

# AI Penetration Testing

TOKEN LEAK  
|  
INJECTION VECTOR  
|  
RESPONSE DEVIATION

One AI plays.  
Another records.

**Register Now**

**CONTACT US**  
FOR MORE DETAILS



+91 95993-87841



[www.ignitetechnologies.in](http://www.ignitetechnologies.in)

# TABLE OF CONTENTS

01

## AI AND LLM SECURITY MODULES

Introduction to Large Language Models (LLMs)  
Overview of LLMs, their capabilities, limitations, and real-world applications

02

## LLM ARCHITECTURE

Deep dive into the structural design and functioning of large language models, including training, tokenization, and inference mechanisms.

03

## LLM SECURITY PRINCIPLES

Core security concerns and challenges specific to the deployment and operation of LLMs.

04

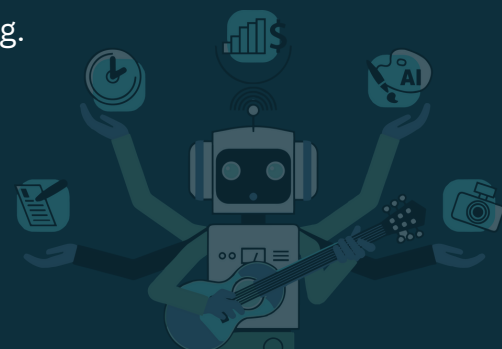
## DATA SECURITY IN AI SYSTEMS

Best practices for safeguarding training and inference data, including encryption, anonymization, and access control.

05

## MODEL SECURITY

Strategies to protect AI models from threats such as model inversion, extraction, and poisoning.



## TABLE OF CONTENTS

06

### INFRASTRUCTURE SECURITY

Ensuring the underlying hardware, cloud environments, and networking components supporting LLMs are secure and resilient.

07

### OWASP TOP 10 FOR LLMS

Application of the OWASP Top 10 security vulnerabilities tailored to LLM-based systems and AI integrations.

08

### LLM INSTALLATION AND DEPLOYMENT

Step-by-step guide for setting up and deploying LLMs securely in development and production environments.

09

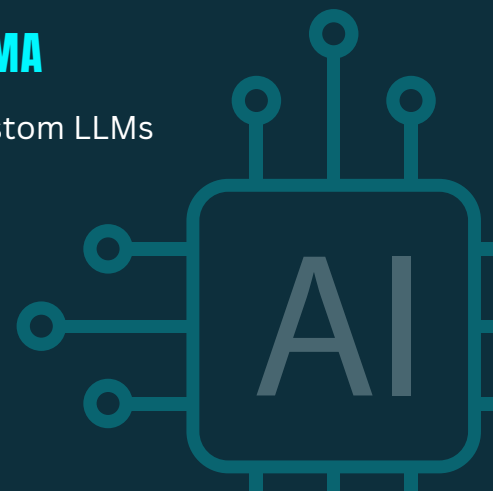
### MODEL CONTEXT PROTOCOL (MCP)

Introduction to MCP and its role in maintaining safe and consistent context handling in LLM applications.

10

### PUBLISHING YOUR MODEL USING OLLAMA

Securely publishing and managing your custom LLMs using the Ollama platform.



## TABLE OF CONTENTS

11

### INTRODUCTION TO RETRIEVAL-AUGMENTED GENERATION (RAG)

Understanding the RAG architecture and its use in combining LLMs with external knowledge sources.

12

### MAKING YOUR AI APPLICATION PUBLIC

Guidelines and precautions for exposing AI services to external users or clients.

13

### TYPES OF ENUMERATION USING AI

Exploration of enumeration techniques in cybersecurity powered by AI for reconnaissance and threat identification.

14

### PROMPT INJECTION ATTACKS

Analysis of prompt injection vulnerabilities and techniques for prevention and detection.

15

### EXPLOITING LLM APIS: REAL-WORLD BUG SCENARIOS

Examination of vulnerabilities and bugs commonly found in LLM APIs, with practical examples.

## TABLE OF CONTENTS

16

### PASSWORD LEAKAGE VIA AI MODELS

Risks and real-world cases where LLMs have unintentionally leaked sensitive credentials.

17

### INDIRECT PROMPT INJECTION TECHNIQUES

Advanced manipulation strategies to indirectly influence model behavior through user-generated content.

18

### MISCONFIGURATIONS IN LLM DEPLOYMENTS

Identifying and mitigating common configuration errors that can lead to security breaches.

19

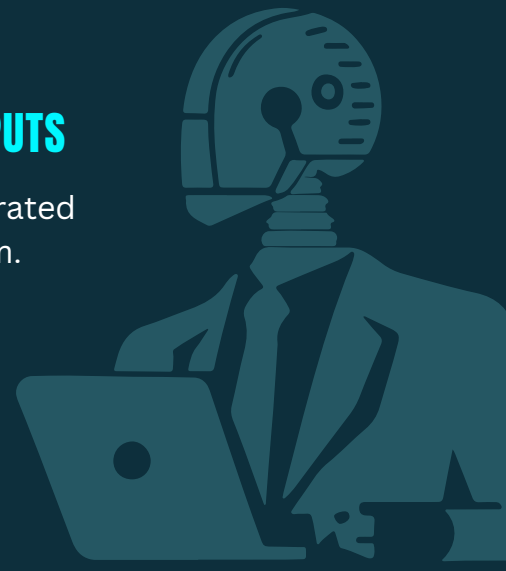
### EXPLOITATION OF LLM APIS WITH EXCESSIVE PRIVILEGES

Assessing how overly permissive APIs can be abused to perform unauthorized actions.

20

### CONTENT MANIPULATION IN LLM OUTPUTS

Techniques used to manipulate LLM-generated responses and how to defend against them.



## TABLE OF CONTENTS

21

### DATA EXTRACTION ATTACKS ON LLMS

Investigating attacks aimed at extracting training data or sensitive information from LLMS.

22

### SECURING AI SYSTEMS

Holistic approaches to AI system security, covering model, data, access, and deployment layers.

23

### SYSTEM PROMPTS AND THEIR SECURITY IMPLICATIONS

The role of system-level prompts and their influence on model behavior and output integrity.

24

### AUTOMATED PENETRATION TESTING WITH AI

Leveraging AI and LLMS for conducting automated security assessments and vulnerability discovery.



CONTACT US



+91 95993-87841



[www.ignitetechnologies.in](http://www.ignitetechnologies.in)