OWASP® | TOP 10 LLM APPLICATIONS & GENERATIVE AI

genai.owasp.org

LLM and Gen AI Security Solution Landscape Guide

CHEAT SHEET - SERIES

Q1, 2025

https://genai.owasp.org/ai-security-solutions-landscape/

OWASP | TOP 10 LLM APPLICATIONS & GENERATIVE AI

CHEAT SHEET

LLM & GenAI Security Landscape - 2025, Q1

https://genai.owasp.org/ai-security-solutions-landscape/

🟩 Open Source

Operate

aqua
securiti AI Security & Governance
Llama Guard Meta
ZenGuard AI
NRI SECURE AI Blue Team
cisco AI Firewall®
LLM GUARD
BLUETEAM AI
AIM aim security
PRISMA by Palo Alto Networks
TROJ.AI
paloalto networks

Deploy

TROJ.AI
cisco AI Firewall®
BLUETEAM AI
Code Shield Meta
paloalto networks
securiti AI Security & Governance
Operant
PRISMA by Palo Alto Networks

Release

securiti AI Security & Governance
cisco AI Validation
CycloneDX
PRISMA by Palo Alto Networks
LEGIT SECURITY AI-SPM
paloalto networks
aqua

Test & Evaluate

pillar SECURITY
cisco AI Validation
Prompt Fuzzer
promptfoo
aqua
Enkrypt AI
Giskard
Synack
LangCheck
MODELSCAN
securiti AI Security & Governance
CYBERSECEVAL Meta
ZenGuard AI
LLM vulnerability scanner
HARMBENCH
Cobalt
PROTECT AI
WATCHTOWER BY AISHIELD
PRISMA by Palo Alto Networks
MINDGARD
TROJ.AI
Citadel AI
AIShield Powered by Bosch
Cymetrics

Develop & Experiment

Code Shield Meta
Mend.io
TRAIL OF BITS
aqua
cisco AI Validation
snyk
securiti AI Security & Governance
pangea
Operant
PRIVACY Raven
Cloaked AI
TROJ.AI
PRISMA by Palo Alto Networks

Augment, Fine Tune Data

Cloaked AI
securiti AI Security & Governance
UNSTRUCTURED.IO
BLUETEAM AI
PRISMA by Palo Alto Networks

Scope & Plan

MITRE ATLAS
BLUETEAM AI
Seezo
paloalto networks
STRIDE GPT
pillar SECURITY
securiti
PRISMA by Palo Alto Networks

Monitor

aqua
cisco AI Validation
AIM aim security
BLUETEAM AI
AIShield Powered by Bosch
HIDDENLAYER
LAKERA
Meta Prompt Guard
Operant
paloalto networks
PROTECT AI
securiti
splx AI
TROJ.AI
ZenGuard AI

Govern

AIM aim security
cisco AI Validation
BLUETEAM AI
Lasso SECURITY
paloalto networks
PRISMA by Palo Alto Networks
Prompt Security
securiti
Tumeryk AI GUARD
unbound security
AI VERIFY FOUNDATION

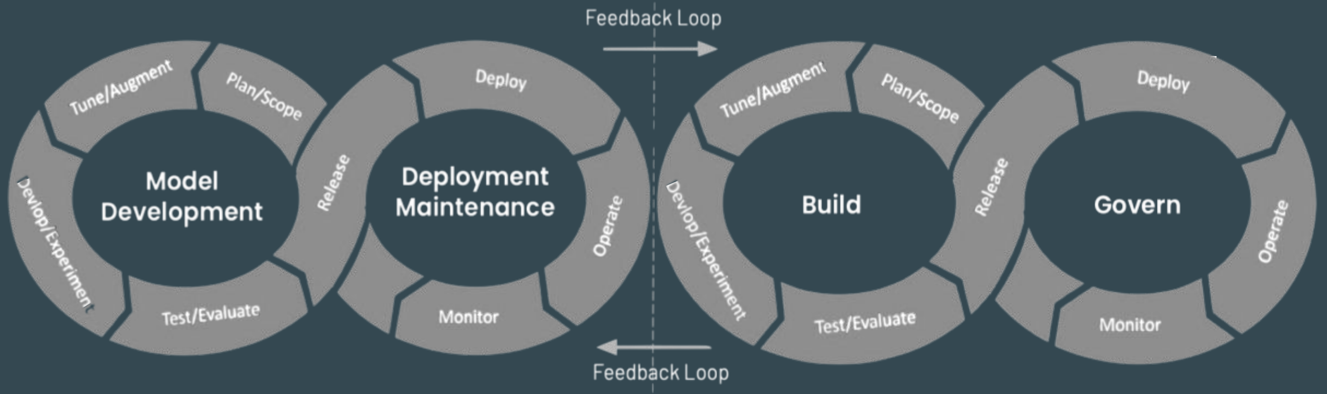
Source; OWASP Gen AI Security Solutions Landscape Guide 2025. Q1

OWASP | TOP 10 LLM APPLICATIONS & GENERATIVE AI

CHEAT SHEET

LLM and Gen AI App SecOps Framework

https://genai.owasp.org/ai-security-solutions-landscape/



The OWASP LLMSecOps Framework was captured to help better align LLMOps processes and the security roles and dependencies for each stage. While LLMOps and MLOps are rooted in the same foundational principles of lifecycle management, they can diverge significantly in their focus and requirements, as one is focused primarily on model development, while the other extends DevOps to include support for various LLM, Gen AI and application patterns.

Plan & Scope

- Access Control and Authentication Planning
- Compliance and Regulatory Assessment
- Data Privacy and Protection Strategy
- Early Identification of Sensitive Data
- Third-Party Risk Assessment (Model, Provider, etc.)
- Threat Modeling

Augment & Fine Tune Data

- Data Source Validation
- Secure Data Handling
- Secure Output Handling
- Adversarial Robustness Testing
- Model Integrity Validation (ex: serialization scanning for malware)
- Vulnerability Assessment

Dev & Experiment

- Access, Authentication, and Authorization (MFA)
- Experiment Tracking
- LLM & App Vuln Scanning
- Model and Application Interaction Security
- SAST/DAST
- Secure Coding Practices
- Secure Library/Code Repository
- Software Comp Analysis

Test & Evaluation

- Adversarial Testing
- Application Security Orchestration and Correlation
- Bias and Fairness Testing
- Final Security Audit
- Incident Simulation, Response Testing
- LLM Benchmarking
- Penetration Testing
- IAST
- Vulnerability Scanning

Release

- AI/ML Bill of Materials (BOM)
- Digital Model\Dataset Signing
- Model Security Posture Evaluation
- Secure CI/CD pipeline
- Secure Supply Chain Verification
- Static and Dynamic Code Analysis
- User Access Control Validation
- Model Serialization Defenses

Deploy

- Compliance Verification
- Deployment Validation
- Digital Model\Dataset Verification
- Encryption, Secrets management
- Multi-factor Authentication
- Network Security Validation
- Secure API Access
- Secure Configuration
- User and Data Privacy Protections

Operate

- Adversarial Attack Protection
- Automated Vuln Scanning
- Data Integrity and Encryption
- LLM Guardrails
- LLM Incident Detection and Response
- Patch Management
- Privacy, Data Leakage Protection
- Prompt Security
- Runtime Self-Protection
- Secure Output Handling

Monitor

- Adversarial Input Detection
- Model Behavior Analysis
- AI/LLM Secure Posture Management
- Patch and Update Alerts
- Regulatory Compliance Tracking
- Security Alerting
- Security Metrics Collection
- User Activity Monitoring
- Observability
- Data Privacy and Protection
- Ethical Compliance

Govern

- Bias and Fairness Oversight
- Compliance Management
- Data Security Posture Management
- Incident Governance
- Risk Assessment and Management
- User/Machine Access audits

Source; OWASP Gen AI Security Solutions Landscape Guide 2025. Q1

Project Sponsors

Gold HIDDENLAYER

Gold paloalto NETWORKS

Gold snyk

Gold Mend.io

Silver Cobalt

Silver pangea

Silver Prompt

Silver Synack

Silver Lasso SECURITY

Silver securiti

Silver PROMPTARMOR

Project Supporters

Accenture	BeDisruptive	Comcast	GitHub	Lakera	NuBinary	Securiti	VE3
AddValueMachine Inc	Bit79	Complex Technologies	Google	Lasso Security	Palo Alto Networks	Securiti AI	WhyLabs
Aeye Security Lab Inc.	Blue Yonder	Credal.ai	GuidePoint Security	Layerup	Palosade	See-Docs & Thenavigo	Yahoo
AI informatics GmbH	BroadBand Security, Inc.	Databook	HackerOne	Legato	Praetorian	ServiceTitan	
AI Village	BuddoBot	DistributedApps.ai	HADESS	Linkfire	Preamble	SHI	
aigos	Bugcrowd	DreadNode	IBM	LLM Guard	Precize	Smiling Prophet	
Aon	Cadea	DSI	iFood	LOGIC PLUS	Prompt Security	Snyk	
Aqua Security	Check Point	EPAM	IriusRisk	MaibornWolff	PromptArmor	Sourcetoad	
Astra Security	Cisco	Exabeam	IronCore Labs	Mend.io	Pynt	Sprinklr	
AVID	Cloud Security Podcast	EY Italy	IT University Copenhagen	Microsoft	Quiq	stackArmor	
AWARE7 GmbH	Cloudflare	F5	Kainos	Modus Create	Red Hat	Tietoevry	
AWS	Cloudsec.ai	FedEx	KLAVAN	Nexus	RHITE	Trellix	
BBVA	Coalfire	Forescout	Klavan Security Group	Nightfall AI	SAFE Security	Trustwave SpiderLabs	
Bearer	Cobalt	GE HealthCare	KPMG Germany FS	Nordic Venture Family	Salesforce	U Washington	
BeDisruptive	Cohere	Giskard	Kudelski Security	Normalyze	SAP	University of Illinois	

View the Latest Project Sponsors and Supporters on the Web: https://genai.owasp.org/supporters/