R3KON GPT

Security Intelligence & Assessment Assistant

Aethar Tech

1. Overview of R3KON GPT

R3KON GPT is an offline-first, security-focused AI assistant designed to help users analyze, understand, and improve cybersecurity posture through intelligent assessment, explanation, and reporting.

The system emphasizes:

- **Security awareness**
- **Risk identification**
- **Defensive best practices**
- **Clear technical explanations**

R3KON GPT is not designed to perform active attacks or system exploitation. Instead, it supports secure development, monitoring, and decision-making through AI-assisted analysis.

2. Core Functional Architecture

R3KON GPT operates as a modular toolkit, where each cybersecurity function is independent but interconnected through a shared AI reasoning layer.

Key architectural principles:

- **Local processing by default**
- **User-controlled inputs**
- **Structured outputs**
- **Minimal data retention**

3. Existing Cybersecurity Functions

3.1 Code Scanner

Purpose:
The Code Scanner analyzes source code to identify potential security weaknesses, unsafe patterns, and poor practices that may introduce risk into applications.

How it works:

- **The user provides code snippets or files.**
- **R3KON GPT examines logic flow, input handling, and sensitive data usage.**
- **Findings are categorized by risk type and severity.**

What it provides:

- **Identification of risky coding patterns**
- **Contextual explanations of why a pattern is unsafe**
- **High-level guidance on safer coding approaches**

Why it matters:
Many vulnerabilities originate from insecure coding decisions. This function helps developers detect issues early in the development lifecycle, reducing long-term risk.

3.2 API Analyzer

Purpose:
The API Analyzer evaluates API design and configuration to assess security posture, exposure risks, and misuse potential.

How it works:

- **The user describes or provides API specifications, endpoints, or responses.**
- **The system reviews authentication logic, data exposure, and access patterns.**

What it provides:

- **Analysis of access control design**
- **Detection of excessive data exposure risks**
- **Observations on API security hygiene**

Why it matters:
APIs are a major attack surface in modern systems. Understanding design weaknesses early helps prevent data leaks and abuse.

3.3 Password Check

Purpose:
The Password Check evaluates password strength and authentication practices without storing or transmitting credentials.

How it works:

- **The analysis runs locally and ephemerally.**
- **The system evaluates password length, complexity, and predictability.**

What it provides:

- **Strength classification (weak, moderate, strong)**
- **Explanation of entropy and predictability**
- **Safer password construction guidance**

Why it matters:
Weak authentication remains one of the most common causes of security incidents. This tool promotes secure identity practices while preserving privacy.

3.4 Log Analyzer

Purpose:
The Log Analyzer helps users interpret system and application logs to identify unusual behavior, errors, or security-relevant events.

How it works:

- **Users provide log files or excerpts.**
- **R3KON GPT classifies entries and highlights patterns.**

What it provides:

- **Event categorization (authentication, system, application)**
- **Timeline-based summaries**
- **Indicators of abnormal or repeated behavior**

Why it matters:
Logs often contain early warning signs of incidents. This function helps users understand logs without requiring deep SOC experience.

3.5 OWASP Check

Purpose:
The OWASP Check maps application characteristics against widely accepted web security risk categories to provide structured risk awareness.

How it works:

- **The user describes their application type and features or pastes the websites URL.**
- **R3KON GPT aligns this information with OWASP risk categories.**

What it provides:

- **Risk profiling aligned to OWASP principles**
- **Prioritization of common security concerns**

- **High-level mitigation guidance**

Why it matters:
OWASP standards are globally recognized. This function helps developers and teams speak a common security language.

4. Memory and Session Handling

4.1 Chat History(To be added)

R3KON GPT supports local session-based chat history, allowing users to:

- **Resume previous assessments**
- **Track decisions and findings**
- **Maintain continuity across analyses**

Session data is stored locally and remains under user control.

4.2 Context Awareness

Within a session, R3KON GPT maintains context such as:

- **Application type**
- **Security focus areas**
- **Previously identified risks**

This enables more consistent and relevant analysis across tools.

5. System Strengthening Areas (Non-Offensive)

To enhance reliability, usability, and trustworthiness, the following areas require continued development:

5.1 Explanation Consistency

- **Standardized output formats across all tools**
- **Clear severity definitions**
- **Consistent terminology**

5.2 Data Handling Controls

- **Explicit user consent for saving summaries**
- **Automatic redaction of sensitive information**
- **Session-based memory expiration**

5.3 Knowledge Refresh

- **Regular updates to security standards and best practices**
- **Alignment with evolving OWASP guidance**

- **Improved contextual accuracy over time**

6. Online Update Capability

When internet connectivity is available, R3KON GPT can:

- **Check for updated rules, prompts, and knowledge files**
- **Download verified updates without affecting user data**
- **Remain fully functional offline if updates are unavailable**

This ensures the system remains current without constant connectivity.

7. Positioning Summary

R3KON GPT is positioned as:

- **A security assessment and learning assistant**
- **A developer and student support tool**
- **A privacy-conscious, offline-capable system**

It focuses on understanding, prevention, and improvement, not exploitation.