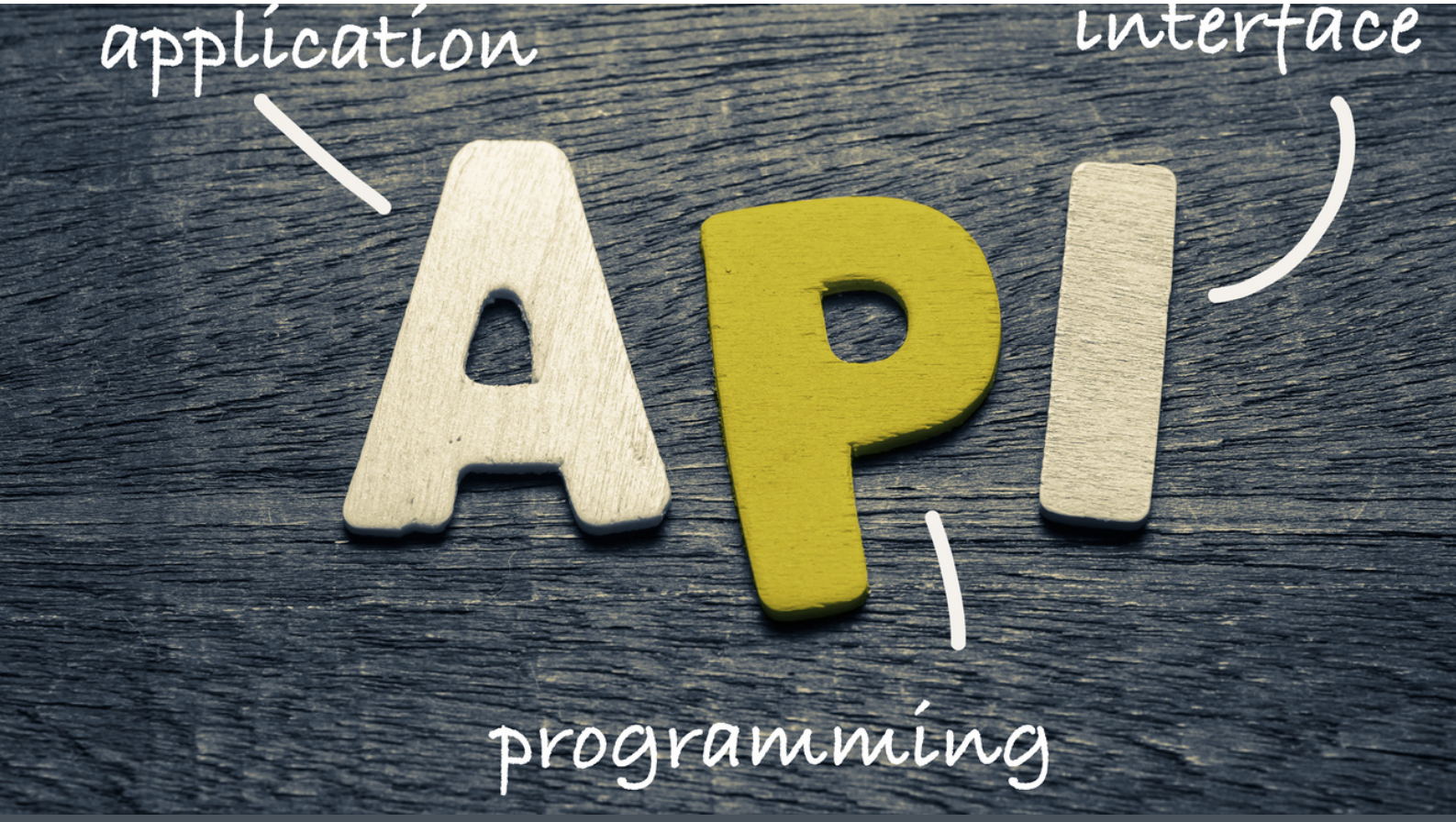
CYTAD




# API Security Quick -Audit Checklist

FOLLOW

CYTAD

# API SECURITY AUDIT CHECKLIST

| # | API Security area | Security Checks | Findings | Pass / Fail |
|---|---|---|---|---|
| 1 | **API Key Management:** | Are API keys managed securely, and is their distribution restricted to authorized users or applications? | | |
| | | Are API keys adequately protected from unauthorized access or exposure? | | |
| 2 | **OAuth 2.0 Implementation:** | Are API keys managed securely, and is their distribution restricted to authorized users or applications? | | |
| | | Are API keys adequately protected from unauthorized access or exposure? | | |
| | | Is OAuth 2.0 correctly implemented to provide secure user authentication | | |
| | | Are access tokens and refresh tokens properly issued, validated, and revoked when necessary? | | |
| 3 | **Rate Limiting Controls** | Is there a rate-limiting mechanism in place to prevent abuse or excessive use of the API? | | |
| | | Are rate limits enforced and configured appropriately to minimize the risk of service disruptions? | | |
| 4 | **Input Validation Procedures** | Are input validation and data sanitization mechanisms effectively preventing injection attacks, such as SQL injection and cross-site scripting (XSS)? | | |
| 5 | **CORS Configuration** | Is Cross-Origin Resource Sharing (CORS) properly configured to restrict cross-origin requests and protect against unauthorized access? | | |
| | | Are security headers like Content Security Policy (CSP), Strict-Transport-Security (HSTS), and X-Content-Type-Options in place to enhance security? | | |
| 6 | **Error Handling Practices** | Are error messages designed to avoid revealing sensitive information and provide generic responses? | | |
| | | Are errors properly logged, and is there a process for monitoring and incident response when security incidents occur? | | |
| 7 | **Audit Logging** | Are comprehensive audit logs maintained to record API requests, including source, timestamp, and actions performed? | | |
| | | Is there an effective monitoring and alerting system in place to detect and respond to suspicious activities or anomalies? | | |
| 8 | **Versioning Strategy** | Is versioning effectively implemented to ensure backward compatibility while introducing new features and changes to the API? | | |
| | | Is backward compatibility maintained to avoid breaking changes in existing API versions? | | |
| 9 | **File Upload Security** | If the API allows file uploads, is there a mechanism to restrict uploads to safe file types and scan for potential malware? | | |
| | | Are uploaded files stored securely and not executed as scripts? | | |
| 10 | **Data Encryption** | Is data transmitted over the API encrypted using secure protocols like HTTPS (TLS/SSL)? | | |
| | | Is sensitive data, including user credentials, stored in an encrypted form? | | |
| 11 | **API Documentation** | Is there comprehensive and up-to-date documentation available to guide developers in using the API securely? | | |
| | | Do developers receive proper training and education on security best practices when interacting with the API? | | |
| 12 | **Third-Party API Security** | When integrating with third-party APIs, is there a process for assessing their security practices and ensuring data protection and validation? | | |
| 13 | **DoS Protection Mechanisms** | Are there measures in place to mitigate the risk of DoS attacks, such as rate limiting, traffic analysis, and web application firewalls (WAFs)? | | |
| 14 | **API Key Management Procedures** | Are API keys securely managed and rotated regularly to minimize the risk of unauthorized access in the event of key compromise? | | |
| 15 | **Security Assessment Procedures** | Is there a process for conducting regular security assessments and penetration testing on the API using tools like OWASP ZAP, Postman, or Burp Suite? | | |
| | | Are identified vulnerabilities addressed promptly and documented for audit purposes? | | |
| 16 | **Compliance Checks** | Is the organization's API security practices configured to meet legal and regulatory compliance requirements relevant to the industry and jurisdiction? | | |
| 17 | **Feedback and Improvement Process** | Is there a feedback loop for collecting input from developers, security professionals, and auditors to drive continuous improvement of API security practices? | | |

Follow CYTAD on Linkedin for security advisories, checklists, mentoring, services, insights and much more

CYTAD

CYber Thinkers Advisors Doers

CYTAD - WA Channel