PENTESTERRA
SEE THE REAL RISK

WEB APPS
APIs
BUSINESS LOGIC
REAL IMPACT

SAME ATTACKER MINDSET.
A MORE RESILIENT TOMORROW.

BEYOND VULNERABILITIES
TOWARDS REAL SECURITY.

AWAP MODULE

Automated Web Application Pentest

60+ attack modules. First findings in **~15 minutes.**

Black-box/grey-box web app testing that chains findings the way a real pentester does — not a vuln scanner with a fresh coat of paint.

PENTESTERRA — AWAP / TARGETS / SCAN — Live Scan

- Dashboard
- Web Applications
- Targets
- Scans
- Findings
- Attack Chain
- Reports
- Integrations
- Settings

Target: https://acme-corp.com — Scanning...
Automated Web Application Pentest (AWAP)

New Scan

Overview | Requests | Findings (12) | Attack Chain | Technology | Progress

Endpoints Discovered	Vulnerabilities Found	Modules Running	WAF/CDN Detected	Scan Progress
1,248 (+342 new)	12 (3 critical)	60+ (38 active)	Cloudflare (Adaptive Evasion On)	65% Est. 6 min remaining

Live Scanning

```
$ pentesterra-awap --target https://acme-corp.com
[INFO] Initializing 60+ attack modules...
[INFO] Loading payload libicatios..
[INFO] Fingerprinting application and defenses...
[INFO] Detected WAF: Cloudflare (adaptive evasion enabled)
[INFO] Discovering endpoints (JS, robots.txt, sitemap)...
[INFO] Running SQLi tests on 248 parameters...
[INFO] Testing for XSS (reflected, stored, DOM)...
[INFO] Testing for IDOR/BOLA...
[INFO] Verifying findings...
[+] First finding in 00:14:37
[INFO] Continuing scan ...
```

Vulnerable Request — CRITICAL

```
GET /api/v1/products?id=1' OR '1'='1 HTTP/1.1
Host: acme-corp.com
User-Agent: Pentesterra/1.0
Accept: application/json
```

Response (200 OK)

```
{
  "status": "success",
  "data": [
    {
      "id": 1,
      "name": "Admin User",
      "email": "admin@acme-corp.com",
      "role": "admin"
    }
  ]
}
```

Finding Verified
SQL Injection (Boolean-based)
Verified by real exploit • PoC attached • Added to Attack Chain
View Finding →

Attack Surface & Findings

Endpoint Discovery	Parameter Analysis	WAF/CDN Fingerprinting	Active Testing
1,248 endpoints	342 parameters	Cloudflare	60+ modules

Top Findings (verified) — View All →

CRITICAL	SQL Injection	/api/v1/products	Verified
HIGH	Stored XSS	/admin/settings	Verified
HIGH	IDOR (BOLA)	/api/v1/users/123	Verified
MEDIUM	Open Redirect	/auth/redirect	Verified

What it does

- 60+ active modules across 21 vulnerability classes: SQLi/NoSQLi, XSS (reflected/stored/DOM + CSP bypass), SSRF (incl. cloud IMDS v1/v2 pivoting), SSTI, XXE, IDOR/BOLA, JWT tampering, CSRF, open redirect, deserialization, race conditions, request smuggling, prototype pollution
- Passive (JS analysis, robots.txt, sitemap, Swagger/OpenAPI) + active (parameter discovery) endpoint discovery: tech stack + WAF/CDN fingerprinting with adaptive payload evasion
- CVE enrichment from detected tech stack via the platform knowledge base
- AI/LLM-specific coverage: prompt injection (OWASP LLM01:2025)
- Business logic testing: broken authorization, mass assignment, bypassable workflows, state transition flaws
- Every finding runs through the verification pipeline — PoC attached, not just a severity label
- Distributed execution across scanner nodes — parallel modules, no single-node bottleneck

Why Pentesterra

- **Verification-first:** a finding is not a vulnerability until it is confirmed by a real exploit
- **Cross-domain correlation:** web findings become nodes in the Attack Chain together with network and code
- **WAF evasion** is built into the scanning engine, not bolted on as a separate feature

> *Real exploits.*
> *Real environments.*
> *Real security.*
> — PENTESTERRA

WEB APPLICATIONS
API SECURITY
BUSINESS LOGIC
ATTACK CHAIN
REAL ADVANTAGE

THE AWAP WORKFLOW

1. **Discover** — Map endpoints
2. **Fingerprint** — Identify stack & defenses
3. **Test** — Run active modules
4. **Verify** — Attach PoC
5. **Correlate** — Add to Attack Chain

21 vulnerability classes | Verification-first | Adaptive WAF evasion | Attack Chain ready | Distributed execution | AI / LLM coverage

Validate what is truly exploitable.

Explore AWAP →

PEOPLE
PROCESS
TECHNOLOGY
STRONGER TOGETHER

PENTESTERRA

WEB APP PENTEST (AWAP)

60+ Attack Modules. First Findings in ~15 Minutes.

Black-box/grey-box web app testing that chains findings the way a real pentester does - not a vulnerability scanner with a fresh coat of paint.

60+
Attack modules across 21 vulnerability classes

~15 min
Mean time to first findings

1.5-12 hrs
Full pentest, depending on target complexity

WHY NOW

A new feature shipped last sprint, and nobody re-tested the app for it. Most web app breaches don't come from the vulnerability class you tested for last year - they come from the endpoint that didn't exist yet when you did.

WHAT IT COVERS

Core Injection & Client-Side

The high-impact exploit paths and client-side attack surface, tested actively - not just pattern-matched.

- → SQLi (error/boolean/time-based), NoSQLi & RCE escalation, SSTI, XXE, prototype pollution
- → Reflected, stored & DOM XSS with CSP bypass, DOM clobbering, postMessage injection
- → Command injection, unrestricted file upload, second-order injection

Web Infrastructure & Cloud

The edge, cache, and cloud-native surface most scanners skip entirely.

- → HTTP request smuggling, cache poisoning, web cache deception
- → SSRF/RFI with AWS/GCP/Azure IMDS v1/v2 pivoting, cloud metadata exposure
- → CORS misconfiguration, host-header injection, subdomain takeover

AI, Business Logic & Emerging Threats

The application-layer risks that came out of the last two years of real incidents, not a static OWASP Top 10 checklist.

→ LLM/AI prompt injection (OWASP LLM01:2025)

→ IDOR, broken authorization, mass assignment, bypassable workflows, state transition flaws

→ WebAuthn/passkey downgrade attacks, ReDoS

Verification-First, WAF-Aware

A finding is not a vulnerability until it is confirmed by a real exploit - and the scanning engine adapts to what is actually in front of it.

→ Tech stack fingerprinting, WAF/CDN detection with adaptive payload evasion

→ Every finding runs through the verification pipeline - PoC attached, not just a severity label

→ Distributed execution across scanner nodes - parallel modules, no single-node bottleneck

WHY PENTESTERRA

Cross-domain correlation: web findings become nodes in the Attack Chain graph together with network and code findings - a medium on a login form and a low on an internal API can be one critical path, not two disconnected tickets.

FREQUENTLY ASKED QUESTIONS

How quickly does Pentesterra find the first vulnerability?

Mean time to first findings is approximately 15 minutes from scan start. A full web and network pentest typically completes in 1.5 to 12 hours depending on target complexity and depth.

Does Pentesterra test business logic vulnerabilities?

Yes. The platform tests for IDOR, broken authorization, mass assignment, bypassable workflows, and state transition flaws. The DevGuard module adds business process detection (BP-PAY-001, BP-AUTH-001) with regulatory scope mapping.

What does the pentest report include?

An executive summary, findings overview, detailed vulnerability entries with CVSS scores, OWASP/MITRE ATT&CK mapping, PCI-DSS compliance impact, evidence and PoC, and prioritized remediation guidance. Available as PDF or via the Reporting API.

Is this automated only, or does a human review it?

Available as part of the continuous platform or as a stand-alone PTaaS engagement with senior pentesters validating critical findings and remediation paths - choose the delivery that matches your program's maturity.

Get your first findings in 15 minutes

Point Pentesterra at a web app or API and watch the scan run live.

info@pentesterra.com
pentesterra.com/web-app-pentest