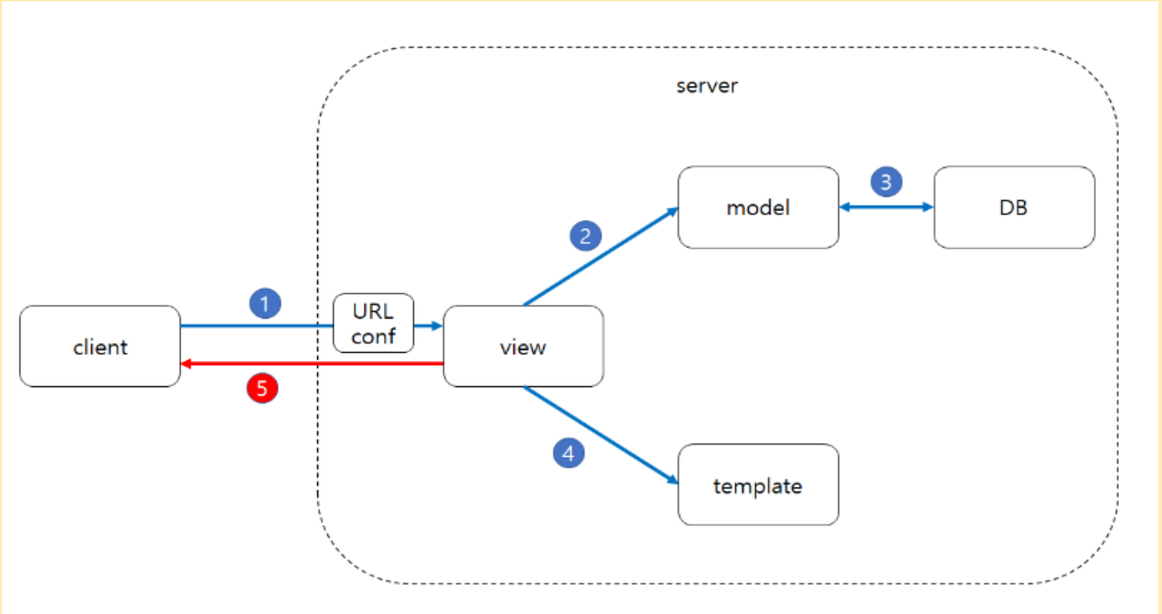
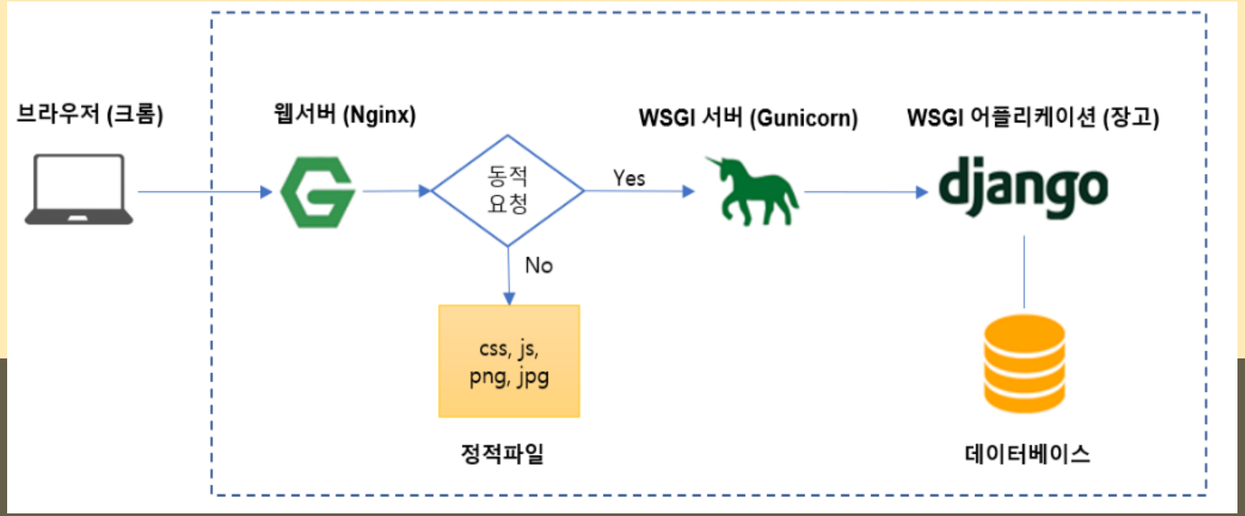
yANUs

개발
환경 & 기술





yANUs

OWASP 웹 보안 서비스 종합 포털사이트 설계 및 구현

THE SECULAB

WWW.THESECULAB.SITE:8080

소프트웨어융합학과

YANUS 보안셀 동아리 개발2팀

김선혁, 최태용, 전보경, 김유진, 안수윤, 김선민

yANUs

목차

yANUs

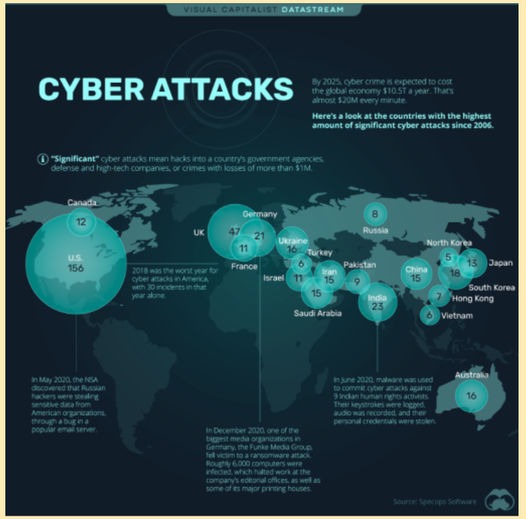
프로젝트 배경

01

현대 사회의 디지털 변환

02

사이버 보안 위협 증가



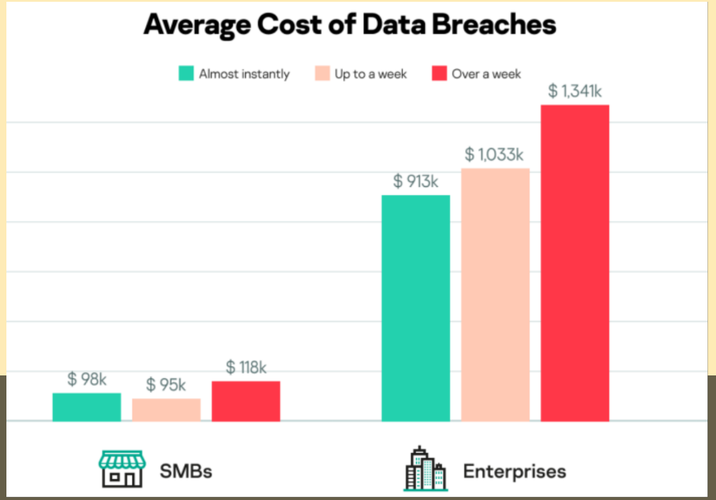
OWASP
Open Web Application Security Project

03

OWASP Top 10 의 중요성

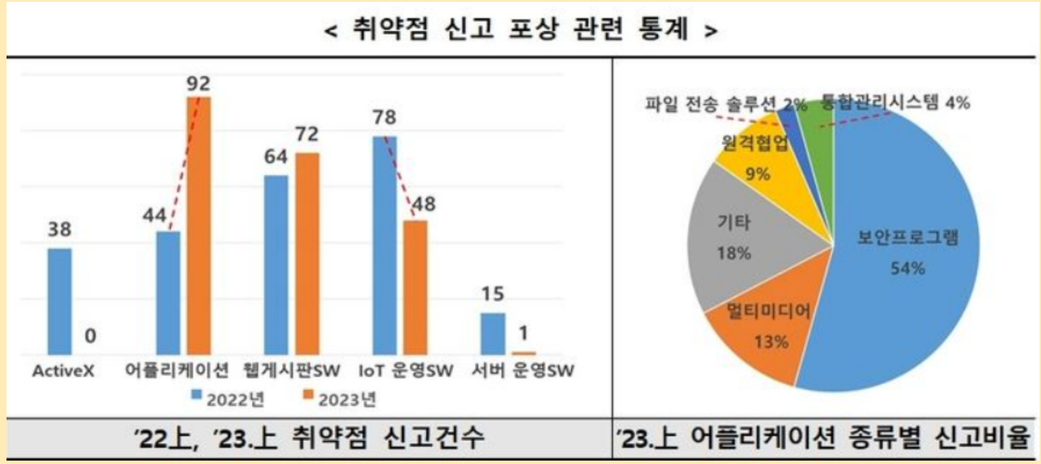
04

인식 제고의 필요성



yANUs

필요성 및 동기



보안 취약점은 심각한 결과를 초래하고 기업의 평판과 재정에 영향을 미친다.

웹 애플리케이션의 보안을 강화하는 것은 기업의 지속 가능성에 중요하다.

본 프로젝트는 OWASP Top 10 지침을 통해 웹 개발자들이 웹 애플리케이션의 보안 위협을 자가 진단하고 대응할 수 있도록 지원한다.

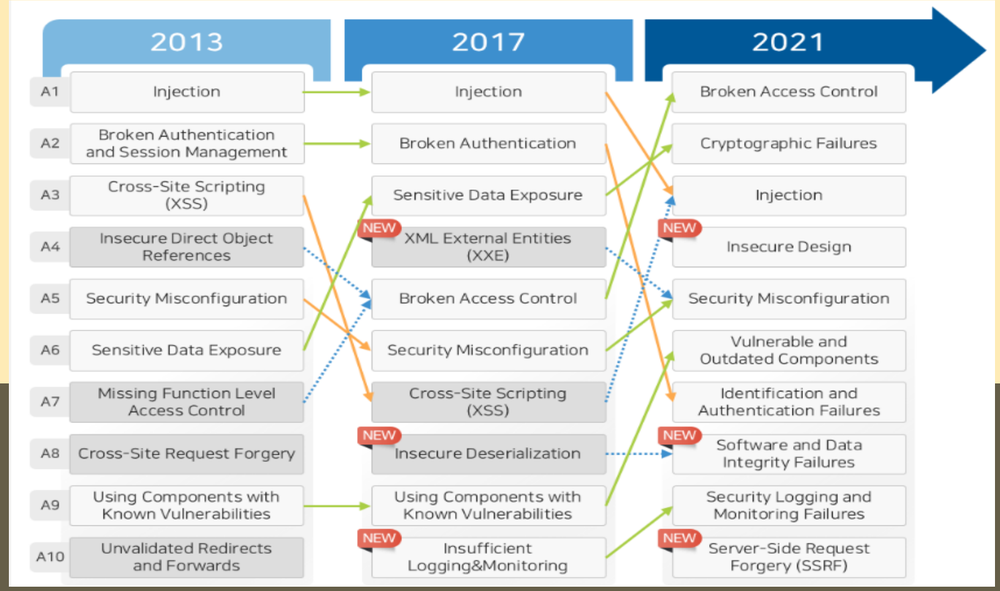
OWASP TOP 10의 중요성

Open Web Application Security Project

Broken Access Control	잘못된 접근 제어
Cryptographic Failures	암호화 오류
Injection	인젝션
Insure Design	안전하지 않은 설계
Security Misconfiguration	보안 설정 오류
Vulnerable and Outdated Components	취약하고 오래된 컴포넌트
Identification and Authentication Failure	식별 및 인증 실패
software and Data integrity Failure	데이터 무결성 확인 문제
Security Logging and Monitoring Failures	보안 로깅 및 모니터링 실패
Server-side Request Forgery	서버 측 요청 위조

yANUs

분류	2013	2017	2021
기반	애플리케이션 보안 전문 7개 기업, 8개 데이터 세트를 기반	애플리케이션 보안 전문 회사가 제출한 40개 이상의 데이터와 업계 순위조사 (500명)을 기반	8개의 범주 : 데이터에서 선택 2개의 범주 : 업계 설문 조사에서 선택
데이터	수백 개 기업, 수천 개의 애플리케이션에 걸친 500,000개 이상의 취약점들을 포함	• 수백 개의 조직과 10만개가 넘는 실제 애플리케이션 및 API에서 수집된 취약점을 포함 • CWE 데이터를 규정된 하위 집합에서 수집	• 500,000개 이상의 애플리케이션에 대한 데이터를 진행 • CWE에 대한 제한 없이 데이터를 수집
우선 순위	악용 가능성, 탐지 가능성 및 영향의 확산 및 추정치를 기반으로 목록을 선택하고 우선순위를 지정	공격 가능성, 탐지 가능성 및 영향도를 합의 추정한 값으로 보정한 데이터에 따라 선별되고 우선순위 지정	• 악용 가능성과 영향에 대한 데이터를 사용 • 발생률로 우선순위 지정
데이터 셋의 수	-	약 30 CWE	약 400 CWE

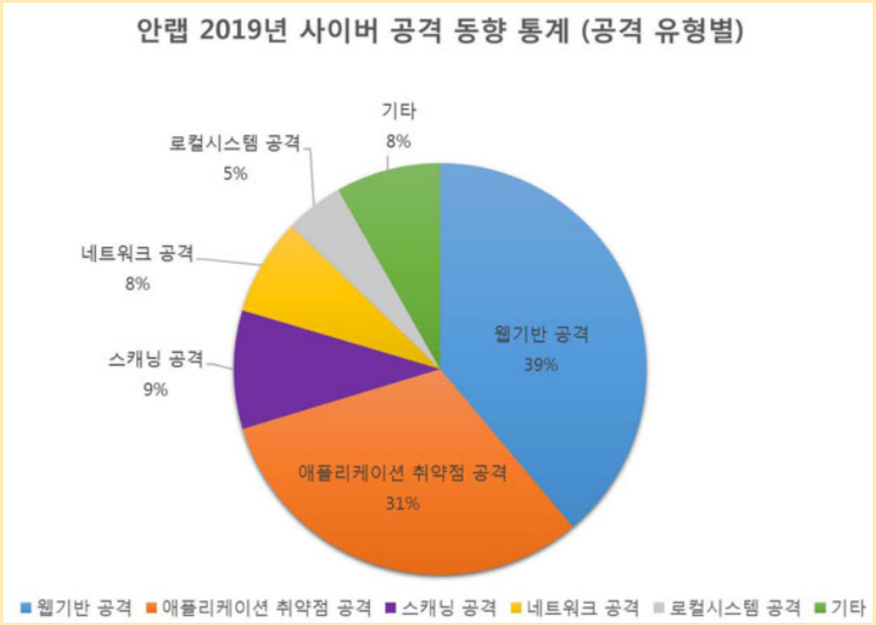


yANUs

웹 애플리케이션 보안의 현 상황

Open Web
Application
Security Project

◇ 2016년 4분기 취약점 유형별 웹 공격 [그래프=씨디네트웍스]



yANUs

프로젝트의 목적

01

교육 및
인식 증진

02

자동화된
취약점 분석

03

보안 개선
가이드라인

04

커뮤니티 형성

yANUs

기대 효과

01

보안 인식 향상

02

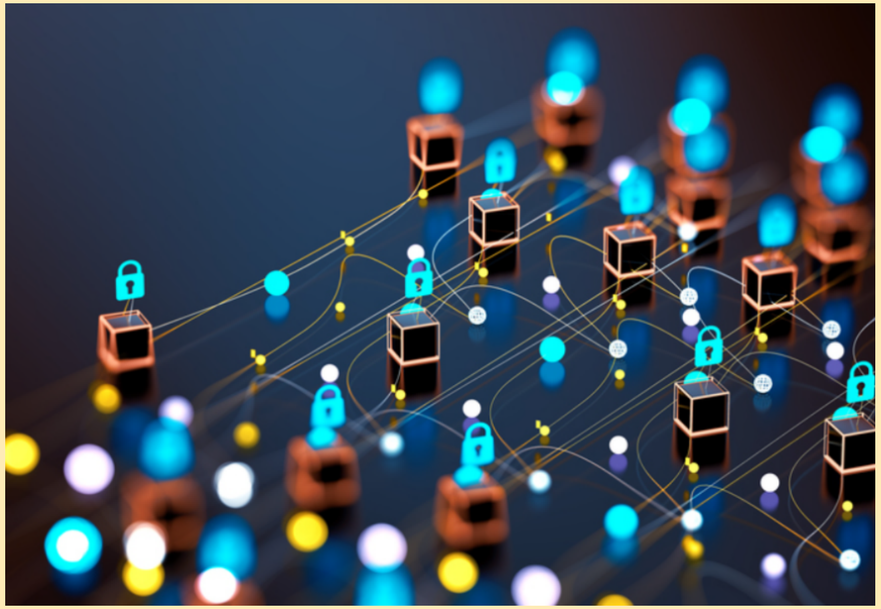
사고 예방

03

비용 절감

04

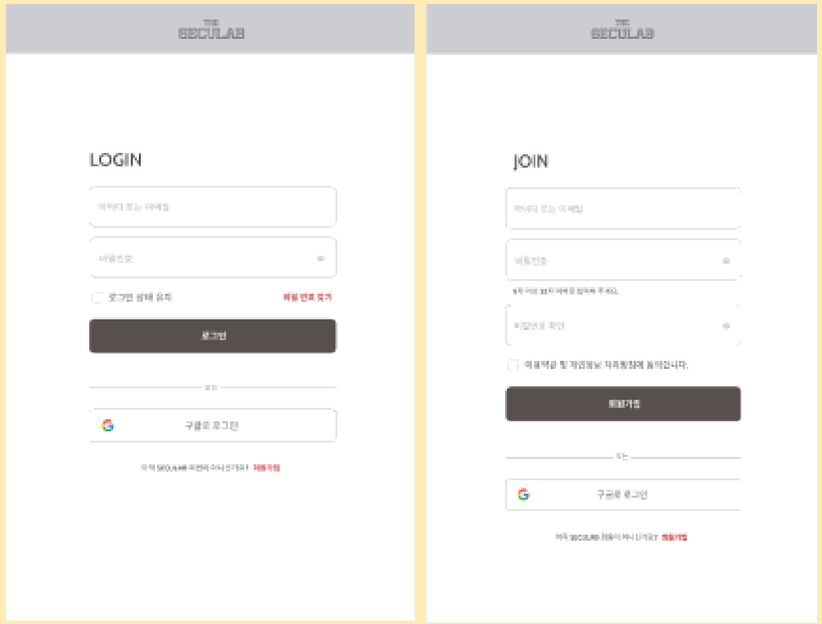
사용자 신뢰도 증가



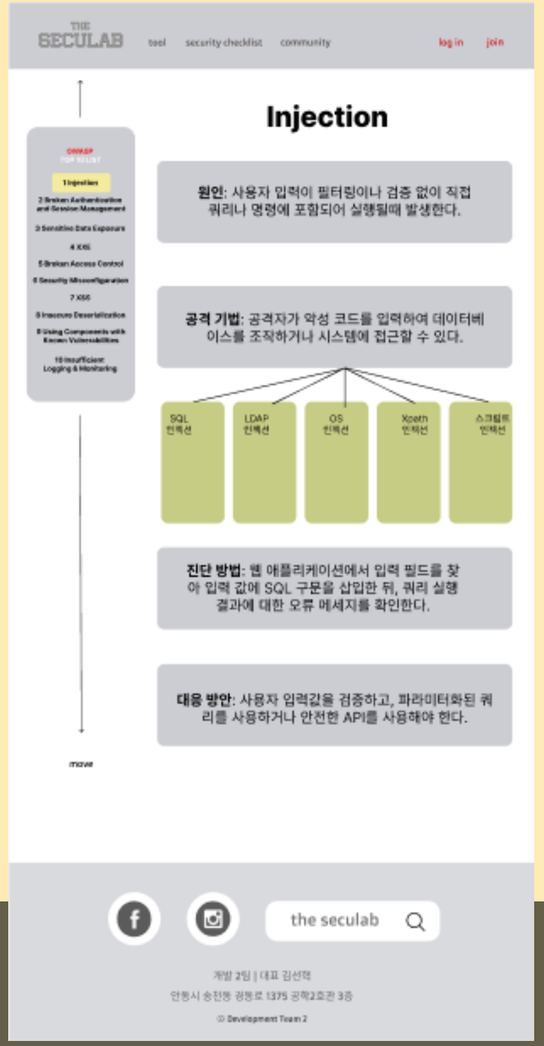
시스템 설계

UI/UX 설계

메인 페이지



로그인 및 회원가입

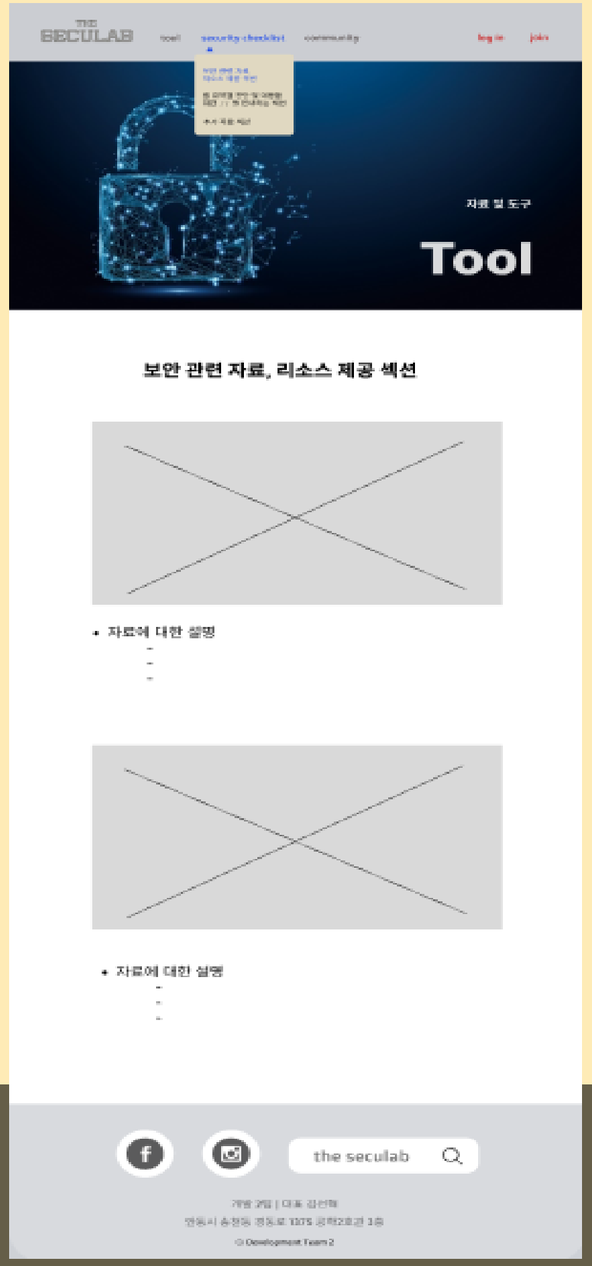


취약점 상세페이지

시스템 설계

UI/UX 설계

yANUs



자료 및 도구 페이지

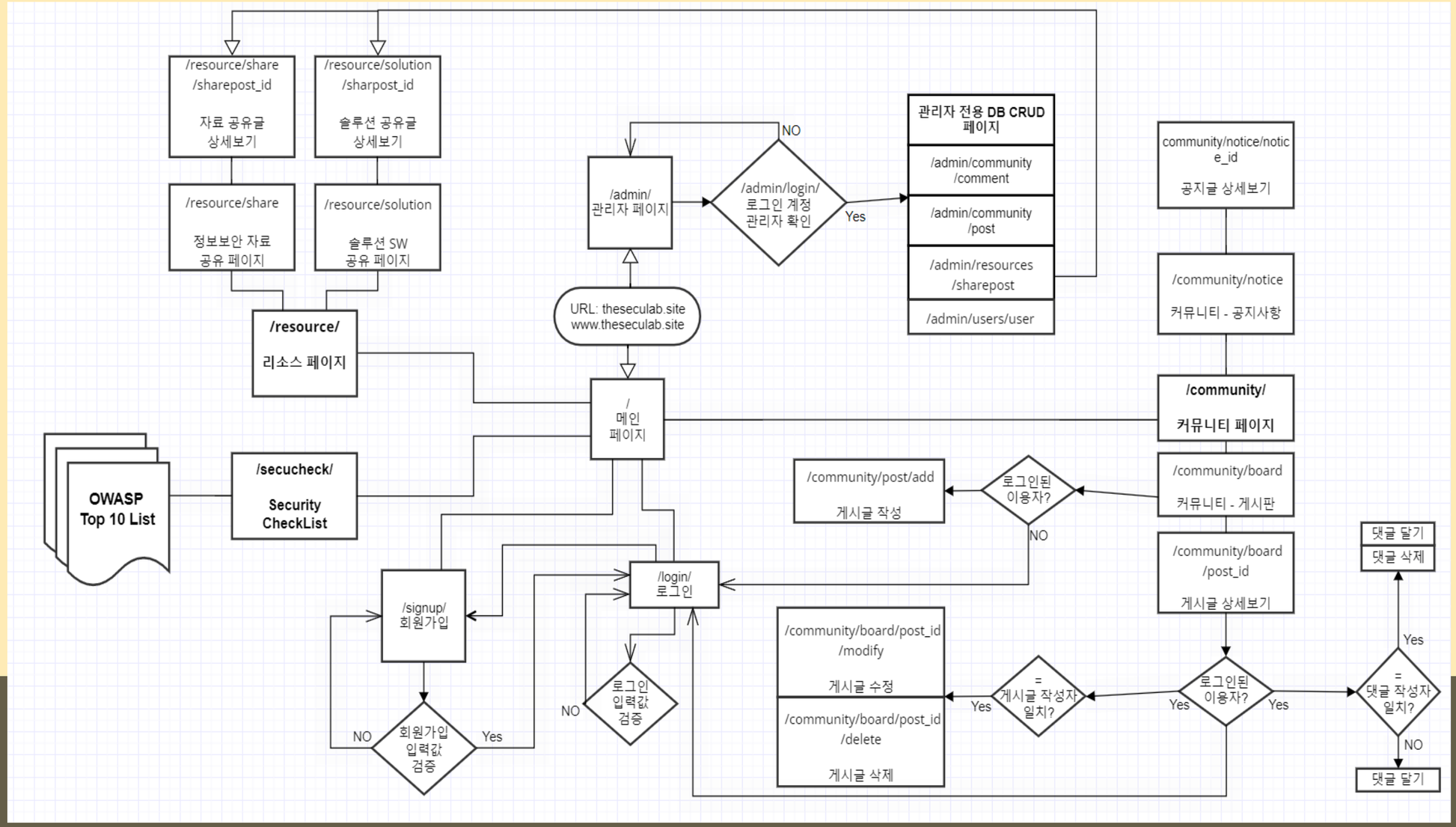
커뮤니티 및 지원페이지

게시글 등록 페이지

yANUs

시스템 설계

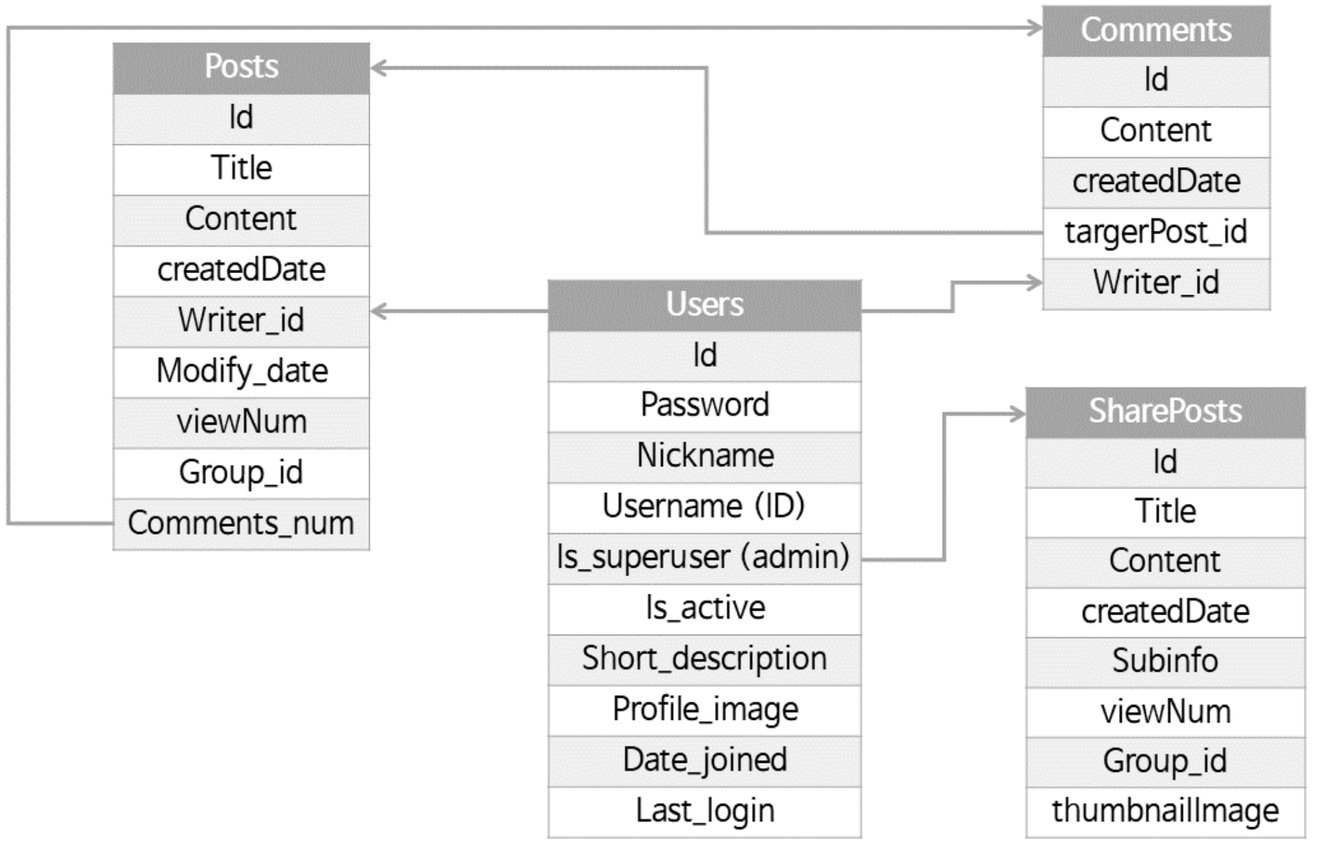
Service Flowchart



yANUs

시스템 설계

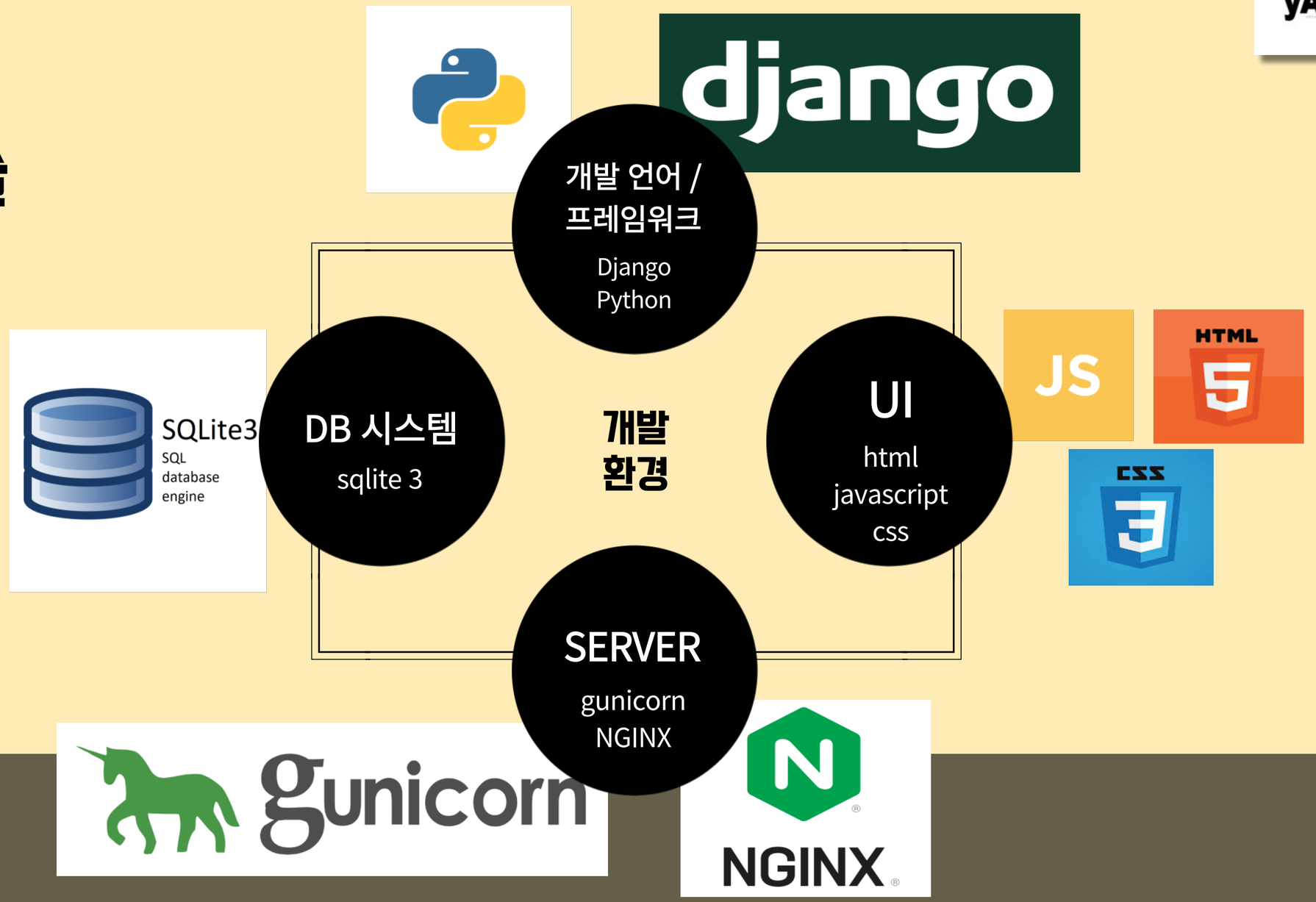
DB Schema



yANUs

개발
환경 & 기술

사용된 언어 및
개발 프레임워크



yANUs

개발
환경 & 기술

사용된 언어 및
개발 프레임워크

01. 팀원 총원이 python에 익숙함
- 파이썬 : 다양한 pip 패키지 지원

02. 강력한 admin 관리자 페이지 기능

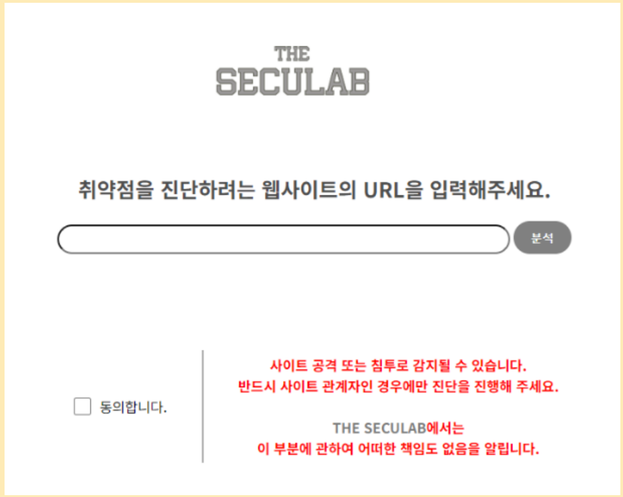
03. ORM (객체 관계 매핑) 지원

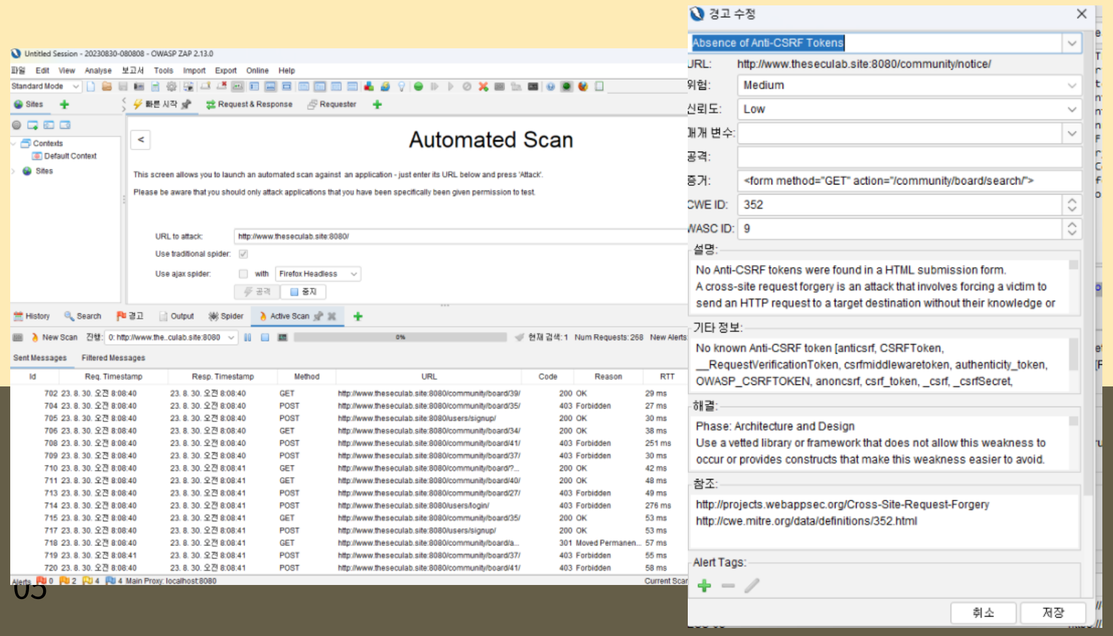
04. MVC 패턴 기반 MTV(Modle-Template-View) 패턴 웹 설계

주요 기능 및 서비스

01

자동화된 취약점 분석 제공





01. OWASP ZAP을 사용한 자동화된 취약점 분석

02. 파이썬과 ZAP API로 프록시 설정 조정 및 분석 실행

03. Spider를 통한 웹 페이지 크롤링과 취약점 스캔

04. 장고를 활용한 분석 결과의 실시간 분류 및 제공

주요 기능 및 서비스

02

자동화된 취약점 분석 제공

	A	B	C	D	E	F
1	date	title	writer	link	content	image
2	2023-08-21 16:10	"투기하여 정년" 블라인드 내 이혜진 기자	sunset@ch	https://n.news.naver.com/mnews/article/0	직장인 커뮤니티 '블라인드'에 21일 올라온 짤부터 '예고글 / 블라인드'로우면 안직하든가.' 직장인 익명 온라인 커뮤니티 '블라인드'에 연국인을 조롱한 글을 올린 내 직원 계정의 주인공은 1년간 경찰 수사에도 결국 찾지 못했다. 강남에 업무 집 예고로 국민을 위한한 경찰 계정은 찾을 수 있을까. 이번 에는 경찰 계정으로 업부된을 '예고하는 글이 올라오자 공회근 경찰청장이 직접 경찰청 사이버대라수사대에 수사를 지시하고 작성자 색출에 나섰다.21일 경찰에 따르면, 경찰청 사이버대라수사대는 이날 '블라인드' 게시판에 경찰청' 소속으로 명시된 작성자가 올린 업부된 예고글에 대한 수사에 착수했다. 이날 오전 이 커뮤니티에는 '오늘 저녁 강남역 1번 출구에서 집회할꺼다'라는 제목의 게시글이 올라왔다. 곧 내	https://imgnews.pstatic.net/image/023/2023/08/21/0003782865_001_20230822100106912.jpeg?type=w
3	2016-03-22 10:41	이메일을 암호화 취약점 해소...	손경호	sontech@zdnet.c	https://n.news.naver.com/mnews/article/0	(지디넷코리아=손경호 기자)아이큐브, 구글, 마이크로소프트, 페이스북, 야후 등 글로벌 IT업들이 이메일 암호화 기술에서 발견된 취약점을 해결하기 위해 협업한다. 이들 기업은 이메일 전송용 프로토콜(SMTP)에 적용되는 확장기능 중 하나인 '스타트TLS(STARTTLS)'라는 암호화 통신 기술을 채택한다. 일반적으로 SMTP를 통해 평문 형태로 전송되는 이메일을 암호화 해 전송하는 것이다. 문제는 스타트TLS가 가장 기본적인 암호화 통신 기능을 제공하고 있어 누군가 이메일 흐름을 가로챘을 경우 이러한 기능을 무력화시킬 수 있다는 점이다. 스타트TLS는 한번 암호화 통신을 시도했다가 실패하면 다시 평문 형태로 통신을 시도한다. 이같은 방식을 두고 '기회주의적인 암호화(opportunistic encryption)'라고 부른다.(관련링크)	https://imgnews.pstatic.net/image/092/2016/03/22/sontech_IpKCk1QnHPnV_99_20160322104104.jpg?t
4	2023-09-24 18:37	"이집트 정권 ... 유력 여권 대선주	김지연	cherora@yna.co	https://n.news.naver.com/mnews/article/0	정권 비판해온 정치인...'결탁 안 해도 검열할 수 있는 공격, 시도는 실패' 이집트 야권 대선 주자 아흐메드 엘탄타위 엘탄타위 페이스북 영상 캡처, DB 및 개한에 공지 (서울=연합뉴스) 김지연 기자 = 내년 초로 예상되는 이집트 대선의 유력한 야권 주자가 정권의 해킹 표적이 됐다고 미국 일간 워싱턴포스트(WP)가 21일(현지시간) 보도했다. 구글과 사이버 위협을 감시하는 캐나다 토론토대학 연구소 '시티즌랩'의 조사 결과에 따르면, 압델 파타 엘시시 대통령에게 도전을 선언한 아흐메드 엘탄타위 전 카라야당 대표의 휴대전화가 프레데터 스파이웨어의 공격을 받은 사실이 확인됐다. 프레데터는 지난 7월 미국 상무부가 "사이버 공격으로 전 세계 개인과	https://imgnews.pstatic.net/image/001/2023/09/24/AKR20230924042700009_02_i_P4_20230924183808


```
        page = makePgNum(1)
        url = "https://search.naver.com/search.naver?where=news&sm=tab_pge&query=" + search + "&start=" + str(page)
        urls.append(url)
    print("생성url: ", urls)
    return urls

# html에서 원하는 속성 추출하는 함수 만들기 (기사, 추출하려는 속성값)
def news_attrs_crawler(articles,attrs):
    attrs_content = []
    for i in articles:
        attrs_content.append(i[attrs[attrs]])
    return attrs_content

# ConnectionError방지
headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/98.0.4758.102"}

#html생성해서 기사크롤링하는 함수 만들기(url): 링크를 반환
def articles_crawler(url):
    #html 불러오기
    original_html = requests.get(i,headers=headers)
    html = BeautifulSoup(original_html.text, "html.parser")

    url_naver = html.select("div.group_news ) ul.list_news ) li div.news_area ) div.news_info ) div.info_group ) a.info")
    url = news_attrs_crawler(url_naver, 'href')
    return url


#####크롤링 시작#####

#검색어 입력
search = ["정근권한취약점", "임호화실패", "임호화오류", "SSRF", "CSRF", "취약한컴포넌트", "오래된컴포넌트", "OWASP"]
#검색 시작할 페이지 입력
page = 1
#검색 종료할 페이지 입력
page2 = 10

#뉴스 크롤러 실행
news_titles = []
finding_url = []
news_contents = []
news_dates = []
news_image = []
news_writer = []
```

01. Python과 BeautifulSoup을 사용하여 NAVER 뉴스에서 보안 관련 기사를 크롤링하는 알고리즘 개발

02. OWASP Top 10 취약점 관련 키워드 리스트를 생성하고 해당 키워드로 뉴스 기사 검색

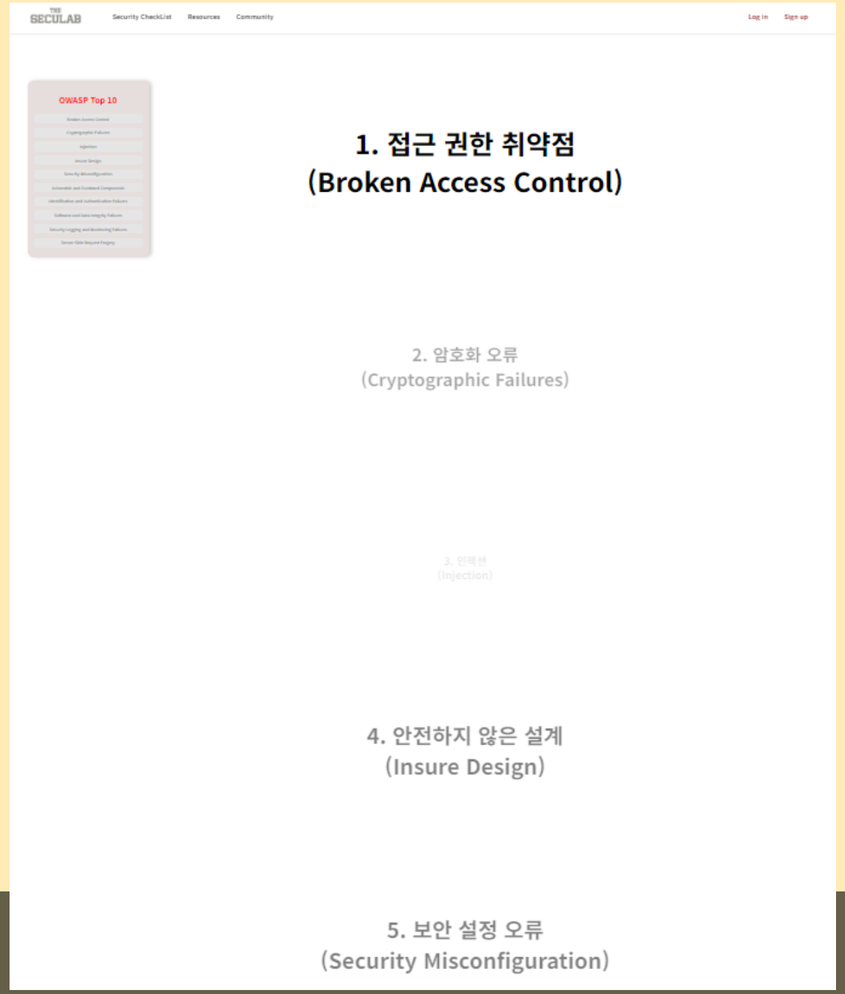
03. 크롤링한 데이터를 pandas로 가공하고 "피해액", "피해 사례" 등의 키워드로 2차 필터링

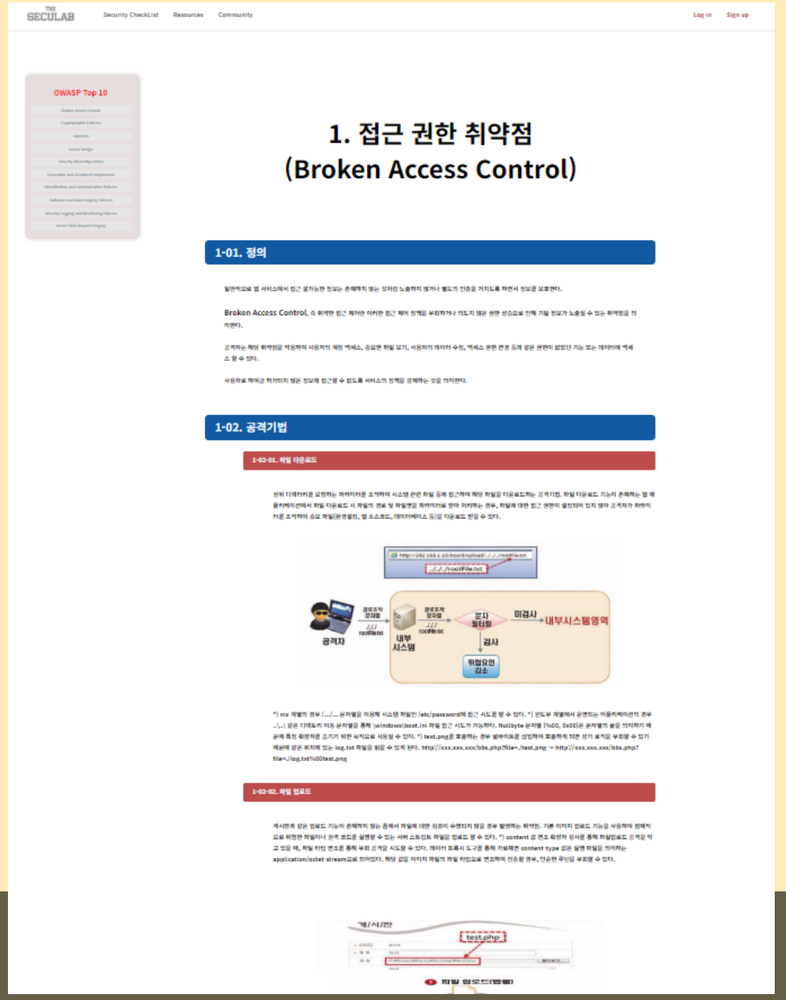
04. 가공된 데이터를 CSV 파일로 저장하고 Django ORM으로 데이터베이스에 저장하여 웹 포털에서 제공

주요 기능 및 서비스

03

Security CheckList 제공

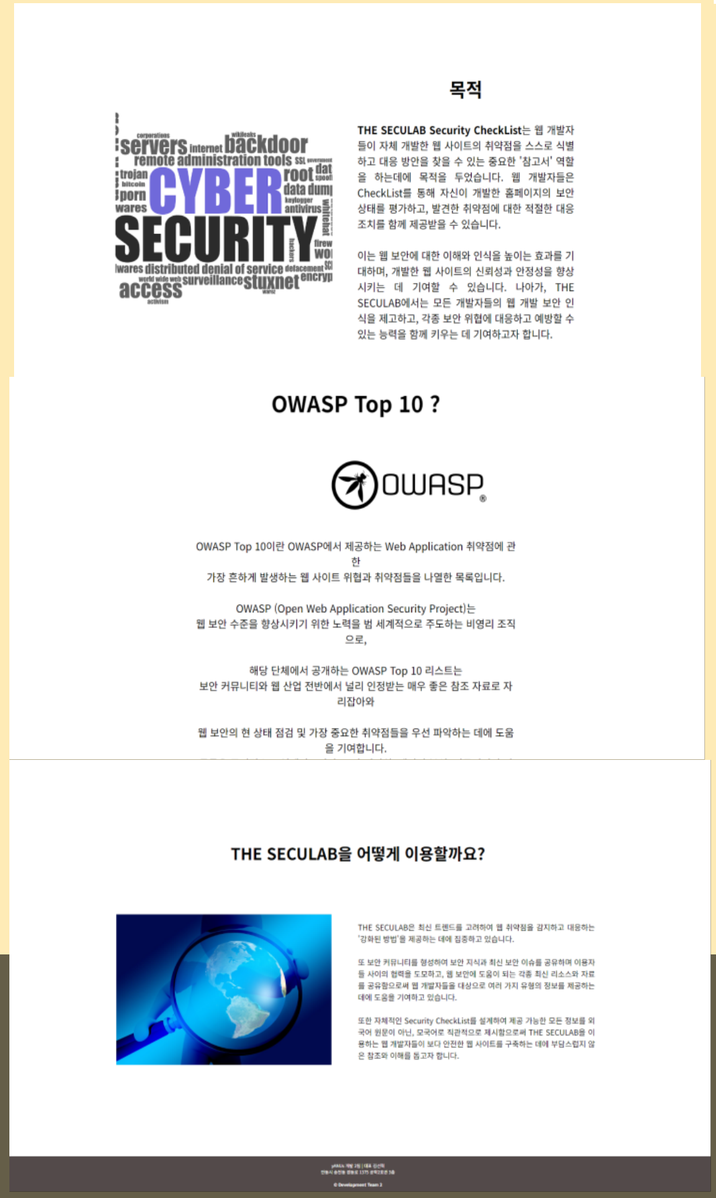




구현
웹페이지
및
기능 소개

http://www.theseculab.site/

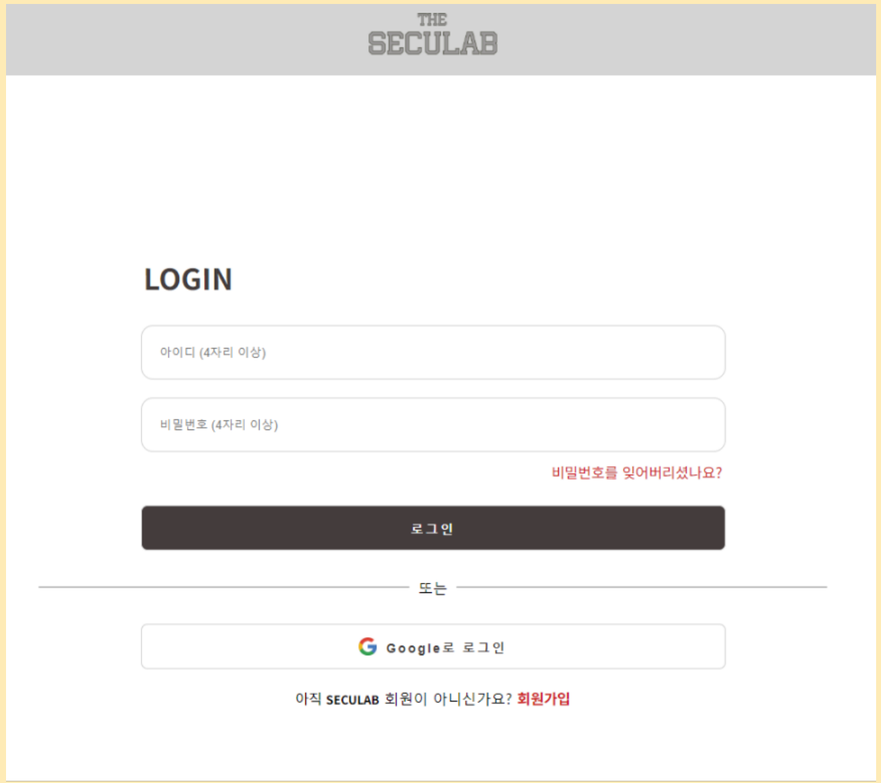
메인 페이지



yANUs

구현 웹페이지 및 기능 소개

로그인/ 회원가입 페이지



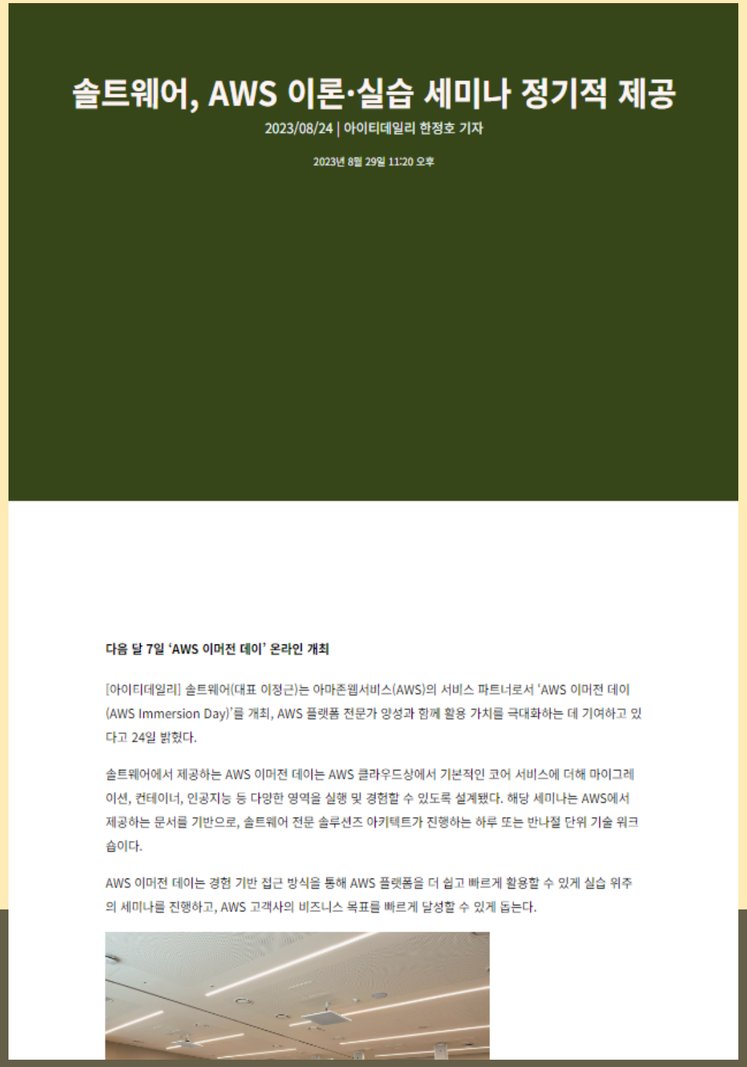
http://www.theseculab.site/

Resource - 정보보안리소스 페이지

yANUs

구현 웹페이지 및 기능 소개

http://www.theseculab.site/



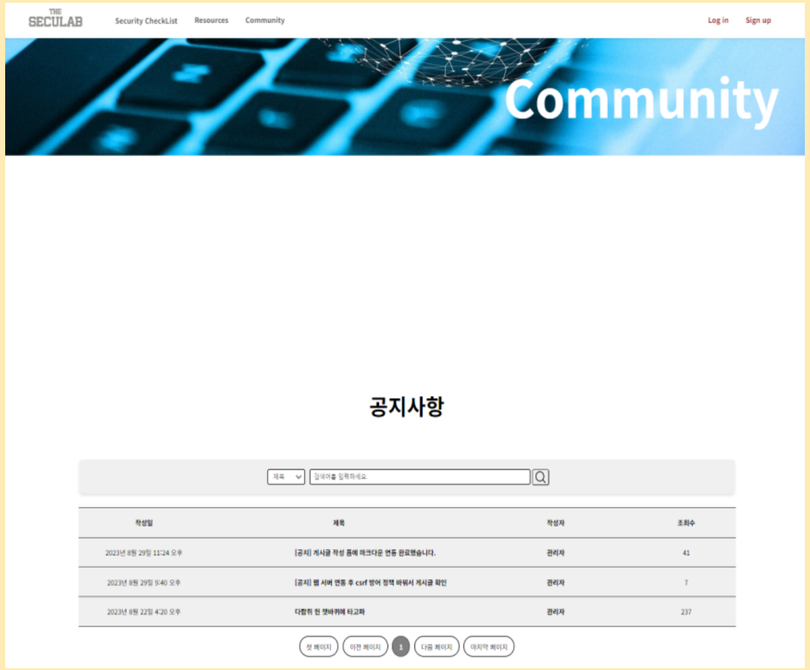
상세페이지

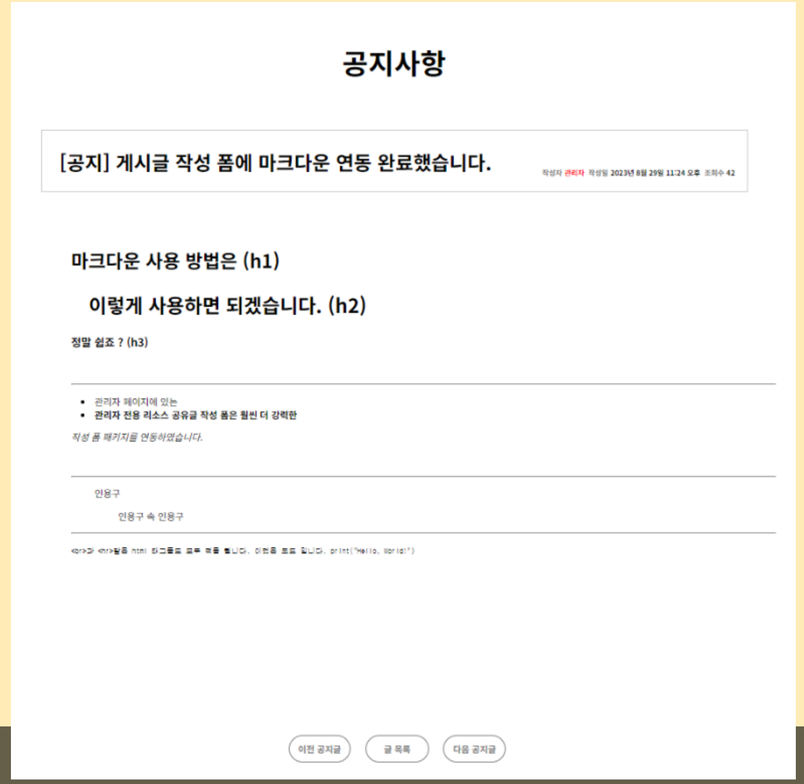
Community 페이지

yANUs

구현 웹페이지 및 기능 소개

http://www.theseculab.site/



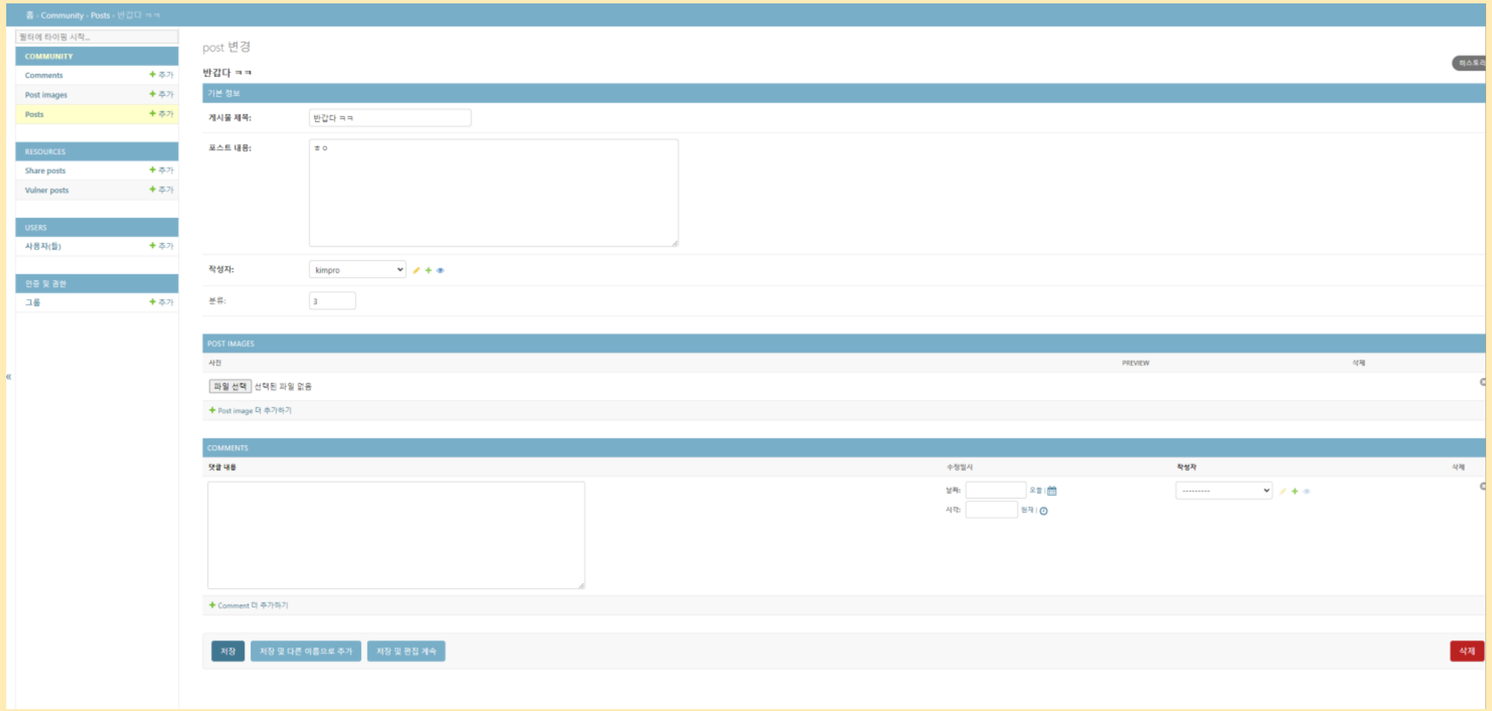


상세 보기 페이지

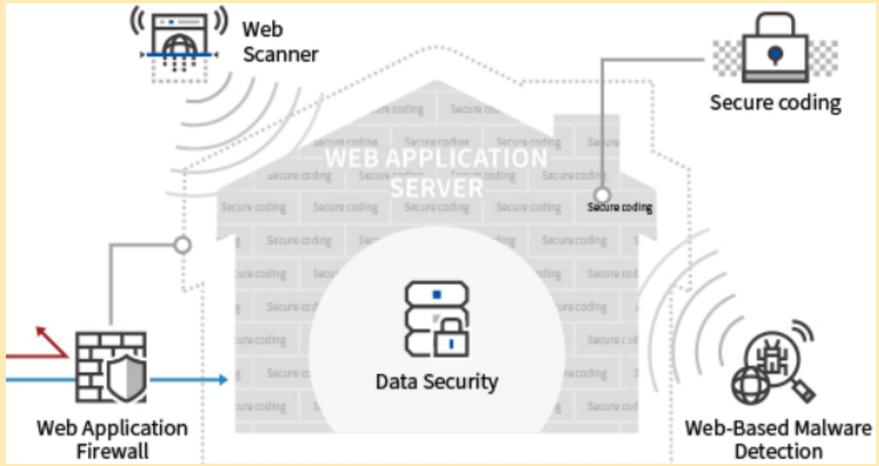
구현 웹페이지 및 기능 소개

http://www.theseculab.site/

관리자 페이지 (모든 DB C/R/U/D 가능)



성과 및 분석



- 본 서비스에서 자체 제공하는 Security CheckList를 통하여 공통적인 웹 어플리케이션 보안 요구사항에 대한 표준화 제시 가능

- 웹 어플리케이션 보안에 대한 일반 사용자의 접근성과 이해도를 높이고, 웹 사이트의 안정성 향상 도모 가능

- 웹 개발자들이 웹 애플리케이션의 보안 상태를 자체적으로 진단하고 점검할 수 있는 자동화 취약점 분석 서비스 제공

yANUs

향후 계획 및 개선점

yANUs

감사합니다

THE SECULAB

야누스 개발 2팀