Pentera AI Attack Engine

AI ADVERSARIAL TESTING YOU CAN TRUST

The Challenge

AI enables adaptive, context-aware adversarial testing, but probabilistic execution introduces new challenges for enterprise security validation and trust.

- **Harder to control:** AI-driven decisions can vary, making test execution more difficult to govern.
- **Difficult to repeat:** Enterprises need validation outcomes that are reproducible, auditable, and trusted.
- **Requires guardrails:** Adversarial testing must remain controlled and non-disruptive, especially in production.

The Pentera AI Advantage:

Pentera combines AI-driven decisioning with deterministic execution, enabling context-aware security validation that remains controlled, traceable, and repeatable.

REPEATABLE VALIDATION

Prove security posture with safe, repeatable attack execution guided by deterministic guardrails.

CONTEXT-AWARE EXECUTION

Test real-world conditions with AI-driven execution and payloads shaped by your environment.

PREDICTABLE COST AT SCALE

Scale AI-powered testing without usage-based pricing or unpredictable compute costs.

Deterministic + AI Execution: Trusted Exposure Validation

Deterministic Attack Engine
Execute attacks safely and consistently with built-in guardrails for repeatable, auditable testing.

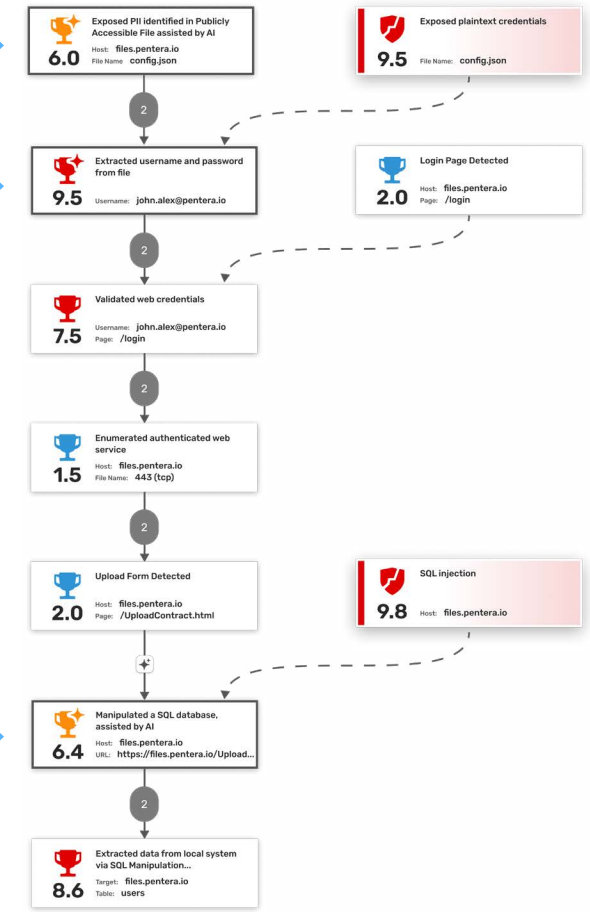
AI-Driven Attack Execution
Tailor adversarial testing to your environment with AI-driven execution flows and automated real-time payload generation.

AI User Interface
Set up tests, explore results, and get context-aware remediation guidance using natural language.

AI Insights & Reporting
Track proven risk, remediation progress, and security outcomes across tests.

AI-Powered Adversarial Testing Without Compromising Control

1. **Identify sensitive data exposure**
2. **Detect and harvest credentials**
3. **Manipulate SQL to validate impact**



ABOUT PENTERA

Pentera is the market leader in AI-powered Security Validation, equipping enterprises with the platform to proactively test all their cybersecurity controls against the latest cyber attacks. Pentera identifies true risk across the entire attack surface, and automatically orchestrates remediation workflows to effectively reduce exposure. The company's security validation capabilities are essential for Continuous Threat Exposure Management (CTEM) operations. Thousands of security professionals around the world trust Pentera to close security gaps before threat actors can exploit them.