OWASP API Top 10	OWASP Web Top 10	RASP	WAF	Traceable
	Overall protection score (out of 36)	11	16	28
API1:2019 - Broken Object Level Authorization	A5:2017 - Broken Access Control	✗	✗	✓
API2:2019 - Broken Authentication	A2:2017 - Broken Authentication	✓	✓	✓
API3:2019 - Excessive Data Exposure	A3:2017- Sensitive Data Exposure	✓	✓	✓
API4:2019 - Lack of Resources and Rate Lmting	-	✓	✓	✓
API5:2019 - Broken Function Level AuthZ	A5:2017-Broken Access Control	✗	✗	🗓
API6:2019 - Mass Assignment	A5:2017-Broken Access Control	✗	✗	✓
API7:2019 - Security Misconfiguration	A6:2017-Security Misconfiguration	✓	✗	✗
API8:2019 - Injection	A1:2017 - Injection A4:2017-XML External Entities (XXE)	✓	✓	✓
API9:2019 - Improper Assets Management	A9:2017 - Using Comps with Known Vulns	✓	✗	🗓
API10:2019 - Insufficient Logging and Monitoring	A10:2017- Insufficient Logging & Monitoring	✓	✓	✓
	A7:2017 - Cross-Site Scripting (XSS)	✓	✓	✓
	A8:2017 - Insecure Deserialization	✗	✓	✓
Category	**Attacks/Anomalies**			
Other Attacks	SSRF	✓	✗	✓
	Path manipulation	✗	✓	✓
	Local file inclusion (LFI)	✓	✓	✓
	Remote code execution	✓	✓	✓
	HTTP request smuggling	✗	✓	✓
Anomaly Detection	Missing consistent parameter	✗	✗	✓
	Unseen parameter types	✗	✗	✓
	Double parameter / parameter confusion	✗	✗	✓
	Unexpected wildcard	✗	✗	✓
	Unexpected length	✗	✗	✓
	Unexpected enum value	✗	✗	✓
	Unknown HTTP header	✗	✗	✓
	Unknown device	✗	✗	✓
	Unexpected content type	✗	✗	✓
	Unexpected content length	✗	✗	✓
	Browser accessed non-browser endpoint	✗	✗	✓
	Request size mismatch	✗	✗	✓
	Unexpected HTTP method	✗	✗	✓
	Unexpected response code	✗	✗	✓
	Bad hop headers	✗	✓	🗓
	Double encoding	✗	✓	🗓
	Invalid encoding	✗	✓	🗓
	Missing "Content-Type" request header	✗	✓	🗓
	No user agent	✗	✓	🗓

✓ has runtime protection for 🗓 roadmap ✗ doesn't have runtime protection for