Dvuln

Addressing the Risks of Untested Technologies

OpenAI Gemini

Secure Your LLM Applications Against Real-World Threats

Implementing new and untested technologies like LLMs comes with significant risks. Dvuln is one of the few companies with a proven public track record of hacking AI/LLM systems.

- Comprehensive LLM Security Coverage

  Modern LLM applications are complex, involving various data inputs, processing mechanisms, and outputs. We evaluate the entire data flow, from training data to deployed models, identifying and mitigating potential security risks.

- Over a Decade of Experience

  Dvuln's pentest team brings over a decade of experience in cybersecurity, applying proven methodologies to assess and enhance the security of LLM applications.

- Innovative Testing Techniques

  If you want a simple vuln scan, there‘s plenty of automated tools that can do that for free, if that‘s all you need then this isn‘t for you.

Dvuln

End-to-end AI & LLM Security Review

OWASP LLM01 Prompt Injection

Your AI system could be manipulated through crafted inputs, causing unintended actions by the LLM.

OWASP LLM03 Training Data Poisoning

Compromised training data can introduce vulnerabilities or biases, compromising your AI's security and effectiveness.

OWASP LLM05 Supply Chain Vulnerabilities

Third-party datasets, pre-trained models, and plugins can introduce vulnerabilities throughout the AI application lifecycle.

OWASP LLM07 Insecure Plugin Design

Plugins with insecure inputs and insufficient access control can result in severe vulnerabilities, including remote code execution.

OWASP LLM09 Over-reliance

Dependence on LLMs without proper oversight can lead to misinformation, legal issues, and security vulnerabilities.

OWASP LLM02 Insecure Output Handling

Unscrutinised LLM outputs may expose backend systems to severe risks like XSS, CSRF, SSRF, and privilege escalation.

OWASP LLM04 Model Denial of Service

Attackers could induce resource-heavy operations, leading to service degradation or high operational costs.

OWASP LLM06 Sensitive Information Disclosure

Your AI might inadvertently reveal confidential data in its responses, leading to unauthorised data access.

OWASP LLM08 Excessive Agency

LLM-based systems might undertake actions with unintended consequences due to excessive permissions.

OWASP LLM10 Model Theft

Unauthorised access or exfiltration of proprietary LLM models can lead to economic losses and compromised competitive advantage.