

AI기반 웹취약점 진단 시스템

(AI-Based Web Vulnerability Diagnosis System)

팀 명	Log X
지도교수	유승재 교수님
팀 원	박 성 준 (팀장) 김 정 민 박 지 우 윤 서 연

2025. 11. 4

중부대학교 미래융합공학부 정보보호학전공

목 차

1. 서론
 - 1.1 연구 배경
 - 1.2 연구 필요성
 - 1.3 연구 목적 및 주제선정 이유
2. 관련 연구
 - 2.1 기존 로그 분석 방법
 - 2.2 AI를 활용한 로그 이상 탐지 연구
 - 2.3 로그 수집·검색 기술(Elasticsearch 등)
 - 2.4 웹 기반 로그 분석 시스템 및 시각화
3. 본론
 - 3.1 시스템 구성
 - 3.2 학습·평가 대상 공격 유형
4. 결론
 - 4.1 결론 및 기대효과
 - 4.2 향후 계획
5. 참고 자료
6. 별첨
 - 6.1 폼 보드
 - 6.2 프로젝트 소개
 - 6.3 팀 소개
 - 6.4 발표 자료

1. 서론

1.1 연구 배경

현대의 IT 환경에서는 시스템, 네트워크, 애플리케이션 등 다양한 영역에서 방대한 양의 로그데이터가 지속적으로 발생한다. 이러한 로그데이터는 단순한 기록 이상의 의미를 가지며, 보안 침해 시도 탐지, 시스템 장애 예측, 서비스 성능 최적화 등 다양한 목적으로 활용될 수 있다. 그러나 기존 로그 분석방식은 다음과 같은 한계를 가지고 있다.

수동 분석의 비효율성으로 인해 사람이 직접 로그를 검토하기에는 데이터의 양이 너무 많아 실시간 대응이 어렵다. 실시간 탐지의 어려움으로 기존 로그 관리 시스템은 공격이나 장애를 즉시 식별하지 못하고 사후 분석에 그치는 경우가 많다. 또한 패턴 인식의 한계로 기존 룰 기반 탐지 방식은 새로운 보안 위협이나 변종 공격을 효과적으로 감지하기 어렵다. 이러한 한계로 인해 AI기반의 지능적이고 자동화된 로그 분석 기술의 필요성이 대두되고 있다.

1.2 연구 필요성

최근 기업과 기관의 디지털 전환이 가속화되면서 클라우드, 마이크로서비스, IoT 기기 등 IT 인프라가 급격히 복잡해지고 있다. 이러한 복잡성은 시스템 간의 상호작용을 증가시키고, 그 결과로 생성되는 로그데이터의 규모와 다양성 또한 폭발적으로 증가하고 있다. 로그데이터는 시스템의 상태를 이해하고, 장애를 신속하게 진단하며, 보안 위협을 조기에 탐지하는데 핵심적인 자원이다.

그러나 이러한 방대한 로그를 사람이 직접 검토하고 분석하는 기존의 방식은 더 이상 유효하지 않다. 특히 다음과 같은 문제점들이 존재한다. 로그의 양이 너무 많아 이상 징후를 실시간으로 탐지하기 어렵고, 사람이 수동으로 분석할 경우 오탐 및 누락 가능성이 높으며, 문제 발생 후 원인 분석에 과도한 시간과 인력이 소요된다. 이러한 비효율성은 결과적으로 서비스 장애의 장기화나 보안 사고의 골든 타임 상실로 이어질 수 있다. 따라서 AI를 활용한 자동화된 로그 분석 시스템은 이러한 한계를 해결할 수 있는 핵심 기술적 대안으로 주목받고 있다. AI 모델을 적용함으로써 로그데이터 내에서 패턴을 학습하고, 새로운 유형의 위협이나 이상 징후를 빠르게 감지할 수 있으며, 이를 기반으로 보안 및 운영 효율성의 극대화가 가능하다.

1.3 연구 목적 및 주제선정 이유

본 연구의 목적은 AI 기술을 활용하여 대규모 로그데이터를 자동으로 분석하고, 웹 서비스에서 발생하는 보안 취약점을 탐지·진단할 수 있는 웹 기반 로그 분석 시스템을 구축하는 것이다. 현대 웹 환경은 다양한 네트워크 트래픽과 수많은 사용자 요청이 오가며, 이 과정에서 수집되는 로그 데이터는 방대하고 복잡하다. 이러한 로그 데이터는 서비스 운영 상태를 파악하거나 보안 이상 징후를 감지하는데 매우 중요한 자원이지만, 전통적인 수동 분석 방식으로는 데이터의 양과 속도를 감당하기 어렵다. 특히, 공격자의 기법이 고도화되고 자동화됨에 따라 관리자가 모든 이벤트를 직접 점검하는 것은 비효율적이며, 실제 공격 발생 시 신속한 대응이 어렵다는 문제가 존재한다.

이러한 한계를 극복하기 위해 본 연구는 AI 모델을 도입하여 로그데이터 내에서 정상 패턴과 비정상 패턴을 구분하고, 공격 행위를 탐지할 수 있는 구조를 구현하고자 한다. 특히 SQL injection, XSS(Cross-Site Scripting) 등의 대표적인 웹 공격 유형을 학습 데이터를 활용하여 AI가 패턴을 자동 탐지하는 것을 목표로 한다. 또한, 본 연구는 Elasticsearch를 활용한 로그 수집·검색 구조를 설계하고, 이를 AI 모델과 결합하여 보안 이벤트를 조기에 탐지할 수 있는 효율적인 분석 체계를 구축하고자 한다. 이러한 시스템은 로그 분석의 자동화 및 효율화를 실현함과 동시에, 운영자의 부담을 줄이며, 보안 위협에 대한 대응 능력 향상을 기대할 수 있다.

본 연구를 통해 개발되는 AI 기반 웹 취약점 진단 시스템은 로그 분석 도구를 넘어 보안 위협 대응 자동화 시스템으로 발전할 수 있는 기반을 마련한다. 사용자는 웹 인터페이스를 통해 공격 유형별 탐지 결과를 쉽게 확인할 수 있으며, 시스템은 지속적인 학습을 통해 탐지 정확도를 높여 나갈 수 있다. 이로써 더 적은 인력과 시간으로 보안 관제를 수행할 수 있으며, 이상 탐지 및 빠른 대응이 가능한 보안 환경을 구축할 수 있다.

2. 관련 연구

2.1 기존 로그 분석 방법

로그 데이터는 서버, 네트워크 장비, 애플리케이션 등 다양한 IT 인프라에서 지속적으로 생성되며, 시스템의 성능을 모니터링하고 보안 이벤트를 탐지하는 핵심 정보 자원으로 활용된다. 기존의 로그 분석 방식은 주로 수동 검토 또는 룰 기반 분석에 의존하였다. 룰 기반 분석은 사전에 정의된 규칙이나 조건에 따라 특정 이벤트를 탐지하는 방식으로 구현이 단순하고 명확하다는 장점이 있지만 다음과 같은 한계가 존재한다. 첫째, 새로운 유형의 공격이나 예상치 못한 이상 패턴을 탐지하기 어렵다. 사전에 정의되지 않은 이벤트는 규칙에 걸리지 않기 때문에 탐지가 불가능하다. 둘째, 대규모 로그 데이터를 사람이 직접 분석하기에는 한계가 있다. 로그 발생 속도가 초당 수천~수만 건에 이르는 환경에서는 수동 검토로 실시간 대응이 불가능하다. 마지막으로 운영 효율성 저하 및 인적 오류 가능성이 높다. 관리자가 모든 로그를 일일이 확인해야 하기 때문에 시간과 인력이 많이 소모되며, 실수로 이상 징후를 놓칠 위험도 존재한다. 이러한 한계는 서비스 장애나 보안 사고 발생 시 원인 파악과 대응이 지연되는 결과를 초래할 수 있다.

2.2 AI를 활용한 로그 이상 탐지 연구

최근에는 머신러닝(ML)과 딥러닝(DL) 기술의 발전으로, 로그 데이터 분석에 인공지능을 적용하려는 연구가 활발히 진행되고 있다. AI 기반 로그 분석의 핵심 아이디어는 ‘정상 로그의 패턴을 학습한 뒤, 그와 다른 형태의 로그를 이상치로 탐지하는 것’이다. 대표적인 비지도 학습 기반 알고리즘으로는 Isolation Forest, Autoencoder, LSTM(Long Short-Term Memory) 모델 등이 있다. Isolation Forest는 이상치를 데이터 공간에서 고립시키는 방식으로 빠르고 효율적인 탐지가 가능하다. Autoencoder는 입력 데이터를 압축 후 복원하면서 재구성 오차를 측정하여, 정상 패턴과 다른 로그를 탐지할 수 있다. LSTM은 시계열 로그 데이터를 처리하는데 강점을 가지며, 로그 발생 순서의 패턴을 학습해 시간적 이상 행동을 탐지할 수 있다.

이러한 접근 방식은 기존 룰 기반 시스템보다 새로운 공격 패턴이나 비정상 이벤트를 유연하게 감지할 수 있다는 점에서 큰 장점이 있다. 또한 모델 학습 이후에는 대량의 로그를 실시간으로 자동 분석할 수 있어 운영 효율성과 정확도 모두 향상할 수 있다.

2.3 로그 수집 및 검색 기술

로그 분석의 정확성과 효율성은 데이터를 얼마나 잘 수집하고 관리하느냐에 달려 있다. 이를 위해 현재 가장 널리 사용되는 오픈소스 도구는 Elasticsearch, Logstash, Kibana (일명 ELK 스택)이다. 효율적인 저장과 검색을 위해 Elasticsearch, Logstash, Kibana와 같은 오픈소스 기술이 활용된다. Elasticsearch는 분산형 검색 및 분석 엔진으로, 로그 데이터를 JSON 문서 형태로 저장하고 Inverted Index 구조를 통해 빠른 검색과 집계를 지원한다. Logstash는 다양한 소스로부터 로그를 수집하고, 필터링 및 전처리 과정을 수행한 후 Elasticsearch로 전송하는 역할을 담당한다. Kibana는 저장된 로그 데이터를 시각화하여, 관리자가 대시보드를 통해 실시간으로 시스템 상태를 모니터링할 수 있도록 도와준다.

이러한 ELK 스택은 로그 관리의 표준적인 구조로 자리 잡았으며, 대규모 로그 처리와 실시간 분석에 매우 효과적이다. 따라서 효율적인 로그 수집 및 검색 시스템은 AI 기반 이상 탐지의 기반이 되며, 본 연구에서도 Elasticsearch를 중심으로 이러한 기술을 적용한다.

2.4 웹 기반 로그 분석 시스템 및 시각화

웹 기반 로그 분석 시스템은 사용자가 웹 환경에서 실시간으로 로그를 확인하고, 분석 결과를 시각화된 형태로 제공받을 수 있는 시스템을 의미한다. Kibana와 같은 기존 시각화 도구는 시간대별 이벤트 그래프, 히트맵, 로그 빈도 분석 등의 기능을 제공하지만, AI 기반 이상 탐지 기능은 직접적으로 제공하지 않는 한계가 있다. 최근 연구에서는 이러한 한계를 극복하기 위해, AI 모델과 웹 시각화 기술을 결합한 통합 로그 분석 시스템이 활발히 개발되고 있다. AI가 로그의 이상 여부를 판별하고 웹 대시보드에서 탐지된 이벤트를 시각화하여 사용자가 직관적으로 결과를 확인할 수 있도록 하는 형태이다.

본 연구에서는 이러한 흐름을 기반으로, Elasticsearch를 통한 로그 저장 및 검색 구조와 AI 기반 이상 탐지 모델 그리고 React 기반 웹 시각화 인터페이스를 결합한 로그 분석 시스템을 구현하였다. 이를 통해 로그 분석 과정을 자동화하고, 관리자에게 실시간으로 분석 결과를 제공하여 운영 효율성과 보안 대응 능력을 동시에 향상하는 것을 목표로 한다.

3. 프로젝트 내용

3.1 시스템 구성

본 시스템은 웹 기반 인터페이스에서 로그를 수집·전송하고, 수집된 로그를 Elasticsearch에 저장한 뒤 AI 모델로 이상 탐지를 수행하여 결과를 시각화하는 전체 파이프라인으로 구성된다. 주요 구성 요소는 다음과 같다.

1) 웹페이지 (로그인 및 로그 전송)

- ①사용 목적: 사용자가 서비스에 로그인하여 로그데이터를 업로드하거나 실시간으로 전송할 수 있는 인터페이스를 제공한다.
- ②사용 기술: HTML/CSS/JavaScript 및 React(대시보드 UI), Node.js+Express(백엔드 API)
- ③기능: 사용자 인증(로그인/회원가입), 로그 업로드(파일 업로드/실시간 전송), 로그 전송 상태표시, 기본 검색·필터링 UI를 제공한다.

2) Elasticsearch (로그 저장 및 검색)

- ①사용 목적: 웹페이지에서 수집된 로그 데이터를 효율적으로 저장하고 고속 검색·집계를 제공한다.
- ②이론 및 개념:
Elasticsearch는 분산형 검색·분석 엔진으로 JSON 문서를 색인하여 빠른 검색을 제공한다. Index는 문서들의 논리적 집합(데이터베이스 역할)이며, Inverted Index 구조를 통해 텍스트 기반 검색을 효율화한다.
- ③기능: 실시간 색인(인덱싱), 복합 쿼리·집계(aggregation), Bulk API를 통한 대량 색인한다.

3) AI 모델 (Isolation Forest, Scikit-learn)

- ①사용 목적: 로그 데이터에서 비정상 패턴(이상치)을 자동으로 탐지한다.
- ②이론 및 개념:
 - Isolation Forest: 비지도 학습 기반의 이상치 탐지 알고리즘으로, 데이터 샘플을 무작위 분할하여 고립된 샘플을 이상치로 판단한다.
 - Scikit-learn: 모델 학습·평가를 위한 주요 라이브러리.
- ③모델 직렬화: joblib 또는 pickle을 사용해 학습된 모델을 저장하고 불러온다.
- ④기능: 입력된 로그(또는 로그의 특징 벡터)를 받아 이상도 점수(anomaly score) 및 이상 여부를 반환한다.

4) AI 서비스화: REST API (Flask 또는 FastAPI)

- ①사용 목적: AI 모델을 독립된 서비스로 제공하여 웹 백엔드 또는 다른 시스템이 HTTP 요청으로 실시간 분석을 요청할 수 있게 한다.
- ②이론 및 개념:
 - Flask: 간단한 API 구현에 적합하다.

-FastAPI: 비동기 처리와 자동 문서화(OpenAPI)를 지원하여 높은 성능과 개발 생산성을 제공한다.

③동작 흐름: 클라이언트(웹 또는 백엔드)가 로그 데이터를 POST → AI API가 모델로 분석 → JSON 형태로 이상도 점수 및 결과 반환한다.

5) Elasticsearch ↔ AI API 연동 (분석된 로그 저장)

①사용 목적: AI가 탐지한 이상 로그를 Elasticsearch에 다시 저장하여 검색·대시보드에서 조회 가능하도록 한다.

②이론 및 개념:

-Bulk API를 사용해 대량의 분석 결과를 효율적으로 색인한다.

-필요에 따라 Logstash를 사용해 전처리 파이프라인을 구성할 수 있다.

③기능: 원본 로그 문서에 이상도 점수/태그를 추가해 별도의 인덱스에 저장하거나 원본 인덱스에 업데이트한다.

6) Kibana 대시보드 (데이터 시각화)

①사용 목적: Elasticsearch에 저장된 로그와 AI 분석 결과를 시각화해 운영자/관리자가 이상 탐지 결과를 직관적으로 확인하도록 한다.

②이론 및 개념: 대시보드에는 테이블, 시계열 그래프, 히트맵 등을 포함해 경향 분석·이상 이벤트 추적이 가능하다.

7) Kibana API ↔ Chart.js (웹페이지 내 시각화 연동)

①사용 목적: Kibana(또는 Elasticsearch)에서 제공하는 API를 통해 웹페이지 내에서 커스텀 차트(Chart.js)를 렌더링하여 사용자 맞춤형 대시보드를 제공한다.

②이론 및 개념: Kibana/ES API로 쿼리 하여 JSON 결과를 받아 React 컴포넌트에서 Chart.js로 시각화한다.

3.2 학습·평가 대상 공격 유형

본 연구에서는 AI기반 로그분석 웹페이지의 학습 및 성능평가 대상으로 대표적인 웹 공격 유형을 선정하였다. 선정 기준은 공격의 발생 빈도, 실제 서비스에서의 영향도, 로그 상에서의 식별 가능성이며, 초기 학습에서는 다음과 같은 공격 유형을 중심으로 모델을 학습시킨다.

1) SQL 인젝션 (SQL Injection)

- ①개념: 데이터베이스에 비정상적인 쿼리를 삽입하여 정보 탈취, 변조 또는 삭제를 수행하는 공격을 의미한다.
- ②로그 발생 형태:
 - 웹서버 로그에서 비정상적 쿼리 문자열이 존재한다.
 - 쿼리 내 `OR 1=1 --` 등 특수 문자 및 SQL 키워드 패턴을 가지고 있다.
- ③분석 대상: 요청 URL, 쿼리 파라미터, 사용자 입력 값
- ④학습 목적: AI 모델이 정상 요청과 SQL 공격 로그를 구분하여 이상 여부를 판단한다.

2) 크로스 사이트 스크립팅 (XSS Attack)

- ①개념: 웹 페이지에 악성 스크립트를 삽입하여 사용자의 쿠키, 세션, 개인정보 등을 탈취하는 공격을 의미한다.
- ②로그 발생 형태:
 - HTTP 요청 파라미터에 `<script>` 태그 또는 JavaScript 코드를 삽입한 형태이다.
 - URL, POST 데이터, 쿠키 필드에 비정상 문자열이 존재한다.
- ③분석 대상: 요청 헤더, 파라미터, 응답 상태 코드
- ④학습 목적: 입력 값 패턴을 기반으로 정상/비정상 요청을 판단한다.

4. 결론

4.1 결론 및 기대효과

본 연구는 AI 기반 로그 이상 탐지 시스템을 웹 환경에서 구현함으로써, 기존의 수동적이고 비효율적인 로그 분석 과정을 자동화하고 시각적으로 제공할 수 있는 웹페이지를 구축하였다.

기존의 로그 분석은 관리자가 직접 로그를 확인하는 방식이 주를 이루었으나, 본 연구에서는 AI 모델을 적용하여 비정상적인 패턴을 자동으로 탐지하고 이상 여부를 점수화하는 기능을 구현하였다. 이를 통해 방대한 로그 데이터를 사람이 일일이 확인하지 않아도 자동으로 이상 징후를 탐지할 수 있었으며, 그 결과 운영 효율성과 보안 대응 속도가 크게 향상되었다.

또한 Elasticsearch를 활용하여 대용량 로그 데이터를 효율 적으로 저장하고 검색이 가능한 데이터베이스 환경을 구축하였다. 이와 더불어 Chart.js를 활용한 시각화 기능을 통해 탐지된 이상 로그를 그래프 및 차트 형태로 직관적으로 확인할 수 있도록 구현하였다. 이를 통해 사용자는 로그 데이터를 업로드하는 것만으로 AI 모델의 분석 결과를 시각적으로 즉시 확인할 수 있으며, 관리자는 이상 탐지 결과를 기반으로 신속하고 효율적인 대응을 수행할 수 있다.

이와 같은 구현을 통해 본 연구는 다음과 같은 기대효과를 얻을 수 있다.

1) 운영 효율성 향상

로그 데이터의 자동 분석 및 시각화를 통해 관리자의 업무 부담이 감소하고, 시스템 운영 효율이 향상된다.

2) 보안 대응력 강화

AI 기반 이상 탐지를 통해 공격 패턴이나 비정상 행위를 조기에 탐지함으로써, 보안 사고 대응 시간을 단축시킬 수 있다.

3) 데이터 가시성 확보

Elasticsearch 및 Chart.js를 활용한 시각적 분석을 통해 복잡한 로그를 한눈에 파악할 수 있으며, 이를 통해 문제 원인 분석과 트렌드 파악이 용이해진다.

4) 확장성과 실용성 확보

Flask 또는 FastAPI 기반의 REST API 구조를 적용함으로써, 다른 시스템과의 연동이 용이하고 실제 서비스 환경에서도 활용 가능한 구조로 확장할 수 있다.

이를 통해 로그 분석의 자동화와 보안 대응의 지능화를 동시에 실현하였으며, 향후 AI 기반 보안 자동화 시스템으로의 확장 가능성을 확인할 수 있다.

4.2 향후 계획

본 AI 로그 분석 시스템은 현재 이상 탐지와 시각화 기능을 중심으로 동작하지만, 향후 더욱 완성도 높은 서비스로 발전시키기 위해 다음과 같은 네 가지 핵심 영역을 중심으로 고도화 및 개선을 추진할 계획이다.

1) 홈페이지 UI/UX 개선

사용자가 분석 결과를 더 빠르고 직관적으로 파악할 수 있도록 홈페이지의 UI(사용자 인터페이스) 및 UX(사용자 경험)를 전면 개선한다.

- ①시각화 대시보드 강화: 탐지된 공격 유형, 공격 빈도가 높은 IP, 시간대별 공격 추이 등을 한눈에 파악할 수 있는 동적 그래프와 차트를 도입한다.
- ②사용자 편의성 증대: 로그 업로드 과정을 간소화하고, 분석 결과를 필터링하거나 상세 내역을 확인하는 과정을 더 사용자 친화적으로 개선한다.

2) 로그데이터 분석 속도 향상

대용량 로그 파일도 신속하게 처리할 수 있도록 분석 엔진의 성능 최적화를 진행한다.

- ①파싱 로직 개선: 다양한 로그 형식을 더 빠르게 처리할 수 있도록 파싱 모듈을 경량화하고 효율화한다.
- ②병렬 처리 도입: 대규모 데이터를 여러 CPU 코어에서 동시에 처리하는 병렬 처리 방식을 도입하여, 전체 분석 시간을 획기적으로 단축시키는 것을 목표로 한다.

3) AI모델 정확도 향상

지속적인 모델 튜닝과 최신 데이터 학습을 통해 AI의 탐지 정확도를 향상한다.

- ①오탐 및 미탐 최소화: 오탐과 미탐을 줄이는 것을 최우선 목표로 합니다. 이를 위해 최신 공격 패턴 데이터를 주기적으로 추가 학습시킨다.
- ②딥러닝 모델 도입 검토: 기존 머신러닝 모델 외에, 문맥 이해도가 더 높은 딥러닝 모델 도입을 검토하여 예측 성능을 한층 더 고도화할 것이다.

4) 탐지 가능한 공격 유형 확대

현재 탐지 가능한 SQL인젝션, XSS 외에도 분석 가능한 공격 범위를 확대하여 포괄적인 보안 시스템으로 발전시킨다.

- ①신규 공격 패턴 추가: RAW_STRICT 및 RAW_FUZZY 규칙 목록에 NoSQL 인젝션, 템플릿 인젝션, SSRF, LFI 등 최신 웹 취약점 공격 패턴을 추가한다.
- ②이상치 탐지 고도화: IsolationForest 모델을 고도화하여, 알려지지 않은 새로운 유형의 공격 시도를 더 효과적으로 식별할 수 있도록 개선한다.

5. 참고 자료

- (1) <https://www.elastic.co/docs> (elk 구축 참고자료)
- (2) <https://ko.react.dev/> (React 웹 구성 참고자료)

6. 별첨

6.1 품보드

LogX

2025 졸업작품 전시회

AI 기반

웹취약점 진단 시스템

개요

AI를 활용하여 웹 로그를 자동 분석하여 보안 위협을 탐지하는 시스템을 개발

Elasticsearch 기반의 로그 수집 및 검색 구조 와 AI 모델을 결합하여

XSS와 SQL Injection 공격 패턴을 탐지·분류하여

직관적인 시각화 결과를 웹 기반으로 제공

개발내용

로그 파일 업로드 → 로그 저장 및 검색 → AI 모델 학습

분석 결과 저장 ← Isolation 기법 응용 로그 분석

데이터 시각화 → 시각화 + 결과값 제공 → 대시보드 UI

구상도

분석 결과 페이지

기대효과

로그 데이터의 자동 분석 및 시각화를 통해

관리자의 업무 부담이 감소하고, 시스템 운영 효율이 향상

AI 기반 이상 탐지를 통해 공격 패턴이나 비정상 행위를

조기에 탐지함으로써, 보안 사고 대응 시간 단축

팀원소개

박성준 [팀장]

김정민 [팀원]

박지우 [팀원]

윤서연 [팀원]

2025 정보보호학과 졸업작품 전시회 @LogX

6.2 프로젝트 소개 (깃허브 주소, 웹 서비스 주소, 시연 영상,)

- ① 깃허브 주소 : <https://github.com/jeongmin20010108-sketch/10-23-logx-project>
- ② 웹 서비스 주소 : <https://logxproject.netlify.app/>
- ③ 시연 영상 (파일 별도 첨부)

6.3 팀 소개



[팀장]

이름 : 박성준

전공 : 정보보호학과

학번 : 91913440

깃허브 주소 : <https://github.com/cark753>



[팀원]

이름 : 김정민

전공 : 정보보호학과

학번 : 92016049

깃허브 주소 : <https://github.com/jeongmin20010108-sketch>



[팀원]

이름 : 박지우

전공 : 정보보호학과

학번 : 92113607

깃허브 주소 : <https://github.com/qkrwldn38>



[팀원]

이름 : 윤서연

전공 : 정보보호학과

학번 : 92360798

깃허브 주소 : <https://github.com/westkite05>

6.4 발표 자료 (발표 PPT 별첨)