OWASP API Security Top 10

APIs drive business so attackers have placed them firmly in the crosshairs which is why Cloudflare API Gateway protects against OWASP API risks.

API security risks

APIs are a critical part of modern business, powering mobile, IoT, and web applications. Companies use them to interact with partners and to share data both publicly and internally. APIs can expose application logic or share sensitive data, which is why APIs are now a key target for attackers.

As part of its API Security Project, OWASP published its list of top security risks for APIs, the **API Security Top 10**. These API risks are real - Cloudflare now sees API endpoints globally receive more malicious requests compared to standard web applications.

1. Broken Object Level Authorization
2. Broken User Authentication
3. Excessive Data Exposure
4. Lack of Resources & Rate Limiting
5. Broken Function Level Authorization
6. Mass Assignment
7. Security Misconfiguration
8. Injection
9. Improper Assets Management
10. Insufficient Logging & Monitoring

Key risk: Improper Assets Management (Shadow APIs)

It is common for organizations not to track the APIs in production, leading to Shadow APIs with no visibility into API endpoints in use -- or the activity occurring on them.

Key risk: Authentication and authorization

Authentication and authorization have long been issues for applications and remain so for APIs. Authenticated users may be able to gain illicit access to sensitive data — even worse, data might not be authenticated at all.

Key risk: Lack of resources

This is when API backends are overwhelmed because no rate limts are in place or restrictions on the size or number of resources that can be requested. This can take API endpoints offline.

The dedicated API security of API Gateway keeps customers APIs safe from OWASP API security risks.

OWASP		CLOUDFLARE
1	Broken Object Level Authorization	Schema validation
2	Broken User Authentication	mTLS Authentication; Rate Limiting and volumetric anomaly detection; stolen credential checks
3	Excessive Data Exposure	Schema validation; Sensitive data detection
4	Lack of Resources & Rate Limiting	Rate Limiting/DDoS and volumetric anomaly detection
5	Broken Function Level Authorization	Schema validation
6	Mass Assignment	Schema validation, Rate Limiting
7	Security Misconfiguration	Sensitive data detection; Schema validation
8	Injection	WAF rulesets; Schema validation
9	Improper Assets Management	API Discovery
10	Insufficient Logging & Monitoring	API Discovery; SIEM integration

Key Cloudflare API protections

- **API Discovery**: Automatically discovers API endpoints to prevent “shadow APIs” through an always up-to-date API inventory.
- **Mutual TLS**: Provides strong authentication by issuing and validating client certificates.
- **Schema Validation**: Use of OpenAPI schemas to validate incoming traffic for a positive security model.
- **Volumetric Abuse Detection**: Cloudflare-suggested rate limits for each endpoint and path based on observed traffic to deter abuse.