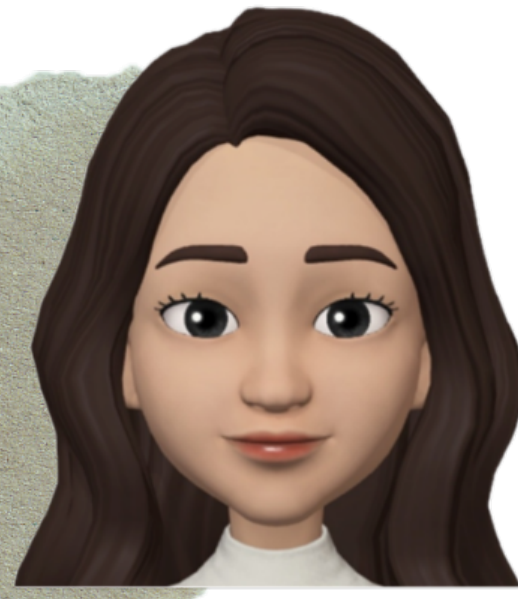


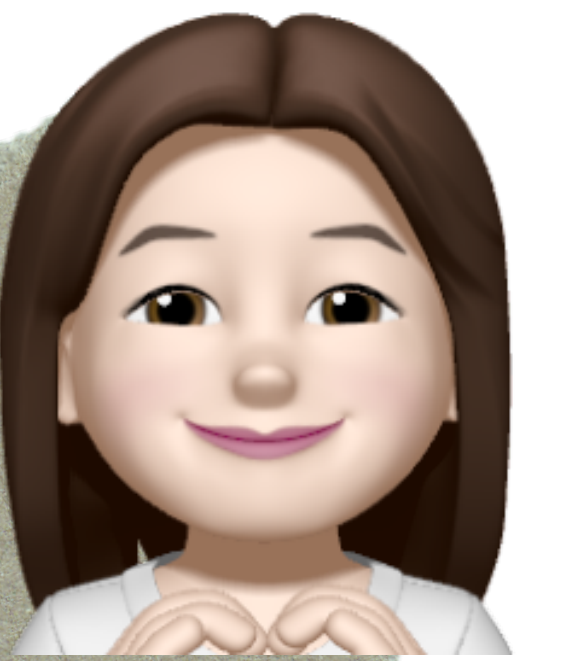
진단도구 & DB

92015350 이지원



프론트엔드 & 백엔드

91913945 이다연



진단도구 & DB

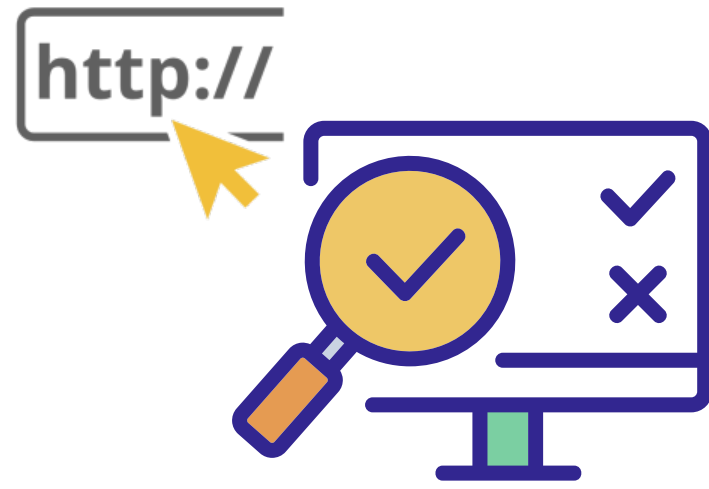
92015324 이유진 (팀장)



DB & 백엔드

92015219 신하린

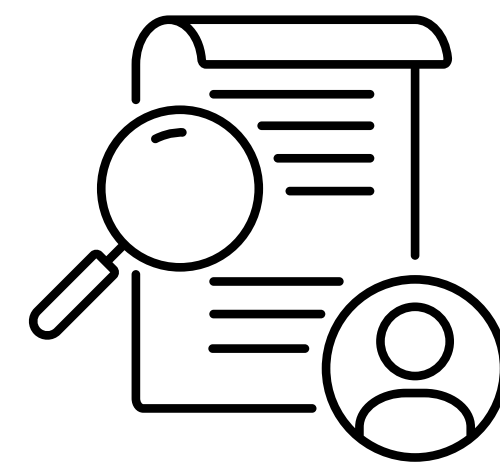
구상도



진단 url 등록 후,
항목 별 진단



진단 완료 후
DB 저장



진단 결과 페이지에서
결과 확인



웹서비스

웹 취약점 진단서비스

Python으로 개발한 자동화도구를 통해 웹사이트를 진단하는 서비스입니다.

수행단계

- 01 사전 준비
로그인
- 02 URL 조회
웹 사이트 URL 입력
- 03 진단 진행
도구 실행
웹 취약점 진단

URL

점검할 웹 사이트의 URL을 입력해주세요
로그인 후, 진단 서비스를 이용할 수 있습니다.

URL을 입력해주세요

조회



진단결과



pdf 다운로드
기능까지 구현

URL : http://192.168.110.131/bwapp/
점검일자 : 2023-10-15

번호	항목	직전 이력	현재 이력
1	SQL Injection (로그인)	Risk	Risk
2	SQL Injection (검색)	Risk	Risk
3	PHP CODE Injection	Risk	Risk
4	관리자 페이지 노출	Risk	Risk
5	디렉터리 리스팅	Risk	Risk
	약점	Safe	Safe

대응방안

대응 방안

일반 사용자가 유추하기 어려운 이름으로 관리자 로그인 페이지 주소 변경 및 관리자 페이지 접근 포트를 변경합니다. 웹 방화벽을 이용하여 특정 IP만 접근 가능할 수 있도록 룰셋을 적용합니다.

불충분한 인증

중요한 내용이 담긴 정보를 HTML 소스에 포함하지 않도록 합니다.

약한 문자열 강도

취약한 계정 및 패스워드를 삭제합니다. 로그인시 패스워드 입력 실패가 일정 횟수를 초과할 경우 관리자에게 통보 및 계정을 잠금 처리합니다. 이때, Server Side Script를 통해 구현합니다.

Blind SQL

정적 쿼리나 동적 쿼리에 사용되는 입력값의 길이나 속성을 검증하여 적절한 필터링 및 제한을 수행합니다. 웹 애플리케이션의 로깅 시스템을 강화하여 의심스러운

Q. 기대효과는 무엇인가요?

자동화된 취약점 진단도구를 이용해 웹사이트의 보안 수준 향상에 필요한 시간과 비용을 절감시킬 수 있습니다.