DATASHEET

LLM Security Testing

Continuous Penetration Testing for AI

Automatically probe, expose, and remediate vulnerabilities across your LLM applications before attackers do.

THE CHALLENGE WITH LLM SECURITY

Large language models introduce an entirely new class of security risk that traditional application testing tools were never built to handle. As organizations race to embed AI into their products and workflows, the attack surface expands with every deployment, yet most security programmes have no structured way to test LLM behaviour against adversarial inputs, prompt manipulation, or data exposure. A single point-in-time assessment is no longer sufficient when models, prompts, and integrations change continuously.

SOLUTION OVERVIEW

Equixly's offensive security platform delivers automated, continuous penetration testing specifically designed for AI applications.

By simulating the full range of adversarial attack techniques mapped to the OWASP Top 10 for LLMs, Equixly gives security and development teams ongoing, evidence-based visibility into where their models are exposed and exactly what to fix.

KEY CAPABILITIES

- Continuous automated red-teaming against live LLM endpoints
- OWASP Top 10 LLM risk coverage with mapped attack scenarios
- Prompt injection and jailbreak simulation across model types
- Sensitive data and PII leakage detection via adversarial probing
- Actionable remediation guidance prioritised by exploitability

HOW IT WORKS

Connect
Integrate your LLM application endpoint into Equixly in minutes

Attack
Automatically attack LLMs like an attacker, mapped to LLM risks

Expose
Vulnerabilities are surfaced and prioritized with risk insights

Remediate
Actionable fixes delivered within existing workflows

OWASP TOP 10 LLM RISKS

1. **Prompt Injection**
2. **Sensitive Information Disclosure**
3. **Supply Chain**
4. **Data and Model Poisoning**
5. **Insecure Output Handling**
6. **Excessive Agency**
7. **System Prompt Leakage**
8. **Vector and Embedding Weaknesses**
9. **Misinformation**
10. **Unbounded Consumption**

USE CASES

- **AI Product Teams**: Validate LLM safety before and after every release
- **Security Teams**: Extend pen testing programmes to cover AI attack surfaces
- **Compliance & Risk**: Demonstrate due diligence against emerging AI security frameworks
- **Regulated Industries**: Meet AI governance obligations

SEE LLM RISK IN MINUTES

Connect your AI applications and Equixly will surface real, exploitable findings across OWASP LLM risks with the evidence and guidance your team needs to act immediately.

BOOK A DEMO