Securing Your API: The OWASP API Top 10

Rob Allen, September 2026

57% of organizations suffered an API-related data breach in the past two years

Traceable 2025 Global State of API Security report

Why are APIs different?

The OWASP API Security Project seeks to provide value to software developers and security assessors by underscoring the potential risks in insecure APIs

OWASP API Security Top 10

OWASP API Security Top 10

Who are you and what can you access?

Authentication and authorisation failures

#1
#2
#3
#4
#5
#6
#7
#8
#9
#10

Broken Authentication

APIs that don't properly verify who you are

Broken Authentication

APIs that don't properly verify who you are

- Weak/no token validation
- Missing expiration on tokens
- Credential stuffing attacks

#1
#2
#3
#4
#5
#6
#7
#8
#9
#10

Broken Authentication

Examples

- API accepts JWT without verifying the signature
- Login endpoint allows unlimited password attempts

#1
#2
#3
#4
#5
#6
#7
#8
#9
#10

Broken Authentication

Prevention

- Use established standards (OAuth 2.0, OpenID Connect)
- Implement proper token validation and expiration
- Rate limiting on auth endpoints

#1
#2
#3
#4
#5
#6
#7
#8
#9
#10

#1
~~#2~~
#3
#4
#5
#6
#7
#8
#9
#10

Broken Function Level Authorisation

Users can access functionality they shouldn't

Broken Function Level Authorisation

Users can access functionality they shouldn't

- Incorrect authorisation check on a function or resource
- Legitimate calls to endpoints that the user shouldn't have access to
- Undocumented open endpoints

#1
~~#2~~
#3
#4
#5
#6
#7
#8
#9
#10

Broken Function Level Authorisation

Examples

- `/debug/dump`
- `/admin/users` doesn't check that the caller is an admin

#1
~~#2~~
#3
#4
#5
#6
#7
#8
#9
#10

Broken Function Level Authorisation

Prevention

- Deny by default
- Check roles/permissions on every endpoint
- Don't rely on hiding endpoints from documentation

#1
~~#2~~
#3
#4
#5
#6
#7
#8
#9
#10

#1
~~#2~~
#3
#4
~~#5~~
#6
#7
#8
#9
#10

Broken Object Level Authorisation

Users can access objects belonging to other users

Broken Object Level Authorisation

Users can access objects belonging to other users

- User can access another user's resource
- Changing an ID or key allows access to privileged data

#1
~~#2~~
#3
#4
~~#5~~
#6
#7
#8
#9
#10

Broken Object Level Authorisation

Examples

- `/users/123/orders` - change to 124 and see someone else's orders
- `/accounts/1/documents/999` checks the account, but not the document

Broken Object Level Authorisation

Prevention

- Implement proper authorisation based on user policies
- Check if the user has access to the requested resource
- Check that the operation is also allowed

#1
~~#2~~
#3
#4
~~#5~~
#6
#7
#8
#9
#10

~~#1~~
~~#2~~
#3
#4
~~#5~~
#6
#7
#8
#9
#10

Broken Object Property Authorisation

Users can read or modify properties they shouldn't

Broken Object Property Authorisation

Users can read or modify properties they shouldn't

- Sending properties that this user shouldn't see
- Allowing this user to change a property they shouldn't

~~#1~~
~~#2~~
#3
#4
~~#5~~
#6
#7
#8
#9
#10

Broken Object Property Authorisation

Examples

- User updates profile, includes `"role": "admin"` in payload
- Profile response includes PII that only admins should see

Broken Object Property Authorisation

Prevention

- Specifically choose object properties to return
- Explicit allowlists for input properties

~~#1~~
~~#2~~
#3
#4
~~#5~~
#6
#7
#8
#9
#10

Exploiting how your API works

Business logic and resource abuse

Rob Allen ~ akrabat.com

~~#1~~
~~#2~~
~~#3~~
#4
~~#5~~
#6
#7
#8
#9
#10

Unrestricted resource consumption

APIs that can be abused through resource consumption

Unrestricted resource consumption

APIs that can be abused through resource consumption

- Expensive operations without throttling
- Exhausting memory through requests for too much data
- Denial of service

~~#1~~
~~#2~~
~~#3~~
#4
~~#5~~
#6
#7
#8
#9
#10

Unrestricted resource consumption

Examples

- `/widgets?page=1&per_page=1000000`
- Resending an OTP that has no throttle; each SMS costs money

#1
#2
#3
#4
#5
#6
#7
#8
#9
#10

Unrestricted resource consumption

Prevention

- Rate limiting (per IP, per user, per endpoint)
- Pagination with maximum limits
- Resource quotas / Timeouts

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
#6
#7
#8
#9
#10

Unrestricted access to business flows

Critical workflows lack protection against automation

Unrestricted access to business flows

Critical workflows lack protection against automation

- Some business flows are more sensitive than others
- Legitimate calls, but unexpected order
- Excessive access may harm the business

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
#6
#7
#8
#9
#10

Unrestricted access to business flows

Examples

- Ticket scalping bots, inventory hoarding
- Book 90% of a hotel's rooms, then cancel at the last minute

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
#6
#7
#8
#9
#10

Unrestricted access to business flows

Prevention

- Device fingerprinting
- Behavioural analysis
- Transaction limits

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
#6
#7
#8
#9
#10

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
~~#6~~
#7
#8
#9
#10

Unsafe consumption of APIs

Your API trusts third-party APIs too much

Unsafe consumption of APIs

Your API trusts third-party APIs too much

- Dependency on another's vulnerabilities
- Malicious data can be injected
- Not accounting for failure

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
~~#6~~
#7
#8
#9
#10

Unsafe consumption of APIs

Examples

- Geolocation API takes 30 seconds to time out and locks your API
- Third-party API redirects your request to an attacker's host

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
~~#6~~
#7
#8
#9
#10

Unsafe consumption of APIs

Prevention

- Validate all external data
- Whitelist redirect URLs
- Implement timeouts

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
~~#6~~
#7
#8
#9
#10

Operational security gaps

Configuration and infrastructure vulnerabilities

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
~~#6~~
#7
#8
#9
~~#10~~

Security misconfiguration

Insecure defaults and missing security hardening

Security misconfiguration

Insecure defaults and missing security hardening

- Default configurations
- Missing security updates
- Unnecessary features enabled
- Header misconfiguration (CORS, etc.)

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
~~#6~~
#7
#8
#9
~~#10~~

Security misconfiguration

Examples

- Error messages return stack traces
- `Access-Control-Allow-Origin:*` on an authenticated endpoint

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
~~#6~~
#7
#8
#9
~~#10~~

Security misconfiguration

Prevention

- Regular security auditing and updates
- Audit and remove unnecessary features
- For APIs against browser-based clients, implement CORS and security headers

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
~~#6~~
#7
#8
#9
~~#10~~

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
~~#6~~
#7
~~#8~~
#9
~~#10~~

Improper inventory management

Do you know your API?

Improper inventory management

Do you know your API?

- Old API versions still running
- Shadow APIs (undocumented endpoints)
- Non-production environments accessible

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
~~#6~~
#7
~~#8~~
#9
~~#10~~

Improper inventory management

Examples

- v1 API wasn't decommissioned
- Staging environment is public

#1
#2
#3
#4
#5
#6
#7
#8
#9
#10

Improper inventory management

Prevention

- Maintain API inventory/catalogue
- API Gateway / automated discovery tools
- Retire old versions with clear timelines

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
~~#6~~
#7
~~#8~~
#9
~~#10~~

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
~~#6~~
#7
~~#8~~
~~#9~~
~~#10~~

Server side request forgery

API fetches remote resources without validation

Server side request forgery

API fetches remote resources without validation

- User-controlled URLs in API requests
- API fetches a remote resource from a user-supplied URL
- Can access internal network endpoints

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
~~#6~~
#7
~~#8~~
~~#9~~
~~#10~~

Server side request forgery

Examples

- `/images?url=http://127.0.0.1:8080/metrics`

~~#1~~
~~#2~~
~~#3~~
~~#4~~
~~#5~~
~~#6~~
#7
~~#8~~
~~#9~~
~~#10~~

Server side request forgery

Prevention

- Validate and sanitise URLs
- Whitelist for domains & media types, etc
- Disable HTTP redirection where possible
- Don't send raw responses to clients

In Closing

OWASP API Security Top 10

- Authentication & authorisation failures
- Business logic & resource abuse
- Configuration & infrastructure vulnerabilities

Security requires

- Defence in depth
- Testing with the mindset of an attacker
- Ongoing attention

Resources

OWASP API Security Project website
owasp.org/www-project-api-security/

REST Security Cheat Sheet
cheatsheetseries.owasp.org/cheatsheets/REST_Security_Cheat_Sheet.html

API Security news
apisecurity.io

"Securing APIs isn't optional; it is the frontline defense for protecting data integrity and maintaining digital trust."

Randy Barr, Cequence Security

Rob Allen ~ akrabat.com