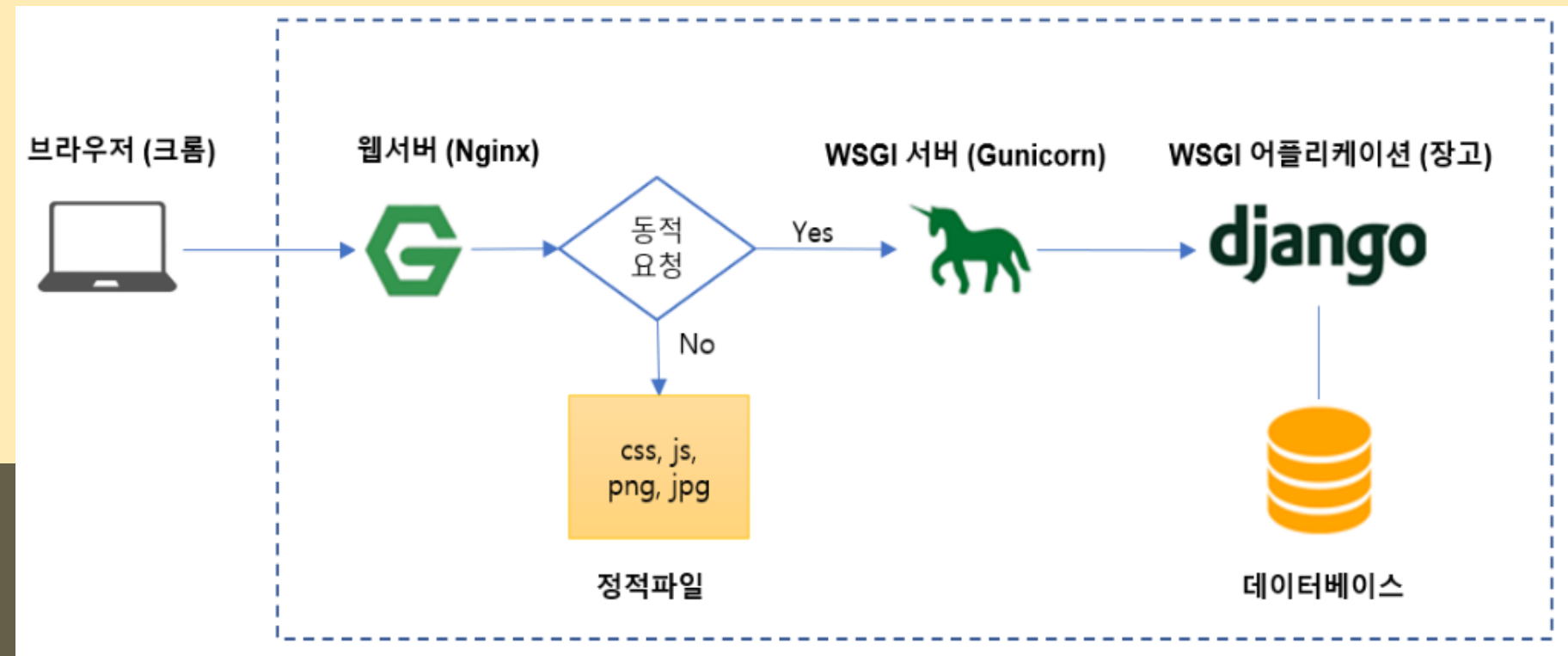
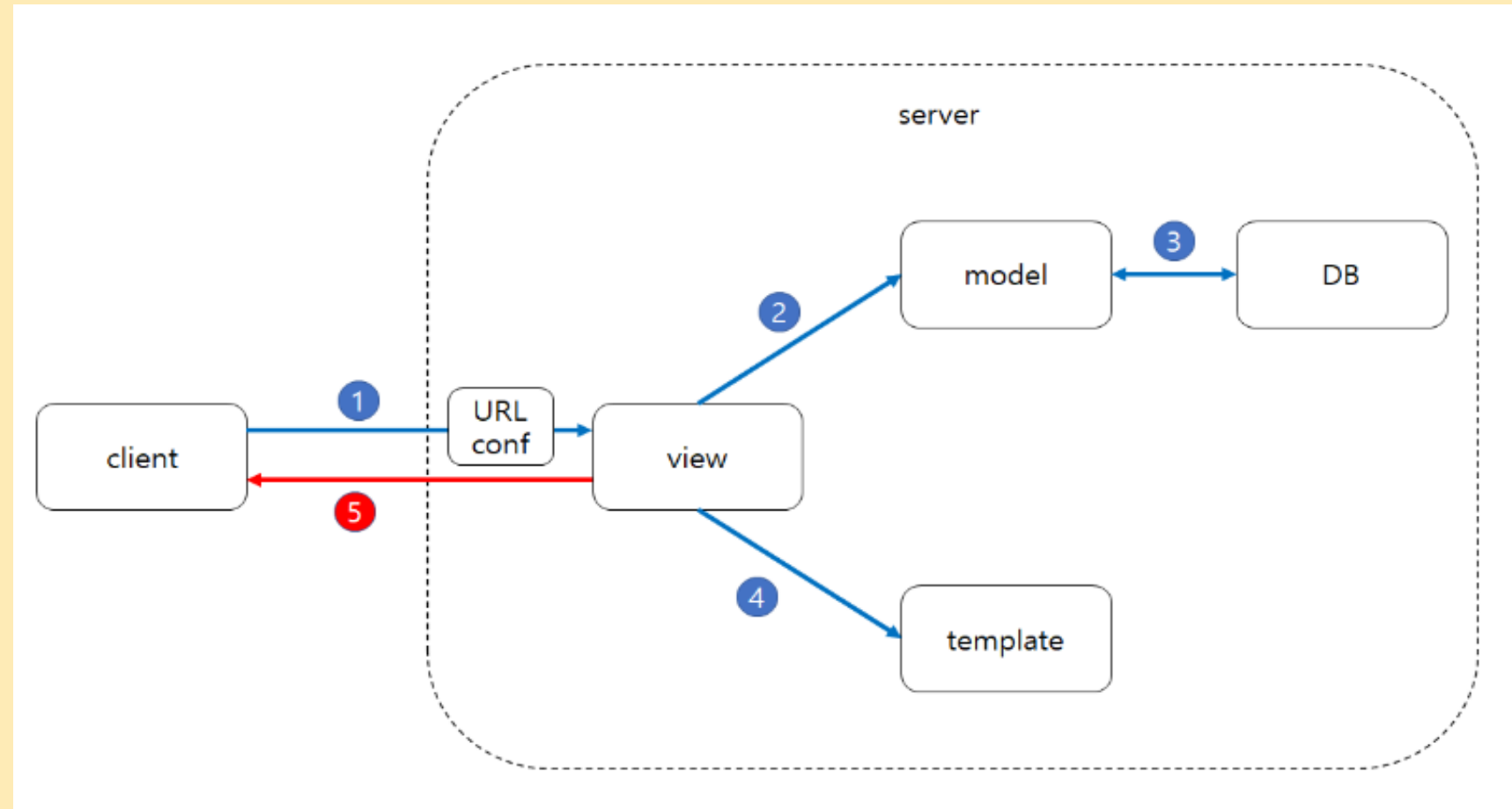


개발 환경 & 기술



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

목차

- 1 서론
- 2 OWASP Top 10 소개
- 3 프로젝트 목표 및 범위
- 4 시스템 설계
- 5 주요 기능 및 서비스
- 6 기술 스택 및 도구
- 7 구현 과정 및 방법론
- 8 시스템 시연
- 9 성과 및 분석
- 10 향후 계획 및 개선점

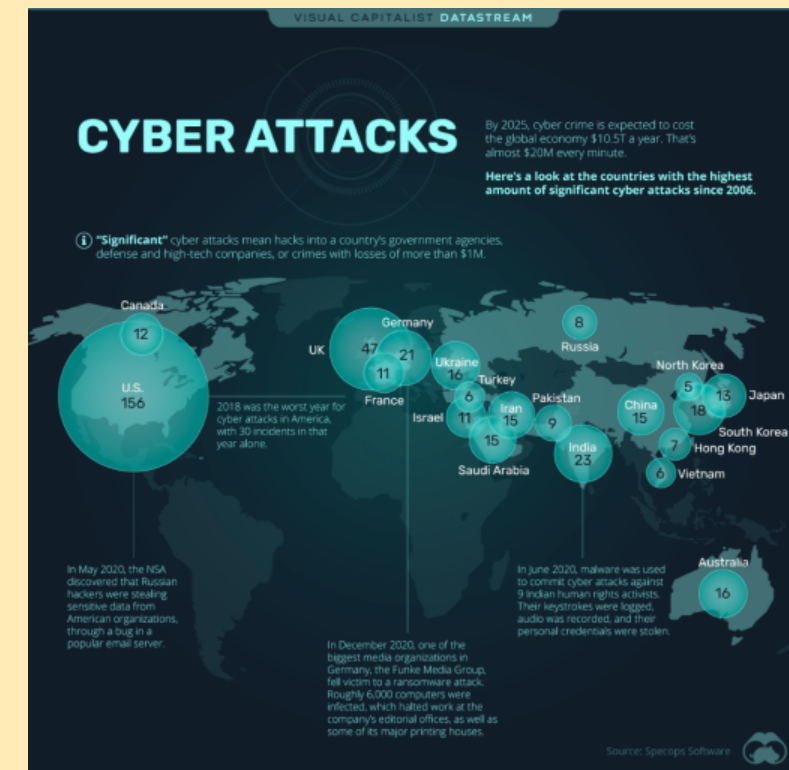
프로젝트 배경

01

현대 사회의 디지털 변환

02

사이버 보안 위협 증가



OWASP

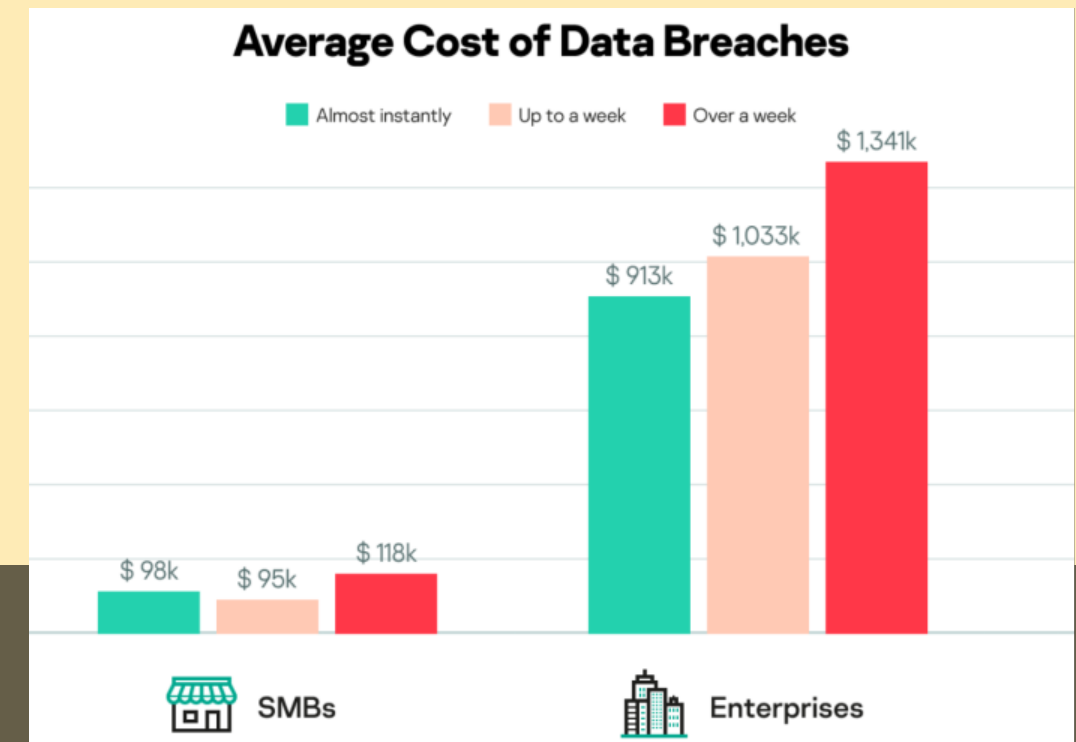
Open Web Application Security Project

03

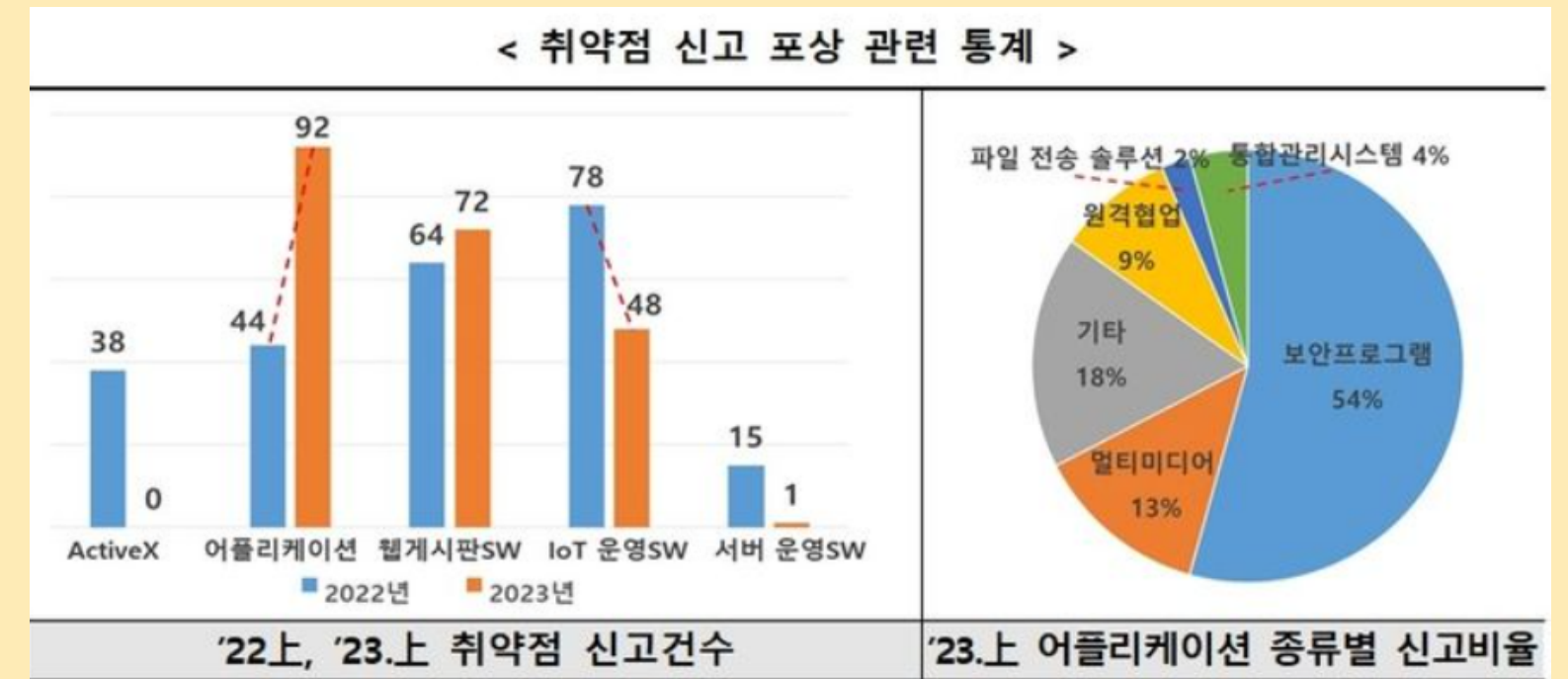
OWASP Top 10 의 중요성

04

인식 제고의 필요성



필요성 및 동기



보안 취약점은 심각한 결과를 초래하고 기업의 평판과 재정에 영향을 미친다.

웹 어플리케이션의 보안을 강화하는 것은 기업의 지속 가능성에 중요하다.

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

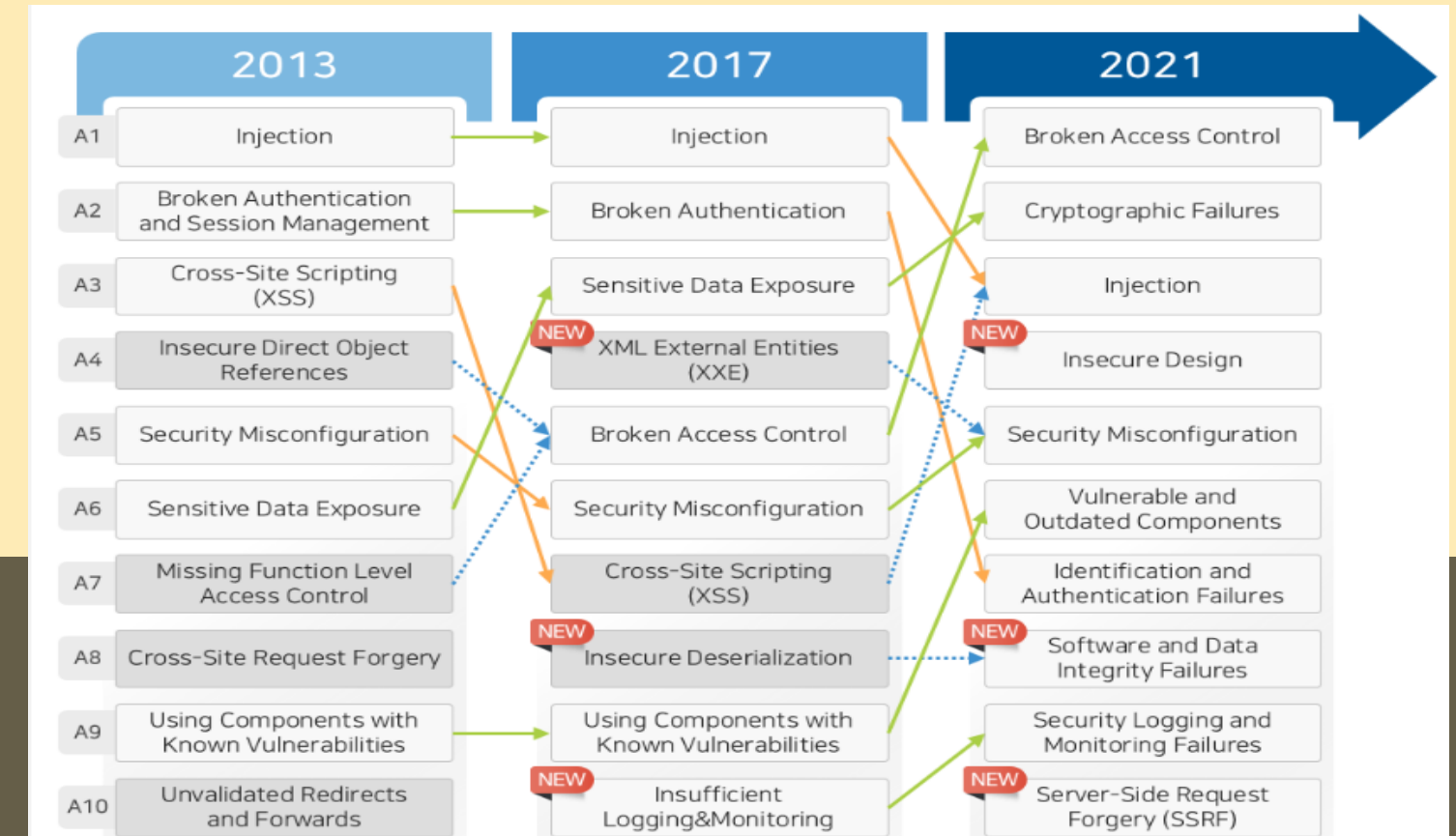
OWASP TOP 10의 중요성

Open Web
Application
Security Project

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failure
- software and Data integrity Failure
- Security Logging and Monitoring Failures
- Server-side Request Forgery

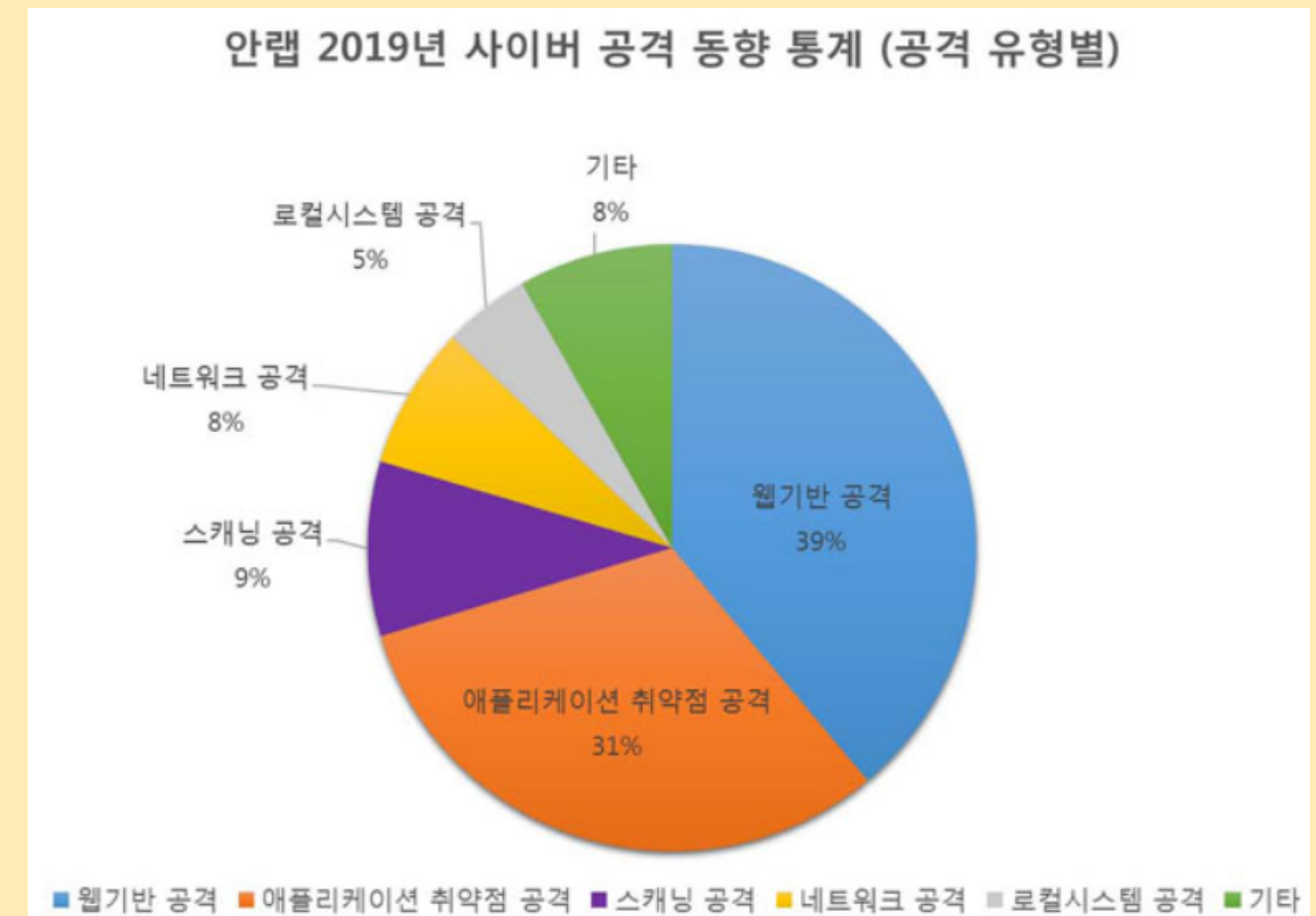
- 잘못된 접근 제어
- 암호화 오류
- 인젝션
- 안전하지 않은 설계
- 보안 설정 오류
- 취약하고 오래된 컴포넌트
- 식별 및 인증 실패
- 데이터 무결성 확인 문제
- 보안 로깅 및 모니터링 실패
- 서버 측 요청 위조

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	<ul style="list-style-type: none"> 수백 개의 조직과 10만개가 넘는 실제 애플리케이션 및 API에서 수집된 취약점들을 포함 CWE 데이터를 규정된 하위 집합에서 수집 	<ul style="list-style-type: none"> 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 합히 추정함 값으로 보정한 데이터에 따라 선별되고 우선순위 지정	<ul style="list-style-type: none"> 악용 가능성과 영향에 대한 데이터를 사용 발생률로 우선순위 지정
데이터 셋의 수	-	약 30 CWE	약 400 CWE



웹 애플리케이션 보안의 현 상황

Open Web
Application
Security Project



프로젝트의 목적

01

교육 및
인식 증진

02

자동화된
취약점 분석

03

보안 개선
가이드라인

04

커뮤니티 형성



기대 효과

01

보안 인식 향상

02

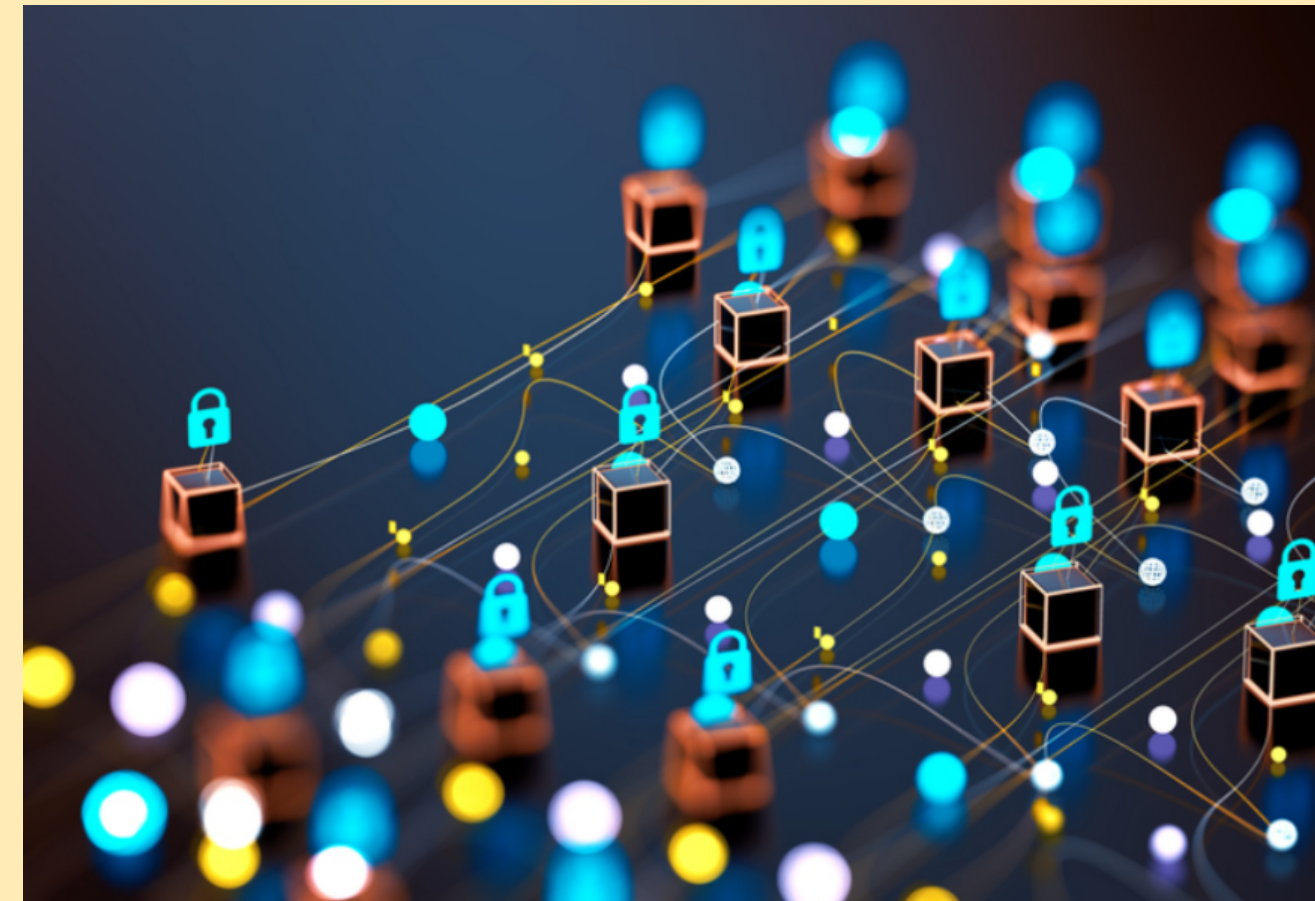
사고 예방

03

비용 절감

04

사용자 신뢰도
증가

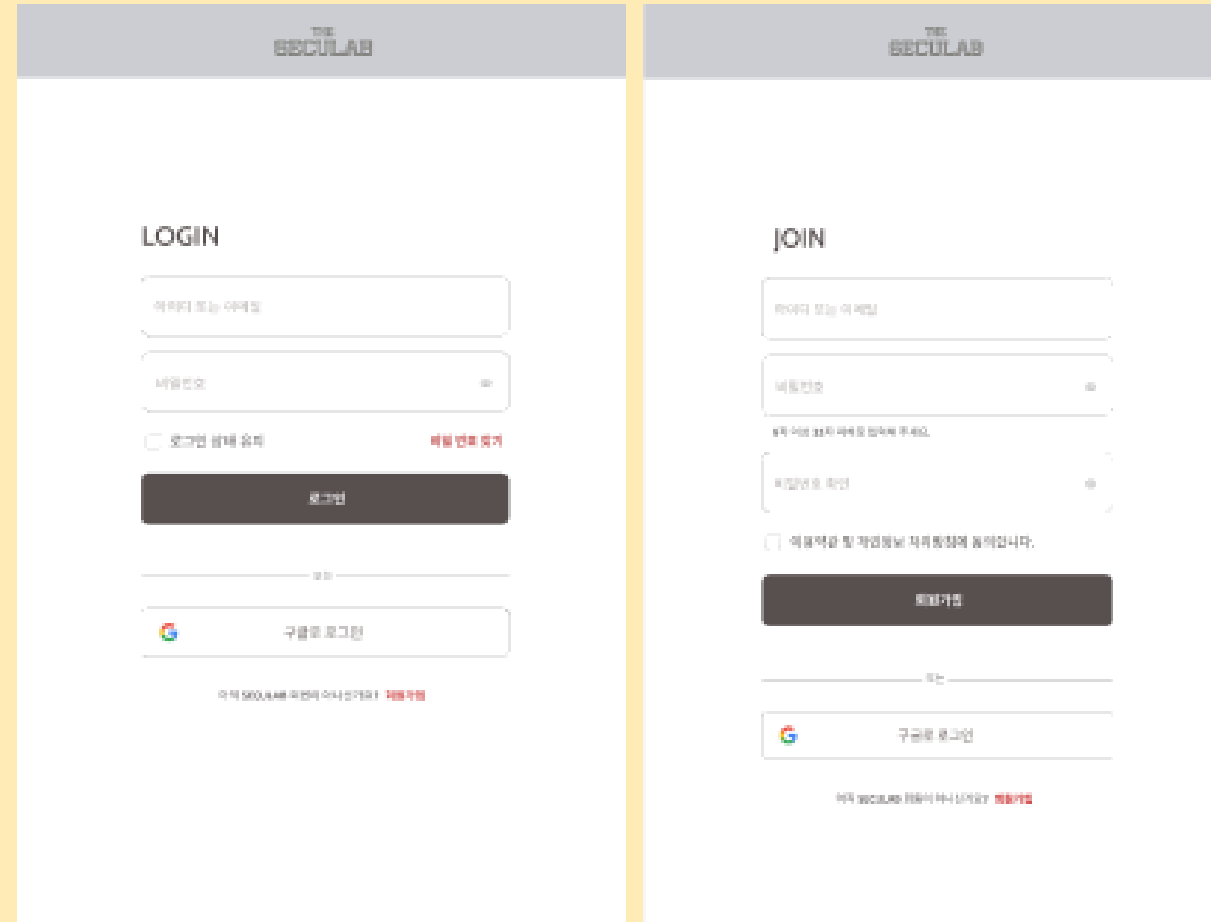


시스템 설계

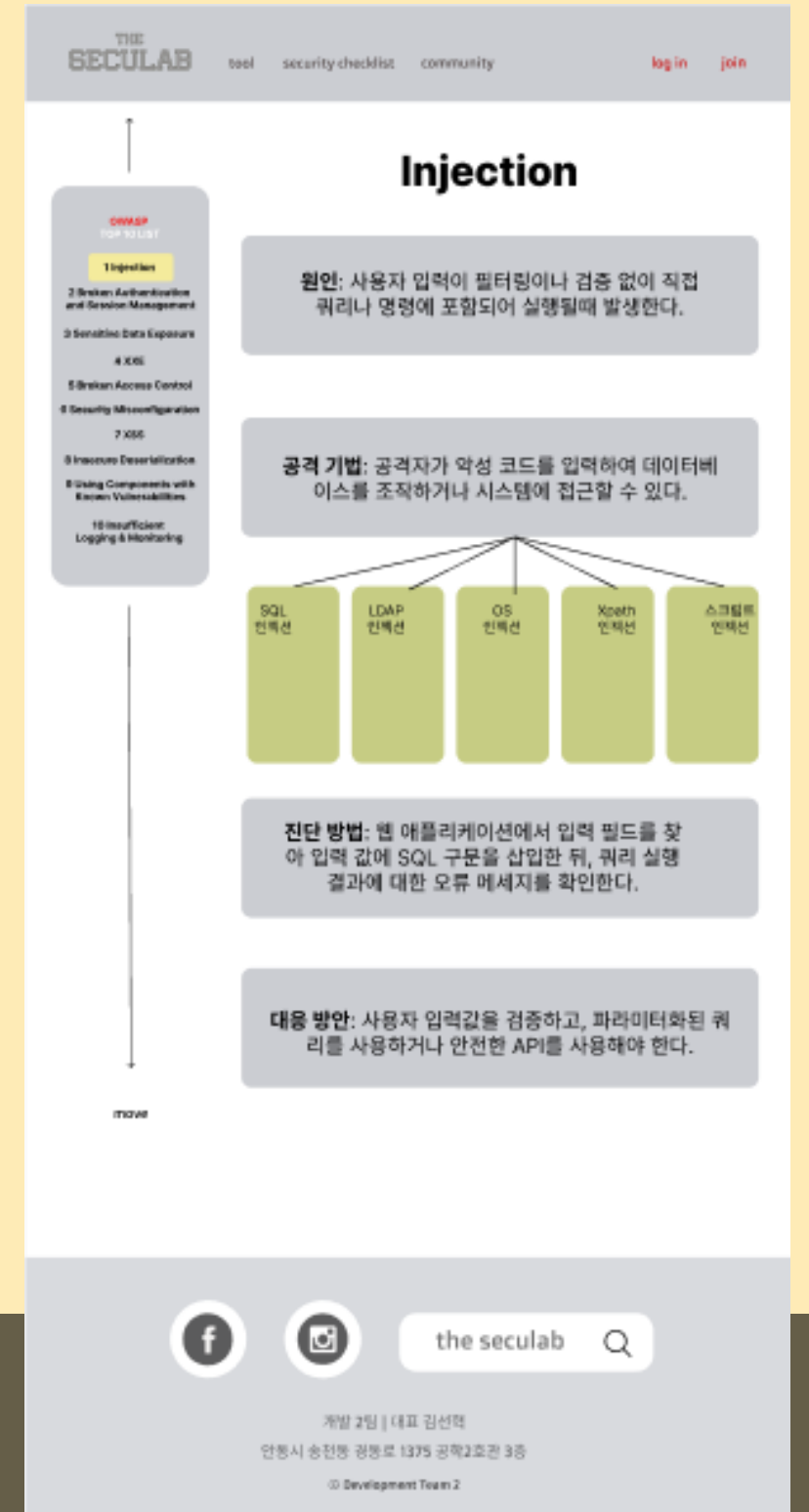
UI/UX 설계



메인 페이지



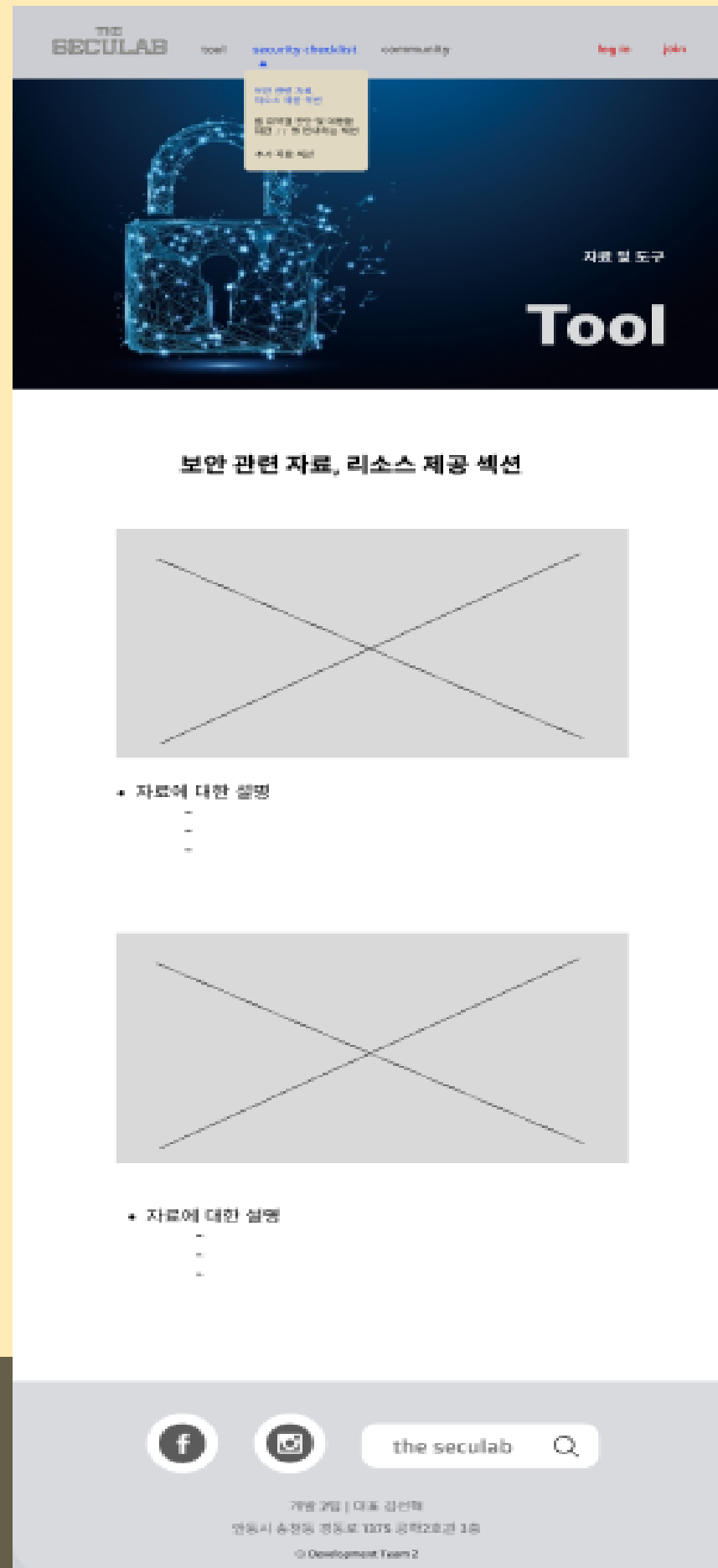
로그인 및 회원가입



취약점 상세페이지

시스템 설계

UI/UX 설계



자료 및 도구 페이지



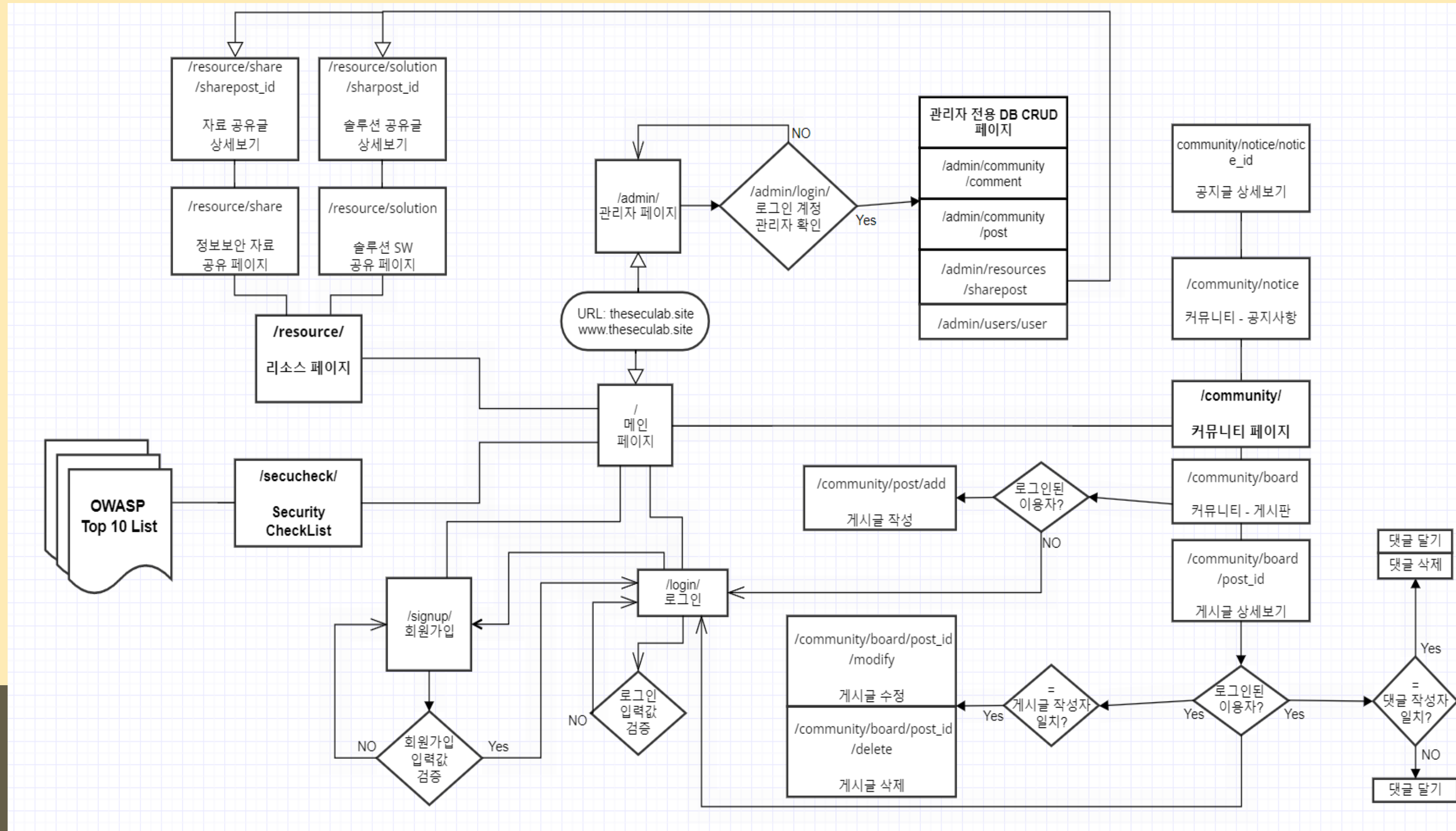
커뮤니티 및 지원페이지



게시글 등록 페이지

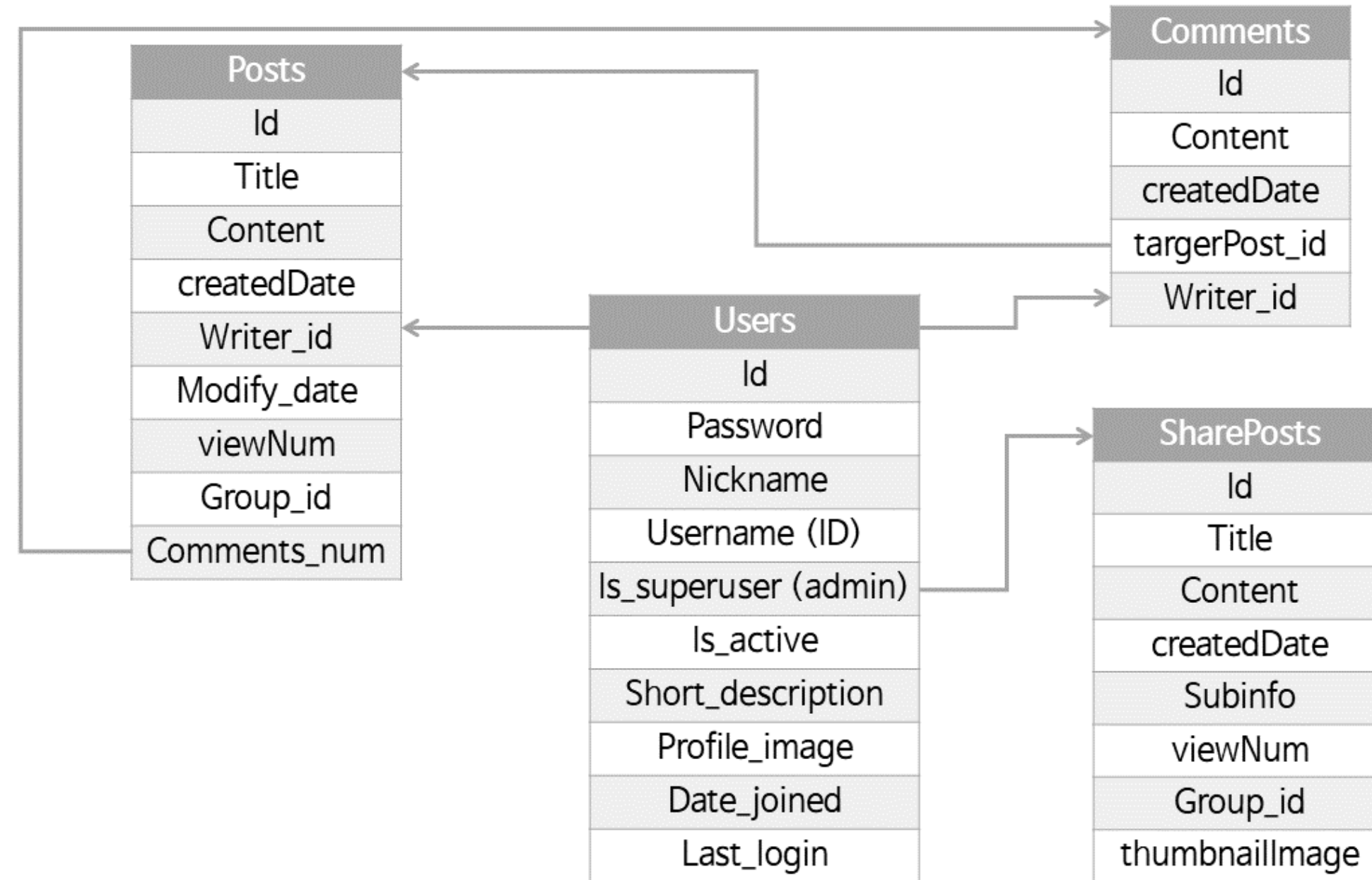
시스템 설계

Service Flowchart



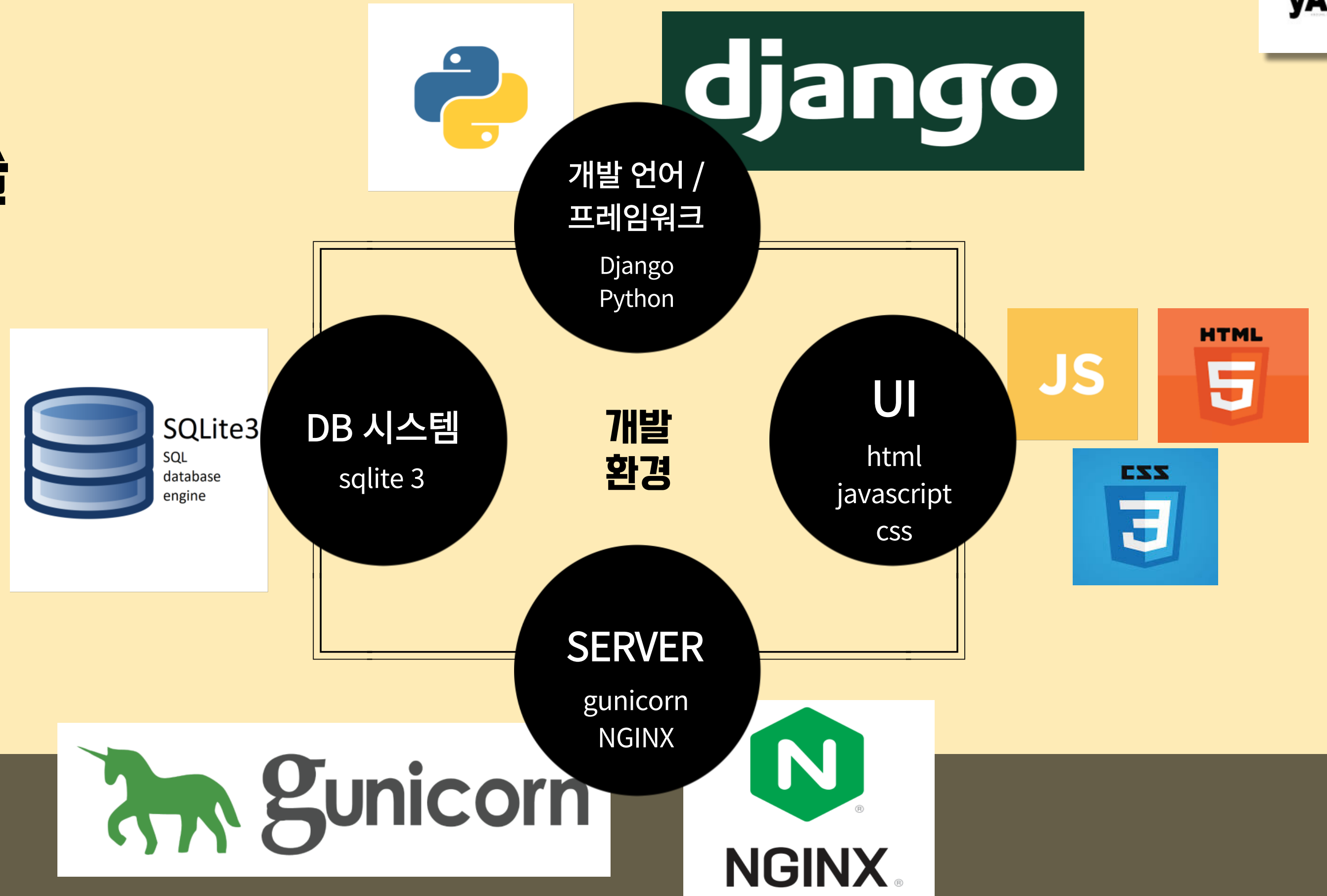
시스템 설계

DB Schema



개발 환경 & 기술

사용된 언어 및 개발 프레임워크



개발 환경 & 기술

사용된 언어 및
개발 프레임워크

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

02. 강력한 admin 관리자 페이지 기능

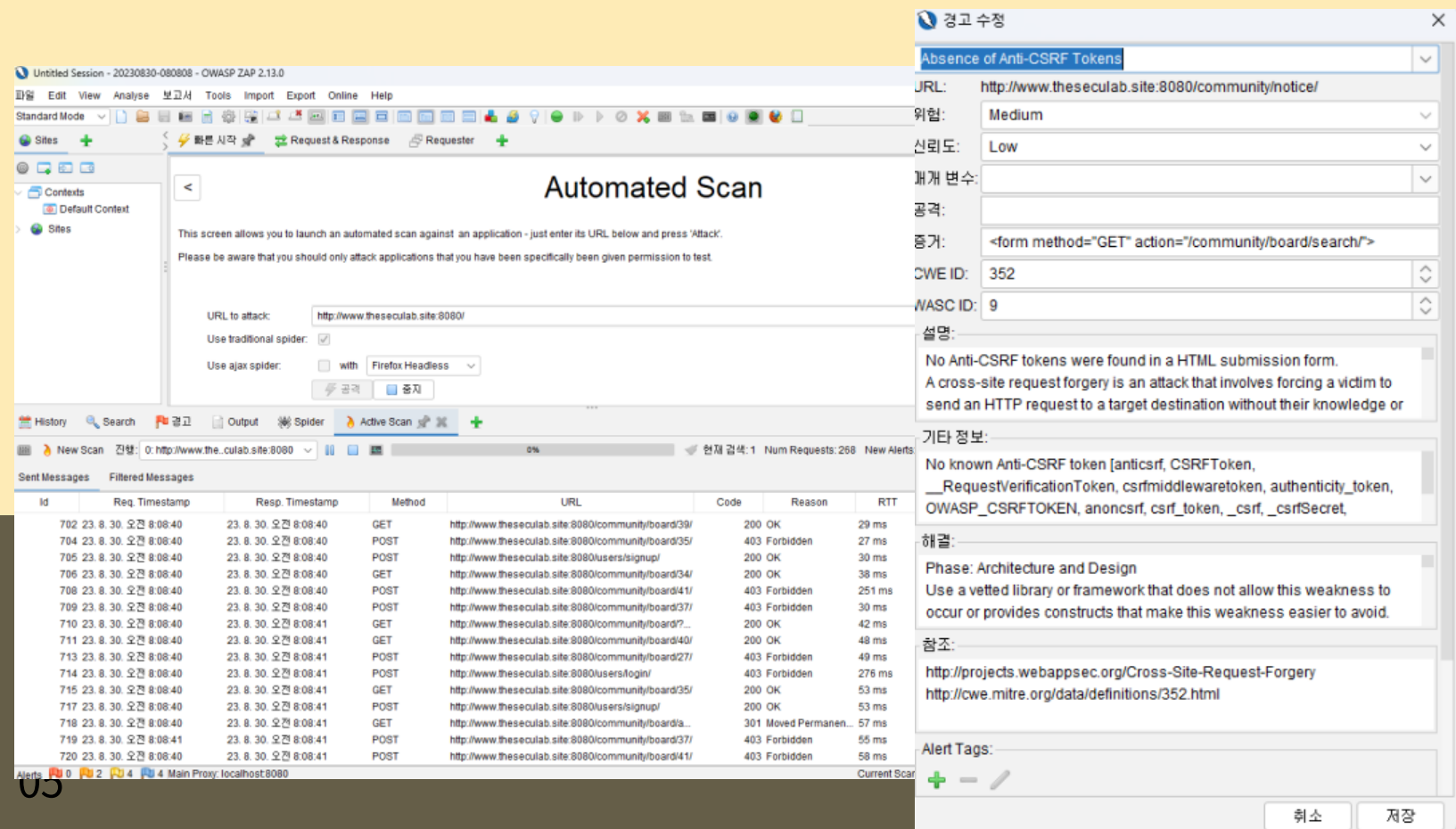
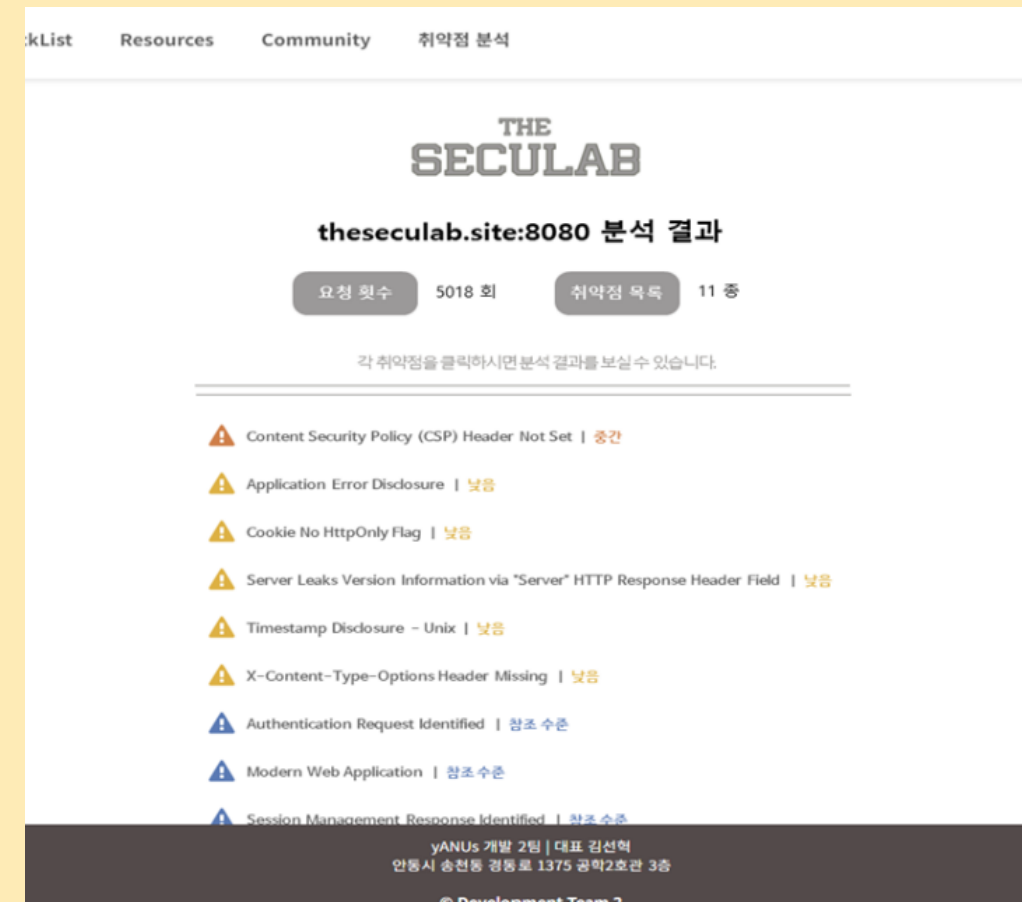
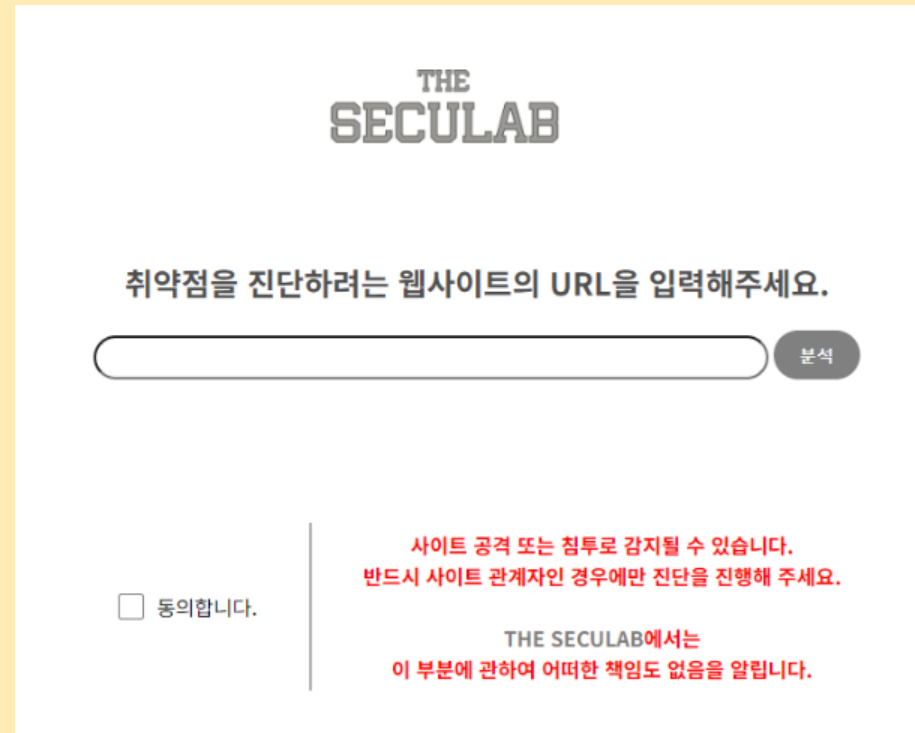
03. ORM (객체 관계 매핑) 지원

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

The Django logo, featuring the word "django" in a white, lowercase, sans-serif font on a dark green rectangular background.

주요 기능 및 서비스

이 자동화된 취약점 분석 제공



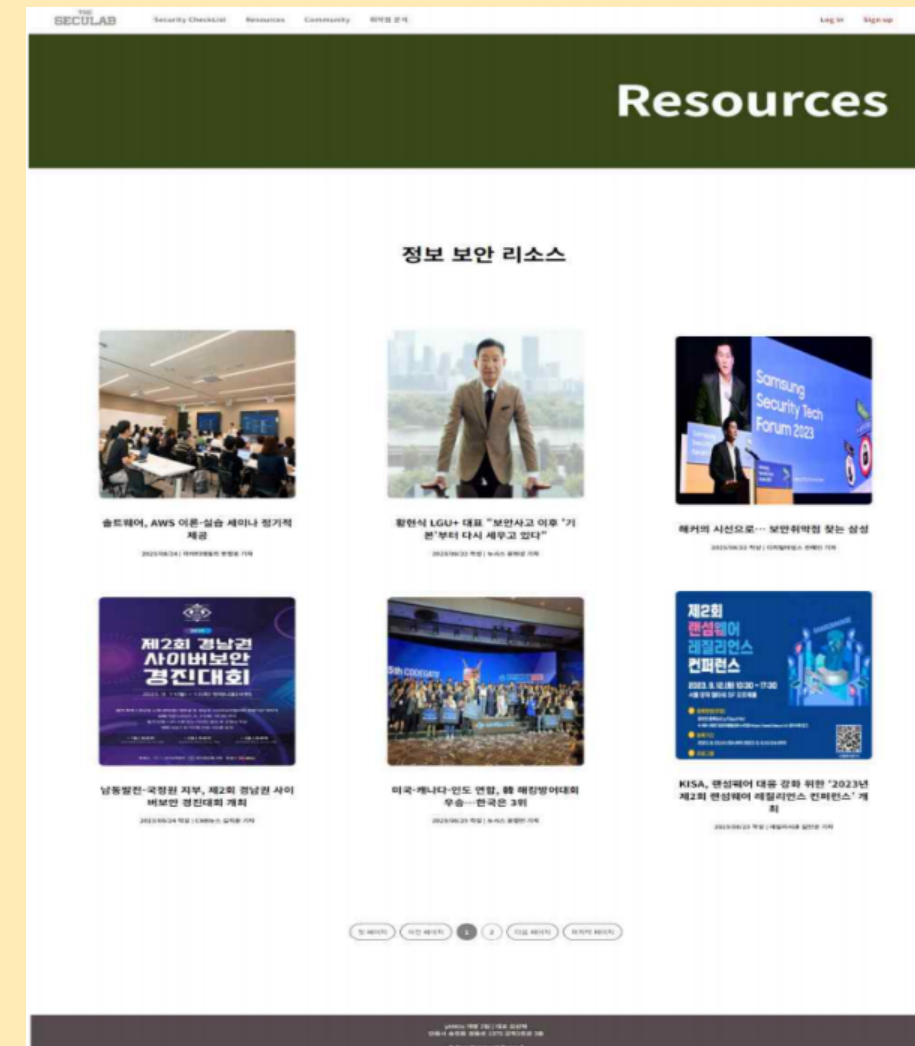
01. OWASP ZAP을 사용한 자동화된 취약점 분석
02. 파이썬과 ZAP API로 프록시 설정 조정 및 분석 실행
03. Spider를 통한 웹 페이지 크롤링과 취약점 스캔
04. 장고를 활용한 분석 결과의 실시간 분류 및 제공

주요 기능 및 서비스

02

자동화된 취약점 분석 제공

1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
1	date	title	writer	link	content	image										
2	2023-08-21 16:10	"투기거래 중단" 블라진드 LH 이혜진 기자 sunset@ch		https://n.news.naver.com/mnews/article/011...	직장인 커뮤니티 블라진드에 21일 올라온 첨부파일 다운로드 / 블라진드 '포우연 어직하로가' 직장인 익명 온라인 커뮤니티 블라진드에 전국민을 조롱한 글을 올린 LH 직원 계정의 주안글은 1년간 경찰 수사에도 결국 찾지 못했다. 강남역 일부 일대교로 국경을 위반한 경찰 계정의 댓글을 봤을 때, 이번 게시는 경찰 계정으로 일부 댓글을 올린 블라진드 유저의 댓글이 경찰청장이 직접 경찰청 사이버테러수사대에 수사를 지시하고 작성자 세상에 나섰다. 21일 경찰청에 따르면, 경찰청 사이버테러수사대는 이날 블라진드 게시물의 경찰청 소속 소부 열사의 작성자가 올린 첨부파일 다운로드에 대한 수사에 착수했다. 이날 오전 이 커뮤니티에는 '오늘 저녁 강남역 1번 출구에서 합류한다'라는 제목의 게시물이 올라왔다. 교 내	https://imgnews.ptstatic.net/image/002/2023/08/21/0003782865_001_20230822100106912.jpeg?perov=										
2	2016-03-22 10:41	이해일을 암호화 취약점 해소... 손경호(bontech@znet)		https://n.news.naver.com/mnews/article/011...	(지디넷코리아=손경호 기자)아래는 구글, 마이크로소프트, 페이스북, 이후 유 구글을 (가)업들이 이해할 암호화 기술에서 발견된 취약점을 해결하기 위해 협업한다. 이들 기업은 이해할 인공물 프로세스(SMT2)에 적용되는 확장가능 용 허니온 스타트(SSTARTS)라는 암호화 통신 기술을 제공해 왔다. 일반적으로 SMT2를 통해 받은 정보는 전송되는 이해할 암호화 해 전송하는 것이다. 문제는 스타트(S)가 가장 기본적인 암호화 통신 기능을 제공하고 있어 누군가 이해할 용어보기를 시도하면 송신 측이 이러한 기능을 부패시킬 수 있다는 것이다. 스타트(S)는 '반복 암호화 통신'을 시도했다가 실패하면 다시 열을 형태로 통신을 시도한다. 이것은 방식을 두고 기(최우의적인 암호화)(opportunistic encryption)라고 부른다.(관련링크)	https://imgnews.ptstatic.net/image/002/2016/03/22/bontech_ipCK1QhPHv_59_20160322104104.jpg?r=										
3	2023-09-24 18:17	"이집트 항공 유력 여객 대안"김지현(cheron@yna.co)		https://n.news.naver.com/mnews/article/011...	항공 비안재는 정치인, "열적 안 재도 감행할 수 있는 공격, 시도는 실패"	https://imgnews.ptstatic.net/image/001/2023/09/24/AKR023092404270009_02_1_24_20230924183806										
					이집트 여객 대안 주자 아흐메드 엘만사리 엘만사리 페이스북에 영상 업로드 28 일 뒤 관련 글자 (서울=연합뉴스) 김지현 기자 = 내년 초로 예상되는 이집트 여객의 유력한 대안 주자가 항공의 핵심 표적이 된다고 미국 일간 워싱턴포스트(WP)가 23일(현지시간) 보도했다. 구글과 사이버 위협을 감시하는 캐나다 정보보호대안 연구소 '기(이)문(문)의 조사 결과에 따르면, 알릴 리아 열사(이)문(문)에게 도전을 선언한 아흐메드 엘만사리 전 카라알 대로의 휴대전화가 프라테타 스파이웨어의 공격을 받은 사실이 확인됐다. 프라테타는 지난 7월 미국 상무부가 '사이버 공격으로 한 세계 개인과											



```

page = makepageint()
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_attr_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 기스크롤링하는 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") li div.news_area div.news_info div.info_group a.info")
    url = news_attr_crawler(url_naver, href")
    return url

#####크롤링 시작#####

#검색어 입력
search = ["질근권위위위위", "입화화화", "입화화화", "SSRF", "CSRF", "위위위위위위", "오래전전전전", "OWASP"]
#검색어 시작할 페이지 입력
page = 1
#검색어 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

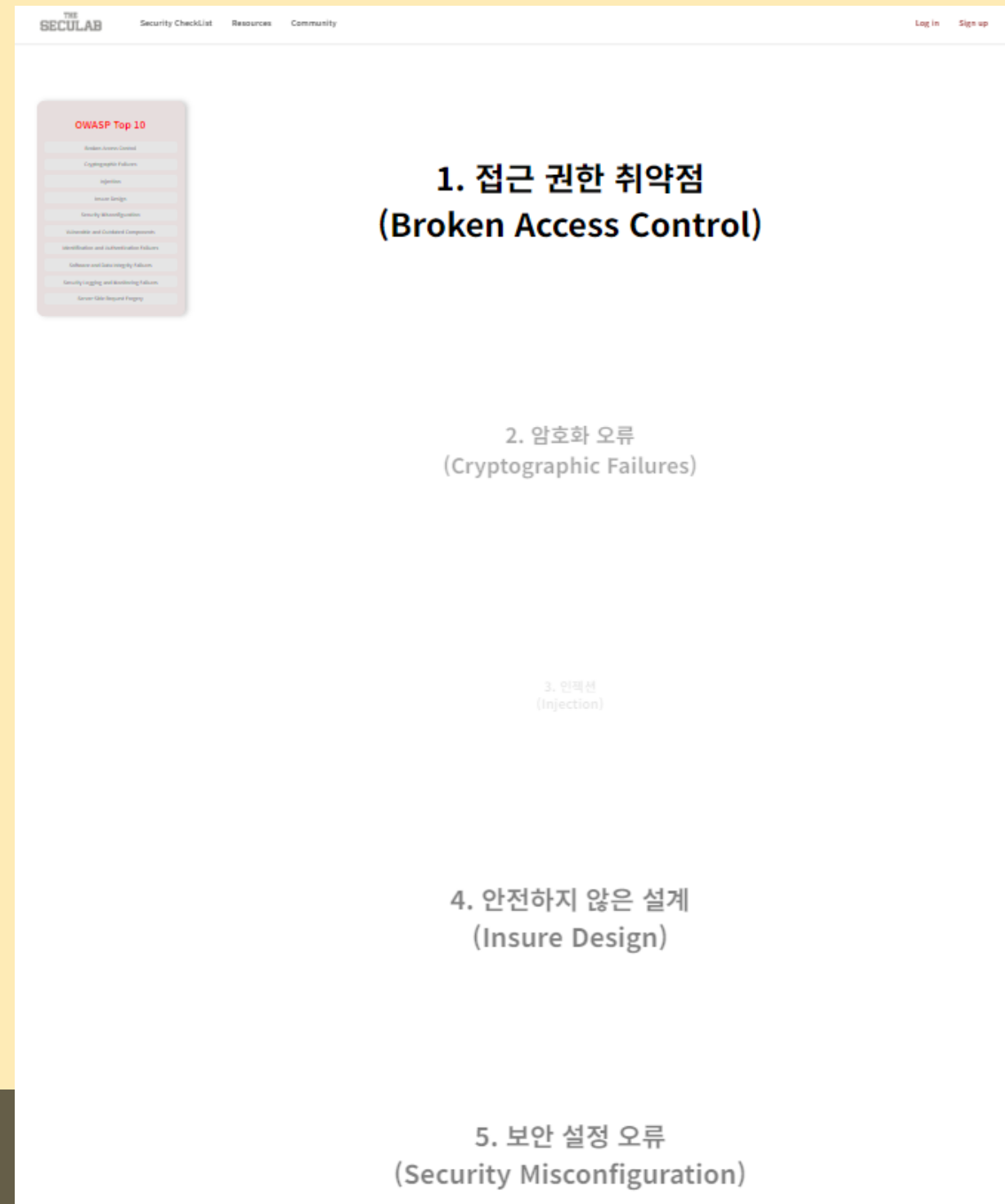
03. 크롤링한 데이터를 pandas로 가공하고 "피해액", "피해 사례" 등의 키워드로 2차 필터링

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

주요 기능 및 서비스

03

Security CheckList 제공



메인 페이지

구현 웹페이지 및 기능 소개

<http://www.theseclab.site/>



“ 당신의 웹을 지키세요 ! ”

소중한 홈페이지를 각종 웹 보안 위협들로부터 지켜내세요.

여러 취약점들의 다양한 공격 기법과 그에 따른 진단 방안, 대응 방안을 숙지하고 다양한 보안 자료와 정보들의 제공을 통해 안전한 웹 사이트를 설계하세요.

THE SECULAB과 함께라면 걱정하실 필요 없습니다.

Web Application 보안이 왜 중요할까요?

웹 사이트는 많은 정보와 데이터들 다루어 보안 위협에 쉽게 노출될 수 있는 환경에 놓여있습니다. 이에 웹 애플리케이션 보안은 매우 중요한 정보보호 이슈로 꾸준히 간주되어 왔으며, 이를 이해하고 적극적으로 대응하는 것은 웹 사이트의 신뢰성과 안정성을 보장하는 핵심적인 요소입니다.



THE SECULAB에서는 웹 개발자들이 보다 안전한 웹 사이트를 구축하고 운영하는 데에 도움이 되는 중요한 각종 정보들을 제공합니다. 웹 사이트 보안에 대한 이해와 대응은 개발 프로세스의 필수 요소로 어느덧 자리 잡고 있으며, 이는 웹 사이트의 잠재적인 취약점을 예방하고 사용자들의 데이터를 보호하는 데에 결정적인 역할을 합니다.

목적

THE SECULAB Security CheckList는 웹 개발자들이 자체 개발한 웹 사이트의 취약점을 스스로 식별하고 대응 방안을 찾을 수 있는 중요한 '참고서' 역할을 하는데에 목적을 두었습니다. 웹 개발자들은 CheckList를 통해 자신이 개발한 홈페이지의 보안 상태를 평가하고, 발견한 취약점에 대한 적절한 대응 조치를 함께 제공받을 수 있습니다.

이는 웹 보안에 대한 이해와 인식을 높이는 효과를 기대하며, 개발한 웹 사이트의 신뢰성과 안정성을 향상시키는 데 기여할 수 있습니다. 나아가, THE SECULAB에서는 모든 개발자들의 웹 개발 보안 인식을 제고하고, 각종 보안 위협에 대응하고 예방할 수 있는 능력을 함께 키우는 데 기여하고자 합니다.

OWASP Top 10 ?

OWASP Top 10이란 OWASP에서 제공하는 Web Application 취약점에 관한 가장 흔하게 발생하는 웹 사이트 위협과 취약점들을 나열한 목록입니다.

OWASP (Open Web Application Security Project)는 웹 보안 수준을 향상시키기 위한 노력을 범 세계적으로 주도하는 비영리 조직으로,

해당 단체에서 공개하는 OWASP Top 10 리스트는 보안 커뮤니티와 웹 산업 전반에서 널리 인정받는 매우 좋은 참조 자료로 자리잡아와

웹 보안의 현 상태 점검 및 가장 중요한 취약점들을 우선 파악하는 데에 도움을 기여합니다.

THE SECULAB을 어떻게 이용할까요?

THE SECULAB은 최신 트렌드를 고려하여 웹 취약점을 감지하고 대응하는 '감지된 방법'을 제공하는 데에 집중하고 있습니다.

또 보안 커뮤니티를 형성하여 보안 지식과 최신 이슈를 공유하며 이용자들 사이의 협력을 도모하고, 웹 보안에 도움이 되는 각종 최신 리소스와 자료를 공유함으로써 웹 개발자들을 대상으로 여러 가지 유형의 정보를 제공하는 데에 도움을 기여하고 있습니다.

또한 자체적인 Security CheckList를 설계하여 제공 가능한 모든 정보를 외국어 뿐만이 아닌, 한국어로 직관적으로 제시함으로써 THE SECULAB을 이용하는 웹 개발자들이 보다 안전한 웹 사이트를 구축하는 데에 부담스럽지 않은 참조적 이해를 돕고자 합니다.

로그인/ 회원가입 페이지

구현 웹페이지 및 기능 소개

<http://www.theseclab.site/>

THE SECULAB

LOGIN

아이디 (4자리 이상)

비밀번호 (4자리 이상)

[비밀번호를 잊어버리셨나요?](#)

로그인

또는

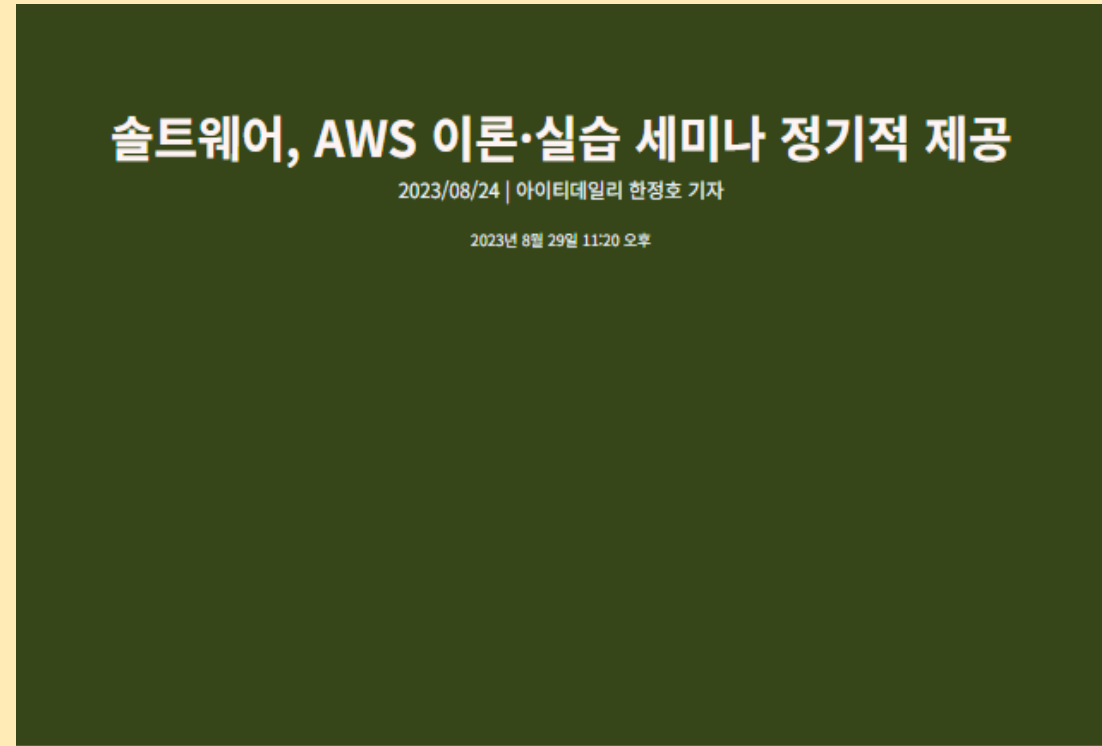
Google로 로그인

[아직 SECULAB 회원이 아니신가요? 회원가입](#)

Resource - 정보보안리소스 페이지

구현 웹페이지 및 기능 소개

<http://www.theseculab.site/>



다음 달 7일 'AWS 이머전 데이' 온라인 개최

[아이티데일리] 솔트웨어(대표 이정근)는 아마존웹서비스(AWS)의 서비스 파트너로서 'AWS 이머전 데이 (AWS Immersion Day)'를 개최, AWS 플랫폼 전문가 양성 및 함께 활용 가치를 극대화하는 데 기여하고 있다고 24일 밝혔다.

솔트웨어에서 제공하는 AWS 이머전 데이는 AWS 클라우드상에서 기본적인 코어 서비스에 더해 마이그레이션, 컨테이너, 인공지능 등 다양한 영역을 실행 및 경험할 수 있도록 설계됐다. 해당 세미나는 AWS에서 제공하는 문서를 기반으로, 솔트웨어 전문 솔루션즈 아키텍트가 진행하는 하루 또는 반나절 단위 기술 워크숍이다.

AWS 이머전 데이는 경험 기반 접근 방식을 통해 AWS 플랫폼을 더 쉽고 빠르게 활용할 수 있게 실습 위주의 세미나를 진행하고, AWS 고객의 비즈니스 목표를 빠르게 달성할 수 있게 돕는다.



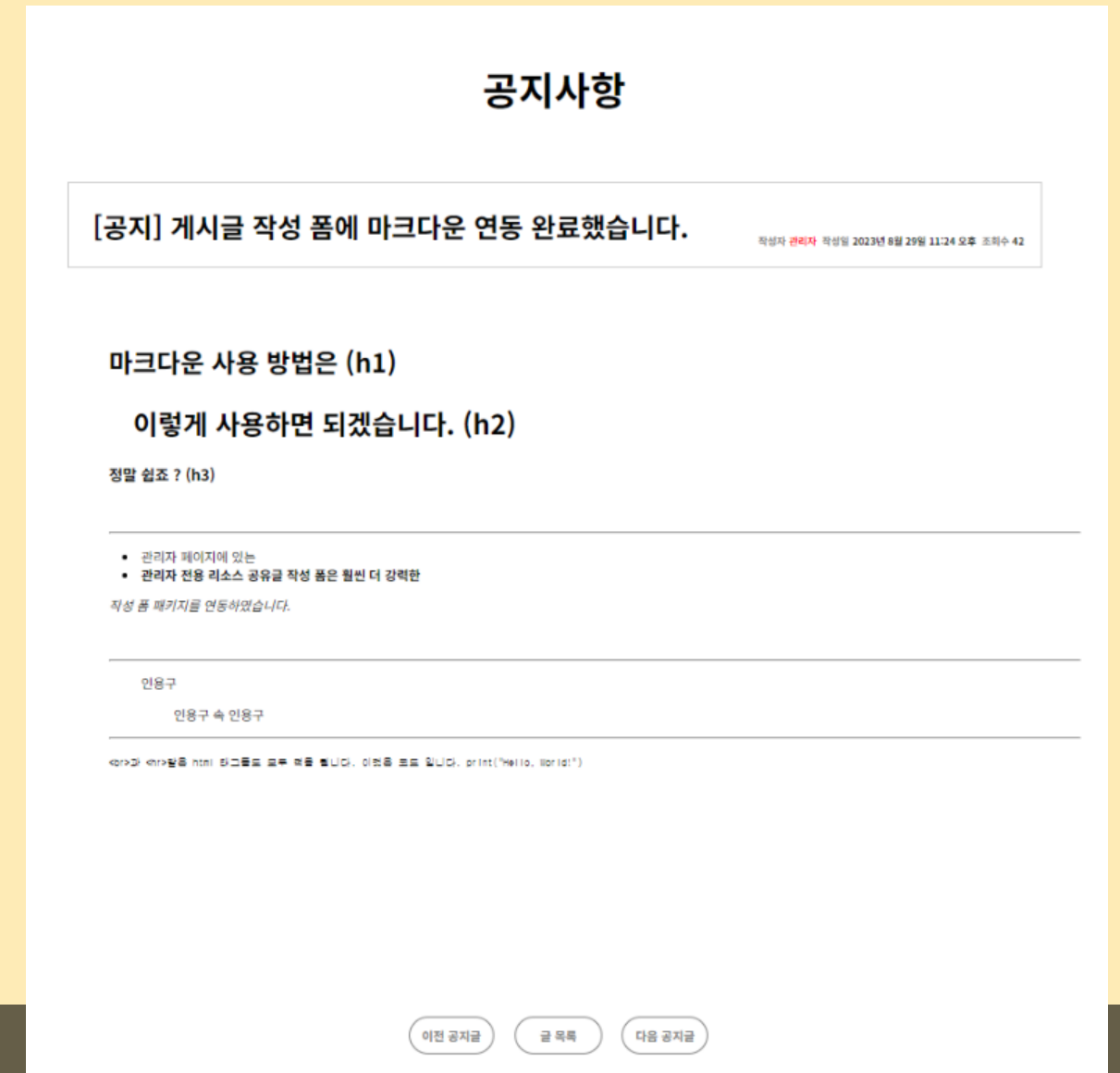
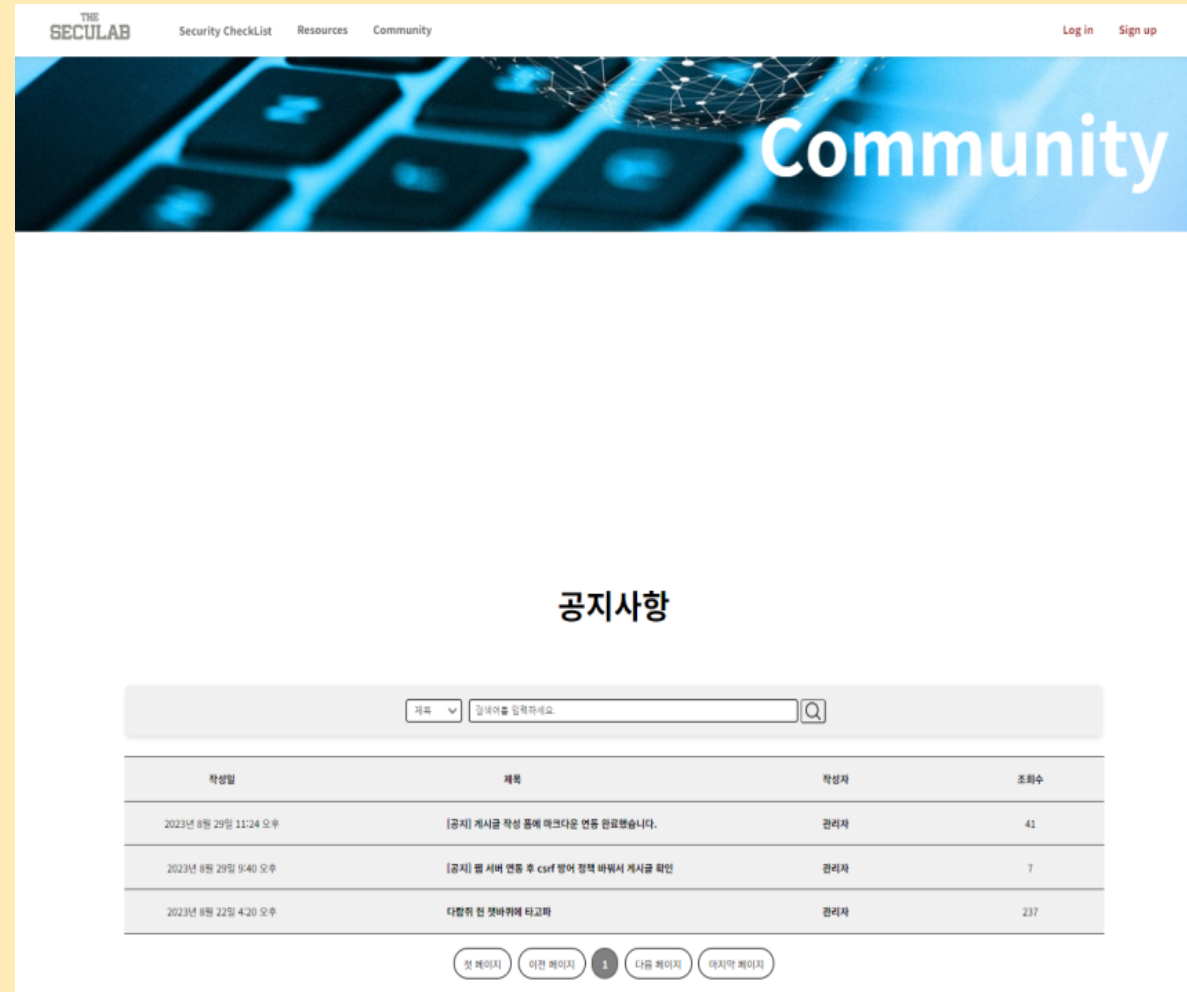
상세페이지



Community 페이지

구현 웹페이지 및 기능 소개

http://www.theseclab.site/

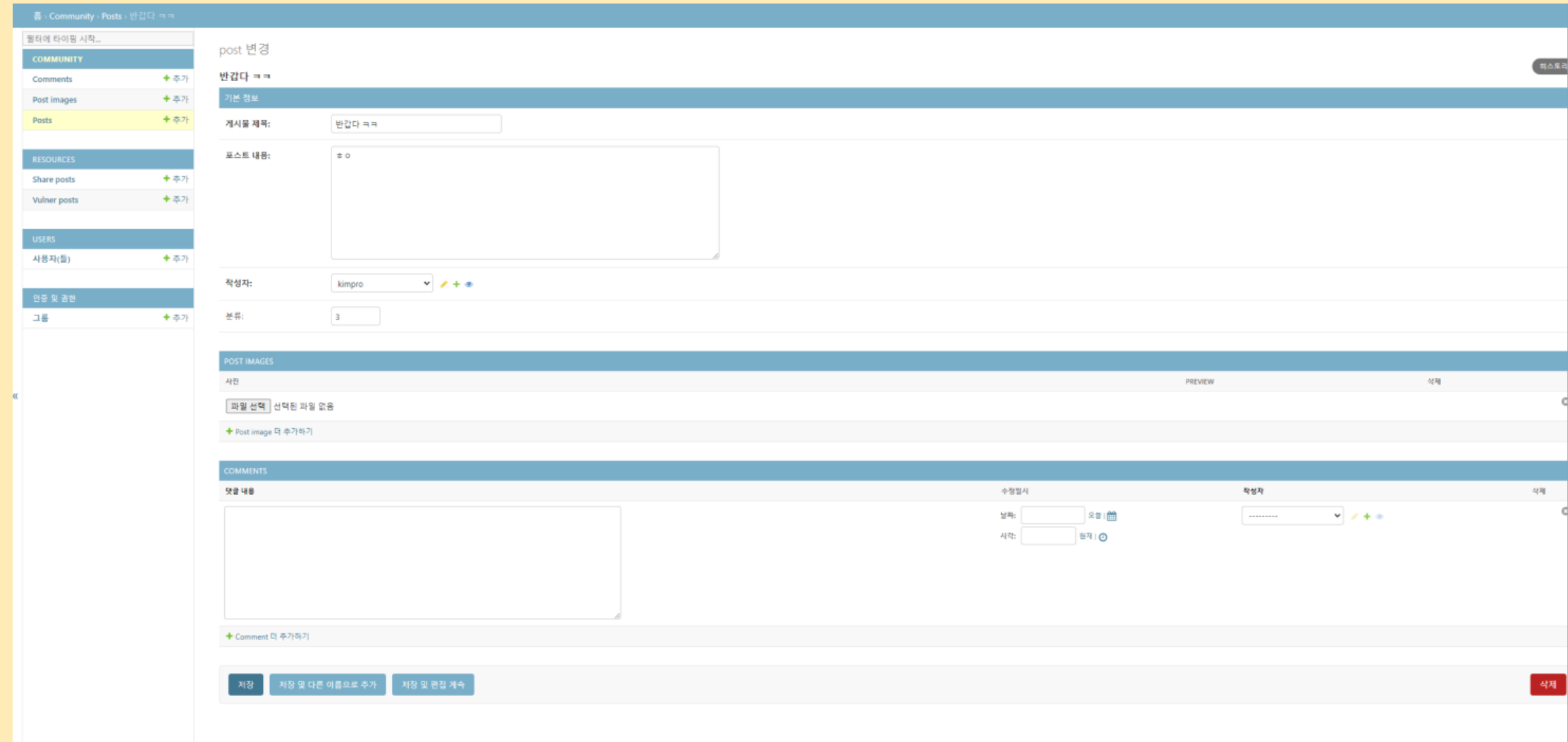


상세 보기 페이지

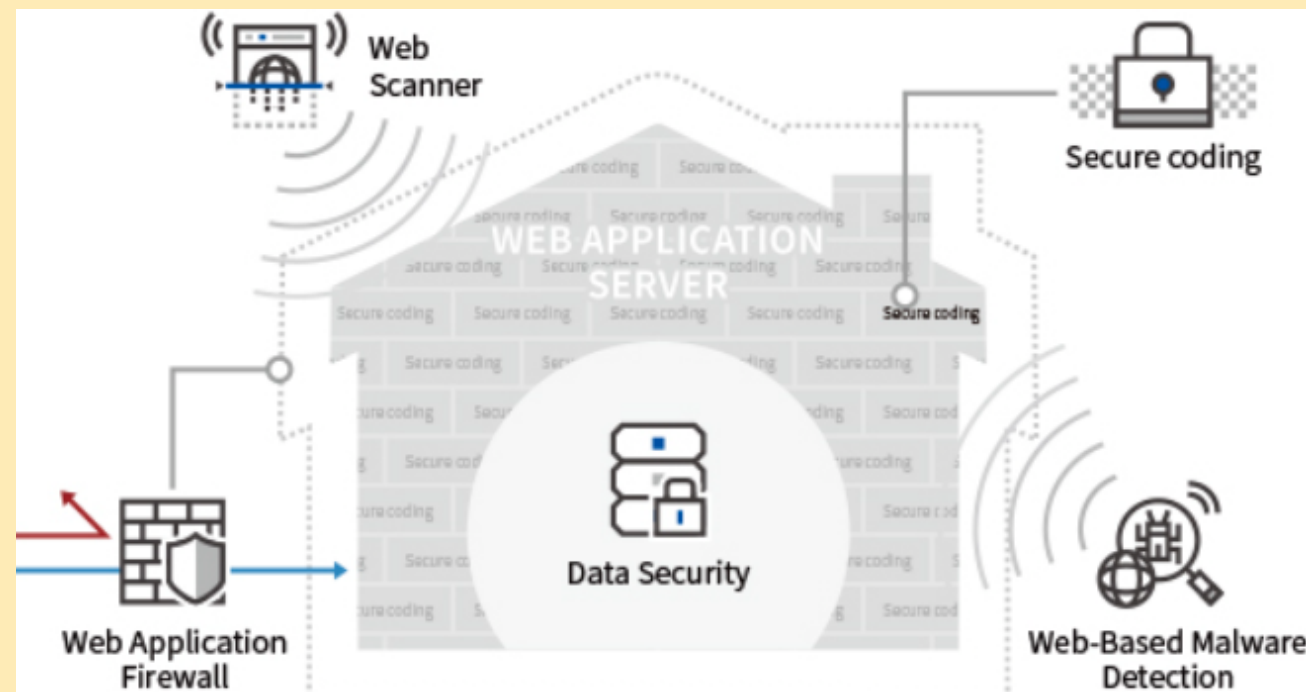
관리자 페이지 (모든 DB C/R/U/D 가능)

구현 웹페이지 및 기능 소개

<http://www.theseclab.site/>



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

향후 계획 및 개선점



감사합니다

THE
SECULAB

야누스 개발 2팀