논문 번호 : CFP-786

제목 : A Lightweight Software Solution for Log Analysis

저자 : 이시헌, 김지윤, 김서현, 황지온
소속 : 협성대학교 이공대학 소프트웨어공학과

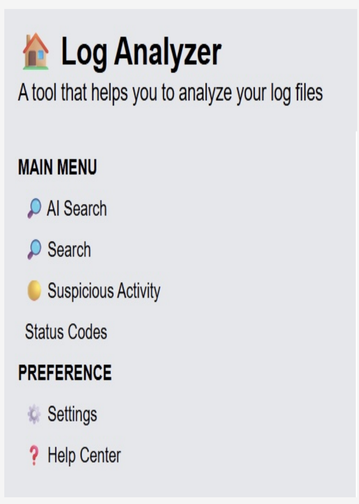
1. 연구 배경 및 목적

고도화되는 사이버 위협과 AI 기술 발달이 맞물리며, AI를 활용한 능동 공격 감지 시스템 구축이 늘어나고 있다. 하지만 이러한 시스템의 도입은 너무 큰 컴퓨팅 자원과 비용을 요구한다. 한편, 많은 GUI 기반 로그 분석 소프트웨어는 실시간 분석 및 경고를 보장하지 못하거나, 웹 로그에 대한 백업 기능을 제공하지 못하며, 설치 과정이 복잡하고 인터페이스가 사용자 친화적이지 않은 경우[1)]가 많다. 그러므로 본 연구는, **'쉽게 설치하여 사용 가능한 경량화 된 범용 로그 해석 도구' 개발을 목적으로 한다.** 이는, 적은 컴퓨팅 자원을 소비하며, 적은 비용으로 운용할 수 있고, 실시간 분석을 보장하며, 웹 로그에 대한 안전한 백업 기능을 제공하며, 설치 과정이 간단하고, 인터페이스가 사용자 친화적인 웹 기반의 로그 분석 도구를 말한다.

1) ModSecurity [1], Web Attack Defender [2], Wash [3] 등의 오픈소스 기반의 로그 분석 솔루션이 이미 존재하지만, 상술한 문제를 갖고 있다.

2. 소프트웨어 설계 및 구현

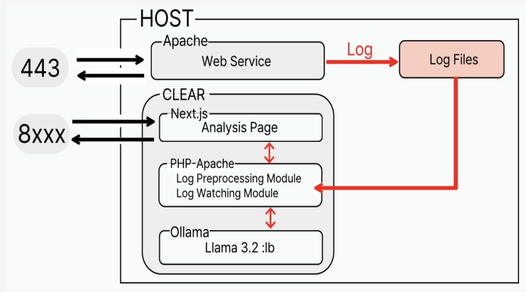
2.1 사용자 인터페이스

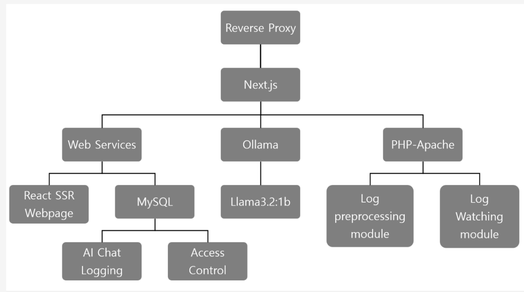


각각의 기능으로 이동하는 네비게이션 바를 구현한다.

- AI Search
  로그를 컨텍스트로 하는 챗봇.
- Search
  전체 로그를 대상으로 하는 키워드 검색 페이지.
- Suspicious Activity
  정규식에 의해 감지된 이상 사용자를 표시하는 페이지.
- Status Code
  상태코드별로 분류된 로그에 대하여 보안 보고서를 출력하는 페이지.
- Settings
  전역 설정 페이지.
- Help Center
  도움말 페이지.

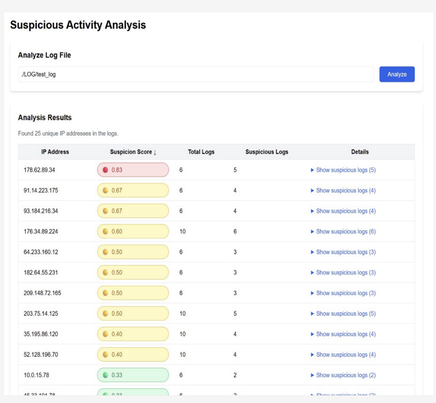
2.2 컨테이너 기반 로그 복제 및 전처리 과정

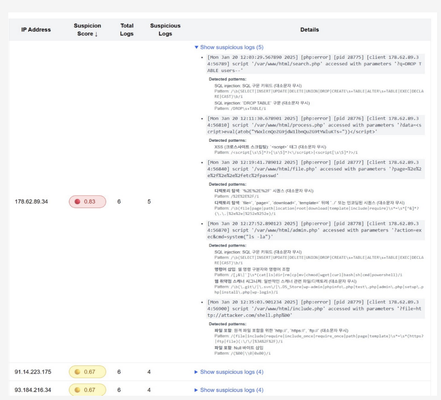




역할을 분리한 다수의 컨테이너로 목표를 달성한다. 리버스 프록시 요청을 처리하는 핵심 컨테이너로 Next.js를 사용하고, 해당 컨테이너와 동일 네트워크로 연결된 다수의 컨테이너로 서비스를 구현한다. Ollama를 사용하여 Llama3.2:1b 모델을 구동시키고, 해당 모델에 입력하기 위한 로그와 Next.js 웹 페이지에서 호출할 수 있는 로그 전처리 모듈을 php-apache 컨테이너로 구축한다. 추가로 Next.js에서 사용할 수 있는 RDBMS container 또한 구축한다. 그리하여 **전체 시스템을 한 줄의 코드로 설치 가능하다.**

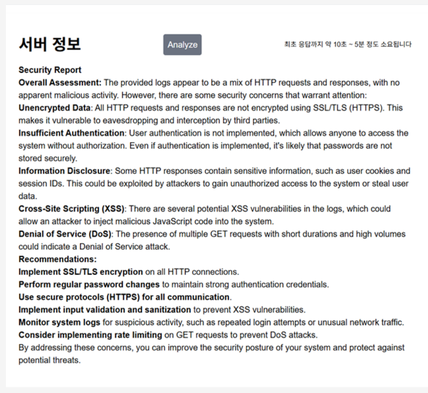
2.3 정규식 기반 공격 감지

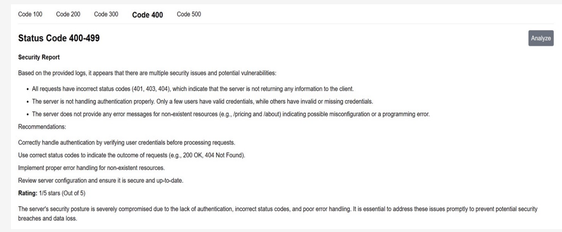




IP별로 그룹화된 전체 로그를 대상으로, 개별 로그에 준비된 정규식 세트를 대조하여 위험도를 계산한다. 각 그룹의 로그에 대하여, 80% 이상 위험한 로그로 판단되었을 때 붉은 색으로, 30% 이상 위험한 로그로 판단되었을 때 노란색으로, 그 미만은 녹색으로 표시한다.

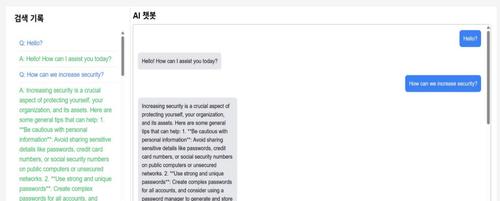
2.4 Local LLM을 사용한 조치 제안





메인페이지에서는 접속자 수를 그래프로 출력하고, 서버의 전체 로그를 대상으로 하는 종합 보안 보고서를 출력한다. 'Status Code' 페이지에서는 상태코드별로 분류된 로그에 대하여 종합 보안 보고서를 출력한다.

2.5 검색 기능과 AI 챗봇



php-apache 컨테이너 내부에 수집된 전체 로그를 대상으로 키워드 검색 기능을 지원한다.
한편, 전체 로그를 컨텍스트로 하는 AI 챗봇에게 질문을 해 볼 수 있다.

2.6 실시간 경고 페이지

새로운 로그가 컨테이너 내부에 병합될 때 마다, 해당 로그가 php-apache 컨테이너 내부의 SQLite3 DB로 저장된다. 신규 로그가 DB에 저장될 때 마다, 실시간 경고 페이지에서 정상 로그인지 위험 로그인지 판별하고, 위험 로그의 경우 붉은 색으로 표시하며 경고한다.

3. 결론 및 향후 연구 방향

- 경량의 로컬 LLM과 정규식에 기반한 로그 분석을 통해, 웹 공격을 능동적으로 감지하고 시각화 하여 제시하는 소프트웨어 개발이 완료되었다.
- 소규모 사업체 혹은 개인이 저비용으로 적용하여 사용 가능한 경량 로그 분석 툴의 배포를 통하여, 개인과 사회 차원에서 발생 가능한 보안사고를 최소화할 수 있을 것이다.
- 공격 징후를 탐지하는 정규식 세트를 개선할 예정이다.
- 추후 BERT 등의 언어모델을 통한 로그 분석 연구 [4]를 수용하여, 감지 정확도를 개선할 예정이다.
- 다른 연구 [5]에서 제안하는 DDoS 감지 체계를 추가할 예정이다.

참고문헌

[1] https://docs.varnish-software.com/varnish-waf/owasp-crs/
[2] 박재연 외, "리눅스 아파치 웹 서버 실시간 로그 분석을 통한 공격 탐지 프로그램 개발", 정보과학회 컴퓨팅의 실제 논문지, Vol.24, No.4, pp. 190-197, 2018.
[3] https://wazuh.com/
[4] 조영복 외, "웹 방화벽 로그 분석을 통한 공격 분류: AutoML, CNN, RNN, ALBERT", Journal of The Korea Institute of Information Security & Cryptology, Vol.34, No.4, Aug, 2024.
[5] 이석우 외, "웹 모니터링 기반 암호화 웹트래픽 공격 탐지 시스템", 한국정보통신학회논문지, Vol.25, No.3, pp. 449-455, Mar, 2021.