Title: Enhanced Web Application and Server Security Using Secure Packet Evaluation and Logging System Using OpenAI GPT-4

Submitted by Team 9.3:

Raghuttama Padakandla

Aviral Avesh

Abstract:

This project implements a Flask-based server with integrated middleware, introducing an innovative method to strengthen online application security. To evaluate the possible maliciousness of incoming packets, the system uses a two-step validation procedure that makes use of OpenAI's GPT-4 capabilities.

In the first stage, incoming packets are received by the Flask server and sent to OpenAI GPT-4 for analysis using middleware. In order to produce a score on a scale of 1 to 10, the system consults GPT-4 to determine the possibility of malicious intent. Packets are marked as possibly malicious if they score more than a set threshold (for example, 6).

The system then logs pertinent data, such as the packet content, IP address, and GPT-4 assessment score, into a safe database. This thorough logging system makes post-analysis easier and enables the detection of trends or new dangers.

Only the IP address is recorded for non-malicious packets in order to protect privacy while still revealing potential attack vectors. This two-tiered logging strategy provides a compromise between security and user privacy while enabling a sophisticated analysis of online traffic.

The suggested solution improves the overall security posture of online applications by utilizing OpenAI GPT-4 to provide proactive threat detection and response tactics. The system's modular structure enables scalability and flexibility in response to changing cybersecurity problems.