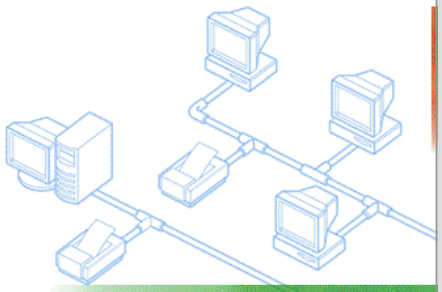
PS ScanW3B C/S

Enterprise Edition

국내 최초 웹 어플리케이션 취약점 분석도구

== PS ScanW3B (피에스 스캔웹) **==**



Copyright© 2010 by
Panicsecurity Co., LTD.

No part of this publication may be reproduced, stored in a retrieval system,
Or transmitted in any form or by any means electronic, mechanical, photocopying,
recording, or otherwise without the permission of Panicsecurity.com

Version : 1.0.2

제품 개요

PS ScanWEB CS 도입 필요성

www.panicsecurity.com

최근의 네트워크 해킹은 시스템의 취약점을 이용한 공격보다는 **웹 어플리케이션 공격에 집중**되고 있습니다.
이것은 많은 웹 어플리케이션들이 **보안에 취약한 형태**로 개발되어 침투가 비교적 쉽고
웹이라는 특성상 해킹 흔적이 거의 남지 않는 점 때문입니다.

모의해킹을 통한 웹 취약점 점검

URL 자동 수집
- 시작 페이지로부터 파생된 모든 URL 수집
- Javascript, Flash 분석을 통한 URL 자동 추출

숨겨진 URL 탐색
- 추측 가능한 중요 URL 추출 (/admin 등)
- 개발자 부주의로 인해 관리되지 않은 백업, 로그 파일 추출

XSS 점검
- 추출된 모든 URL에 대해서 Cross Site Scripting 가능성 점검

SQL/Command Injection 점검
- 추출된 모든 URL에 대해서 SQL Injection, Command Injection 등의 가능성 점검

Upload Download 점검
- 추출된 모든 URL에 대해서 파일 업로드 및 중요 파일 다운로드 가능성 점검

기업 환경 지원
- 점검자 조직을 그룹별로 관리
- 다수의 점검자가 동시에 점검작업을 수행하도록 구성

취약점 점검 분산
- 취약점 점검을 수행할 점검서버를 여러 대 분산
- 동시에 여러 점검작업을 효과적으로 분산

점검 권한의 통제
- 중앙 정책저장소를 통하여 점검자가 점검할 수 있는 웹자원을 관리하고 점검 권한을 통제

취약점 결과 관리
- 취약점 결과 검색
- 보고서 생성
- 웹서버별 취약점 추이
- 취약점 항목별 처리상태 관리

시스템 모니터링
- 웹서버별, 점검자별, 분산된 점검서버별 점검작업을 모니터링
- 원격으로 점검작업을 제어

제품 개요

PS ScanW3B CS 도입 효과

www.panicsecurity.com

국내 최초로 개발된 웹 취약점 점검도구 **시장 점유율 1위**인 PS ScanW3B를 기반으로 하고 있는 기업용 제품입니다.
강력한 취약점 점검 기능을 통하여 개발부서 또는 **다수의 보안 담당자**를 통하여
반복적인 점검 작업을 수행하는데에 최적의 환경을 제공합니다.

다수의 점검자를 위한 웹 취약점 점검환경의 구성

사내 인트라넷이나 웹을 통하여 고객에게 서비스를 제공하는 모든 환경에서 편리하게 구축하고, **웹 취약점을 점검**할 수 있습니다.

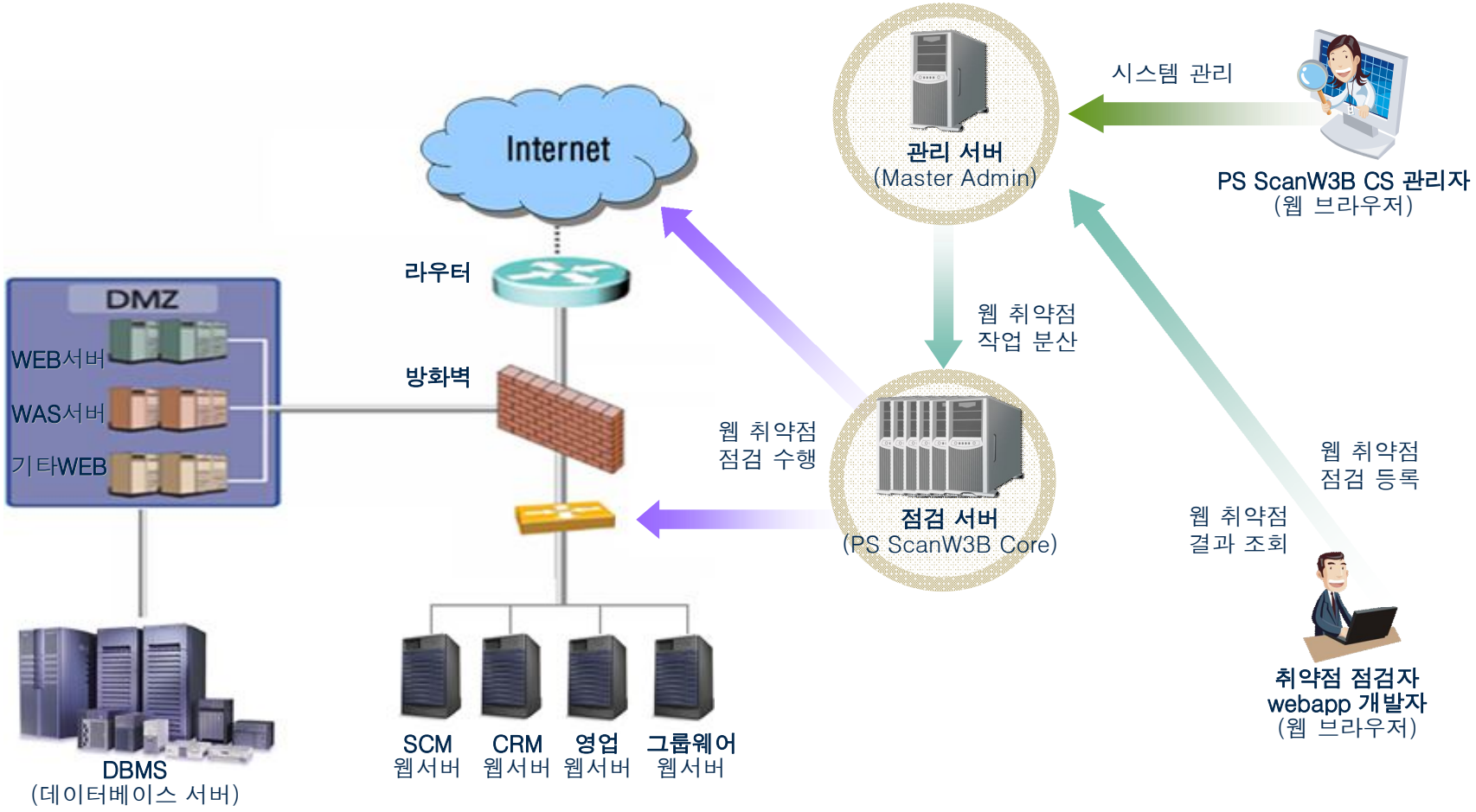
웹 취약점에 대한 점검 작업은 사후 관리 뿐만 아니라, 개발이 진행되고 있는 웹 어플리케이션에 대해서도 필요에 따라 점검을 수행하고, 취약점 결과에 대한 **조치내역을 관리**합니다.

웹 어플리케이션의 취약점을 점검하고 개발을 진행하거나 웹 서버을 유지보수하는 과정에서 귀사의 **시스템을 안전하게** 지켜드립니다.

제품 구성

PS ScanW3B CS 구성 개요

www.panicsecurity.com



제품 구성

PS ScanW3B CS 구성 요소

www.panicsecurity.com

❑ Master Admin

- 관리 서버
  - → 점검작업을 다수의 점검서버로 분산하여 처리하도록 작업을 중계합니다.
  - → 분산된 점검서버에서 실행 중인 점검작업의 실시간 모니터링 및 작업의 원격 통제를 지원합니다.
- 웹 인터페이스
  - → 일반 점검자를 위한 점검을 위한 작업 환경을 제공합니다. (브라우저 기반)
  - → 관리자의 시스템 관리 환경을 제공합니다. (브라우저 기반)

❑ PS ScanW3B Core

- 점검 서버
  - → 웹 취약점 점검을 수행하는 중요 모듈로서, URL 수집 및 각종 취약점의 존재 여부를 판단합니다.
  - → 점검 결과에 따라 보고서를 생성하고 관리합니다.
- 분산 환경
  - → 2개 이상의 점검 서버를 등록하여 효과적인 점검의 분산 환경을 구축할 수 있습니다.

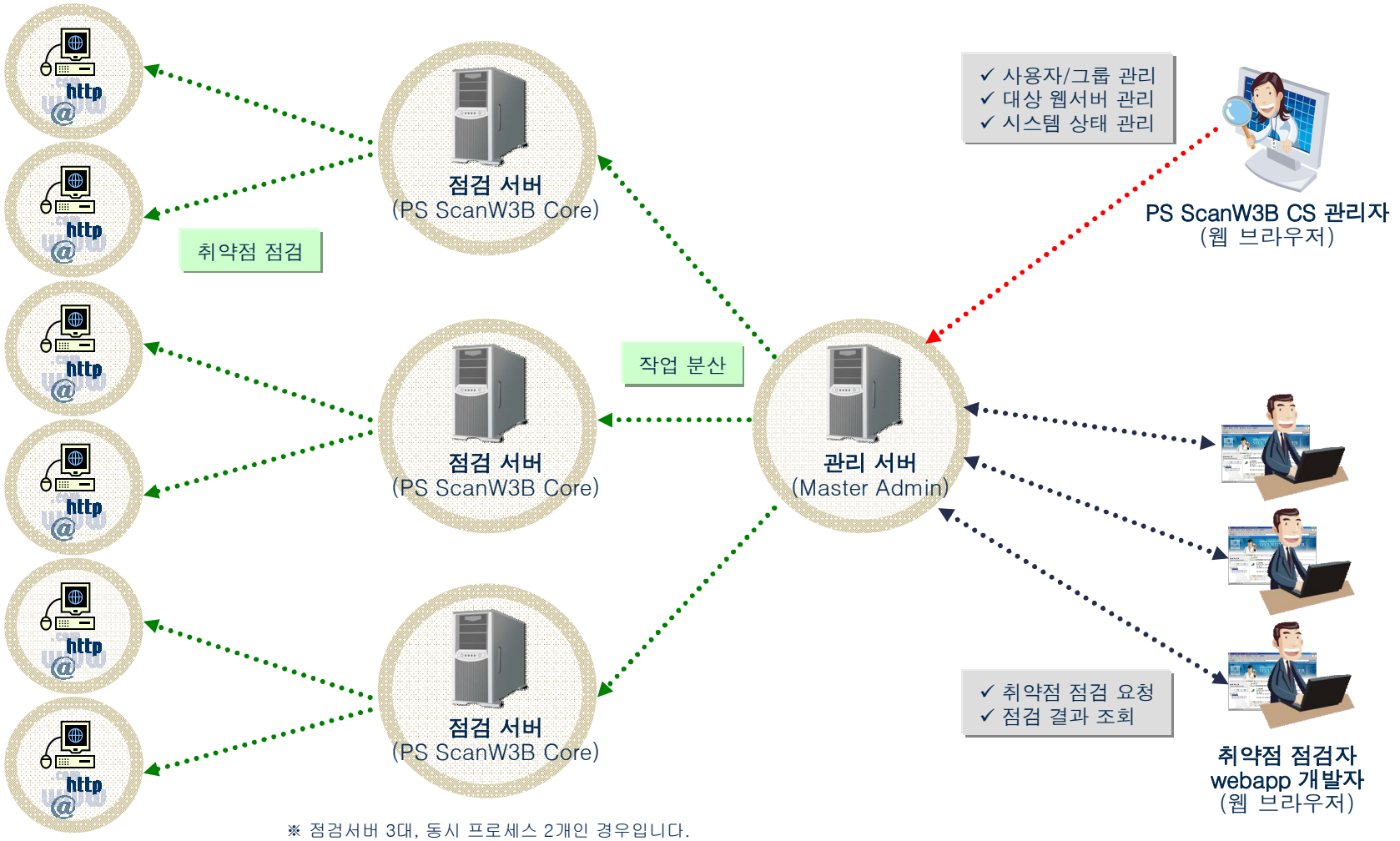
❑ Database

- 시스템 정책 및 결과 관리
  - → 시스템 계정 및 점검 권한 관리를 위한 중앙 데이터베이스입니다.
  - → 점검자 별로 점검 권한에 대한 정보를 관리합니다.
  - → 웹 취약점의 점검 결과 및 보고서 생성 정보를 관리합니다.

제품 구성

PS ScanW3B CS 서비스 형태

www.panicsecurity.com

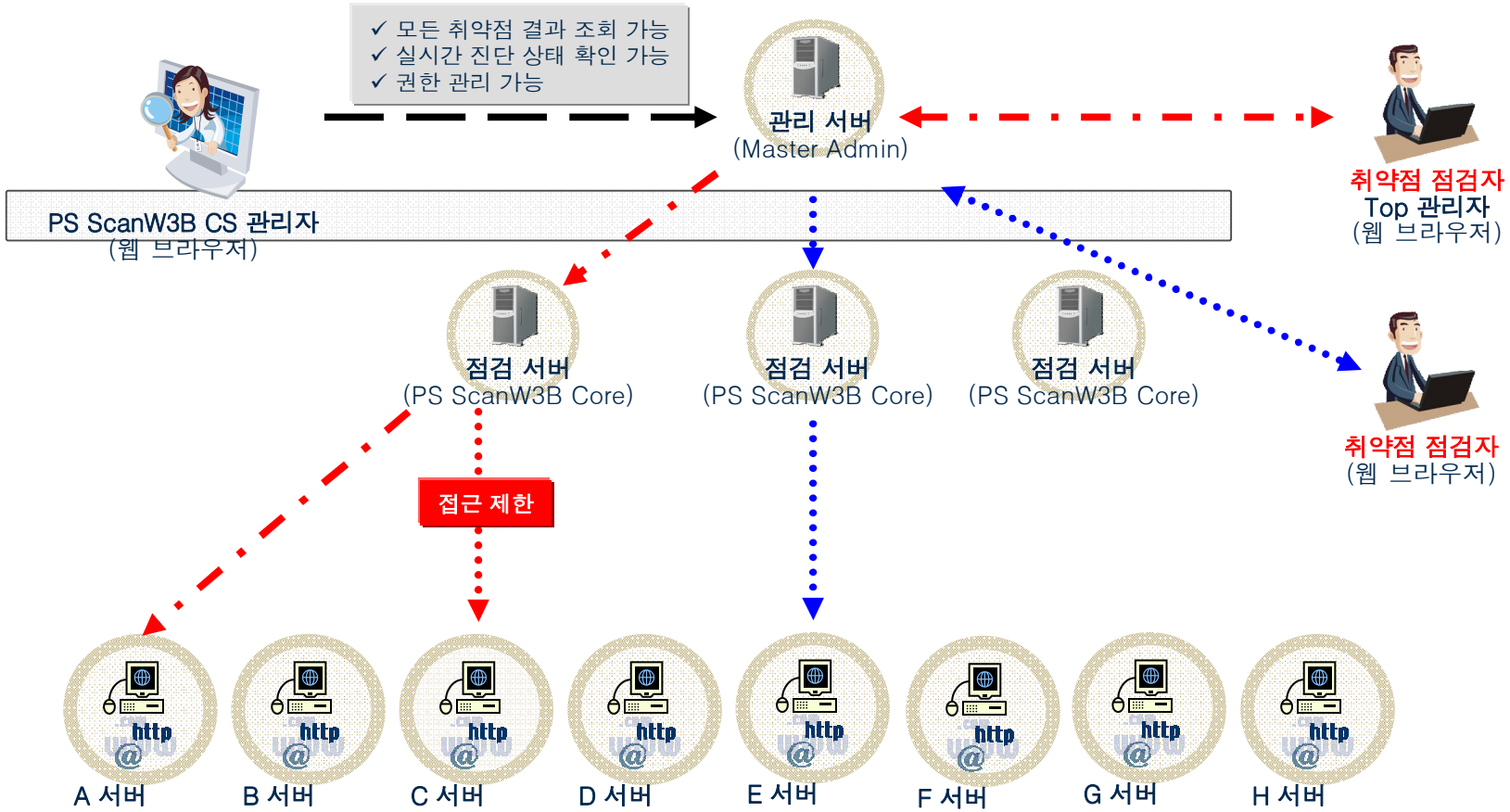


※ 점검서버 3대, 동시 프로세스 2개인 경우입니다.

제품 구성

PS ScanW3B CS 기능 구성도

www.panicsecurity.com



제품 기능

PS ScanW3B CS 주요 기능

www.panicsecurity.com

❑ 메인 페이지

- 최근 점검결과 요약
- 웹서버별 취약점 현황표
- 최근 취약점 점검내역

❑ 점검 의뢰

- 일반 점검 환경
- 고급 점검 환경 (고급 사용자용)
- 점검 예약 및 정기점검 지원

❑ 진행 상황

- 점검자 및 웹서버별 작업 모니터링
- 진행 중이거나 대기중인 작업에 대한 원격제어

❑ 결과 조회

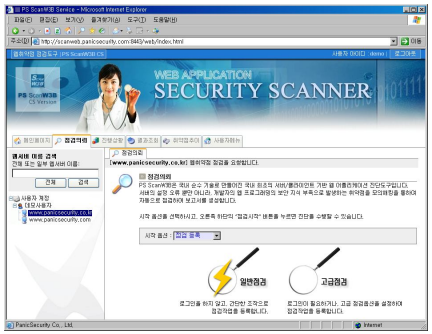
- 기간에 대한 점검자 및 웹서버별 점검내역 조회
- 취약점 종류 및 위험도에 따른 온라인 보고서
- 암호화된 PDF 점검 보고서 다운로드

❑ 취약점 추이

- 기간에 대한 웹서버별 취약점 상태 그래프
- 주요 취약점에 대한 추이 그래프

웹취약점 점검 요청 (1/2)

❑ 점검 요청



▪ 점검 형태

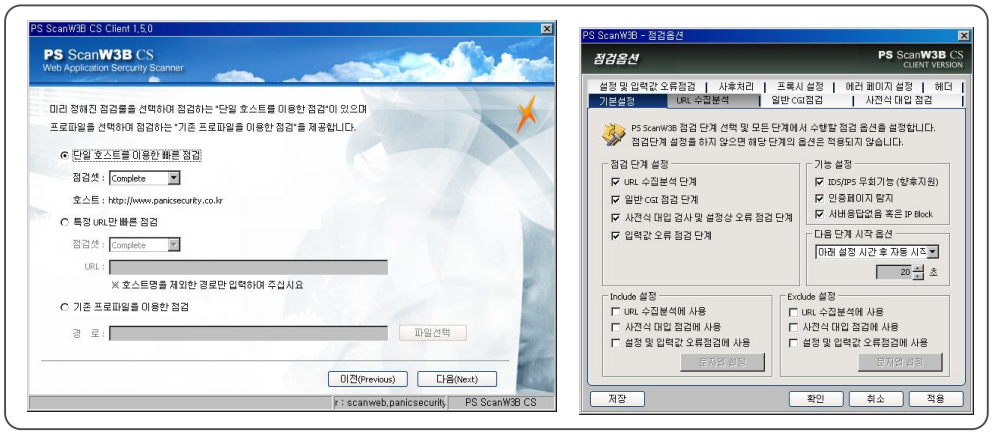
→ 관리자를 통하여 권한이 부여된 웹 서버에 대해서 취약점 점검을 요청할 수 있습니다.

→ 일반 또는 초급 사용자를 위한 '일반점검' 모드와 고급 사용자를 위한 '고급점검' 모드로 제공합니다.

→ 점검을 시작하는 시점을 정의하기 위해 3가지 형태의 점검 일정을 지원하여, 작업을 예약할 수 있습니다.

▪ 점검 옵션

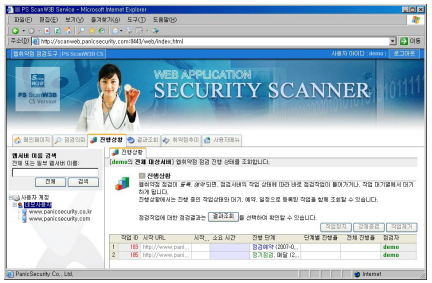
→ 고급점검 모드에서 웹 서버에 맞는 최적의 점검 옵션을 설정할 수 있습니다.



제품 기능

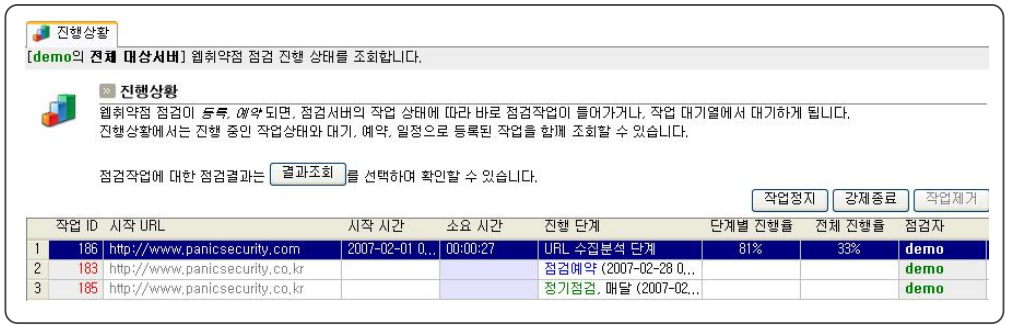
웹취약점 점검 요청 (2/2)

❑ 진행 상태



- 분산 점검
  - → 관리서버에 의해서 점검을 수행할 점검서버로 작업이 효과적으로 분배됩니다.
  - → 현재 진행 중인 작업을 실제로 수행하는 점검서버의 정보를 함께 확인할 수 있습니다.

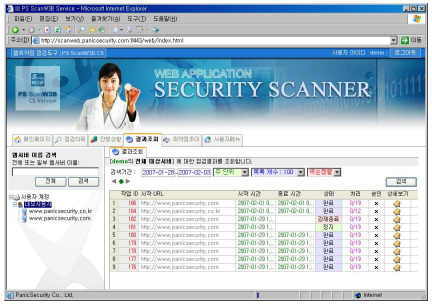
- 작업 통제
  - → 취약점 점검의 요청이 완료된 작업에 대해서, 현재 진행 상태를 조회할 수 있습니다.
  - → 진행 상태에 따라, '작업 대기', '점검 예약', '정기 점검'으로 나타나며, 각 상태별 상세보기를 제공합니다.
  - → 진행 중인 작업에 대하여 '점검 정지', '점검 종료' 기능을 제공하여, 원격에서 점검 작업을 통제합니다.



제품 기능

웹취약점 결과 조회 (1/4)

❑ 결과 조회



▪ 결과 검색

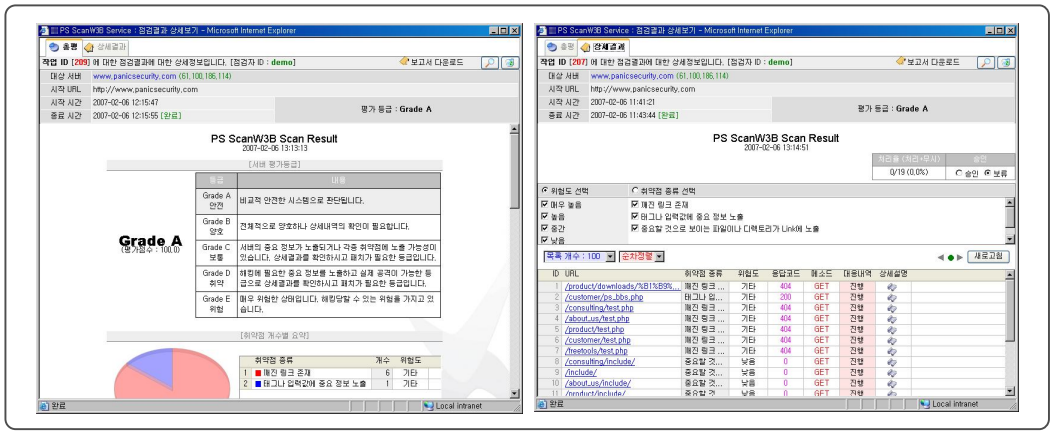
→ 메인 페이지를 통해서 최근의 점검 결과에 대해서 간단히 조회할 수 있습니다.

→ 결과 조회 페이지를 통해서 점검자 및 웹서버 별로 기간에 대한 취약점 점검 내역을 조회합니다.

→ 점검 작업의 수행 시간 및 점검 상태, 대응 내역, 승인 여부 등을 확인할 수 있습니다.

▪ 상세보기

→ 해당 점검 내역에 대해서 상세보기를 선택하면, 점검 결과에 대한 상세 정보 및 취약점 검색이 가능합니다.



웹취약점 결과 조회 (2/4)

❑ 상세 보기

▪ 총평

→ 점검 결과에 대한 요약 정보를 제공합니다.

→ 수집된 URL의 개수, 위험도별 취약점의 분포 현황, 주요 취약점 목록 등을 쉽게 확인할 수 있습니다.

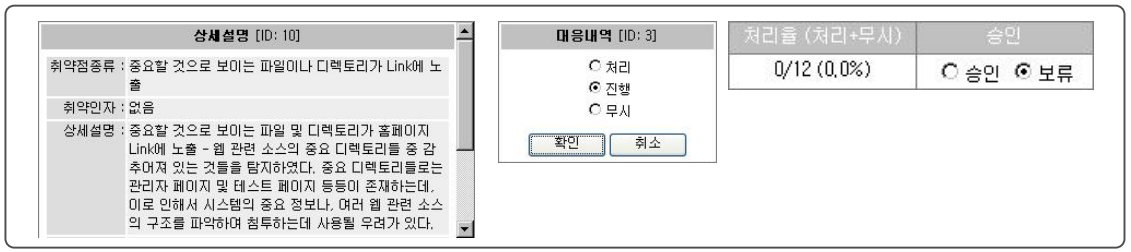
▪ 상세결과

→ 위험도별, 취약점 종류별로 취약점 내역을 선택하여, 취약점 목록을 상세 검색할 수 있습니다.

→ 특정 취약점에 대해서 상세설명을 통하여 '대응방법' 등을 확인할 수 있습니다.

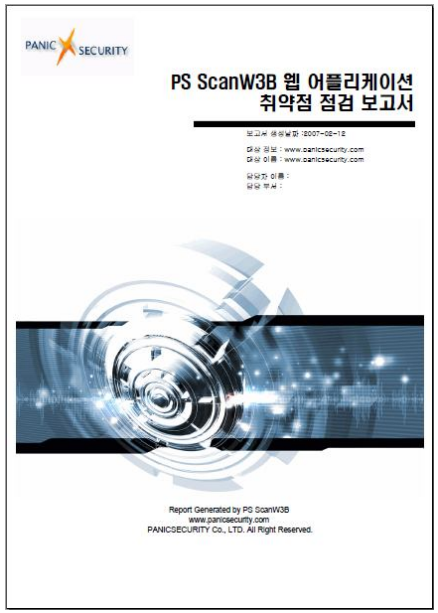
→ 특정 취약점에 대해서 대응 내역을 변경하고, 이를 공유할 수 있습니다.

→ 전체 점검 결과에 대해서 관리자는 대응 내역 전체에 대한 '승인' 여부를 변경하고, 이를 공유할 수 있습니다.



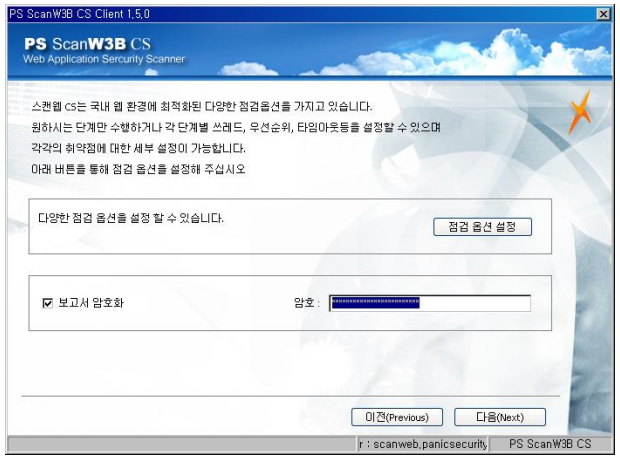
웹취약점 결과 조회 (3/4)

❑ 보고서 보기



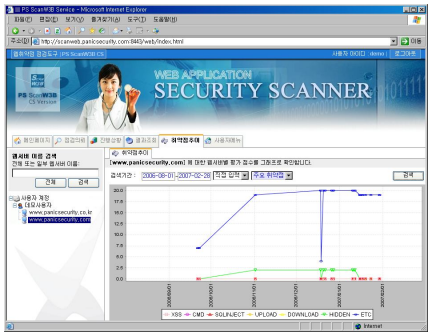
- PDF 보고서
  - → 상세 페이지를 통하여 취약점 점검 작업의 결과에 대해 자동으로 생성된 PDF 보고서를 확인할 수 있습니다.
  - → PDF 보고서는 해당 점검 결과에 대한 취약점 목록과, 영역별 통계, 취약점 상세 정보 및 대응 방안을 모두 포함하고 있습니다.

- 보고서 암호화
  - → 생성된 PDF는 점검작업의 등록 시에 입력한 보고서 암호를 통한 암호화를 지원합니다.
  - → '일반점검' 또는 '고급점검' 요청 시에 암호를 입력할 수 있습니다.



웹취약점 결과 조회 (4/4)

❑ 취약점 추이



▪ 취약점 추이

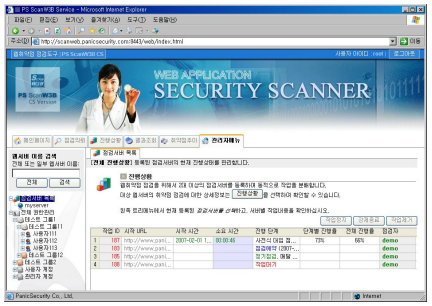
→ 웹서버 또는 점검자에 할당된 모든 웹서버에 대해서, 기간에 대한 취약점 추이 그래프를 조회할 수 있습니다.

→ 평가 점수(등급)의 추이 상태를 확인할 수 있습니다.

→ 주요 취약점(Cross Site Scripting, SQL Injection 등)에 대한 추이 상태를 확인할 수 있습니다.

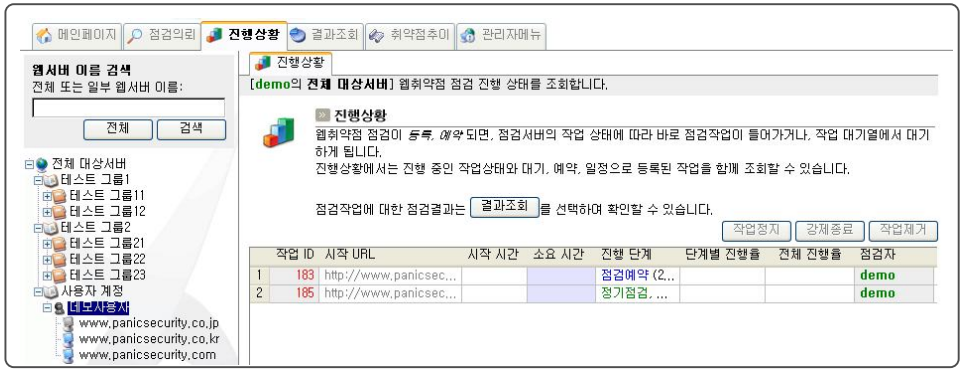
→ 웹 서버에 대해 반복적인 취약점 점검 작업에 대해서, 전체적인 위험도의 변화 상태를 확인하여, 점검자 및 관리자에게 적절한 대응을 취할 수 있도록 하고 있습니다.

❑ 상태 관리



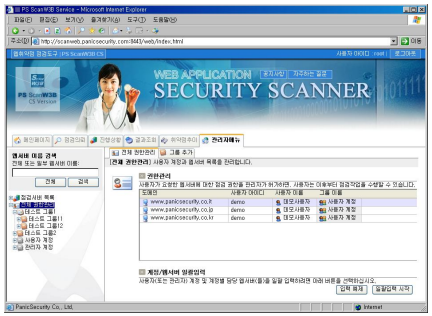
- 점검 서버, 웹 서버에 대한 진행 상황 통제
  - → 관리자 메뉴를 통해서, 시스템에 운용중인 점검서버 목록 및 현재 상태(정상 운용 여부)를 조회합니다.
  - → 전체 시스템에 등록되어 있는 예약된 점검 작업 및 진행 중인 점검 작업 및 상세 정보를 점검 서버 별로 확인 할 수 있습니다.

  - → 관리자는 '진행 상황' 탭을 통하여 사용자별, 웹서버별 점검 상태를 상세 조회할 수 있습니다.



시스템 관리 (2/2)

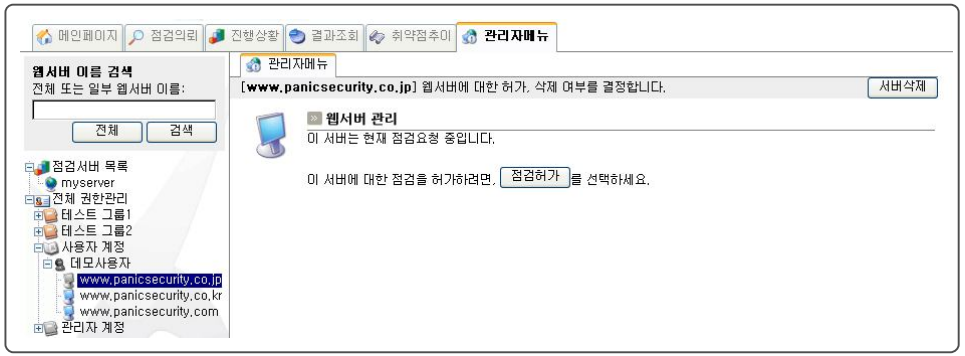
❑ 권한 관리



- 그룹 및 계정 관리
  - → 점검자 계정에 대한 논리적인 집합인 그룹을 지원하여 효과적인 계정 관리를 지원합니다.
  - → 그룹을 선택하여 하위 그룹을 추가하거나, 사용자 계정을 추가할 수 있습니다.

- 권한 관리
  - → 모든 점검자를 대상으로 점검 가능한 웹 서버를 조회하고 통제할 수 있습니다.
  - → 관리자 페이지를 통한 수동 입력과 함께, 그룹 및 사용자 계정에 대한 권한 정보에 대한 일괄 입력 기능을 통하여, 관리 작업을 자동화할 수 있습니다.

  - → 점검자에 의해서 요청된 웹 서버 목록을 확인하고 권한 할당 여부를 확인할 수 있습니다.



납품 실적

공급처		공급처	
대법원	국민은행	대한생명	삼성카드
금융결제원	금융감독원	정보통신부	삼성전자
교원나라자동차보험	국가보안기술연구소	한국정보보호진흥원	삼성네트웍스
하나로텔레콤	넥슨	중소기업은행	한국전력공사
신한은행	마사회	삼성화재	GS홈쇼핑
KTF	KT	부산은행	서울대학교
국군기무사령부	다음	CJ시스템즈	LG카드

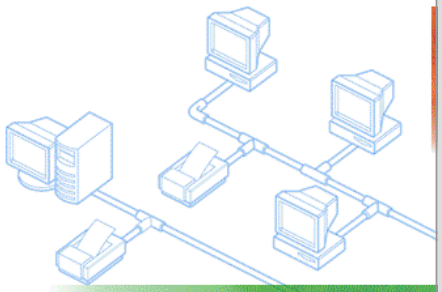
납품 실적

공급처		공급처	
증권선물거래소	예천군청	대한주택공사	서울시청
경기도청	금융감독원	CJ인터넷	은평구청
한국과학기술정보연구원	예금보험공사	양천구청	관악구청
산림청	삼성SDS	영동군청	시흥시청
의성군청	항공우주연구원	농촌진흥청	한국정보통신기술협회
구미시립도서관	대구시청	영천시	울산 교육청
서울시청	한국정보보호진흥원	삼성테크윈	한국교육학술정보원

웹 패닉시큐리티 PS ScanW3B 인가?

구분	왜 패닉시큐리티의 PS ScanW3B인가?	비고
인증서 기반 웹 점검이 가능한 유일한 제품	국내 인터넷 환경의 암복호화는 PKI 환경을 채택하여 공인/사설 인증서를 사용하는 것이 보편적입니다. 본 제품은 국내 보안업체에서 개발된 여러 PKI 제품과 연동한 개발이 이루어져, 최적의 상태로 점검을 수행합니다.	
은행권 웹 보안의 표준도구	금융결제원에서 금융 ISAC 서비스용 웹 보안 감사 도구로 채택되어, 금융 ISAC 서비스를 제공받는 대부분의 은행 웹 보안 감사를 위해 이용되고 있습니다.	
감사 기관에서 채택	한국정보보호진흥원(KISA), 국가보안연구소, 국방과학연구소, 한국교육학술정보원(KERIS), 한국과학기술정보연구원(KiSTi), 금융결제원 등에서 웹 취약점 스캐너로 도입	분야별 감사 기관
엔진 레벨에서 고객 요구사항 반영이 가능 (커스토마이징)	100% 국내 기술에 의해 개발되어, 핵심 엔진 단위의 고객 요구 내역에 대한 반영이 가능합니다. 또한 타 ESM, RMS 등과 같은 통합보안 시스템과의 연동이 가능하도록 커스토마이징의 제공이 가능합니다.	삼성그룹 보안표준 커스토마이징
국내 최고의 모의해킹 전문가 집단	❑ 08년 5월 세계 최대의 국제해킹대회인 데프콘 (Defcon) 예선에서 아시아 1위로 본선 진출에 성공 ❑ 08년 8월 미국 라스베가스에서 열린 본선 대회에서 전체 4위 입상으로 국내 역대 최고 성적 획득	'08 국제 해킹대회 Defcon' 에서의 뛰어난 성적

※ 금융 ISAC : 금융 ISAC (Korea Financial Information Sharing and Analysis Center) 은 은행권 등 금융기관의 주요 정보통신기반시설에 대한 각종 전자적 침해행위와 사이버테러에 대응하기 위한 조직 임.

㈜패닉시큐리티는
고객의 만족과 보안 향상을 위해
최선의 노력을 다 하겠습니다.
감사합니다.

(주)패닉시큐리티
www.panicsecurity.com