Write something...

Date of Last Penetration Test

Enter date...

Penetration Test Scope and Methodology

Write something...

Data Exposure Prevention

Implement controls to prevent unintentional exposure of sensitive data through APIs.

Data Masking Implementation?

- [ ] Fully Implemented
- [ ] Partially Implemented
- [ ] Not Implemented

Number of fields masked/redacted?

Enter a number...

Sensitive Data Types Exposed?

- [ ] PII (Personally Identifiable Information)
- [ ] Financial Data
- [ ] Health Records
- [ ] Proprietary Business Data
- [ ] None

Description of data redaction/masking techniques used.

Write something...

Review of data access policies performed?

- [ ] Yes
- [ ] No
- [ ] In Progress

Compliance & Standards

Ensure API security practices align with relevant industry regulations and security standards (e.g., GDPR, SOC 2).

Applicable Regulatory Frameworks (Select all that apply)

- [ ] GDPR
- [ ] CCPA
- [ ] HIPAA
- [ ] SOX
- [ ] ISO 27001
- [ ] Other (Specify in Long Text)

If 'Other' selected above, please specify which framework(s) apply and why.

Write something...

Date of last compliance assessment

Enter date...

Version Number of Compliance Documentation

Enter a number...

Upload Compliance Assessment Report (PDF preferred)

Upload File

Type of Certification (e.g., Internal Audit, Third-Party Audit)

- [ ] Internal Audit
- [ ] Third-Party Audit
- [ ] Self-Assessment

Access Control & Privilege Escalation

Validate appropriate access controls are in place to prevent unauthorized data access or privilege escalation.

Least Privilege Principle Applied?

- [ ] Yes
- [ ] No
- [ ] Not Applicable

Number of User Roles Defined

Enter a number...

Which Role-Based Access Controls (RBAC) are implemented?

- [ ] Data Access
- [ ] Functional Access
- [ ] Transaction Approval
- [ ] System Configuration

Authorization Review Frequency?

- [ ] Daily
- [ ] Weekly
- [ ] Monthly
- [ ] Quarterly
- [ ] Annually

Describe the process for granting new privileges.

Write something...

Are temporary privileged accounts used?

- [ ] Yes
- [ ] No

If yes, describe the temporary account lifecycle and controls.

Write something...