PRODUCT INTRODUCTION

U-SAFE Web v1.0

운영 중인 웹 애플리케이션을 직접 요청해 취약점을 찾는
웹 동적 보안점검(DAST) 솔루션

- 능동·수동 점검
- OWASP·행안부·국정원
- 로그인·접근통제
- 증적 중심 보고서

CONTENTS

목 차

소스코드가 아닌 '동작하는 웹'을 점검하는
U-SAFE Web v1.0의 주요 내용을 소개합니다.

01 **제품 소개**
도입 배경과 제품 개요

02 **핵심 점검 엔진**
크롤링 · 능동/수동 점검 · 접근통제 검증

03 **주요 기능**
점검 대상 · 동적 점검 · 취약점 · 통계 · 보고서

04 **제품 특장점**
실증성 · 준거성 · 안전성 · 협업성 · 편의성

05 **구성 및 기대효과**
배포 형태와 도입 기대효과

도입 배경 Why Web DAST

운영 중인 웹 애플리케이션은 주기적인 보안취약점 점검이 요구되며, 발견된 약점은 증거와 함께 조치·보고해야 합니다.

제도 요구사항

1 「정보통신망법」·「전자정부법」

정보시스템의 보안취약점을 주기적으로 점검·보완하도록 규정합니다.

2 주요정보통신기반시설 취약점 분석·평가

KISA·국정원 웹 취약점 점검 가이드에 따라 운영 서비스를 진단합니다.

3 감리 · 보안성 검토 대응

웹 취약점 점검 결과와 조치 내역을 근거 자료로 제출해야 합니다.

현장의 어려움

! 높은 도입·유지 비용

상용 DAST 도구는 라이선스·유지보수 비용 부담이 큽니다.

! 수동 점검 공수

로그인·권한별 점검을 사람이 반복 수행해야 합니다.

! 범위 통제의 어려움

운영 중인 서비스를 과도하게 건드릴 위험이 있습니다.

! 증적·보고서 수작업

요청/응답 증거를 양식에 맞춰 다시 정리해야 합니다.

U-SAFE Web 은 탐색 → 점검 → 확인 → 증적 → 보고 전 과정을 하나의 도구로 해결합니다.

U-SAFE Web v1.0 Product Overview

승인된 웹 애플리케이션을 직접 요청·탐색하며 취약점을 찾아내는 설치형 웹 동적 보안점검(DAST) 솔루션입니다.

DAST	Top 10	3 종	10 단계
실행 기반 동적 점검	OWASP 국제표준 대응	점검 기준(행안부·OWASP·국정원)	보안약점 조치 상태

실행 기반 동적 점검

크롤링으로 화면·요청을 수집하고 능동(Active)·수동(Passive) 플러그인으로 운영 중 상태를 직접 점검합니다.

로그인·멀티계정 접근통제

폼/세션 로그인 후 계정별 접근 차이를 비교해 접근통제 취약점을 자동으로 판정합니다.

허용 범위 내 안전한 점검

승인된 대상·범위(scope)와 요청 예산 안에서만 요청해 서비스 영향을 통제합니다.

증적 중심 보고서

요청/응답 증거와 증적 이미지를 PDF·Excel·SARIF 보고서로 클릭 한 번에 생성합니다.

점검 범위 Coverage

웹 애플리케이션에서 자주 발생하는 취약점 유형을 점검하고, 국제·국내 보안 기준으로 결과를 분류합니다.

점검 유형	대표 취약점
인젝션	SQL · 명령 · XPath · LDAP · SSI 삽입
크로스사이트	XSS(반사·저장·DOM) · CSRF
접근통제	인가 우회 · 경로 조작 · 권한 상승
인증 · 세션	취약한 인증 · 세션 관리 · 쿠키 속성
설정 · 정보노출	보안 헤더 · 디렉터리 · 오류 · 백업 파일
전송 · 요청위조	TLS 설정 · SSRF · 오픈 리다이렉트

대응 점검 기준

W **OWASP Top 10 (2021)**
A01 접근 통제 ~ A10 SSRF

M **행정안전부 웹 취약점**
공공 웹 서비스 점검 기준

N **국정원 웹 취약점 8종**
N1 SQL 인젝션 ~ N8 접근 제어

점검 대상

· HTTP / HTTPS 웹 애플리케이션
· SPA(화면 렌더링)로 동적 링크까지 탐색
· 승인·등록된 대상, 허용 범위(scope) 내에서만 점검

동적 점검 엔진 Dynamic Scan Pipeline

운영 중인 웹을 직접 탐색하고 요청을 보내 반응을 관찰함으로써, 실제로 동작하는 취약점을 확인합니다.

1 **탐색(크롤링)** 화면·링크·폼 수집 › 2 **요청 생성** 경로·파라미터 조합 › 3 **페이로드 주입** 능동 점검 입력 › 4 **응답 분석** 변화·오류 관찰 › 5 **증거 수집** 요청/응답 저장

수동 점검 Passive

오가는 요청/응답을 관찰만 해 보안 헤더·정보노출·쿠키 설정을 점검합니다. 서비스를 변경하지 않습니다.

능동 점검 Active

실제 페이로드를 주입해 인젝션·XSS 등 취약점의 반응을 확인합니다. 승인된 범위에서만 수행합니다.

점검 예시 · 인젝션 반응 확인

```
요청  GET /board/view?id=1' OR '1'='1
응답
HTTP 500  SQL syntax error near ''1''…   → 주입 지점 반응 확인
판정
WEB-01 SQL 인젝션  ·  심각도 높음  ·  요청/응답 전문을 증거로 저장
```

로그인 · 멀티계정 접근통제 점검 Access Control

로그인 뒤 화면까지 점검하고, 여러 계정의 접근 차이를 비교해 접근통제 취약점을 자동으로 찾아냅니다.

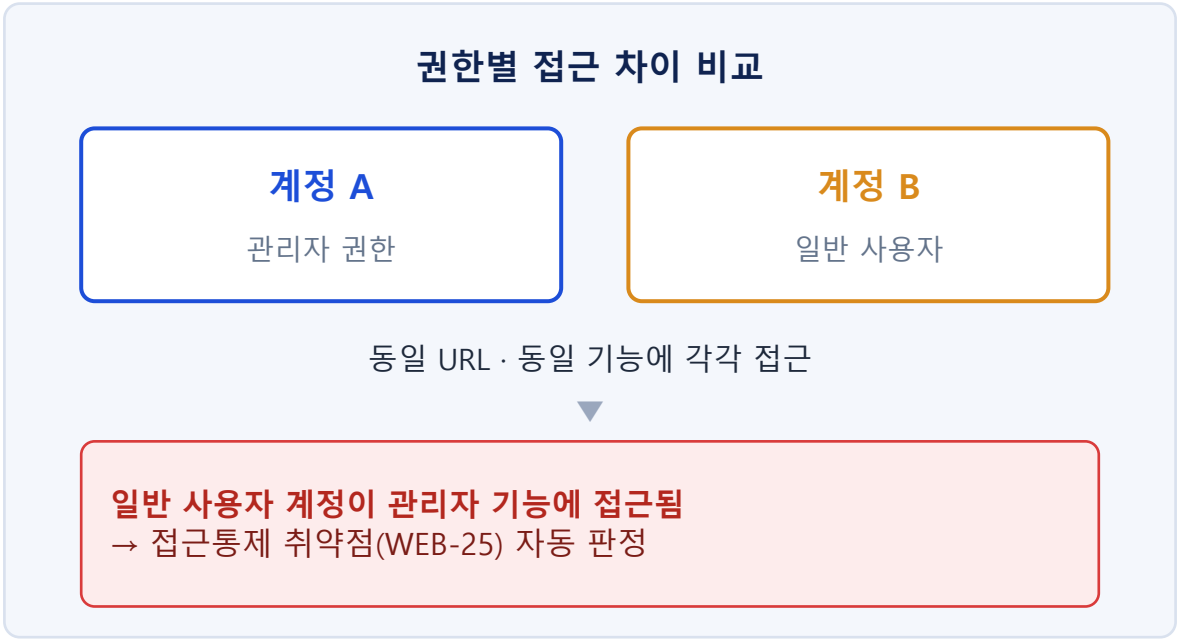
1 폼 · 세션 로그인

아이디·비밀번호를 암호화 저장하고, 점검 시작 시 자동 로그인해 인증이 필요한 화면까지 점검합니다.

2 멀티계정 접근 비교

여러 계정으로 같은 기능에 접근해 권한별 응답 차이를 자동 비교합니다.

3 접근통제 취약점 판정



안전장치 승인된 대상만 점검 · 허용 범위(scope) 제한 · 요청 예산으로 과도한 요청 방지 · 운영 서비스 영향 최소화

대시보드 Dashboard

전체 프로젝트의 점검 현황과 위험 수준을 한 화면에서 파악하고, 카드·차트를 눌러 해당 목록으로 바로 이동합니다.

1 핵심 지표 카드

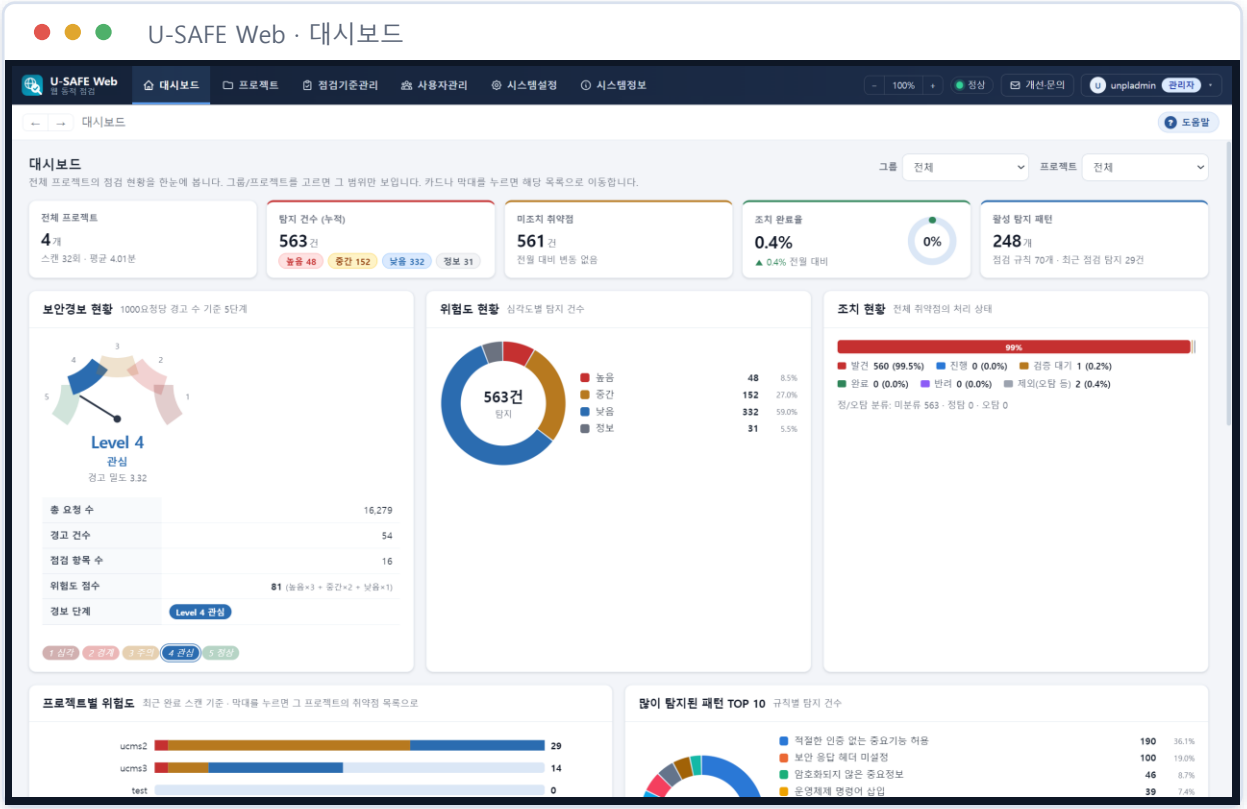
프로젝트 · 탐지 건수 · 미조치 취약점 · 조치 완료율 · 활성 탐지 패턴

2 보안경보 5단계

1,000요청당 경고 밀도로 심각·경계·주의·관심·정상을 표시

3 위험도 · 조치 현황

심각도 분포 · 처리 상태 · 프로젝트별 위험도 · 많이 탐지된 패턴 TOP 10



점검 대상 · 범위 관리 Target & Scope

점검할 웹 애플리케이션을 등록·승인하고, 허용 범위와 요청 예산을 지정해 안전한 점검 환경을 준비합니다.

1 **대상 URL 등록 · 승인**

점검 권한을 확인한 대상만 등록해 점검 범위를 통제

2 **허용 범위(scope) 지정**

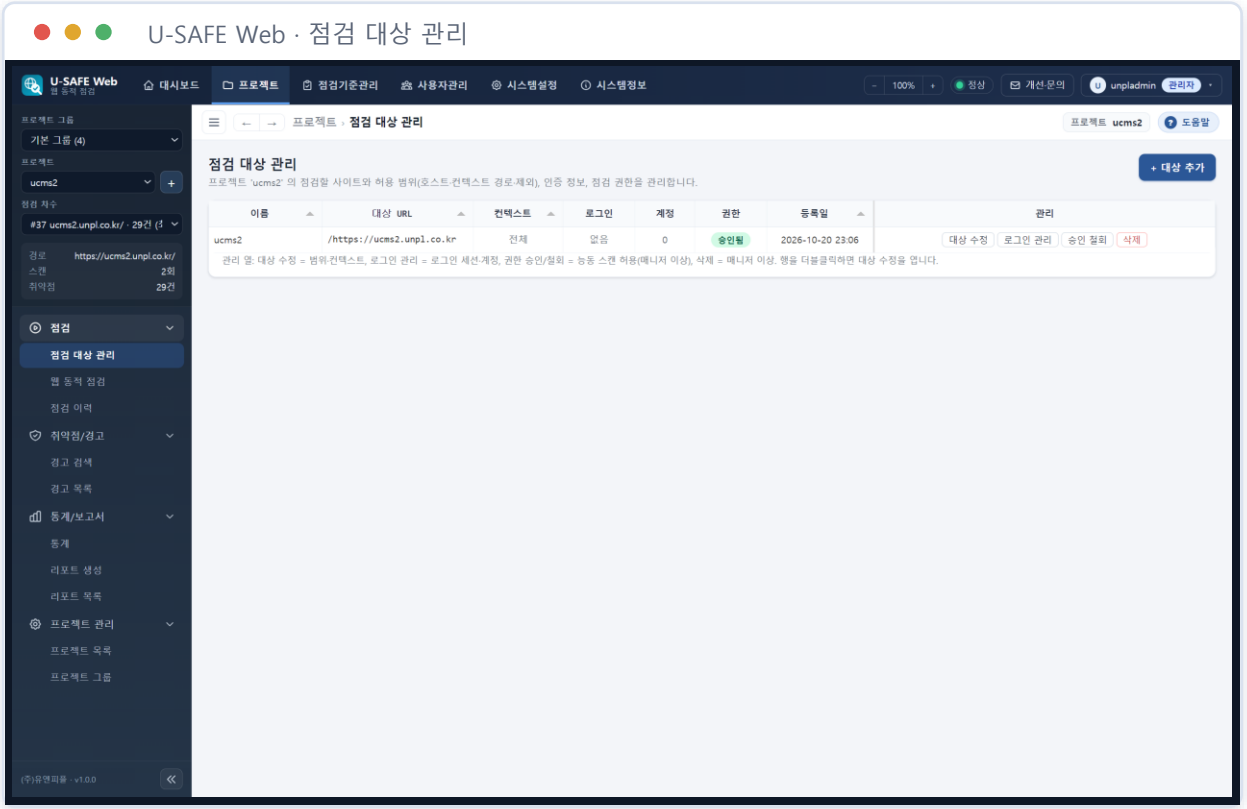
점검을 허용할 경로만 지정하고 그 밖은 자동 제외

3 **요청 예산 · 제외 경로**

최대 요청 수를 정해 요청 폭발을 방지하고 민감 경로는 제외

4 **로그인 자격증명 보관**

아이디·비밀번호를 암호화해 저장하고 점검 시 자동 로그인



웹 동적 점검 실행 Dynamic Scan

대상과 범위를 고르면 4단계 마법사로 크롤링과 능동·수동 점검을 한 번에 수행합니다.

STEP 1

대상 선택

등록·승인된 점검 대상을 고릅니다.

STEP 2

범위 · 옵션 설정

능동/수동 점검, 로그인, 요청 예산을 지정합니다.

STEP 3

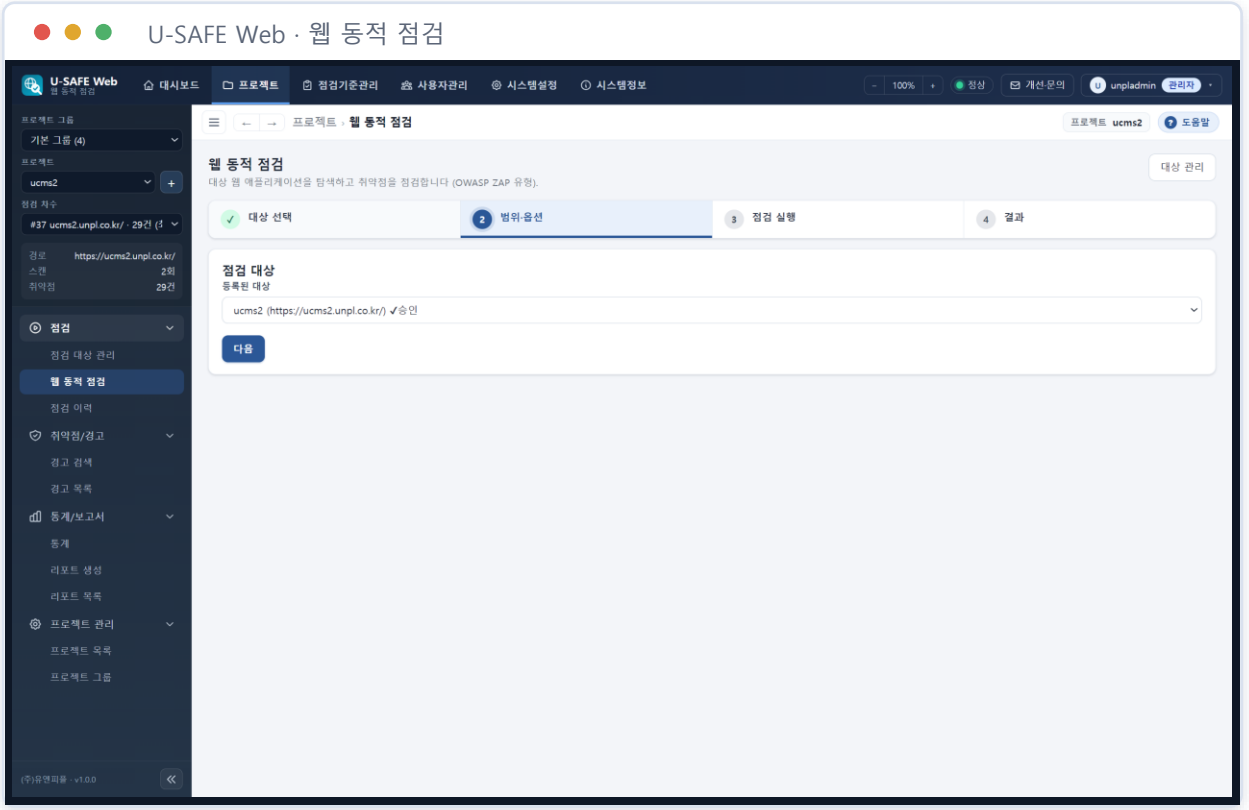
점검 실행

화면을 탐색(크롤링)하고 취약점을 점검합니다.

STEP 4

결과 확인

차수별 이력을 저장하고 신규/기존을 구분합니다.



※ 공용 서버형에서는 여러 진단자가 점검 결과를 공유하며 함께 조치합니다.

취약점 · 경고 관리 Finding Management

탐지된 경고를 다양한 조건으로 검색하고, 여러 건을 골라 상태 변경·정/오탐 분류를 한 번에 처리합니다.

1 상세 조건 검색

프로젝트 · 점검 항목 · 탐지 패턴 · 심각도 · 상태 · 점검 기준

2 일괄 처리

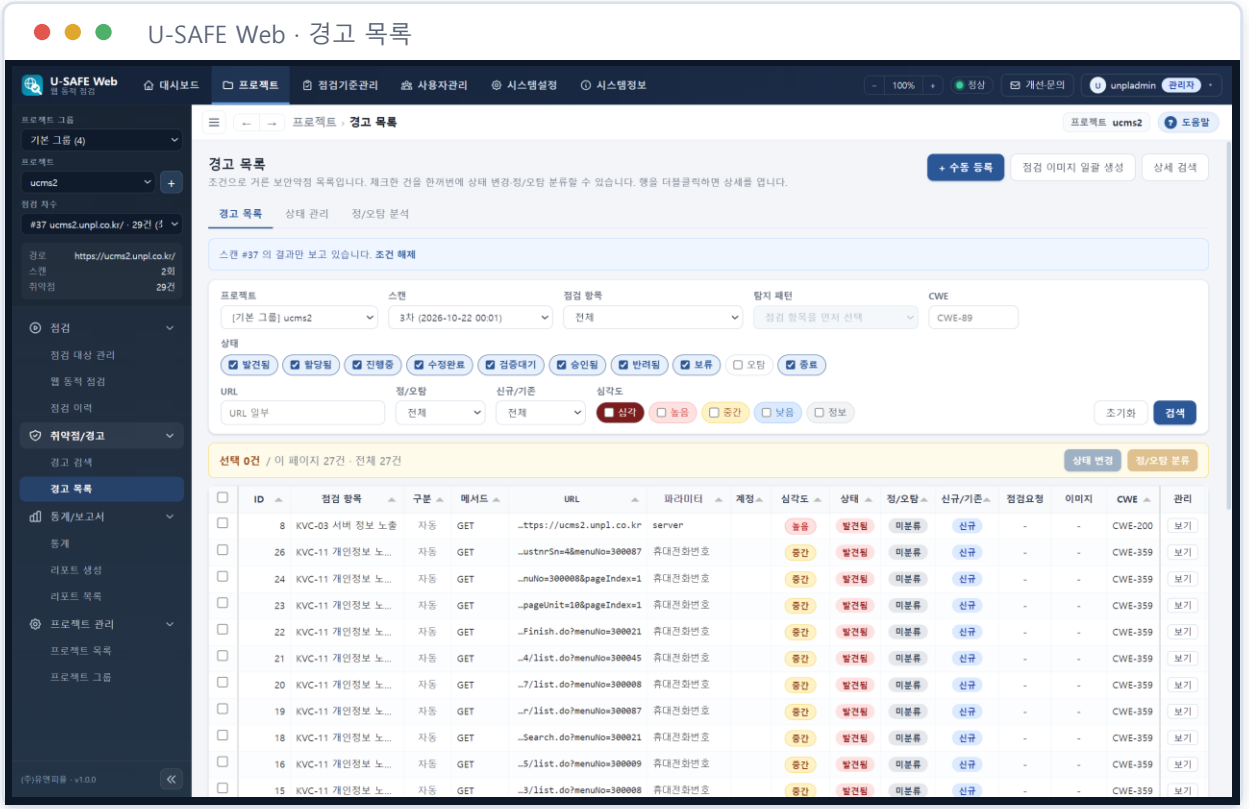
체크한 건을 한꺼번에 상태 변경 · 정/오탐 분류 · 담당자 할당(서버형)

3 증거 중심 상세

요청/응답 전문과 증적 이미지를 함께 확인(더블클릭으로 상세)

4 수동 점검 등록

자동 점검으로 찾기 어려운 항목을 수동 차수로 직접 등록



03 주요 기능

조치 워크플로우 Remediation Workflow

보안약점마다 10단계 처리 상태를 관리하고, 역할별로 허용된 상태 전환만 할 수 있도록 통제합니다.



보류 · 반려됨 · 오탐 상태로도 전환할 수 있고, 검증 반려 시 재조치합니다. ※ '할당됨'은 공용 서버형 전용 — PC 설치형은 발견됨 → 바로 진행중

역할별 상태 전환 권한

※ 뷰어는 조회만 · [1] 공용 서버형

개발자	선임 개발자	감사자	매니저 · 관리자
진행중 · 수정완료	승인 · 반려 (+할당[1])	승인 · 반려 · 오탐 · 종료 (+할당[1])	모든 상태 전환

상위 역할은 하위 역할의 권한을 모두 포함합니다.

정/오탐 분석 · 제외 관리 False-Positive Control

검토 결과를 정탐/오탐으로 분류하고, 제외 규칙을 등록하면 다음 점검부터 자동으로 반영됩니다.

1 **URL · 경로 제외**

점검이 필요 없는 경로를 제외해 점검 범위를 정리

2 **점검 규칙 제외**

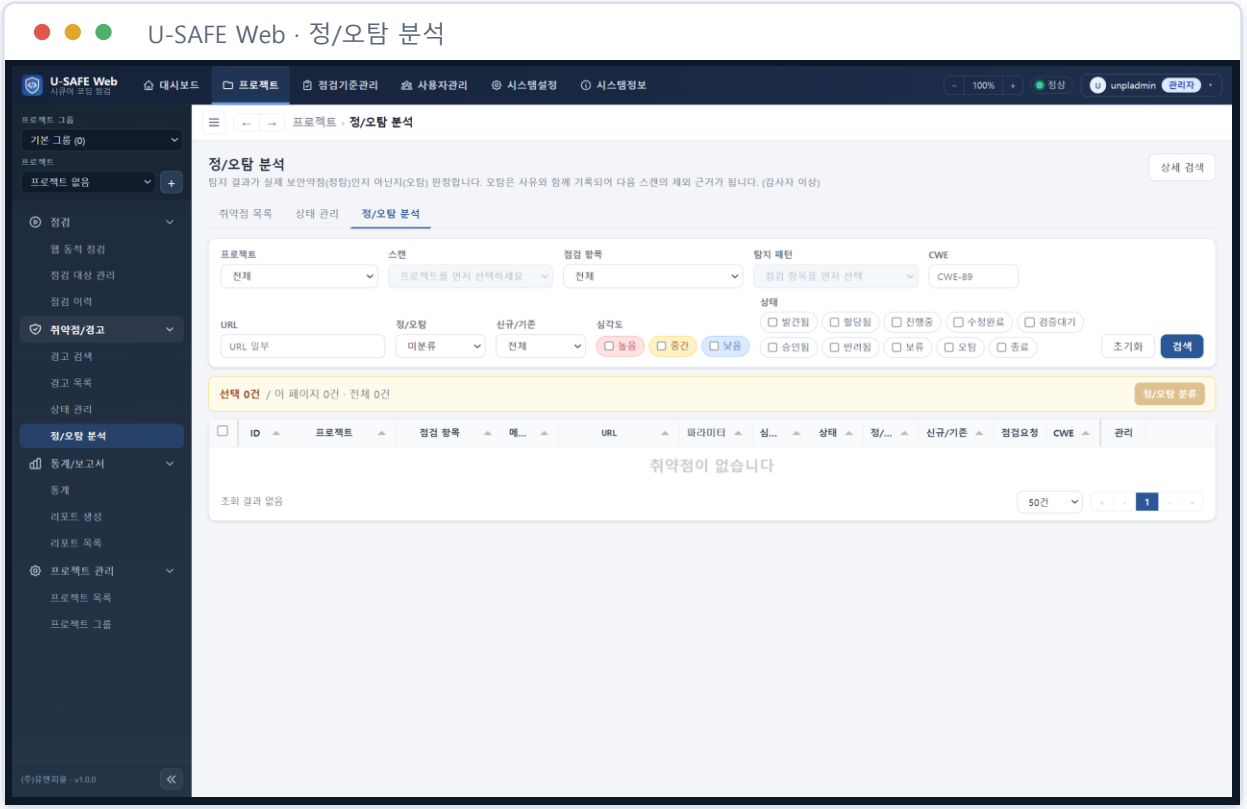
대상에 해당하지 않는 점검 규칙을 비활성화

3 **화이트리스트**

안전하다고 확인된 경로·패턴을 등록

4 **False Positive 자동 제외**

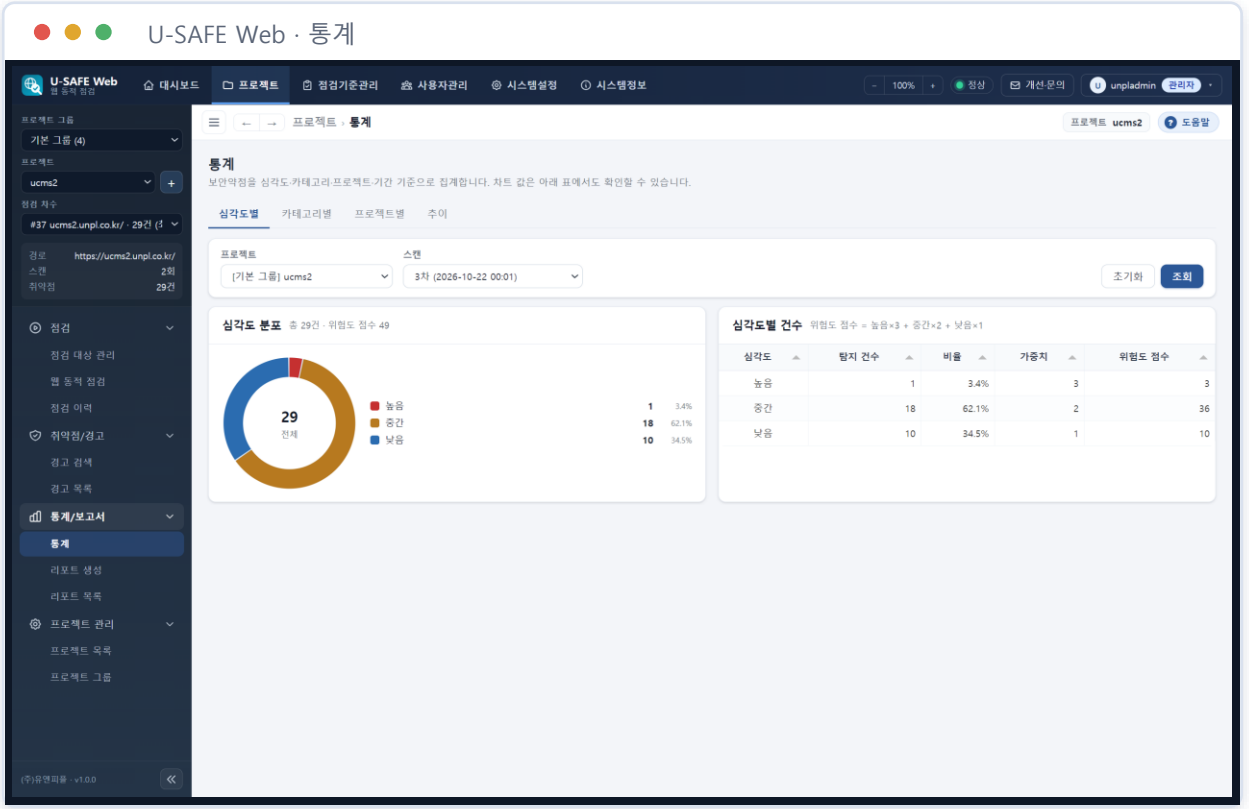
같은 경로·규칙의 오탐은 다음 점검에서 자동 제외



통계 · 위험도 분석 Statistics

보안약점을 심각도·항목·프로젝트·기간·담당자(서버형) 기준으로 집계하고, 위험도 점수로 조치 우선순위를 정합니다.

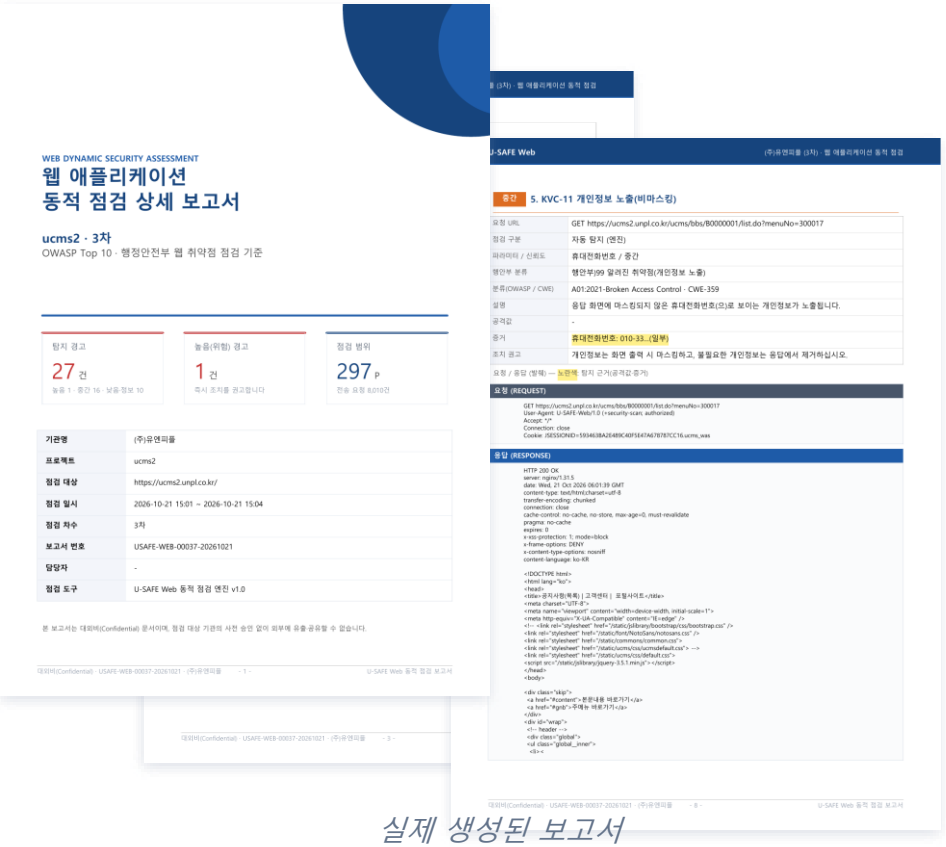
- **심각도별**
  높음 · 중간 · 낮음 분포와 위험도 점수
- **점검 항목 · 기준별**
  OWASP · 행안부 · 국정원 기준별 탐지 현황
- **프로젝트별**
  프로젝트 간 위험 수준 비교
- **추이**
  차수 · 기간별 탐지와 조치 변화
- **담당자별 (서버형)**
  담당자별 할당 · 조치 진행 현황



위험도 점수 = 높음×3 + 중간×2 + 낮음×1 · 보안경보 5단계(1,000요청당 경고 밀도)

보고서 자동 생성 Report Automation

점검 결과를 요청/응답 증거와 함께 PDF 상세 보고서 · Excel 로우데이터 · SARIF로 클릭 한 번에 생성합니다.


WEB DYNAMIC SECURITY ASSESSMENT
웹 애플리케이션
동적 점검 상세 보고서
ucms2 · 3차
OWASP Top 10 · 행정안전부 웹 취약점 점검 기준
U-SAFE Web
5. KVC-11 개인정보 노출(비마스킹)

실제 생성된 보고서

PDF

PDF 상세 보고서

표지 · 점검 요약 · 항목별 결과에 요청/응답 증거와 증적 이미지까지 수록

XLSX

Excel 로우데이터

점검 결과를 표 형식으로 제출하거나 추가 가공

SARIF

SARIF

표준 결과 포맷으로 다른 보안 도구·파이프라인과 연계

기준

기준별 · 상세/요약 선택

OWASP · 행안부 · 국정원 기준으로 다시 분류하고 목적에 맞게 상세/요약 출력

점검 기준 · 다중 기준 매핑 Multi-Standard

한 번의 점검 결과를 OWASP Top 10 · 행정안전부 웹 취약점 · 국정원 8종으로 각각 분류해 보고합니다.

1회 점검

탐지 결과 · CWE

OWASP Top 10 (2021)

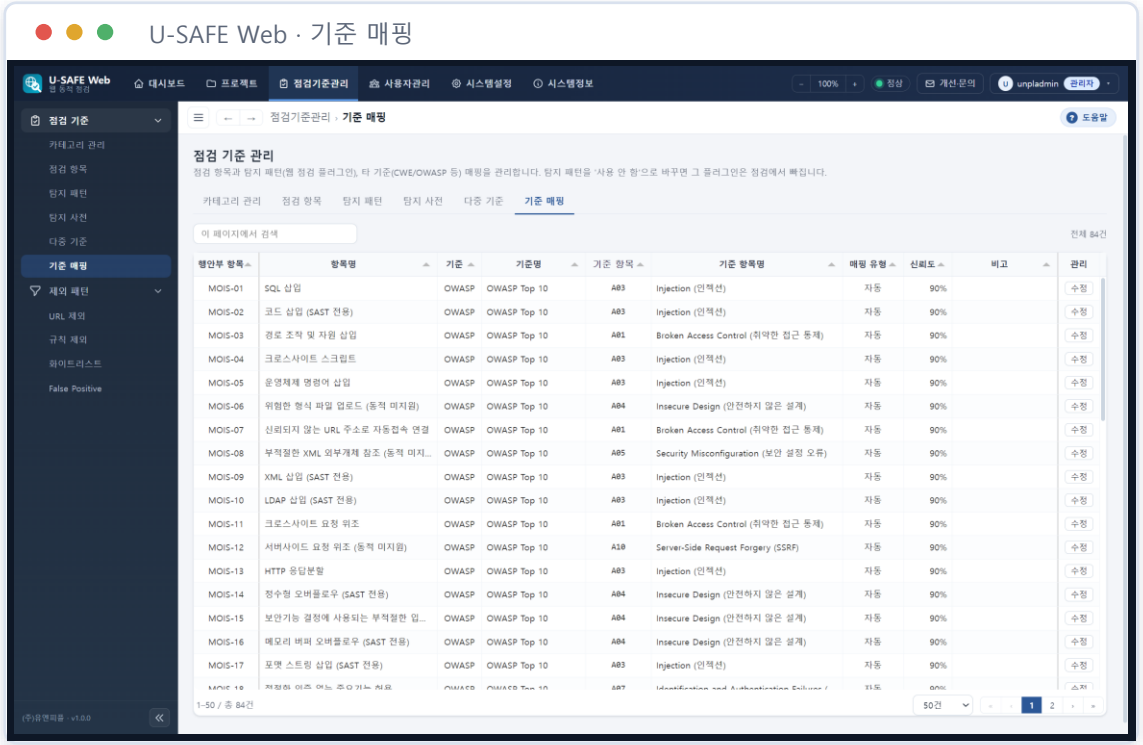
A01 접근 통제 ~ A10 SSRF

행정안전부 웹 취약점

공공 웹 서비스 점검 기준

국정원 웹 취약점 8종

N1 SQL 인젝션 ~ N8 접근 제어



재점검 없이 기준만 바꿔 보고서·통계 생성

카테고리 · 점검 항목 · 탐지 패턴 · 탐지 사전을 직접 관리

사용자 · 역할 권한 Role-based Access Control

6단계 역할 체계로 기능별 접근 권한을 통제하고, 보안 정책과 감사 로그로 사용 이력을 관리합니다.

1 **관리자 · 매니저**

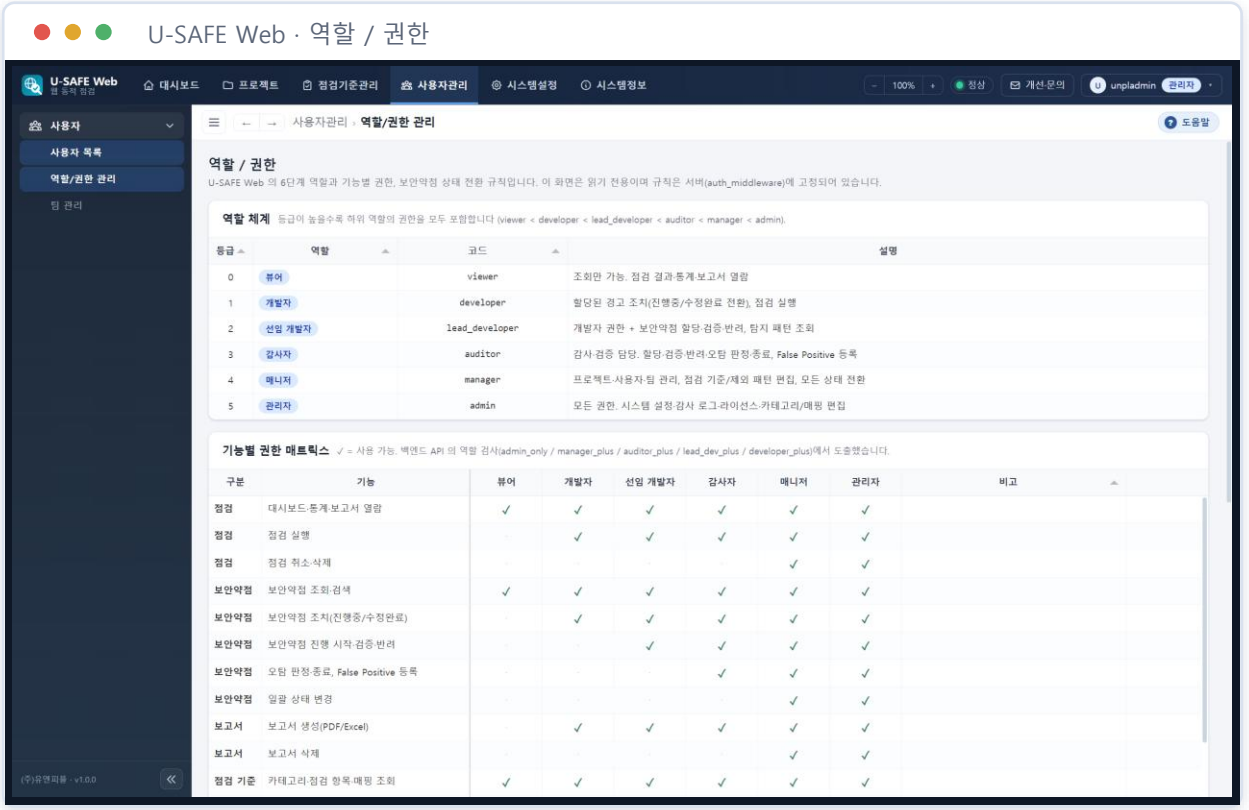
시스템 설정 · 감사 로그 · 라이선스 · 프로젝트/사용자 관리

2 **감사자 · 선임 개발자**

보안약점 검증 · 반려 · 오탐 판정(서버형은 할당도)

3 **개발자 · 뷰어**

개발자는 조치·점검 실행, 뷰어는 결과·통계·보고서 열람



04 제품 특장점

제품 특장점 Key Strengths

증거 기반 점검부터 조치·보고까지, 공공 웹 취약점 점검에 필요한 기능을 하나의 제품에 담았습니다.

1

실증성

Evidence

실제 요청/응답으로 확인한 증거 기반 결과

2

준거성

Compliance

OWASP·행안부·국정원 기준 매핑과 양식 보고서

3

안전성

Safety

승인 대상·범위·요청 예산 내 통제된 점검

4

협업성

Collab.

10단계 상태·역할 권한, 서버형은 담당자 할당

5

편의성

Usability

설치 하나로 엔진·DB 포함, 로그인·SPA 자동 처리

점검 방식 비교

구분	U-SAFE Web	단순 점검 방식
실행 기반 동적 점검	● 크롤링 + 능동/수동 점검	△ 정적 룰 · 수동 위주
접근통제 점검	● 멀티계정 자동 비교	× 사람이 직접 확인
증적 보고서	● 요청/응답 · 증적 자동	× 결과를 수작업 정리
범위 · 요청 통제	● scope · 요청 예산	× 통제 수단 부족

제품 구성 · 배포 형태 Deployment

규모와 환경에 맞춰 PC 설치형과 공용 서버형(Windows · Linux) 중 선택하며, 서버형은 웹 브라우저 접속도 지원합니다.

PC 설치형
Desktop

- 설치 파일 하나로 점검 엔진 · 데이터베이스 자동 구성
- 개인 · 소규모 팀이 별도 서버 없이 바로 사용
- 자동 업데이트 · 온라인/오프라인 라이선스 등록
- 1인 점검용: 담당자 할당 없이 상태 · 정/오탐 관리

공용 서버형
Server · 별도 문의

- 여러 진단자가 점검 결과를 공유해 함께 조치
- Windows 서비스 / Linux(Rocky · RHEL · Ubuntu)
- 웹 브라우저 · 전용 클라이언트로 접속(HTTPS)
- 담당자 할당 · 알림으로 협업 점검

운영 환경 Windows 10/11 (x64) · Windows Server · Rocky / RHEL / Ubuntu Linux

도입 기대효과 Expected Benefits

U-SAFE Web 도입으로 웹 취약점 점검 의무 대응과 점검·조치 효율을 함께 높일 수 있습니다.

01

웹 취약점 점검 의무 대응

OWASP·행안부·국정원 기준 점검과 증적 보고서로 감리·보안성 검토에 바로 대응

02

점검 공수 절감

크롤링·능동/수동 점검 자동화로 반복 점검 공수를 크게 줄임

03

증적·조치 가시화

요청/응답 증거와 10단계 상태 이력으로 점검·조치 현황을 투명하게 추적

04

통제된 안전한 점검

승인 대상·범위·요청 예산 안에서 운영 서비스 영향을 최소화

05

상시 점검 내재화

배포 전·운영 중 주기적 점검으로 웹 취약점을 조기에 제거하는 문화 정착

CONTACT US

감사합니다

안전한 웹 서비스의 시작, U-SAFE Web v1.0과 함께하세요.

Phone & Fax

02-855-7471

Fax 070-8650-0110

Online

idtong@unpl.co.kr

www.unpl.co.kr

Location

서울특별시 구로구 디지털로31길 38-9

803호 (구로동, 에이스테크노타워1차)

(주)유엔피플 | UNPEOPLE Co., Ltd.