진단부터 조치까지 한 번에
웹 취약점 원스탑 서비스

당신의 웹사이트, 지금 건강한가요?

해킹은 겉으로는 보이지 않지만 내부에서 이미 진행 중일 수 있습니다.
사람이 병을 초기에 발견하면 치료가 쉽듯, 웹사이트도 조기 점검이 핵심입니다.

항목	건강검진	웹 취약점 점검
목적	질병 조기 발견	해킹 예방
검사 방식	CT / X-ray	AppScan / Burp 등
검사자	의사	보안전문가
결과 대응	치료	취약점 조치
권장 주기	연 1회	연 1~2회

보안 사고는 점검 후 방치에서 시작됩니다

**최근 웹사이트 대상 자동화 해킹·봇 공격·개인정보 유출 시도가 증가하고 있지만,
많은 기업은 보안 진단 이후 실제 조치까지 이어지지 못하고 있습니다.**

공격 시도 증가

자동화된 해킹·봇 공격
개인정보 유출 시도 확대
스팸·악성 스크립트 유입

›

진단 후 미조치

KISA 무료 점검 등
보안 진단은 받았지만
실제 조치는 지연·방치

›

보안 사고 발생

점검만 받고 방치된 사이트
해킹·스팸 공격 반복
기업 신뢰도·운영 리스크 확대

보안의 완성은 “진단”이 아니라 “조치완료”입니다.

아이티이지는 진단부터 조치까지 실행합니다

점검만 해주는 서비스는 많습니다.
하지만 아이티이지는 복잡한 보안업무를 전문가가 대신 처리해드립니다.

고객 요청 › 1차 점검 › 리포트 제공 › 보안조치 진행 › 재점검 및 이행 보고서 작성 › 완료 및 정기점검 제안

복잡한 과정 없이 점검 → 조치 → 이행 문서까지 One-Stop 제공

합리적인 가격의 보안 패키지

웹사이트 규모와 필요에 따라 선택할 수 있습니다.

		소규모 웹사이트용	BEST 중소기업 추천	대기업 및 전문 서비스
		Light	Standard	Premium
	1회	~~780,000원~~ 50% 390,000원	~~1,975,000원~~ 60% 790,000원	~~4,970,000원~~ 70% 1,490,000원
진행과정	진단	기본 웹취약점	전체 취약점	심화 취약점
	조치	주요 취약점 최대 30건	주요 취약점 최대 50건	무제한
	리포트	기본	상세 + 조치가이드	맞춤형 보안 가이드
	이행점검	1회 (3개월 이내)		
	추가지원	-		긴급 대응 지원

무료점검과는 확실히 다릅니다

항목	KISA 무료 점검	웹취약점 원스탑 서비스
사용 도구	IBM AppScan 기반 (제한적 구성)	Acunetix, Burp Suite, ZAP 등 상용 스캐너
분석 방식	자동 점검 위주	맞춤형 진단 + 개발 환경 고려
점검 정밀도	중저위험 위주 점검	크리티컬 포함 전 범위 커버
조치 지원	없음 (고객사 자율 조치)	취약점 조치까지 포함
문서 제공	결과 리포트만 제공	이행조치 보고서, 재점검 리포트까지 제공
보고서 활용	제한적	입찰/감사 보고용 활용 가능
진행 속도	수주 소요	3~5일 내 완료

KISA는 진단, 아이티이지는 해결입니다.

이런 경우에 꼭 필요합니다

신규 홈페이지 제작, 리뉴얼

보안이슈 사전차단

해킹 사고 피해 기업

취약코드 수정+재발방지

중견기업, 내부보안 점검 대상

조치 보고서, 감사 대응 자료

의료기기, 제약사

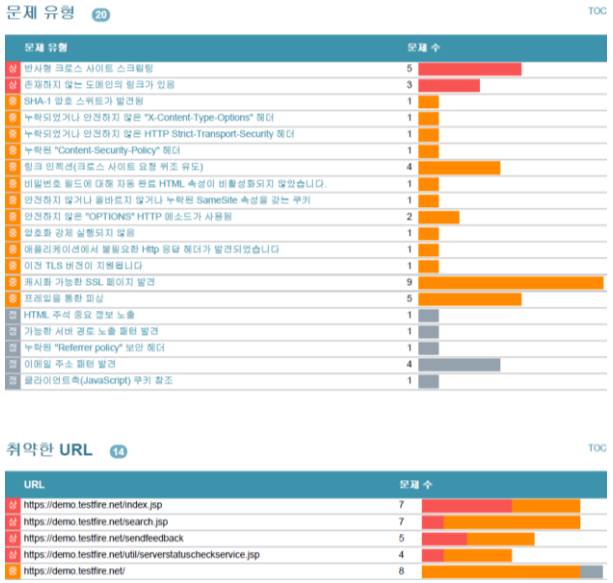
e-IFU 구축/심사 대응

공공입찰, 과제수행기업

이행 증빙/보고서

리포트 샘플

진단 리포트 예시 (스크린샷 / 위험도 분류)



3. 취약점 세부 요약

SQL 인젝션		
위험도	:	Critical
URL	:	https://demo.testfire.net/bank/ccApply https://demo.testfire.net/bank/doTransfer https://demo.testfire.net/bank/showAccount https://demo.testfire.net/bank/showTransactions https://demo.testfire.net/doLogin
원인	:	사용자 입력에서 유해한 문자의 무결 처리가 올바르게 수행되지 않았습니다.검증되지 않은 사용자 입력을 포함하는 쿼리를 동적으로 생성하면 SQL 삽입 공격으로 이어질 수 있습니다. 공격자는 쿼리가 안전하지 않은 방식으로 동작하도록 할 수 있는 SQL 명령 또는 수정자를 사용자 입력에 삽입할 수 있습니다.사용자가 제어 가능한 입력에 대한 충분한 유효성 검사 및 캡슐화 없이 생성된 SQL 쿼리는 해당 입력이 원래 사용자 데이터가 아닌 SQL로 해석되도록 할 수 있습니다. 이것은 보안 검사를 우회하도록 쿼리 논리를 수정하거나, 시스템 명령 실행을 포함하여 백엔드 데이터베이스를 수정하는 추가적인 구문을 삽입하는 데 사용될 수 있습니다.SQL 페이로드는 사용자 입력, 이전에 데이터베이스에 저장된 데이터, 파일, 타사 API 등을 포함하여 신뢰할 수 없는 데이터를 통해 시스템에 진입할 수 있습니다.
위험	:	잠재적 영향에는 다음에 대한 손실이 포함됩니다. 기밀성 - 일반적으로 SQL 데이터베이스는 민감한 데이터를 포함하고 있으므로 기밀성 손실은 SQL 삽입 취약성과 관련하여 자주 발생하는 문제입니다. 인증 - 사용자 이름과 암호를 검사하기 위해 잘못된 SQL 명령이 사용되는 경우 암호를 알지 못하는 상태로 다른 사용자로 시스템에 연결할 수 있습니다. 권한 부여 - 권한 부여 관련 정보가 SQL 데이터베이스에 있는 경우 SQL 삽입 취약성을 악용하여 이 정보를 변경할 수 있습니다. 무결성 - 민감한 정보를 읽을 수 있는 것과 마찬가지로, SQL 삽입 공격을 통해 이 정보를 변경하거나 삭제할 수도 있습니다.

이행조치 보고서 예시 (전/후 비교)

페이지 (page) 체크 전

```
$pageTotal  = ceil($dataCount / $pagingItemMax);
if ($_GET['page'] == ""){ $_GET['page'] = 1; }
$fromLimit = ($_GET['page'] - 1) * $pagingItemMax;

$rs = Queryi("SELECT * FROM $tableName WHERE $where ORDER BY $orderBy_normal LIMIT $fromLimit, ".$pagingItemMax, $params);
```

페이지 (page) 체크 후

```
$pageTotal  = ceil($dataCount / $pagingItemMax);
if ($_GET['page'] == ""){ $_GET['page'] = 1; }

// 페이지 값 체크
if (!ctype_digit(trim($_GET['page'])) || strlen($_GET['page']) > 9) {
    $_GET['page'] = 1;
} else {
    $_GET['page'] = intval($_GET['page']);
}

$fromLimit = ($_GET['page'] - 1) * $pagingItemMax;

$rs = Queryi("SELECT * FROM $tableName WHERE $where ORDER BY $orderBy_normal LIMIT $fromLimit, ".$pagingItemMax, $params);
```

FAQ

KISA(한국인터넷진흥원)에서도 무료로 점검해주는데, 왜 유료 점검을 받아야 하나요?

KISA의 무료 점검은 진단 중심입니다. 사용 도구는 IBM AppScan 기반이며 범용성이 떨어지고, 결과 보고서 외 조치는 지원하지 않습니다.
저희는 고급 스캐너(Acunetix, BurpSuite 등)로 더 정밀한 진단을 하고, 즉시 조치 및 재점검, 보고서 작성까지 원스톱으로 제공합니다.

우리 회사 홈페이지는 오래된 플랫폼인데, 점검 가능한가요?

네. PHP, ASP, 워드프레스 등 다양한 기술스택과 그누보드, 카페24 등 CMS 기반 사이트도 모두 점검 가능합니다.
서버 접근 권한 없이도 기본 점검이 가능합니다.

문서나 결과 리포트는 어떤 형식으로 제공되나요?

점검 전·후 리포트, 이행조치서, 스크린샷 등 입찰·감사·내부 보고용 문서 형태로 제공됩니다.
형식은 맞춤화도 가능합니다 (PDF, PPT 등).

예전에 KISA 점검은 받았는데 조치를 못했어요. 그것만으로도 보완 가능한가요?

가능합니다. KISA 리포트를 보내주시면 분석 후, 해당 항목의 조치 가능 여부와 예상 비용을 안내드립니다.
또한 누락된 항목이나 추가 위험 요소가 있는지도 함께 진단합니다.

점검 결과에 따라 조치를 꼭 받아야 하나요?

점검 후 위/중요도가 높은 항목이 발견되면, 이를 방치할 경우 실제 해킹, 정보 유출로 이어질 수 있습니다.
조치까지 함께 받으시는 것을 강력히 권장드립니다.

무상으로 처리해주는 부분은 없나요?

진단 항목 중 간단한 관리자 설정 변경 등 경미한 항목은 무상 처리가 가능합니다.
단, 시스템 코드 수정이나 구조 변경이 필요한 경우는 조치 건수에 포함됩니다.

감사합니다

웹 취약점 원스톱 서비스는 진단, 조치, 보고서까지
보안 실무를 끝까지 책임집니다.

고객센터
1600-8324
sales@iteasy.co.kr