Checklist

The API Security Checklist

Learn what you need to build a strong organizational API security posture.

escape

Are you looking to build or strengthen your API Security Program?

This quick checklist shows you how.

Feel free to tailor and use these guidelines to fit your company's needs, and keep in mind that this list might not cover every single API security detail. Certain points depend on your specific organizational circumstances.

Action Plan

Integrate the action plan below into your Application Security roadmap to strengthen your organizational API security posture:

Discovery & Risk Assessment

- [ ] **INVENTORY**
  Begin by creating an inventory of all first-party APIs. This includes public-facing APIs and those that are meant for internal use only.

- [ ] **CLASSIFICATION**
  Categorize APIs based on sensitivity, usage, and the data type they handle. This helps in prioritizing which APIs require immediate attention.

- [ ] **DOCUMENTATION**
  Ensure all APIs are properly documented. This includes input/output parameters, authentication methods, and intended functionality.

Design & Architecture

- [ ] **SECURE DESIGN PRINCIPLES**
  Train your development teams in secure coding practices and secure design principles.

- [ ] **API GATEWAY**
  Implement an API gateway to centralize access control, rate limiting, and logging.

- [ ] **DATA FLOW DIAGRAMS**
  Create diagrams that showcase how data moves through your API ecosystem, identifying potential points of vulnerability.

Authentication & Authorization

- [ ] **OAUTH2/OIDC**
  Adopt OAuth2 and OpenID Connect (OIDC) for token-based authentication.
- [ ] **SCOPE & ROLE-BASED ACCESS**
  Ensure API endpoints enforce proper scope or role-based access controls.
- [ ] **JWT SECURITY**
  If using JWT, ensure secure handling, validation, and storage.

Input Validation & Output Encoding

- [ ] **STRONG TYPING**
  Enforce strict type constraints on inputs.
- [ ] **VALIDATION**
  All input must be validated against a defined schema.
- [ ] **OUTPUT ENCODING**
  Ensure data returned from APIs is properly encoded to prevent issues like Cross-Site Scripting (XSS).

Threat Modeling & Penetration Testing

- [ ] **THREAT MODELING**
  Identify potential threats and vulnerabilities in your API design.
- [ ] **PENETRATION TESTING**
  Regularly conduct pen-tests on your APIs to identify vulnerabilities.
- [ ] **AUTOMATED SCANNING**
  Incorporate automated vulnerability scanning tools in your CI/CD pipeline.

Rate Limiting & Quotas

- [ ] **RATE LIMITING**
  Implement rate limiting to protect against DDoS and brute-force attacks.
- [ ] **QUOTAS**
  Set quotas for users or IP addresses to prevent abuse.

Data Protection

- [ ] **ENCRYPTION**
  Ensure data in transit is encrypted using protocols like TLS.
- [ ] **DATA MASKING & REDACTION**
  Mask or redact sensitive data in API responses and logs.

Monitoring & Logging

- [ ] **CENTRALIZED LOGGING**
  Ensure all API logs are sent to a centralized logging system.
- [ ] **ALERTING**
  Set up alerts for suspicious activities such as spike in error rates, repeated failed logins, etc.
- [ ] **AUDIT TRAILS**
  Maintain detailed logs for all activities, especially changes and access to sensitive data.

Error Handling

- [ ] **CONSISTENT RESPONSES**
  Use consistent error response formats.
- [ ] **INFORMATION DISCLOSURE**
  Ensure error messages do not disclose sensitive or internal system details.

API Versioning

- [ ] **VERSIONING STRATEGY**
  Adopt a versioning strategy that allows for changes without breaking existing clients.
- [ ] **DEPRECATION POLICY**
  Create a policy for deprecating older API versions securely.

Training & Awareness

- [ ] **DEVELOPER TRAINING**
  Continuously train developers on the latest threats and security best practices.
- [ ] **SECURITY CHAMPIONS**
  Assign security champions within development teams to advocate for secure coding practices.

Feedback Loop

- [ ] **INCIDENT RESPONSE**
  Establish an incident response plan tailored to API breaches.
- [ ] **FEEDBACK MECHANISM**
  Implement a mechanism for developers and users to report vulnerabilities or issues.
- [ ] **CONTINUOUS IMPROVEMENT**
  Iterate on the security posture based on feedback, lessons learned, and evolving threats.

escape Checklist

API Security Checklist

Do you need help in assessing your API Security Posture?
We're here for you. With Escape you can:

- Automate the **discovery of all APIs**
- Build an accurate **API inventory**
- Ensure comprehensive **security coverage** with 70+ security tests for GraphQL & REST APIs, including OWASP Top 10, business logic, and access control
- **Shift security left with automated DAST** scanning by plugging Escape into your CI/CD systems
- Gain instant access to the affected repository and d**eveloper-friendly remediation** code snippets

Learn more

If you'd like to contribute to this checklist, reach out to us at ping@escape.tech