웹 보안 점검 및 조치 원-스톱 서비스 제안

점검만 하는 보안은 **반쪽짜리**입니다.

진단부터 조치까지, 원-스톱 보안 서비스

© 2025 HDG Co.,LTD. All rights reserved.

iTEASY CREATIVE WEB PROJECT GROUP

웹 보안 점검 및 조치 원-스톱 서비스 목차

1. 제안 개요
2. 참여사
3. 서비스 구성 및 역할 분담
4. KISA 점검과의 차별성
5. 무료 자가진단 콘텐츠 구성
6. 기대효과
7. 마케팅 및 실행 전략
8. 고객 FAQ 대응
9. 기타

제안 개요

제안 배경 :

최근 웹사이트 대상의 자동화된 해킹, 봇 공격, 개인정보 유출 시도가 빠르게 증가하고 있음

많은 기업이 KISA 무료 점검 등으로 보안 진단은 받았지만, 실제 조치는 하지 않음

이로 인해 실제 해킹이나 스팸 공격이 반복되고 있음

점검만 받고 방치된 사이트 → 보안 사고 발생

기존 구조의 한계 :

대부분의 점검 업체는 스캐닝만 제공하고, 조치는 고객사 몫으로 남겨둡니다.

하지만 보안의 완성은 '조치'에 있으며, 실질적으로 해결해드립니다.

즉, 점검에서 끝나지 않고 '개발자 시점에서 실행 가능한 조치'까지 One-Stop으로 제공합니다.

점검만 받고 방치된 사이트 → 점검 + 즉시 조치 → 보고서 제공

아이티이지 × 에이치디그룹이 협력하여
점검 → 조치 → 이행 문서까지 원-스톱 제공

고객은 복잡한 과정 없이 단일 창구로
실질적인 보안 문제를 해결 가능

제안 개요

보안 점검도 **건강검진**과 같습니다.

건강검진을 받아도 치료하지 않으면 병은 진행됩니다.

웹사이트도 마찬가지입니다.

보안점검만 받고 조치를 하지 않으면,

해킹이라는 병이 그대로 남아 있습니다.

진짜 중요한 건 **"문제를 고치는 것"**입니다.

제안 개요

웹취약점 진단부터 보안조치까지, 한 번에 해결합니다

서비스 포인트:

- **단일 접점** : 고객은 한 곳에만 연락, 양사는 내부 연계
- **기술 전문성 분담** : 진단과 개발을 분리하여 전문성 확보
- **문서화 제공** : 입찰·평가 대응 가능한 보안 문서 확보

점검을 넘어서 '해결'까지.

실질적인 보안 상태 개선을 원한다면, **원-스톱**이 정답입니다.

참여사

함께하는 두 전문 기업

아이티이지 (ITEASY)

보안 전문 기업 / 웹취약점 점검·모의해킹 전담
KISA 등록 보안 전문기업
국내 대기업, 공공기관 다수 수행 이력 보유
상용 스캐너 (Acunetix, Burp Suite Pro, OWASP ZAP 등) 기반의 고정밀 점검
수동 분석 병행을 통해 실무 대응 수준의 진단 리포트 제공
모의해킹 / 서버보안 / 네트워크 보안 등 종합 보안 컨설팅 가능

웹취약점 진단, 보고서 작성, 재점검 제공

iTEASY

에이치디그룹 (HD Group)

웹에이전시 / 개발·보안 조치·유지보수 전문
누적 500여 이상 기업 웹사이트 제작/운영
PHP,ASP 기반 웹시스템 보안 조치 및 대응 경험 다수
스팸차단, SQL Injection, 관리자 페이지 보호, 암호화 적용 등 직접 조치 경험 보유
유지보수 + 웹방어 개발역량 융합 → 실질적 해결 가능

점검 리포트 기반 보안 취약점 조치, 서버 설정 변경, 대응 완료 문서 작성

CREATIVE WEB PROJECT GROUP

서비스 구성 및 역할 분담

진단만 하는 보안 업체도, 개발만 하는 웹업체도 많습니다.

하지만, 함께하는 우리는 **'보안 문제 해결'**까지 합니다.

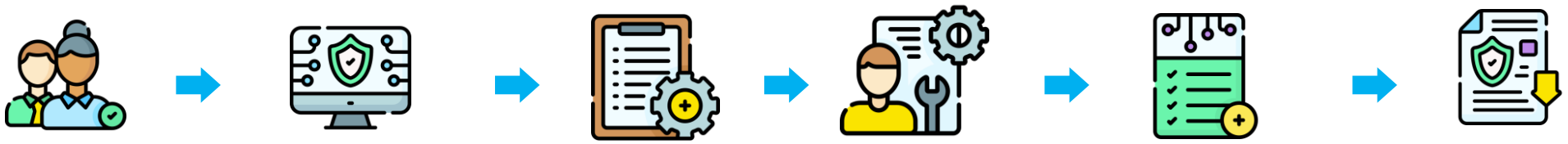
항목	아이티이지	에이치디그룹
주요 역할	점검, 리포트	조치, 대응
보유 역량	고급 스캐너 / 보안인증	실개발 / 유지보수 / 실시간 대응
고객 혜택	신뢰성 및 전문적인 진단	즉시 대응 및 개선 완료

단계	아이티이지	에이치디그룹
점검 준비	대상 사이트 등록	사전 기술 구조 전달(서버환경 및 개발언어)
스캔 및 진단	자동 / 수동 취약점 점검리포트 작성	리포트 수령 후 항목 검토
대응 조치	(재점검 시 확인 대응)	보안 취약점 소스코드 수정유 인증, 업로드 필터링 강화서버 설정 및 SSL 강화
결과 확인	재스캔 및 risk level 조정	조치 완료 보고서 작성 및 고객대응

서비스 구성 및 역할 분담

서비스 구성 흐름도

웹취약점 진단부터 보안조치까지, 한 번에 해결합니다



고객요청 → 1차 점검 (아이티이지) → 리포트 제공 → 보안조치 진행 (에이치디그룹) → 재점검 및 이행보고서 작성 → 완료 및 정기점검 제안

중간에 고객은 1회만 의사결정하면, 이후 전 과정은 양사가 내부 협업으로 처리

KISA 점검과의 차별성

1. 점검 방식 차이

항목	KISA 무료 점검	아이티이지
사용 도구	HCL AppScan 기반 (제한적 구성)	HCL AppScan 기반 (수동검증)
분석 방식	자동 점검 위주	맞춤형 진단 + 개발 환경 고려 (담당 컨설턴트 배정)
점검 정밀도	중저위험 위주 점검	크리티컬 포함 전 범위 커버
조치 결과	점검 결과 내용 부족, 조치 가이드 미제공	상세 점검 결과 보고서, 조치 방안 가이드 제공

2. 후속 조치 여부

항목	KISA	아이티이지 × HD그룹
조치 지원	없음 (고객사 자율 조치)	취약점 조치까지 연계된 원스톱 패키지 제공
문서 제공	결과 리포트만 제공	이행조치 보고서, 재점검 리포트까지 제공

KISA 점검과의 차별성

3. 실무 활용도

- KISA 점검은 진단까지로 끝, 실질적인 문제 해결 어려움
- 아이티이지는 조치 후 재점검 + 이행 문서 제공으로 공공기관 입찰용 제출 문서 활용
- 내부 감사 및 보안 대응 이력 관리

"KISA는 진단, **우리는 해결**입니다."

고객 유형 분석

고객이 '웹취약점 점검'이라는 서비스를
언제, 왜, 어떻게 인지하고 행동하는지 단계별로 파악하여 최적의 개입 시점과 안내 메시지를 설계하는 기반 제공.

① 인지 단계

대표 상황

- 게시판에 스팸글이 급격히 늘어나 불안함을 느낌
- 고객에게 해킹 위험 알림이 도달하거나 웹호스팅 업체로부터 경고 메일 수신
- 공공기관에서 보안점검 이행 통보서 수신

마케팅 메시지 예

"최근 게시판에 이상한 글이 늘어났나요?"

"사이트도 건강검진이 필요합니다."

② 탐색 단계

대표 행동

- KISA(한국인터넷진흥원) 무료 점검을 검색해 시도해봄
- 기존 개발사에 문의하지만 조치 불가하거나 일정 지연
- 검색을 통해 전문 점검업체 탐색

마케팅 메시지 예

"무료 점검은 받았지만, 해결은 안 되셨죠?"

"문제는 진단이 아니라 조치입니다."

③ 상담 단계

대표 행동

- 점검 가능 범위, 도구, 리포트 예시 등을 문의
- 보유 리포트(KISA 등)로 조치 가능성 타진
- 예상 비용 및 소요 시간 문의

응대 포인트

- Before/After 사례 제시
- 리포트 제공 범위와 실질 대응 여부 강조

④ 실행 단계

진행 흐름

- 1차 스캔 → 조치 1~2회차 → 리포트 제공
- 고위험 취약점 우선 대응
- 이행조치 보고서 작성 및 내부결재 지원

고객 반응

조치 후 속도 개선, 스팸차단 확인 등 체감 결과 긍정적

⑤ 사후관리 단계

대표 행동

- 내부 보안 보고용 문서 정리
- 연 1~2회 정기 점검 필요성 인식
- 타 부서/지인에게 서비스 추천

운영 전략

- 리포트 기반 리뷰 요청
- 정기 점검 프로모션 제안
- FAQ/자주 묻는 질문 콘텐츠 연계

무료 자가진단 콘텐츠 구성

아래 항목 중 해당되는 것을 선택해주세요! (중복 선택 가능)

- [ ] 게시판에 스팸이 하루 10건 이상 올라온다
- [ ] 관리자 주소가 /admin 으로 되어 있다
- [ ] 로그인 시 아이디/비밀번호 외 인증 수단이 없다
- [ ] 수집한 고객 정보가 암호화되었는지 모른다
- [ ] 최근 1년간 보안 점검을 받은 적 없다
- [ ] KISA 점검은 받았지만, 보안조치는 하지 않았다

0~2개: 상대적 안전 상태입니다. 연 1회 점검을 권장합니다.

3~4개: 위험 징후가 있습니다. 기본 점검 상품을 권장드립니다.

5개 이상: 심각 단계입니다. 즉시 점검 및 보안조치가 필요합니다.

점검 패키지 확인하기

전문가 상담 신청하기

무료 자가진단 콘텐츠 구성

아래 항목 중 해당되는 것을 선택해주세요! (중복 선택 가능)

☐ 웹 유지보수 담당자

개발 지식은 적지만 웹 운영을 맡고 있음. 관리자 계정 노출, 게시판 스팸 등 실무 불편으로 문의

☐ 내부 보안 담당자

보안 점검 이슈로 외주 컨트롤 필요. 예산 승인과 문서가 필요한 실무자

☐ 중소기업 대표

웹 외에 IT 전반을 통합적으로 관리. '싸고 빠른 해결'을 선호

☐ 공공기관 협력사

입찰용 보안 인증 필요로 단기 대응 목적. 문서화 중요

☐ IT 개발자

KISA 등 점검을 받아본 경험 有. 조치 직접 처리하려다 시간/리소스 부족으로 외주 고려

☐ 무료 점검 경험 기업

KISA 점검을 받아본 후 보안조치는 하지 못한 채 방치. 재문의 후 원스톱 패키지에 관심

"이 서비스는 단지 보안팀만을 위한 것이 아닙니다"

기대 효과

아이티이지

- **서비스 범위 확대**
  단순 점검에서 → 점검 + 조치까지 확대
- **고객 만족도 향상**
  빠른 조치 및 후속 대응으로 신뢰 확보
- **기술적 부담 분산**
  고객의 개발/보안 기술 문의 대응 부담 완화
- **정기 점검 유도**
  만족 고객을 통한 연 1~2회 정기 점검 전환율 상승
- **파트너십을 통한 고객 유입 확대**
  에이치디그룹 고객사에 대한 신규 리드 확보

에이치디그룹

- **기존 고객 대상 수익 다각화**
  유지보수 외 보안 서비스 상품 제공
- **기술적 신뢰도 상승**
  보안 대응력을 인정받아 입찰 경쟁력 강화
- **고정 수익 모델 확보**
  정기 점검 및 재조치 유입 가능
- **위험 분산**
  보안 이슈 발생 시 조치 체계 확보로 무상 대응 범위 축소
- **파트너 기반 기술 협업 구조 확보**
  전문 보안사 연계로 자체 대응력 강화

공통 시너지 효과

- **고객에 대한 설득력 상승**
  KISA 대비 실질적 해결 가능성 강조
- **원스톱 대응 체계 구축으로 경쟁업체 대비 우위 확보 고정 수익 모델 확보**
- **콘텐츠 마케팅 활용 가능**
  점검 + 조치 사례를 통한 공동 브랜딩 및 홍보
- **장기 파트너십 기반의 신규 수익 모델 창출**
- **정부·공공기관 프로젝트에서 공동 제안 가능성 확보**

보안 리포트의 외부 활용성

제약·바이오 업계에서 준비 중인 e-IFU 시스템 심사,
공공 조달/입찰 평가에서 보안 점검 및 조치 리포트는 기술 신뢰도 확보 및 가점 요소로 활용 가능합니다.

→ 단순 대응을 넘어, 대외 신뢰도까지 확보할 수 있는 실무적 장점

마케팅 및 협업 방향

공동 레퍼런스 확보

1차 고객 대상 Before/After 사례 확보

홈페이지, 랜딩페이지, 제안서 활용 콘텐츠 제작

공동 홍보 자료 제작

패키지 상품 PDF 브로셔

웹사이트 및 랜딩페이지 내 홍보 페이지 공유

공동 명의 명함/소개서 등 제작

고객 유입 공유

아이티이지 유입 고객 → **에이치디그룹 기술수정 연계**

에이치디그룹 고객사 → **보안 점검 업셀링 유도**

내부 CRM 또는 시트 공유로 커뮤니케이션

향후 확장 가능성

보안 인증 컨설팅 연계 (ISMS-P 등)

쇼핑몰, 앱, 하이브리드 시스템 보안 확장

마케팅 및 협업 방향

핵심 메시지 정의

"점검은 건강검진, 조치는 수술입니다."

"KISA는 진단, 우리는 해결."

"웹 보안 문제, 이제 원스톱으로 끝내세요."

랜딩페이지 운영

진단형 랜딩페이지

1분 자가 진단(객관식 체크) → **결과에 따라 상담 유도**

예 : "관리자 페이지가 /admin으로 되어 있습니까?" 등

콘텐츠 포인트

- Before/After 이미지 제공
- 리포트 샘플/고객 사례
- KISA 점검 대비 차별 요소 강조

키워드 광고 및 타겟팅

키워드 예시

웹취약점 점검 / KISA 보안점검 /
홈페이지 해킹 / 게시판 스팸 등

타겟 대상

소상공인, 중소기업 IT담당자,
홈페이지 제작·운영 관리자

광고 채널

네이버 검색광고, 구글 키워드,
페이스북/인스타 타겟광고

공동 마케팅 브로셔 및 세미나

공동 명의 브로셔 배포
(아이티이지 × 에이치디그룹)

전문 세미나 or 웨비나 개최

주제

"KISA 점검 이후, 우리가 할 일은?"

기존 KISA 수검 업체 대상 이메일 발송 및 리타게팅

재판매/파트너 확대 방안

- 에이전시/SI업체/디자인 회사와 제휴
- 제작 중이거나 유지보수 중인 고객에 보안 패키지 제안
- 정기 유지보수 계약에 포함
- 연 1회 점검 + 보안 이슈 발생 시 수시 대응 포함

고객 FAQ 대응

웹취약점 점검 + 조치 상품을 운영할 때 고객이 자주 묻는 질문에 대해 사전 대응할 수 있는 문답을 구성했습니다.
아래 내용을 바탕으로 챗봇 시나리오, 메일/문서 응답, 랜딩페이지 Q&A 섹션 등에 활용 가능합니다.

Q1. KISA(한국인터넷진흥원)에서도 무료로 점검해주는데, 왜 유료 점검을 받아야 하나요?

A. KISA의 무료 점검은 진단 중심입니다. 사용 도구는 HCL AppScan 기반이며, 제한 범용성이 떨어지고, 결과 보고서 외 조치는 지원하지 않습니다.
저희는 HCL AppScan + 수동 점검을 병행하여 더 정밀한 진단을 하고, 즉시 조치 및 재점검, 보고서 작성까지
원스톱으로 제공합니다.

Q2. 예전에 KISA 점검은 받았는데 조치를 못했어요. 그것만으로도 보완 가능한가요?

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

Q3. 우리 회사 홈페이지는 오래된 플랫폼인데, 점검 가능한가요?

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

고객 FAQ 대응

Q4. 점검 결과에 따라 조치를 꼭 받아야 하나요?

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

Q5. 문서나 결과 리포트는 어떤 형식으로 제공되나요?

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

Q6. 무상으로 처리해주는 부분은 없나요?

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

기타

리포트 샘플 (이미지 / PDF 미리보기)

Eyeon Security

웹 취약점 진단 점검 결과 보고서

대 외 비
CONFIDENTIAL

웹 취약점 진단 점검 결과 보고서

(기업명 : **[Sample]**)

2024-11-26

㈜아이온시큐리티

자동 진단 도구 특성상 오탐 및 미탐 가능성이 있습니다.

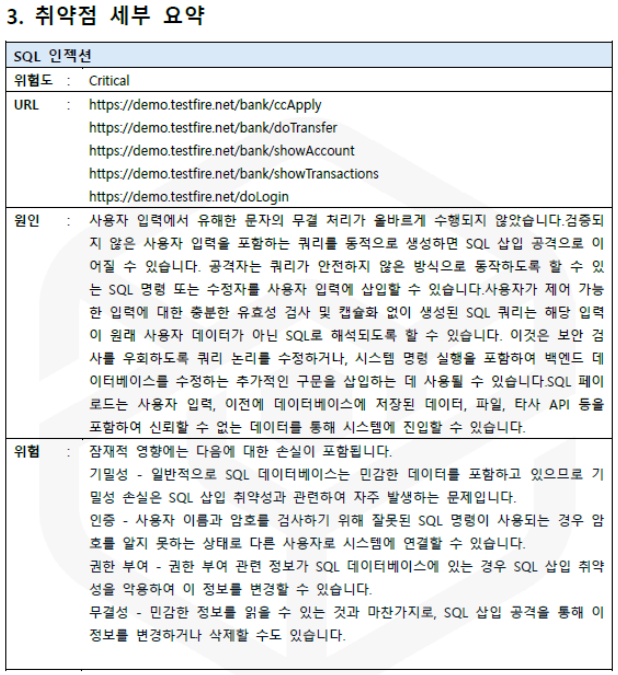
요약

문제 유형 20 TOC

	문제 유형	문제 수
상	반사형 크로스 사이트 스크립팅	5
상	존재하지 않는 도메인의 링크가 있음	3
중	SHA-1 암호 스위트가 발견됨	1
중	누락되었거나 안전하지 않은 "X-Content-Type-Options" 헤더	1
중	누락되었거나 안전하지 않은 HTTP Strict-Transport-Security 헤더	1
중	누락된 "Content-Security-Policy" 헤더	1
중	링크 인젝션(크로스 사이트 요청 위조 유도)	4
중	비밀번호 필드에 대해 자동 완료 HTML 속성이 비활성화되지 않았습니다.	1
중	안전하지 않거나 올바르지 않거나 누락된 SameSite 속성을 갖는 쿠키	1
중	안전하지 않은 "OPTIONS" HTTP 메소드가 사용됨	2
중	압축화 강제 실행되지 않음	1
중	애플리케이션에서 불필요한 Http 응답 헤더가 발견되었습니다	1
중	이전 TLS 버전이 지원됩니다	1
중	캐시화 가능한 SSL 페이지 발견	9
중	프레임을 통한 피싱	5
정	HTML 주석 중요 정보 노출	1
정	가능한 서버 경로 노출 패턴 발견	1
정	누락된 "Referrer policy" 보안 헤더	1
정	이메일 주소 패턴 발견	4
정	클라이언트측(JavaScript) 쿠키 참조	1

취약한 URL 14 TOC

	URL	문제 수
상	https://demo.testfire.net/index.jsp	7
상	https://demo.testfire.net/search.jsp	7
상	https://demo.testfire.net/sendfeedback	5
상	https://demo.testfire.net/util/serverstatuschecksservice.jsp	4
중	https://demo.testfire.net/	8


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.
위협	:	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.

진단 리포트 예시 (스크린샷/위험도 분류)

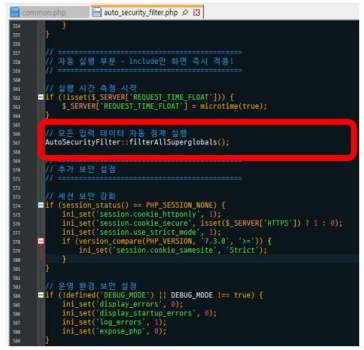
기타

리포트 샘플 (이미지 / PDF 미리보기)

SQL Injection 및 XSS 자동 필터링 함수
SQL 인젝션(30) / 반사형 크로스 사이트 스크립팅(105) / 데이터베이스 오류 패턴 발견(45) / 링크 인젝션(크로스 사이트 요청 위조 유도(32)
프레임을 통한 피싱(34)

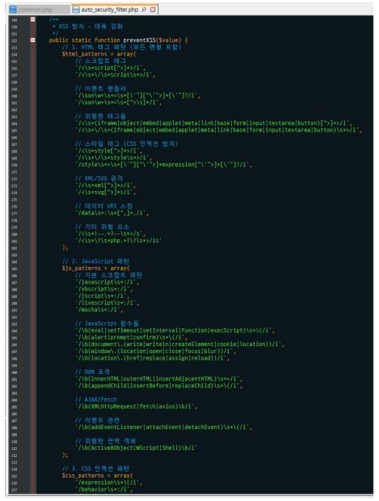
공통파일에 필터링 추가

필터링 함수에서 자동 실행



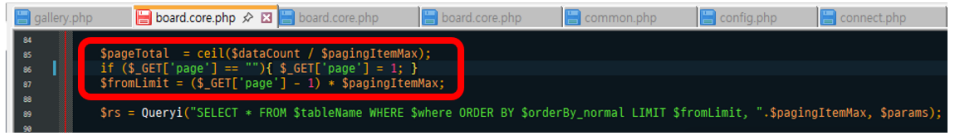
필터링 함수 내 – SQL Injection 관련

필터링 함수 내 – XSS 관련



정수 오버플로우(7)

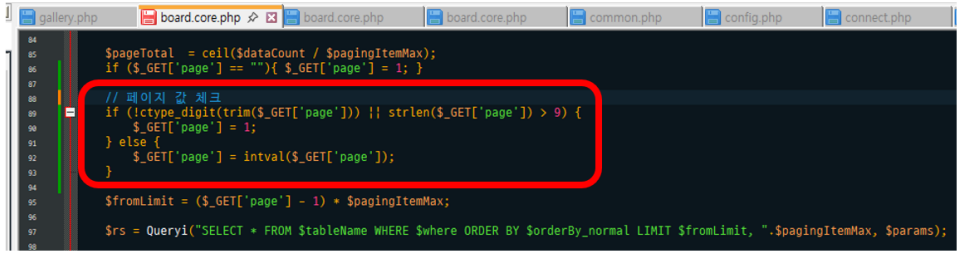
페이지 (page) 체크 전



```
$pageTotal  = ceil($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);
```

이행조치 보고서 예시 (전/후 비교)

기타

e-IFU 심사 및 공공입찰 대응용 보안 점검 리포트 활용 가이드

배경 및 필요성

2027년부터 전면 의무화
예정인 e-IFU(electronic Instructions for Use) 규정은
의료기기 제조사 웹사이트에 PDF 기반 사용설명서 제공
및 보안 확보를 요구합니다.

대부분의 심사 항목은 보안 리스크 대응 여부를 평가하며,
웹 취약점 점검 및 조치 이력이 사전 대응자료로
제출 가능합니다.

보안 심사 대응 자료로 활용 시 장점

이행점검 보고서 및 조치 완료 내역이 있는 경우,
심사 시 "적극적 보안 대응 중"이라는 평가 가능

별도 시스템 인증 없이, 신뢰성 확보 자료로 기능함

공공 입찰·조달사업 대응 시

기술평가 항목 중 '보안', '운영계획',
'리스크 대응방안' 등에서 사전 보안 점검 리포트
제출 시 가점 적용 가능
(지자체·교육청 등 입찰 사례 참고)

실제 사례: 학교 홈페이지 구축 입찰 시,
보안 점검 리포트 제출로 경쟁 우위 확보

보안 점검은 사전 예방이자, 심사/입찰의 전략

점검과 조치는 내부 보안 체계 강화 목적을 넘어서 대외 기관 대응 및 인증 신뢰 확보로 이어지는 실질 자산

향후 e-IFU 도입 대상 고객사에는 심사 대응용 문서 패키지를 함께 제공합니다.