HUNTRIX

Professional Pentesting Services

API Security Testing Checklist

Use it to get you started on your API security testing journey.

Authentication and Authorization

- [ ] Test access without valid tokens
- [ ] Check for invalid/expired tokens handling
- [ ] Test broken object level authorization (BOLA)
  - Manipulate IDs and paths (e.g., `/id=1` to `/id=0`)
- [ ] Test broken function level authorization (BFLA)
  - Access admin functions as a regular user
- [ ] Check for credential stuffing vulnerabilities
  - Test brute force on multiple user accounts
- [ ] Test account lockout/captcha after multiple failed login attempts
- [ ] Verify password strength enforcement
- [ ] Ensure sensitive data (e.g., tokens, passwords) isn't sent in URLs
- [ ] Require password confirmation for sensitive actions (e.g., changing email or password)
- [ ] Validate token authenticity
  - Reject unsigned or weak JWTs (e.g., `{"alg":"none"}`)
  - Verify JWT expiration
- [ ] Check password storage and encryption
- [ ] Test session management
  - Ensure session timeout and logout invalidation
- [ ] Verify microservice authentication
  - Ensure no microservices are accessible without authentication

Input Validation and Data Handling

- [ ] Test for mass assignment vulnerabilities
  - Try adding admin privileges (e.g., `"isadmin":"true"`)
  - Attempt to change user roles (e.g., `"user_role":"admin"`)
  - Check if you can modify sensitive fields (e.g., `"email-verify": true`)
- [ ] Verify input sanitization
  - Test for SQL injection in parameters and request bodies
  - Check for XSS vulnerabilities in reflected responses
  - Attempt command injection in relevant parameters
- [ ] Test file upload functionality (if applicable)
  - Try uploading malicious files
  - Attempt to override file paths (e.g., `"file_path":"../../../../index.php"`)

HTTP Methods and Headers

- [ ] Test all supported HTTP methods (GET, POST, PUT, DELETE, etc.)
- [ ] Check for harmful HTTP methods (e.g., TRACE)
- [ ] Manipulate request headers
  - Test different Content-Type headers
  - Try header injection (e.g., modifying `X-Forwarded-For`)

Error Handling and Information Disclosure

- [ ] Analyze error messages for excessive information
- [ ] Check for internal path disclosure in errors
- [ ] Verify proper handling of invalid inputs

Contact Us

: hello@huntrix.io

: https://huntrix.io/get-started

API Security Testing Checklist

Use it to get you started on your API security testing journey.

API Structure and Versioning

- [ ] Test different API versions
  - Change version in URL path (e.g., `/api/v2/user` to `/api/v1/user`)
  - Modify version in request parameters or headers
- [ ] Check for deprecated or undocumented endpoints
- [ ] Verify consistency between API versions

Data Exposure and Encryption

- [ ] Check for sensitive data in API responses
- [ ] Verify use of HTTPS and strong SSL/TLS configurations
- [ ] Check for exposure of API keys or secrets in responses

Specific GraphQL Tests

- [ ] Test GraphQL introspection
- [ ] Check for GraphiQL endpoints
- [ ] Use tools like InQL Scanner to find hidden queries
- [ ] Test for query depth and complexity limits
- [ ] Verify proper handling of nested queries and fragments

Rate Limiting and Performance

- [ ] Test for lack of rate limiting
  - Rapid-fire multiple requests
  - Use different IP addresses or headers to bypass limits
- [ ] Assess API performance under normal and peak loads
- [ ] Check for resource exhaustion vulnerabilities

Business Logic and Edge Cases

- [ ] Test for race conditions in critical operations
- [ ] Verify proper implementation of business rules
- [ ] Check time-sensitive operations (e.g., password resets)

Miscellaneous

- [ ] Verify API behavior matches documentation
- [ ] Check logging practices for security and privacy
- [ ] Test for CSRF vulnerabilities in state-changing operations
- [ ] Verify proper API key rotation mechanisms

Need a digital copy?
No Problem, check out our free online resources including full markdown checklist, table format and more.

→ https://huntrix.io/blog/api-security-testing-checklist/