OWASP API SECURITY TOP 10 COMPARISON

The OWASP Top 10 is the standard for how organizations have approached security for traditional applications but the increased adoption of APIs has changed the way we need to think about security. The OWASP API Security Top 10 was born out of the need to look at security for modern, API driven applications in a new way.

The following table compares the OWASP API Security Top 10 - 2019 with the OWASP Top 10 2017.

OWASP API Security Top 10 - 2019	OWASP Top 10 - 2017
A1:2019 - Broken Object Level Authorization	**A1:2017** - Injections *(Reduced in rank - moved to A8:2019)*
A2:2019 - Broken Authentication	**A2:2017** - Broken Authentication
A3:2019 - Excessive Data Exposure	**A3:2017** - Sensitive Data Exposure *(Not Included)*
A4:2019 - Lack of Resources & Rate Limiting	**A4:2017** - XML External Entities (XXE) *(Not Included)*
A5:2019 - Broken Function Level Authorization	**A5:2017** - Broken Access Control *(Modified for APIs)*
A6:2019 - Mass Assignment	**A6:2017** - Security Misconfiguration *(Reduced in rank - moved to A7:2019)*
A7:2019 - Security Misconfiguration	**A7:2017** - Cross-Site Scripting (XSS) *(Included in A8)*
A8:2019 - Injection	**A8:2017** - Insecure Deserialization *(Not Included)*
A9:2019 - Improper Assets Management	**A9:2017** - Using Components with Known Vulnerabilities *(Not Included)*
A10:2019 - Insufficient Logging & Monitoring	**A10:2017** - Insufficient Logging & Monitoring

Remained the same in the 2019 API Security Top 10

Moved or modified in the 2019 API Security Top 10

Not included in the 2019 API Security Top 10

The following table shows how Web Application Firewalls (WAFs), API Gateways and the Salt Security solution address each of the new OWASP API Security Top 10 2019.

OWASP API Security Top 10 - 2019	WAFs	API Gateways	Salt Security
A1:2019 - Broken Object Level Authorization	✗	✗	✓
A2:2019 - Broken Authentication	✗	/ Manual	✓
A3:2019 - Excessive Data Exposure	✗	✗	✓
A4:2019 - Lack of Resources & Rate Limiting	✗	/ Manual & Partial	✓
A5:2019 - Broken Function Level Authorization	✗	/ Partial	✓
A6:2019 - Mass Assignment	✗	✗	✓
A7:2019 - Security Misconfiguration	/ Partial	✗	✓
A8:2019 - Injection	✓ (Signature Based)	✓ (Signature Based, Latency Impact)	✓
A9:2019 - Improper Assets Management	✗	/ Manual Conf. & Partial	✓
A10:2019 - Insufficient Logging & Monitoring	/ Partial	/ Partial	✓

More Information

- **Find more on the OWASP API Security Project and the API Security Top 10 on the project page:**
  https://www.owasp.org/index.php/OWASP_API_Security_Project
- **Get additional details on the project and each of the top 10 in this webinar:**
  https://salt.security/owasp-api-security-top-10
- **Participate and provide feedback to the project here:**
  https://www.owasp.org/index.php/OWASP_API_Security_Project#tab=Join