i need to write a resarh paper on WAAP, so give full contents of WAAP and oWASP API vulnerability, its trend and all contents

A Web Application and API Protection solution is a consolidated security platform that combines WAF, API discovery/protection, bot management, and DDoS mitigation to protect modern web apps and APIs end to end. The latest OWASP API Security Top 10 (2023) highlights the most critical API risks organizations must address within WAAP programs, including Broken Object Level Authorization, Broken Authentication, and Unrestricted Resource Consumption, among others.[1] [2] [3] [4]

WAAP in brief

- WAAP extends traditional WAF with native API discovery/protection, bot management, and DDoS defenses to address cloud-native and microservices threats beyond rule-based filtering.[5] [3]
- Core modules typically include WAF, API protection, bot mitigation, and DDoS protection with varying depth and deployment flexibility in cloud and edge environments.[5] [1]
- Modern platforms add ML-driven anomaly detection, granular API policy enforcement, automation via full APIs, and integrations with CDNs, XDR, and threat intelligence for scalable, adaptive defense.[6] [5]

WAAP capabilities

- WAF: Signature and behavioral detections, positive security models, virtual patching, and granular policy management for web traffic.[1] [5]
- API security: Discovery, inventory, schema validation, authentication/authorization enforcement, and protection against abuse and business logic misuse.[5] [1]
- Bot management: ML-driven detection, intent-based classification, and mitigation controls to reduce fraud, scraping, and automated abuse.[3] [5]
- DDoS: Network and application-layer protection with adaptive scaling, edge coverage, and traffic scrubbing.[1] [5]

Architecture and deployment

- Delivery models span cloud-native, on-premises, managed services, and API security gateways, with API-first control planes for automation and CI/CD integration.[3] [5]
- Integrations often include CDN/edge, caching, fraud and risk services, SIEM/SOAR, and XDR for unified telemetry and response.[5] [1]
- Enterprise requirements include detailed audit logging, forensics, compliance reporting, and real-time policy updates across multi-cloud footprints.[1] [5]

WAAP vs. legacy WAF

- Scope: WAAP covers APIs and bot/DDoS threats natively; legacy WAFs focus on HTTP request/response filtering and signatures.[5] [1]
- Adaptability: WAAP emphasizes ML, automation, and API-level policies, aligning with microservices and rapid change; WAFs are more static and rule-centric.[6] [5]
- Visibility: WAAP includes API discovery/inventory and business logic protections; WAFs typically lack deep API object/flow context.[1] [5]

OWASP API Security Top 10 (2023)

- API1: Broken Object Level Authorization—object ID endpoints expand OLAC attack surface; enforce checks on every data access function.[2] [4]
- API2: Broken Authentication—flawed token handling and implementation weaknesses enable account compromise and identity spoofing.[4] [2]
- API3: Broken Object Property Level Authorization—insufficient property-level authorization causing exposure/manipulation; merges Excessive Data Exposure and Mass Assignment.[7] [2]
- API4: Unrestricted Resource Consumption—lack of controls on costly resources leads to DoS and unexpected spend.[2] [4]
- API5: Broken Function Level Authorization—complex role/permission models cause privilege escalation to other users' resources/admin functions.[4] [2]
- API6: Unrestricted Access to Sensitive Business Flows—exposed flows (e.g., checkout) abused at scale absent compensating controls.[7] [2]
- API7: Server-Side Request Forgery—unvalidated remote fetch allows pivoting to internal networks/services.[2] [4]
- API8: Security Misconfiguration—complex stacks and missed hardening expose debug endpoints and weak defaults.[4] [2]
- API9: Improper Inventory Management—insufficient API/host/version inventories lead to shadow/deprecated endpoints and gaps.[7] [2]
- API10: Unsafe Consumption of APIs—over-trusting third-party APIs and weak input handling enable compromise via integrations.[2] [7]

Changes from OWASP API 2019 to 2023

- New entries: Unrestricted Access to Sensitive Business Flows, SSRF, and Unsafe Consumption of APIs; reflect modern abuse and supply-chain risks.[7] [2]
- Merged/renamed: Property-level authorization merges Excessive Data Exposure and Mass Assignment; resource consumption reframes lack of rate limiting themes.[2] [7]
- Continuing risks: BOLA and function-level authorization remain prominent due to pervasive access control complexity in APIs.[7] [2]

WAAP alignment to OWASP API risks

- Access control: Enforce BOLA/FPoLA with object/property-aware policies, JWT validation, and API gateways integrated with WAAP.[5] [1]
- Abuse and flow protection: Bot management and behavioral controls mitigate automation against sensitive business flows and resource exhaustion.[3] [5]
- SSRF and egress control: Outbound request validation, allowlists, and SSRF-specific detections at gateways and WAAP layers.[1] [5]
- Inventory and discovery: Continuous API discovery, documentation, and version governance address improper inventory management.[5] [1]

Market and threat trends

- Consolidation: Organizations prefer unified WAAP platforms to reduce operational overhead and bridge WAF, API, bot, and DDoS under one control plane.[6] [5]
- Growth: Analysts estimate multi-year double-digit CAGR with market sizes in the mid-single-digit billions today, driven by API proliferation and compliance demands.[8] [9]
- Attack volume: Global attack attempts against web apps and APIs continue to rise year over year, underscoring the need for adaptive defenses at scale.[10] [6]

Evaluation criteria for a WAAP

- Coverage: Depth across WAF, API security (discovery, schema, authZ), bot mitigation, and L3–L7 DDoS, including edge/CDN integration.[1] [5]
- Efficacy: ML-driven anomaly detection, virtual patching, low false positives, and real-time signature/behavior updates.[6] [5]
- Operations: API-first automation, CI/CD policy as code, forensics, compliance reporting, and third-party ecosystem integrations.[5] [1]

Reference structure for your paper

- Introduction: Evolution from WAF to WAAP; problem statement for API-first architectures and bot/DDoS threats.[3] [5]
- Background: WAAP components and architecture; deployment models; integrations and automation.[1] [5]

- OWASP API Top 10 (2023): Each risk’s definition, examples, and mitigations mapped to WAAP capabilities and SDLC controls.[2] [7]
- Market and threat landscape: Adoption drivers, growth projections, and attack trends with recent statistics.[8] [10]
- Design and evaluation: Control objectives, KPIs (time-to-protect, false positive rate), and reference architecture for multi-cloud.[5] [1]
- Case studies and best practices: API discovery/inventory, zero trust for APIs, schema enforcement, rate limiting, and anti-automation patterns.[6] [5]

Selected sources for citation in your paper

- WAAP definitions, capabilities, and architectural considerations from vendors and industry analyses.[3] [1] [5]
- OWASP API Security Top 10 (2023) canonical list and change log context.[4] [7] [2]
- Market growth and adoption trend indicators with multi-year projections.[9] [8]
- Threat telemetry on global web and API attack volumes in 2024.[10] [6]

⁂

1. https://www.imperva.com/learn/application-security/web-application-and-api-protection-waap/
2. https://owasp.org/API-Security/editions/2023/en/0x11-t10/
3. https://www.radware.com/cyberpedia/application-security/what-is-waap/
4. https://owasp.org/API-Security/editions/2023/en/0x00-header/
5. https://www.f5.com/pdf/report/2025-kuppingercole-leadership-compass-waap.pdf
6. https://www.oligo.security/academy/web-app-security-in-2025-5-technologies-you-cant-do-without
7. https://apisecurity.io/owasp-api-security-top-10/
8. https://www.verifiedmarketreports.com/product/web-application-and-api-protection-waap-market/
9. https://www.businessresearchinsights.com/market-reports/cloud-web-application-and-api-protection-waap-market-112763
10. https://www.cdnetworks.com/reports/state-of-waap-2024
11. https://www.wallarm.com/what/waap-web-application-api-protection
12. https://www.linkedin.com/pulse/how-web-application-api-protection-waap-works-one-u5m7e
13. https://escape.tech/blog/owasp-api-security-checklist-for-2023/
14. https://www.kuppingercole.com/events/2025/10/breaking-the-firewall
15. https://www.datainsightsmarket.com/reports/cloud-web-application-and-api-protection-waap-1412693
16. https://www.f5.com/company/blog/kuppingercole-recognizes-f5-as-overall-market-leader-in-waap
17. https://www.kuppingercole.com/watch/breaking-the-firewall
18. https://owasp.org/www-project-api-security/
19. https://www.marketsizeandtrends.com/report/distributed-cloud-web-app-and-api-protection-waap-market/

20. https://portswigger.net/web-security/api-testing/top-10-api-vulnerabilities