

# PS ScanW3B 소개서

국내 최초 웹 어플리케이션 취약점 분석도구

**== PS ScanW3B('피에스 스캔 웹') ==**

2021

## 1. Panicsecurity 소개

- 1) 회사소개
- 2) 주요 구성 인력
- 3) 주요 사업 내역
- 4) 회사연혁

## 2. 웹 어플리케이션 보안 현황

## 3. 제품 소개

## 1) 회사소개



회사 명

주식회사 패닉시큐리티

설립 일자

2004년 5월 1일

주요 구성원

정보보호전문업체(정통부 지정) 재직 경력 및  
언더그라운드 해커로 구성

보유기술

모의해킹, 웹 어플리케이션 취약점 분석,  
로그분석 (포렌직), 스마트폰 App 보안검사

연락처

신용재 영업대표 Tel : (017) 549-5765, (02) 2027-2890

E-mail: [service@panicsecurity.com](mailto:service@panicsecurity.com)

홈페이지

<http://www.panicsecurity.com>

# 1) 회사소개

## 특이사항

- 구성원 전체가 해커 출신이며, 최고수준의 기술적 취약점 능력 보유

- 다수의 모의해킹 및 기술적 취약점 분석 프로젝트 수행 경험

국가 K 기관 : 무선랜 보안 컨설팅 수행 경험

L사 쇼핑몰 : 모의해킹을 통한 기술적 취약점 분석 수행 경험 등 다수

- 웹 어플리케이션 취약점 점검 도구 PS ScanW3B 개발

- 국내 최초 인터넷 뱅킹의 메모리 해킹 시연 및 방지 대책 (PS TVS) 발표

금융보안연구소 및 금융결제원에 최초 발표 및 시연

- 국제해킹대회 DEFCON에 아시아 1위 로 본선 진출

- 미국 라스베가스에서 치러진 본선대회에서 전체 4위

## 2) 주요 사업 내역

- 웹 어플리케이션 취약점 점검 도구 - 국내 최초 개발 및 상용화

PS ScanW3B은 국내 최초의 순수 국내기술로 제작된 웹 어플리케이션 진단 도구이며, 해커출신 전문 컨설턴트가 개발에 참여하여, 웹 어플리케이션 자동화 취약성 진단 및 분석도구를 통한 현실적 대안의 제시

- 웹 해킹 징후분석 솔루션 - 국내 최초 개발 및 상용화

보안장비를 통과한 웹로그를 분석하여 웹 침해사고의 징후 분석.  
많은 양의 웹로그를 매일매일 분석/정리하여 침해사고시 원인파악 및 피해범위 파악

- 정보보호 컨설팅 사업 (기술적 취약점 분석에 중점)

다수의 모의해킹(PT, Penetration Test) 컨설팅 수행  
웹 취약점 점검 결과를 이용하여 실제 모의해킹 수행  
삼성전자의 독자 스마트폰 OS인 “BADA” 애플리케이션 보안검사 및 보안모듈 개발/공급

- 인터넷 뱅킹의 메모리해킹 취약점 최초 발표 및 시연

다수의 은행권 및 금융감독원 산하 금융보안연구소, 금융결제원 등에 취약점 최초소개 및 시연

### 3) 회사 연혁 -1

기간	회사연혁	해당기관
2004. 05.	주식회사 패닉시큐리티 설립	
2004. 07.	대법원 등기정보시스템 보안컨설팅 1차 사업수행	법원행정처
2004. 09.	대법원 등기정보시스템 보안컨설팅 2차 사업수행 국내 최초 웹어플리케이션 취약점 분석툴 출시	법원행정처
2004. 10.	포스코 모의해킹 컨설팅 수행 (STG시큐리티 협력)	포스코
2005. 04.	벤처기업 지정 (신기술기업)	중소기업청
2005. 05.	무선랜 보안장비 (Wi-Fi IDS) 개발 과제	중소기업청



### 3) 회사 연혁 -2

기간	회사연혁	해당기관
2005. 02.	사이버독도, GS 홈쇼핑 등 다수의 홈페이지 취약점 스캔 컨설팅	
2006. 03.	금융감독원 연간 유지보수 계약 - 분기별 취약점 분석	GSeShop
2006. 04.	한국정보보호진흥원(KISA) 연간점검 - 분기별 취약점 분석	금융감독원
2006. 07.	“홈페이지 개발자를 위한 훈련공간” 구축 위탁과제	KISA
2006. 09.	국가정보원 보안 적합성 검토 필	KISA
2007. 03.	벤처기업 재 지정	국가정보원
2007. 05.	인터넷 뱅킹의 메모리 해킹 최초 발표 및 시연. 대책 발표	기술보증기금
2008. 05.	<b>국제해킹대회(Defcon) 예선전 아시아 1위로 본선 진출</b>	
2008. 08.	<b>미국 라스베가스에서 치뤄진 본선 대회에서 전체 4위</b>	국내 역대 최고기록

## 1. Panicsecurity 소개

## 2. 웹 어플리케이션 보안 현황

- 1) 웹 어플리케이션 취약점의 현황
- 2) 웹 보안 솔루션 현황
- 3) 웹 취약점 대응 현황
- 4) 웹 보안 고려 요소
- 5) 안전한 웹 보안 대책
- 6) 웹 취약성 진단 도구의 필요성

## 3. 제품 소개

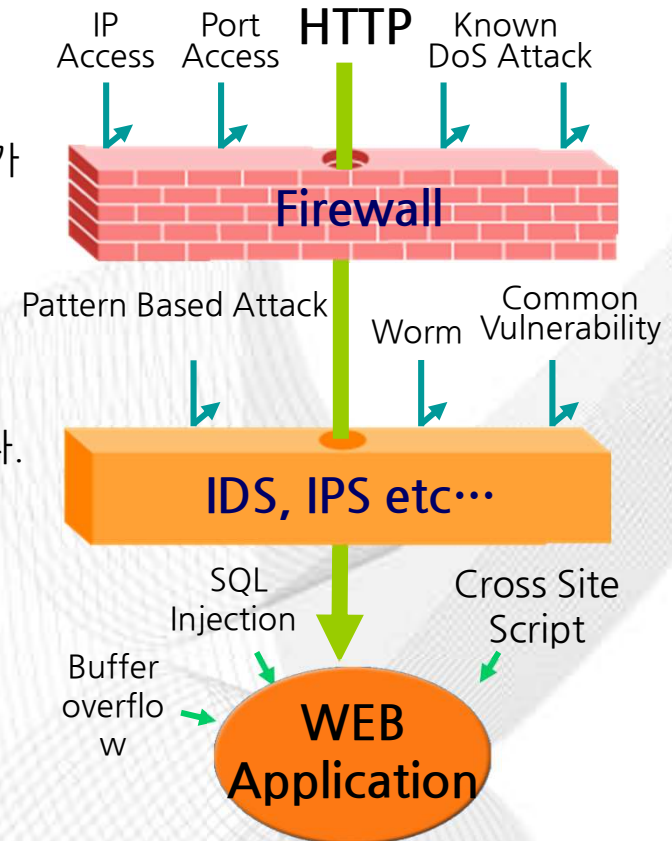


# 1) 웹 어플리케이션 취약점 현황

일반적으로 웹 기반의 침해사고가 발생하는 이유는 웹 응용프로그램의 설계 시에 데이터베이스 접근, 관리자 인증 및 사용자 인증, 웹 응용프로그램의 설계 방식에 대한 보안성 검토가 이루어지지 않기 때문에 발생합니다.

그러나, 웹 서비스에 대한 제어 및 통제는 기존 보안 솔루션인 침입탐지/차단시스템 - IDS(Intrusion Detection System), IPS(Intrusion Prevention System) - 에서 방어가 불가능합니다.

결론적으로 최근 웹 어플리케이션의 취약점을 이용한 공격이 폭발적으로 증가하는 이유는 웹 어플리케이션에 존재하는 취약점의 보안성 검토를 수행하지 못하기 때문이며, 웹 어플리케이션 취약점이 존재할 경우, 현재의 보안 아키텍처 구성으로는 방어가 불가능합니다.



75% 이상의 사이버공격과 인터넷 보안침해 사고는  
인터넷 웹 어플리케이션 취약점을 이용하여 발생한다.

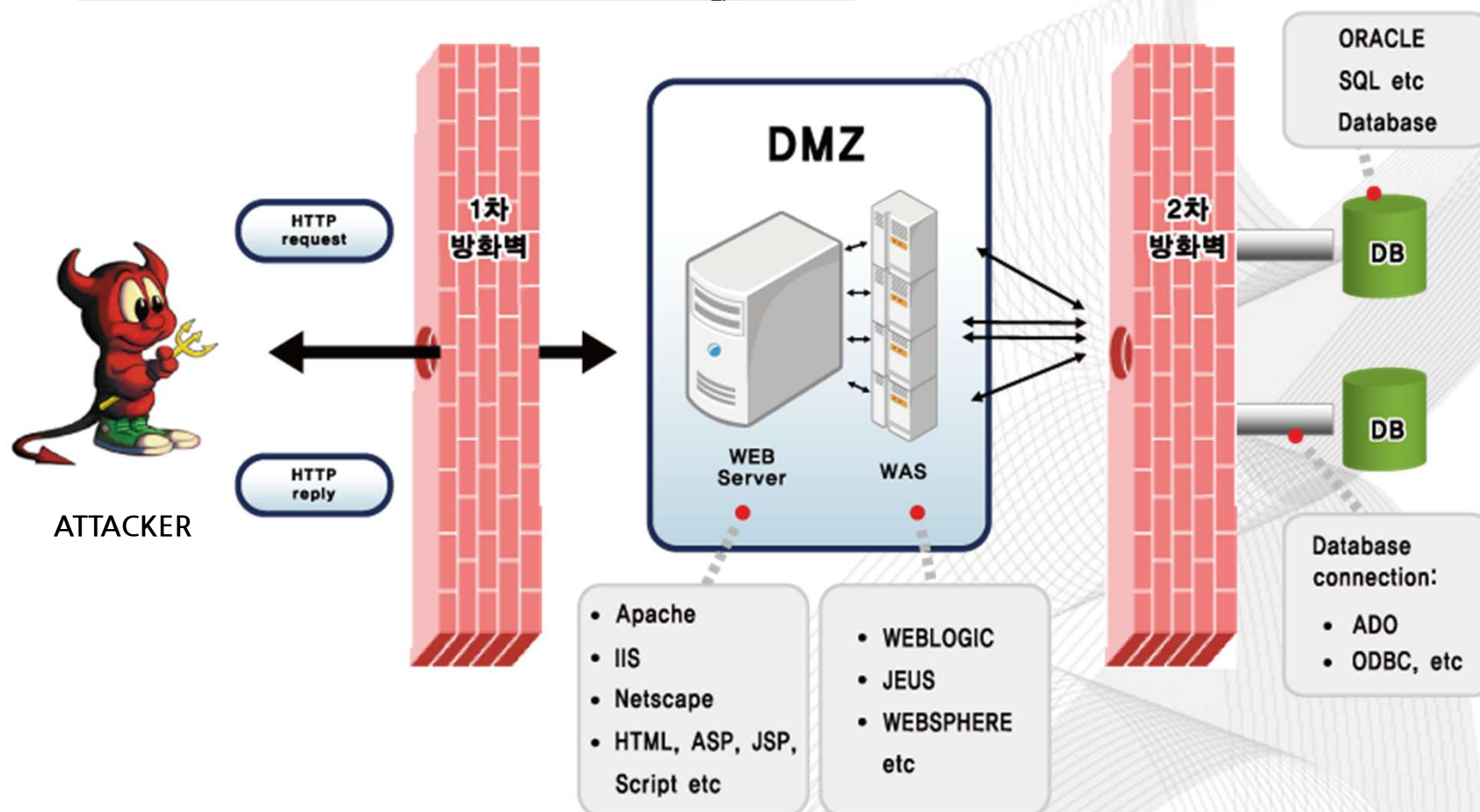
-미국 Gartner Group 보고서-

## 2) 웹 보안 솔루션 현황

종류	기능	제품명	비고
서버 보안 (시큐어OS)	전자서명 인증, 파일 암호화, 접근통제, 침입탐지, 권한분리 등의 여러가지 보안기술로 서버시스템 보호.	- 시큐브(주)의 '시큐브 TOS' - 레드게이트의 '레드 캐슬'	어플리케이션 레벨의 취약점은 탐지 및 방어 불가능
암호화 (+ 전자서명)	- HTTP 프로토콜에서 Plain Text로 전달되는 메시지 및 데이터를 암호화 하여 스니핑 (훔쳐보기) 방지 기능 - 전자서명으로 데이터의 악의적 위변조 방지 기능	-소프트포럼의 XecureWeb -이니텍의 INISAFE	
인증 (PKI, 생체)	사용자 확인과정인 인증의 강도를 높이기 위하여 도용하기 쉬운 ID/PWD 외에 다른 매체 사용	-소프트포럼의 XecureWeb -이니텍의 INISAFE	
웹 어플리케이션 보안	2가지 솔루션 : 웹 스캐너 및 웹 방화벽 - 웹 프로그래밍 취약점/오류 점검 : 웹 스캐너 - 비 정상적인 HTTP 요청 거부 : 웹 방화벽	-패닉시큐리티의 'PS ScanW3B' -WatchFire의 'AppScan' -KAVADO의 'ScanDo'	- 웹 어플리케이션 레벨의 보안 솔루션 - 주민번호, 카드 번호 등 개인정보 노출 여부 점검 가능

### 3) 웹 취약점 대응 현황

웹 서비스 데몬과 WAS(Web Application Server) 및 DB연동을 위한 웹 서비스 시스템의 구성은 네트워크, 서버 OS, 웹 서비스 데몬, 프로그램 언어 선택, 데이터베이스 연동 방식 별로 모두 다른 방식으로 존재하며, 보안성 검증은 사실상 웹 서비스 개발자의 웹 서비스 보안 프로그래밍 기술에 의존할 수 밖에 없는 현실입니다.



## 4) 웹보안 고려 요소

일반적으로 웹 기반의 침해사고가 발생하는 이유는 웹 응용프로그램의 설계 시에 데이터베이스 접근, 관리자 인증 및 사용자 인증, 웹 응용프로그램의 설계 방식에 대한 검토가 이루어지지 않기 때문에 발생합니다.

### 웹 어플리케이션 취약점 보안 고려요소

개발 및 기획 단계에서의 보안성 고려



- 개발자가 보안 프로그래밍 구현 능력이 있는가?
- 웹 서비스 데몬 및 OS 형태에 대한 보안 고려를 통한 웹 어플리케이션 보안을 수행하는가?

사용자 인증 및 각종 Argument의 입력  
정당성 여부의 검증



- 사용자 인증 및 각종 입력매개변수(Argument)에 대한 필터링이 효과적으로 수행되는가?
- SQL Injection, XSS(Cross Site Script)등을 통한 불법적 프로세스의 권한 획득 가능성이 없는가?

데이터베이스 설정 정보의  
악의적 추출 가능성 검증



- 사용자의 Query에 따른 데이터베이스 설정 정보를 가져오는 과정에서의 Cookie Spoofing 및 Session Replay를 통한 타 사용자 정보의 추출이 가능하지는 않은가?

보안 조직에서의 웹 어플리케이션에  
대한 지속적 보안성 검증 및 감사



- 지속적으로 진화하며, 개발 및 지속적 유지보수가 일어나는 웹 어플리케이션에 대한 보안성 검증 및 감사의 수행이 보안조직에 의해 검토 되는가?

## 5) 안전한 웹 보안 대책

웹 보안대책은 기본적으로 웹 보안 프로그래밍 기술에 의한 구현이 Best Practice 라고 할 수 있으나, 전문 웹 보안 개발자의 부족과 웹 개편으로 지속적인 보안 문제가 발생하기 때문에 웹 취약점 스캐너와 웹 방화벽을 이용한 웹 취약점 방어대책의 구현이 필요함.

### 웹 보안대책의 어려움?

1. 취약점 정보의 이해가 어려움
2. 취약점은 서비스 구성에 따라 다르게 나타남
3. 웹 서비스의 지속적 개편 및 수정 시 취약점 수동점검에 따른 비용과 시간의 한계
4. 전문적 웹 보안 개발자의 부족

### 웹 보안 대책?

방안 1. 웹 취약점 점검 도구의 도입

- 점검 도구를 활용한 취약한 웹 소스 수정
- 네트워크 성능 저하 및 오탐없는 근본적 대책

방안 2. 웹 방화벽 도입

- 기존 웹의 수정 없는 방어 대책
- 웹 성능 저하 및 오탐 가능성 내포
- 기능 제한 존재 (파일 업로드 등)
- 계속해서 발생하는 우회공격 대처가 불가능



### 안전한 웹 보안대책

1. 웹 보안 프로그래밍
2. 취약점 스캐너 활용
3. 웹 방화벽 도입
4. 웹 전문 보안 컨설팅을 통한 보안성 검증



## 6) 웹 취약점 진단 도구의 필요성

개발자의 보안 프로그램  
설계 skill 미흡

보안 프로그래밍 기술은 끊임 없이 진화하며,  
개발자의 역량에 의존하는 것은 현실적으로 불가능

수작업 점검의 한계

웹 사이트에 포함된 수많은 URL을 일일이 수작업으로 점  
검하는 것은 불가능

지속적 웹 서비스의  
개발 / 진화

사용자 서비스를 위한 웹 개발은 지속적으로 이루어지며,  
그에 따라 지속적인 보안성 검토 필요

웹 방화벽 등 보안  
솔루션의 검증

웹 방화벽 등의 해킹 방어 솔루션의 정당한 작동 여부 검  
증 필요

웹 어플리케이션 취약성  
자동화 진단 도구 필요

지속적인 웹 서비스의 개발과 진화에 따른 웹 어플리케이션  
취약성 자동화 분석 도구의 필요성이 증가



## 1. Panicsecurity 소개

## 2. 웹 어플리케이션 보안 현황

## 3. 제품 소개

- 1) 제품 개요
- 2) PS ScanW3B 소개
- 3) PS ScanW3B의 점검 결과 예
- 4) 외산 제품과의 차별성
- 5) 납품 실적
- 6) 평가/인증
- 7) 왜 패닉시큐리티 인가?

# 1) 제품 개요

최근의 네트워크 해킹은 시스템의 취약점을 이용한 공격보다는 웹 어플리케이션 공격에 집중되고 있습니다. 이것은 많은 웹 어플리케이션들이 보안에 취약한 형태로 개발되어 해킹 방법이 손쉬우며, 웹이란 특성상 해킹흔적이 거의 남지 않는다는 점 때문입니다.



“ 모의 해킹을 통한 웹 취약점 점검 필수 ”

## PS ScanW3B 주요기능

### URL 자동 수집

- 시작 페이지로부터 파생된 모든 URL추출
- Javascript, flash 파일분석에 의한 URL 자동 추출

### 숨겨진 URL 탐색

- /admin 등 노출되지 않은 각종 숨겨진 URL 추출
- bak, log, org 등 개발자가 부주의하게 남긴 불필요한 파일 추출

### XSS 점검

- 추출된 모든 URL에 대해서 Cross Site Scripting 가능성 점검

### SQL, Command Injection 점검

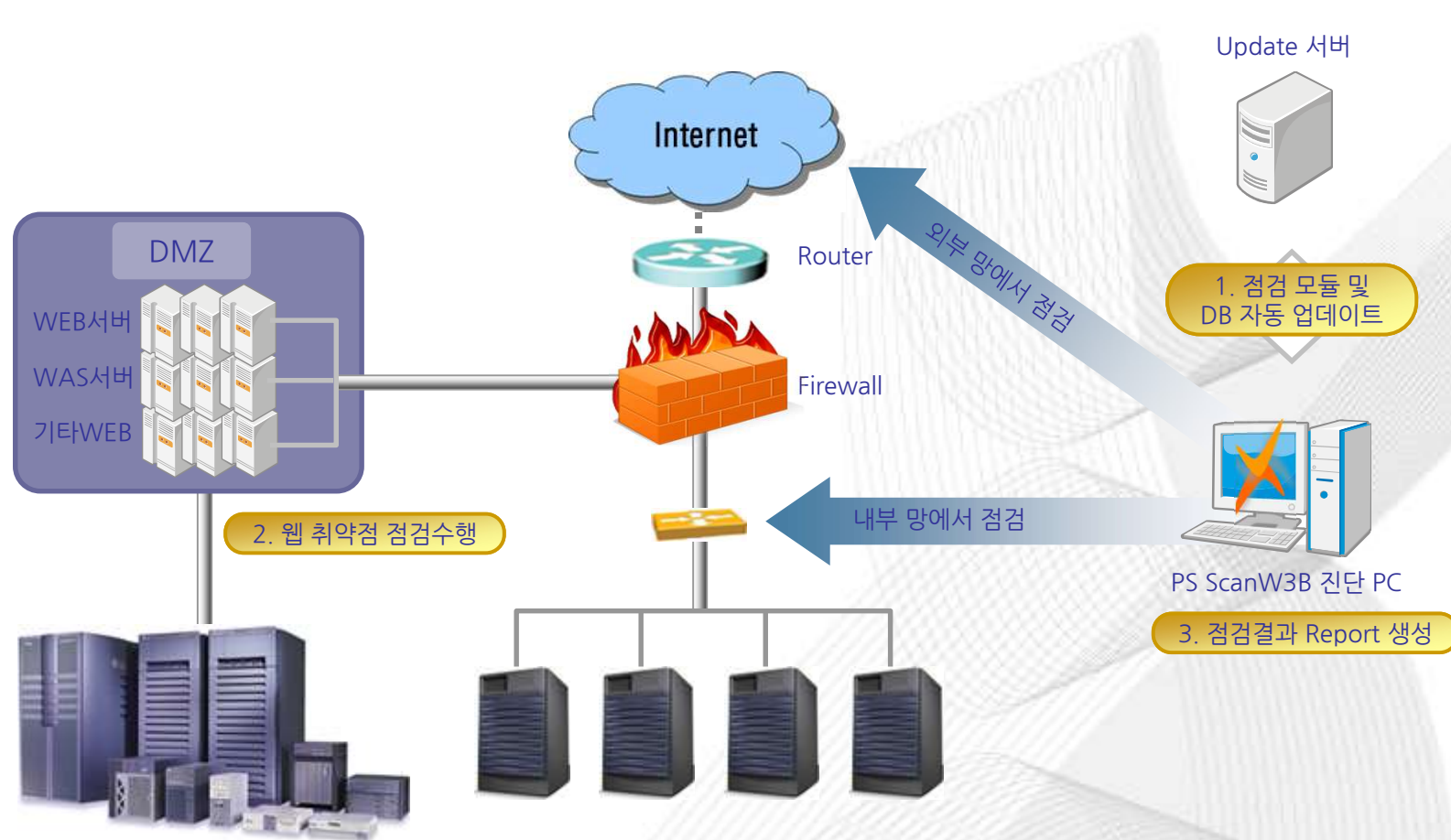
- 추출된 모든 URL에 대해서 injection 가능성 점검

### Upload / Download

- 추출된 모든 URL에 대해서 파일 업로드/다운로드 가능성 점검

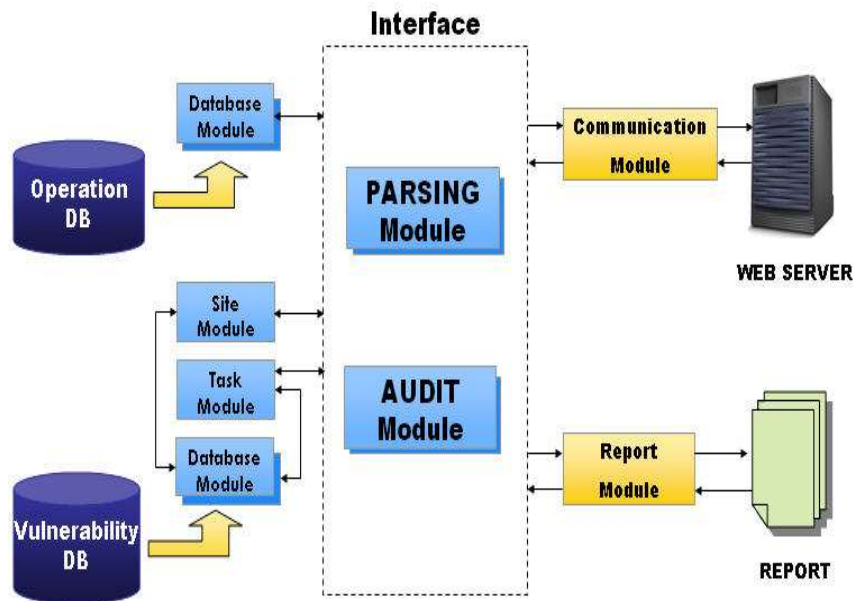
## 2) PS ScanW3B 소개

### 1. PS ScanW3B 진단 구성도



## 2) PS ScanW3B 소개

### 2. 기능 분해도



기능구성	세부 설명
Operation DB	취약점 스캔을 위한 대상 정보 및 일시와 설정 Option, 위험도에 대한 선언이 되는 부분
Vulnerability DB	취약점에 대한 선언과 위험도 및 리포트 추출을 위한 웹 취약점 결과가 생성 및 누적되는 부분
Parsing Module	URL 수집을 위한 Module이며, 2세대 웹 어플리케이션 보안시스템의 핵심적 역할을 담당하는 부분
Audit Module	Parsing Module에서 전달된 Event에 대한 취약점 요소를 선별하는 부분
Communication Module	웹 어플리케이션 정보 (URL 및 각종 Argument)에 대한 수집을 담당하는 부분
Report Module	취약점 결과에 대한 보고서 생성을 담당하는 부분
Site Module	사이트 정보를 호출하고 관리를 담당하는 부분
Task Module	사이트 스캔 시 설정된 옵션 정보 등을 담당하는 부분
Database Module	Operation DB와 Vulnerability DB의 연동을 용이하게 하기 위한 역할을 담당하는 부분

## 2) PS ScanW3B 소개

### 3. PS ScanW3B 주요 기능

#### 보고서 생성

- 다양한 보고서 양식 지원 (DOC, PDF, TEXT)
- 보고서에 추가 및 제거선택, 내용의 수정이 가능
- 기본 보고서 표지 설정 및 사용자 지정 보고서 생성 가능

#### 기타 부가 기능

- 분석 결과 비교 및 분석 기능
- 사용자 설정 특정 단계 재점검 가능
- 점검 URL 트리 확인 가능

#### PS ScanW3B

- 숨겨진 디렉토리 및 파일의 검출 (/admin,/adm,/관리자 등)
- URL 추출 기능 및 패스워드 무한반복대입공격(Brute Force Attack)
- Buffer Overflow, SQL Injection, XSS 취약점 검사
- Cookie Spoofing 검사, Directory Indexing 취약점 검사
- File Upload 및 Download 취약점 검사, Meta 문자악용명령 실행 검사
- CGI 항목에 대한 수동 및 자동 검사
- 주민등록, 신용카드 번호, 핸드폰 번호 등 개인정보 검색

#### 점검 항목

- URL 추출, 수동, 자동 점검 기능에 대한 분석 설정 기능
- 필요한 항목만 선별적으로 선택하여 분석 가능하도록 설정 기능
- 네트워크 Time-Out, Thread 수 설정
- 404, 500 응답 Page 설정 (자동/수동)
- 자체 모듈인 PS Proxy를 통해 통신 정보(Req/Res) 확인 가능

#### 취약점 분석 환경 설정 기능



## 2) PS ScanW3B 소개

### 4. 차별화 된 기능

(1) 국산 게시판 취약점 점검 기능

제로보드, 그누보드, 테크노트, KorWeblog 등 각종 PHP 관련 보드

(2) SSO(Single Sign On) 점검 기능

SSO 인증에 따른 웹 어플리케이션 접근 및 취약 점검 가능

(3) 인증서 기반 사이트 점검 기능

표준 및 사설, 공인 인증서 기반 웹 어플리케이션 환경 점검 가능

(4) 완벽한 한글 웹 점검 지원

엔진, 메뉴, 보고서, 취약한 한글 디렉터리 점검

(5) IDS, IPS 우회 점검 기능

GET, POST, URL, Encoding 등을 이용한 우회 공격 기법 점검 지원

(6) 피싱(Phishing) 취약점 점검 기능

사이트 위장 공격을 통한 악의적 접근에 따른 취약점 점검 기능

(7) 사후 처리 기능

취약점 점검 후 각종 점검용 게시물 등에 대한 제거 기능

(8) 개인 정보 추출 기능

주민등록번호, 핸드폰 번호, 신용카드 번호 등의 외부 유출 사전 제거

(9) 에러페이지를 통한 시스템 정보의 추출

에러페이지에 노출되는 시스템 중요 정보의 탐지

(10) 웹 서버 포트 스캔 기능

80 포트 이외의 웹 서비스 포트에 대한 탐지 기능



## 2) PS ScanW3B 소개

### 5. 신규 취약점에 대한 Update 기능



## 2) PS ScanW3B 소개

### 6. 보고서 기능

#### • 충실한 보고서 내용

충분한 내용의 보고서와 함께 최신의 보고서 양식을 함께 지원하고 있으며 SW보안약점, OWASP 등과 같은 다양한 형태의 보고서를 생성할 수 있습니다.

등 급	내 용
<b>GRADE A</b> 안전	모의 해킹 과정에서 취약점을 발견하지 못하였으므로 비교적 안전한 시스템으로 판단됩니다.
<b>GRADE B</b> 양호	취약점 상태는 양호하나 Email 주소, 핸드폰 번호, 판단됩니다.
<b>GRADE C</b> 보통	서버의 중요 정보가 노출되거나 각종 취약점에 노출 이 등급은 현 상태는 위험한 상태는 아니지만 해킹 포
<b>GRADE D</b> 취약	해킹에 필요한 중요 정보를 노출하고 실제 공격이 가 상제결과를 확인하시고 패치가 필요한 등급입니다.
<b>GRADE E</b> 위험	매우 위험한 상태입니다. 영계등 해결할 수 있는



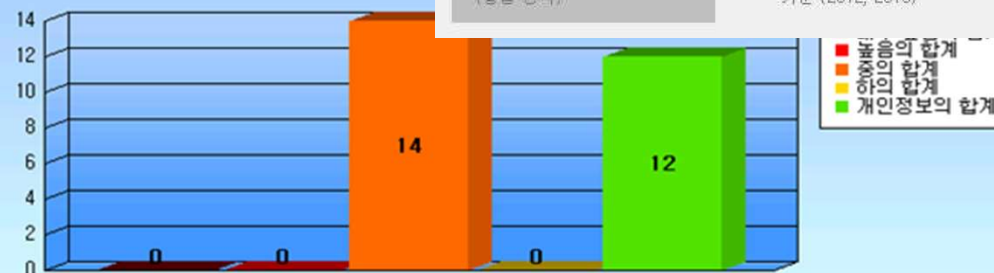
기본 보고서  
PS ScanW3B 기본 양식  
(통합 양식)



SW 보안약점 보고서  
행정안전부, 한국인터넷진흥원  
기준 (2012, 2013)



OWASP 2013  
OWASP Top10 2013



## 2) PS ScanW3B 소개

### 7. 운영효율성 및 관리의 용이성

#### (1) 계정 관리

최고 권한의 관리자 계정 밑에 하위 계정 별로 점검 가능한 도메인을 추가할 수 있습니다.

- 효율적인 점검 계정 생성/수정/삭제 관리 기능
- 편리한 점검 도메인 관리
- 사용자 계정 발급을 통한 담당자 업무 지정 편리성

The screenshot shows the '계정관리' (Account Management) window of the PS ScanW3B Web Application Security Scanner. The window has a title bar with '계정관리' and a close button. The main area is divided into two panes. The left pane shows a tree view with 'Manager' and 'User' under it. The right pane contains a form for creating or editing an account. The form fields are: 이름 (Name) with value '사용자', 계정 (Account) with value 'User', 암호 (Password), 암호확인 (Confirm Password), and 계정설명 (Account Description) with value '사용자\_1'. Below these fields is a table with columns '서버 IP', 'Port', and '호스트명'. The table contains one row with values '211.214.16...', '80', and 'www.panicsec...'. At the bottom of the form are fields for '호스트명' (www.panicsecurity.com) and '서버 IP' (empty) with 'PORT' (80). There are buttons '서버 추가', '서버 수정', and '서버 삭제' below the table. At the very bottom of the window are buttons '추가', '수정', '삭제', and '닫기'.

서버 IP	Port	호스트명
211.214.16...	80	www.panicsec...

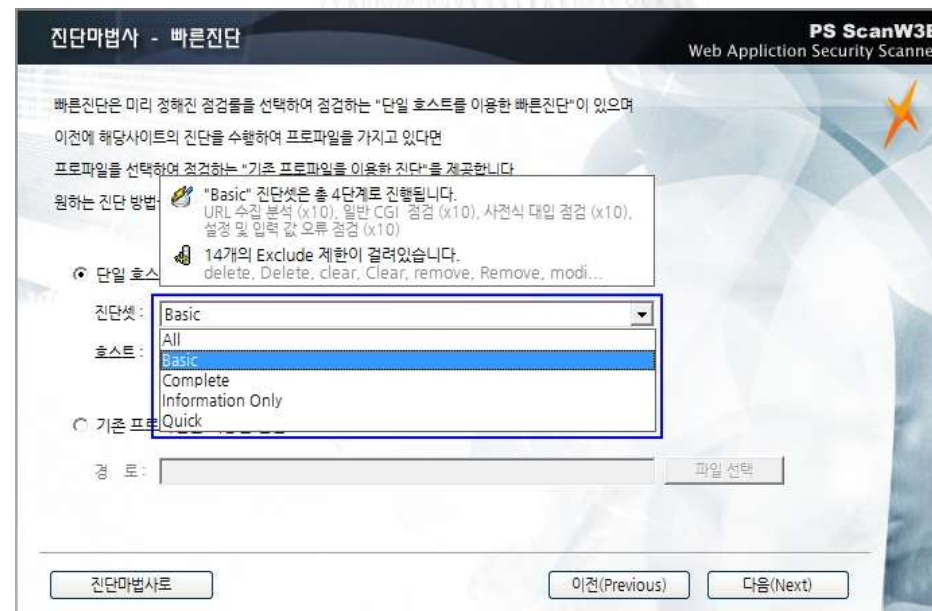
## 2) PS ScanW3B 소개

### 7. 운영효율성 및 관리의 용이성

#### (2) 진단셋 선택 기능

진단셋 저장을 통해 사용했던 점검 옵션을 그대로 불러와 사용이 가능합니다.

- 사용자에 의한 점검셋 추가 가능
- 도메인 별 진단셋 설정을 통한 점검 옵션 관리 가능



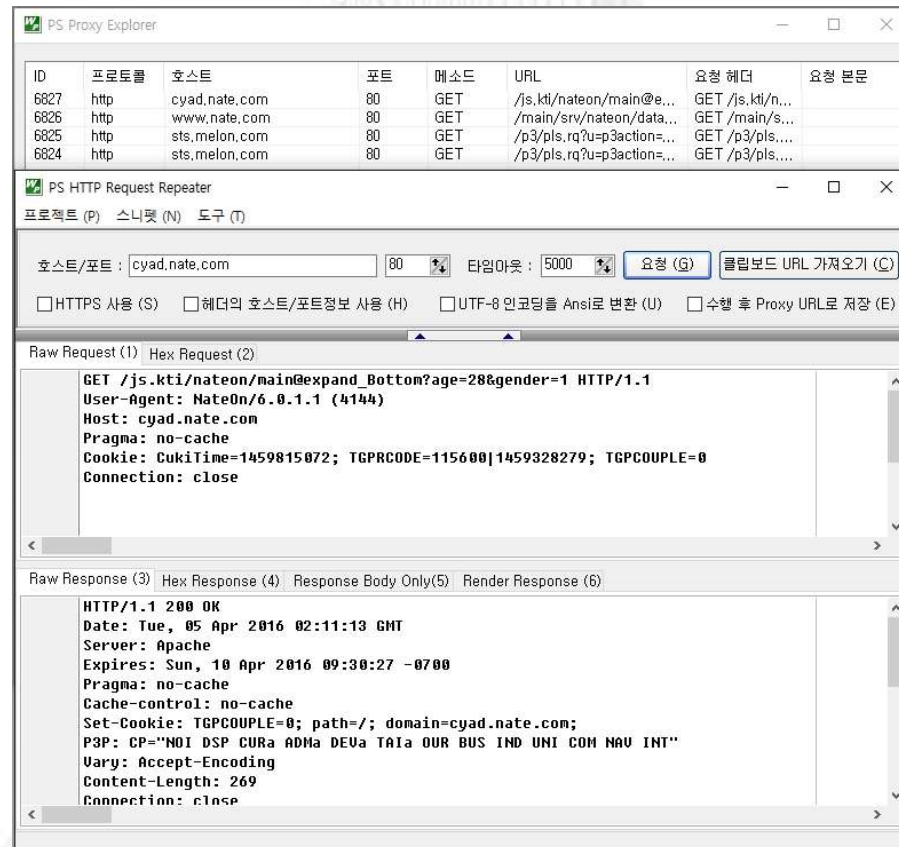
## 2) PS ScanW3B 소개

### 7. 운영효율성 및 관리의 용이성

#### (3) PS Proxy 기능

자체 프록시 모듈인 PS Proxy 모듈을 통해 http 통신 전문 확인이 가능합니다.

- 수동으로 확인이 필요한 http 요청/응답 코드에 대한 확인 가능
- 사용자가 직접 Request 전문을 작성하여 서버에 전달 가능





## 2) PS ScanW3B 소개

### 7. 운영효율성 및 관리의 용이성

#### (4) 수동진단 및 결과저장

자동 점검 뿐 아니라 사용자에게 의한 수동 진단 툴을 지원하며, 점검 결과를 보고서에 추가할 수 있습니다.

- 수동 진단을 통해 보다 정확한 결과를 보고서에 출력 가능

The screenshot displays the '수동 진단 결과 저장' (Manual Diagnosis Result Storage) window of the PS ScanW3B Web Application Security Scanner. The window is titled '수동진단 결과저장' and 'Web Application Security Scanner'. It contains a message: '수동진단 결과를 저장하기 위해서는 몇가지 입력 정보가 필요합니다. 정확하게 입력해야만 정확한 보고서를 얻을 수 있습니다.' (To save manual diagnosis results, some input information is required. Accurate input is needed to obtain accurate reports.)

Fields for manual diagnosis include:

- TASK HOST ID: 40
- URL: http://www.panicsecurity.com/
- 취약한 인자: (empty)
- 응답코드: 200
- 메소드: GET (dropdown)
- 공격타입: PUT를 통한 파일 업로드 가능 (dropdown)
- 요청 헤더: GET / HTTP/1.1, Accept: \*/\*, Referer: http://www.panicsecurity.com/, Accept-Language: ko-KR, User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.2; WOW64; Trident/7.0)

Buttons at the bottom are '다음' (Next) and '취소' (Cancel).

On the right side, there is a '쿠키정보' (Cookie Information) panel showing cookies like '\_utma=180313893.1875391930.1458869421.1459491420.1459821292.4;' and '\_utmb=180313893.2.10.1459821292;'. Below it are buttons: '데이터보기' (View Data), '진단결과보기' (View Diagnosis Results), '수동진단 결과저장' (Manual Diagnosis Result Storage - highlighted with a blue box), '사후처리 필요 URL' (URLs requiring post-processing), 'TXT에서 URL 추가' (Add URL from TXT), and '스크린샷 저장' (Save Screenshot).

At the bottom right, there is a note: '는 파일이나 디렉토리가 Link에 노출' (is exposed as a file or directory in the Link).

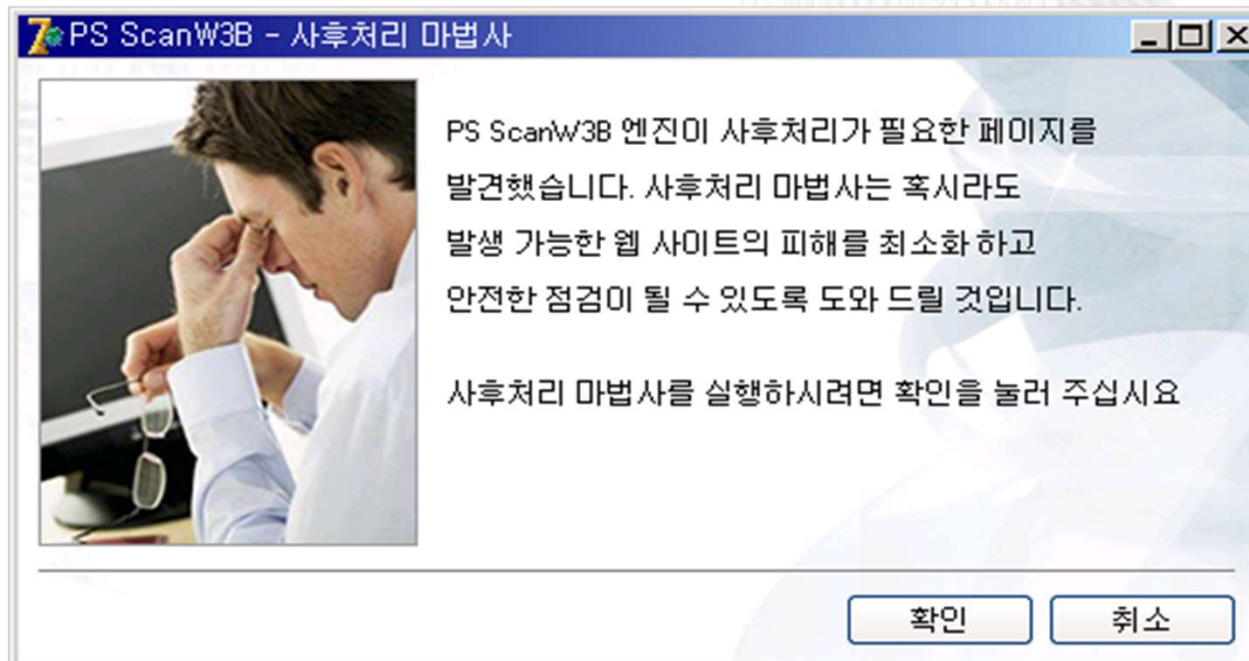


## 2) PS ScanW3B 소개

### 8. 진단 시 제공중인 서비스의 영향

- 사후처리

PS ScanW3B은 진단 시 제공중인 서비스의 영향이 있을만한 URL은 미리 알려주어 사용자가 직접 안전한 URL과 안전하지 않은 URL을 분류하여 점검하는 마법사 기능을 제공합니다.



## 2) PS ScanW3B 소개

### 9. 스캔 소요시간

- 멀티 쓰레드(Multi-Thread) 점검기능

PS ScanW3B은 기본적으로 10개의 멀티 쓰레드를 생성하여 점검하기 때문에 탁월한 점검 시간을 자랑합니다. 또한 각 쓰레드를 사용자가 직접 설정할 수 있으며 Thread 우선순위, Timeout, 재시도 횟수 등을 각각의 단계마다 설정 가능하기 때문에 효율적인 점검을 수행할 수 있습니다.

Thread	점검중인 URL
0	/about_us/greeting.php
1	/customer/images/menu_bar.jpg
2	/customer/images/outline.jpg
3	/customer/images/topline.jpg
4	/customer/images/topmenu_dot.jpg
5	/customer/images/topmenu_contact.jpg
6	/customer/images/main_logo.jpg
7	/customer/images/back.jpg
8	/customer/images/topmenu_home.jpg
9	/consulting/consult.php

#### 연결 정보 설정

동시 연결 요청 수 (Thread) :

보통 10

연결 요청 우선 순위(Thread 우선순위) :

우선 순위 중간

연결 요청시 대기시간(TimeOut, 초) :

보통 10

연결 실패시 재시도 횟수(번) :

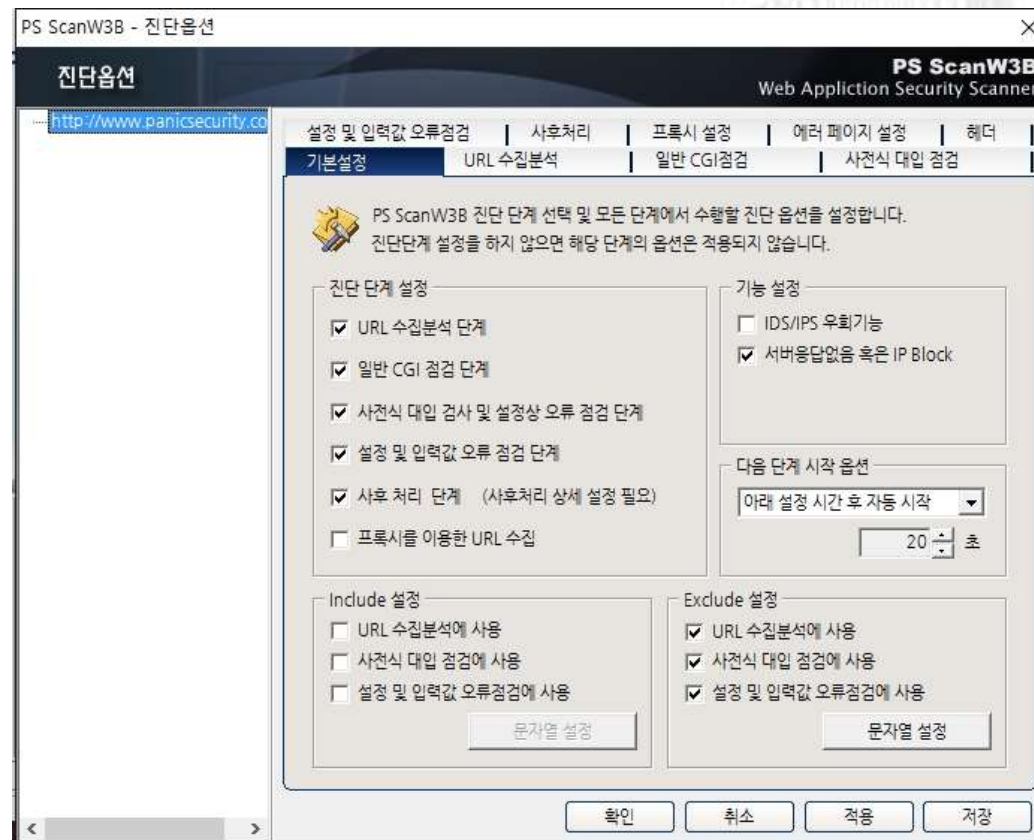
높음 3

## 2) PS ScanW3B 소개

### 10. 점검 옵션 화면

- 다양한 옵션 제공을 통한 점검 옵션 설정

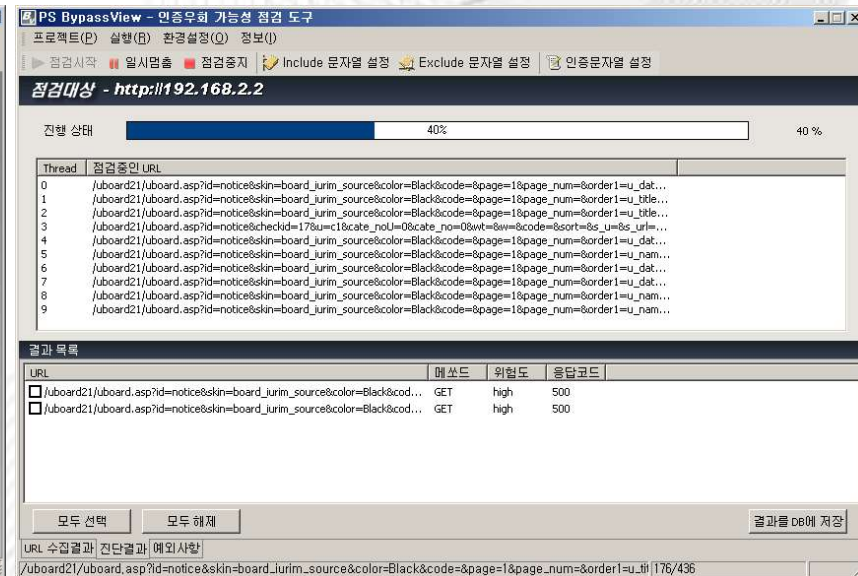
PS ScanW3B은 다양한 형태의 설정을 통하여 사용자가 원하는 점검 룰을 생성할 수 있습니다.



## 2) PS ScanW3B 소개

### 11. 공격 도구 제공

1. File Upload 우회 공격 자동화 툴
2. File Download 취약점을 이용한 소스코드 다운로드 자동화 툴
3. SQL Injection 공격 (MS-SQL, DB열람 및 명령 실행) 자동화 툴
4. 인증우회 : 비인증상태와 인증상태의 페이지 비교
5. 무한대입반복 공격 : 사전 생성 포함
6. Google Dork를 이용한 자동화 공격





### 3) PS ScanW3B의 점검 결과 예 (SQL Injection)

1. 취약점 구분	crawl_sqlcommon : SQL Injection 취약점
2. 위험도	High
3. Original URL	/kor/html/company/company/company05.asp?date1=1998&gubun=43460&page=4
4. 공격 URL	/kor/html/company/company/company05.asp?date1=1998 or&gubun=43460&page=4
5. 공격 인자	date1
6. HTTP 결과 코드	200
7. 설명 및 대책	

#### - 설명 -

SQL injection 은 공격자로 하여금 개발자가 의도하지 않은 SQL 문을 실행시킬 수 있게 하는 공격 기술이다. 사용자가 입력한 값이 직접 SQL 코드로 전달될 때 (저장 프로시저에서 동적 SQL을 사용하거나 혹은 클라이언트 쪽에서 SQL문을 생성시킬 때), SQL injection의 위험이 존재한다. 이 공격방법은 거의 모든 관계 형 데이터베이스 관리시스템(RDBMS, 예를 들면, Oracle, MSSQL, Informix 등등)에 적용된다.

#### - 대책 -

SQL Injection 취약점을 막는 방법으로는 다음과 같은 여러 방법이 있을 수 있다.

1. 웹 서버와 연동되는 DB 의 사용자 권한을 최소한으로 한다.
2. 사용자 입력 값에 대한 Filtering 적용
3. 인자가 숫자를 받아들이는 경우, isnumeric 과 같은 함수를 이용하여 검증하도록 한다.
4. 인자가 문자를 받아들이는 경우, ' 는 ₩'혹은 ''로 변경한다.

## 4) 타 제품과의 차별성



항목	PS ScanW3B (패닉시큐리티)	A (미국 I사 )	차별성 세부 설명	비고
국내 한글 웹 환경 적응 능력 여부	O	X	국산 범용 게시판 (테크노트, 그누보드 등)의 점검이 가능합니다. 또한 페이지나 쿠키에 주민등록번호나 신용카드 번호의 유출 여부를 검 사합니다.	
URL 수집 능력	O	O	웹스캐너의 가장 핵심적인 기능으로, 시작페이지 로부터 모든 페이지를 자동 방문해야 합니다. 이 를 위해 각종 JavaScript 및 Flash 파일의 분석이 필수이며, 국내 여러 대형 사이트에서 탁월한 성 능이 입증 되었습니다.	국민은행, 넥슨, 삼성전자, 삼 성화재, 삼성카드, LG카드 등 주요 사이트에서 BMT로 비교 평가됨.
ActiveX 연동 (공인인증서 지원)	O	Δ	YesSign의 주체인 금융결제원 ISAC실에서 점검도구로 사용하며, 금융결제원의 도움으로 공 인인증서 기반 사이트의 부분 암호화 페이지를 점검할 수 있도록 개발되었습니다.	금융결제원, 금융감독원 자사 제품 사용
사이트 별 대응력 (커스토타이징)	O	X	웹 어플리케이션 개발 방법이 다양하므로, 특이한 형태로 개발된 사이트에도 알맞도록 커스 터마이징 가능합니다.	최다 레퍼런스
결과 분석 도구	O	X	점검결과와 중요도를 판단하기 위한 SQL Injection, File Up/Download 공격용 별도 도구를 제공합니다.	모의해킹 컨설팅 가능
국제 공통 표준 CC 인증	O	X	웹 스캐너 국내 최초로 CC인증 획득. GS 인증 획득.	



## 5) 납품 실적 (1/7)

공급처	공급일자	라이선스	비고	공급처	공급일자	라이선스	비고
 대법원	2004년 6월	Consulting	사용확인서	 대한생명	2005년 6월	Internal	이니텍 Activex 커스토마이징
 금융결제원	2004년 11월	B Internal	금융 ISAC 실 사용	 국군기무사령부	2005년 7월	G1 Internal	C/S 환경 구축
 교원나라자동차보험	2005년 1월	P1 License		 정보통신부	2005년 7월	Internal	2005 정보보호 선진화 사업
 하나로텔레콤	2005년 1월	Internal	사용확인서	 중소기업은행	2005년 7월	Enterprise	C/S 환경 구축
 한국정보보호진흥원	2005년 1월	G1 License	2005 을지훈련 에 사용	 삼성화재	2005년 10월	Enterprise	X인터넷 채용
 신한은행	2005년 2월	P1 License	RMS와 연동	 부산은행	2005년 12월	Internal	뱅크타운 ActiveX 커스토마이징
 KTF	2005년 5월	Internal	신 사업 부문	 CJ시스템즈	2006년 1월	G1 Internal	웹 방화벽 BMT

## 5) 납품 실적 (2/7)

공급처	공급일자	라이선스	비고	공급처	공급일자	라이선스	비고
 금융감독원	2006년 2월	Internal	유지보수	 삼성카드	2006년 9월	Internal	
 국민은행	2006년 2월	Internal	결과보고서 관리 커스토마이징	 삼성전자	2006년 10월	Internal	
 국가보안기술연구소	2006년 3월	Internal		 삼성네트웍스	2006년 10월	Internal	점검의뢰 시스템 커스토마이징
 넥슨	2006년 4월	Internal	뱅크타운 ActiveX 커스토마이징	 한국전력공사	2006년 11월	Internal	한국전력 공사
 마사회	2006년 5월	Internal	웹 방화벽 BMT	 GS홈쇼핑	2006년 11월	Internal Plus	인터넷 쇼핑몰
 KT	2006년 6월	Internal	결과보고서 관리 커스토마이징	 서울대학교	2006년 12월	Enterprise	교육기관
 다음	2006년 7월	Internal	유지보수	국가 A 기관	2006년 12월	Internal	국가기관

## 5) 납품 실적 (3/7)

공급처	공급일자	라이선스	비고	공급처	공급일자	라이선스	비고
 <b>LG 카드</b> LG카드	2006년 12월	Internal	제2 금융권	 <b>대한주택공사</b> 대한주택공사	2008년 2월	Enterprise	대한주택공사
 <b>경기도청</b> 경기도청	2007년 6월	Internal	경기도청	 <b>CJ 인터넷</b> CJ인터넷	2008년 4월	Internal	CJ인터넷 (온라인 게임회사)
 <b>KISTI 한국과학기술정보연구원</b> 한국과학기술정보연구원	2007년 7월	Internal	한국과학기술 정보연구원	 <b>양천구청</b> 양천구청	2008년 4월	P3	서울시 양천구청
 <b>산림청</b> 산림청	2007년 9월	P10	산림청	 <b>영동군</b> 영동군청	2008년 5월	P3	충청북도 영동군청
 <b>의성군청</b> 의성군청	2007년 10월	P3	의성군청	 <b>KERIS</b> 한국교육학술정보원	2008년 5월	P10	한국교육 학술 정보원
 <b>구미시립도서관</b> 구미시립도서관	2007년 11월	P3	시립도서관	 <b>한국거래소</b> 증권선물거래소	2008년 6월	Internal	증권 선물거래소
 <b>서울특별시</b> 서울시청	2007년 12월	Internal	서울시청	 <b>국방과학연구소</b> 국방과학연구소	2008년 6월	P3	국방과학 연구소

## 5) 납품 실적 (4/7)

공급처	공급일자	라이선스	비고	공급처	공급일자	라이선스	비고
 아시아나항공	2008년 6월	Internal	아시아나 항공	 예천군청	2008년 11월	P3	경상북도 예천군
 식품의약품 안전청	2008년 7월	P2	식품의약품 안전청	 예금보험공사	2008년 12월	Internal	예금보험 공사
 강남구청	2008년 7월	P3	서울시 강남구청	 삼성SDS	2008년 12월	P20	삼성SDS
 농촌진흥청	2008년 8월	P10	농촌진흥청	 항공우주연구원	2008년 12월	P3	항공우주 연구원
 현대제철	2008년 8월	Internal	현대제철	 대구시청	2008년 12월	P10	대구광역시청
 영천시	2008년 9월	P3	경상북도 영천시	 한국정보보호진흥원	2008년 12월	P3	추가도입
 삼성테크윈	2008년 10월	Internal	삼성테크윈	 은평구	2009년 1월	P3	서울시 은평구청



## 5) 납품 실적 (5/7)

공급처	공급일자	라이선스	비고	공급처	공급일자	라이선스	비고
 관악구청	2009년 2월	P3	서울시 관악구청	 케이티아이씨씨	2009년 8월	Internal	KT icc
 시흥시	2009년 2월	P10	경기도 시흥시청	 대법원	2009년 10월	Internal	대법원
 한국정보통신기술협회	2009년 3월	P3	한국정보통신 기술협회	 보건복지부	2009년 12월	P3	보건복지부
 울산 교육청	2009년 3월	P10	울산 교육청	 경주시청	2010년 02월	P3	경주시청
 안산시	2009년 4월	P10	경기도 안산시청	 천안시청	2010년 03월	P1	천안시청
 삼성중공업	2009년 6월	Internal	삼성중공업	 삼성전자	2010년 06월	CS Enterprise	
 강원랜드 알펜시아	2009년 7월	P1	강원랜드	 수원시청	2010년 06월	P1	수원시청



## 5) 납품 실적 (6/7)

공급처	공급일자	라이선스	비고	공급처	공급일자	라이선스	비고
 한국직업능력개발원	2010년 07월	P10	한국직업 능력개발원	 Beautiful Gyeongju	2010년 03월	P10	경주시청
 도로교통공단 ROAD TRAFFIC AUTHORITY	2010년 08월	P3		 FAST CHEONAN 희망이 넘치는 미래도시	2010년 03월	P3	천안시청
 미래를 개척하는 현대중공업	2010년 08월	Internal		 병무청	2010년 08월	P3	
 SAMSUNG 삼성SDS	2010년 09월	Internal		 한국교육개발원 KOREAN EDUCATIONAL DEVELOPMENT INSTITUTE	2011년 02월	P30	
 Guro-Gu 구로구	2011년 03월	P10	구로구청	 SAMSUNG 삼성SDS	2011년 04월	Internal	추가 구매
 KiSTi www.kisti.re.kr	2011년 05월	한국과학기술정보연구원		 강동구	2011년 11월	P20	서울시 강동구청
 인천광역시교육청 INCHON METROPOLITAN CITY OFFICE OF EDUCATION	2011년 11월	Internal		 KNU 경북대학교 KYUNGPOOK NATIONAL UNIVERSITY	2011년 11월	P10	

## 5) 납품 실적 (7/7)

공급처	공급일자	라이선스	비고	공급처	공급일자	라이선스	비고
 INFRAWARE	2011년 12월	P3		 KDB산업은행	2011년 12월	Internal	
 한국증권금융 Korea Securities Finance Corp.	2012년 1월	Internal		 나이스정보통신(주) NICE	2012년 2월	P3	
 SAMSUNG	2012년 7월	삼성전자 MSC사업부		 특허청	2012년 11월	Internal	
 ex 한국도로공사	2012년 11월	Internal		 Hyundai Capital	2013년 1월	Internal	
 SAMSUNG 삼성화재	2013년 3월	Internal		 posco 포스코건설	2013년 7월	Internal	
 5678 행복미소 서울도시철도	2013년 8월	Internal		 KTIS www.ictis.kr 한국통신인 타겟기술(주)	2014년 2월	Internal	
 빛과 물이 하나되는 상생의 생명도시 광주·전남공동혁신도시 빛가람	2014년 3월	P3		 NCSoft	2015년 03월	Internal CS	

**PANIC X SECURITY**  
www.panicsecurity.com

[illegible]

## 6) 평가 / 인증

CC인증, 보안적합성, GS인증

적합성 검증필 정보  
Validated Information S

보안인증과 국가정보통신망에 대한  
기본지침」(06.1.1)에 의거하여 “  
시행하고 있습니다.

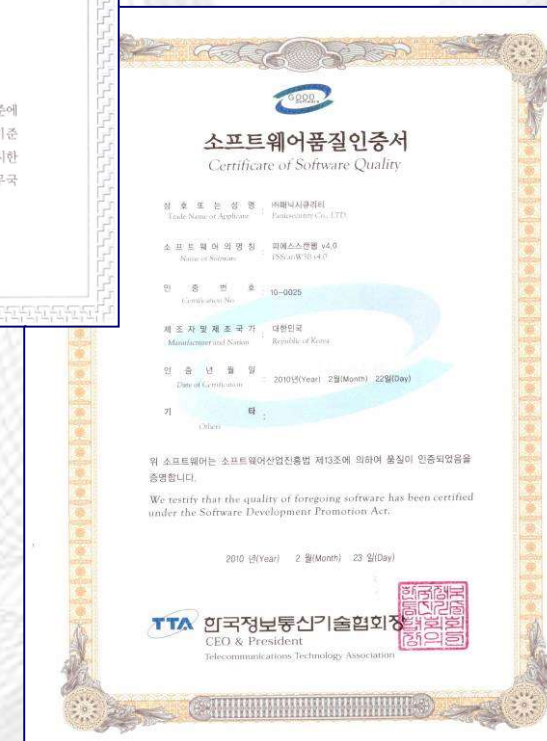
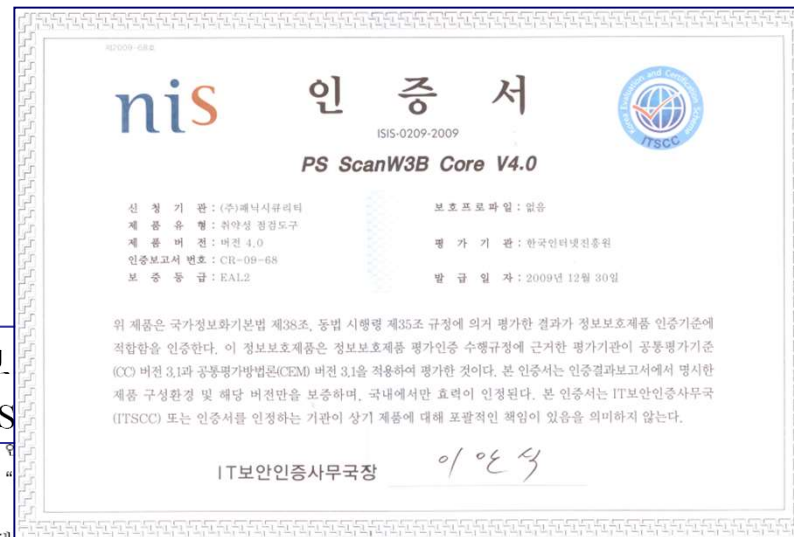
이 목록에 등재된 정보보호시스템은 적합성 검증 결과, 적합기관 조업에 적합  
하다고 판정된 제품입니다.

정보보호 기반 제품군 (ISIS : Information Security Infrastructure System)

취약점 분석 도구

번호	제품명	회사명	인증등급	인증일자	판정일자
9	PS Scan W3B	㈜패닉시큐리티	-	-	2006.09.01

**nis** 국가정보원  
"Power of Intelligence, Power of Korea"






## 7) 왜 패닉시큐리티 인가?

구분	왜 패닉시큐리티의 PS ScanW3B인가?	비고
인증서 기반 웹 점검이 가능한 유일한 제품	국내 인터넷 환경의 암호화는 PKI 환경을 채택하여 공인/사설 인증서를 사용하는 것이 보편적입니다. 본 제품은 국내 보안업체에서 개발된 여러 PKI 제품과 연동한 개발이 이루어져, 웹 HTML 페이지의 부분 암호화 환경을 점검합니다. 이러한 기능은 PS ScanW3B이 유일합니다.	부분 암호화된 HTML 페이지 점검이 가능한 유일한 제품
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	
엔진 레벨에서 고객 요구사항 반영이 가능 (커스터마이징)	100% 국내 기술에 의해 개발되어, 핵심 엔진 단위의 고객 요구 내역에 대한 반영이 가능합니다. 또한 타 ESM, RMS 등과 같은 통합보안 시스템과의 연동이 가능하도록 커스터마이징의 제공이 가능합니다.	삼성그룹 보안표준 커스터마이징
국내 최고의 모의해킹 전문가 집단	<ul style="list-style-type: none"> <li>• 08년 5월 세계 최대의 국제해킹대회인 데프콘 (Defcon) 예선에서 아시아 1위로 본선 진출에 성공</li> <li>• 08년 8월 미국 라스베이거스에서 열린 본선 대회에서 전체 4위 입상으로 국내 역대 최고 성적 획득</li> </ul>	'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.



## <별첨 1> 벤처기업 확인서



제 051134233-1-00703호

### 벤처기업 확인서

업 체 명 : (주)패닉시큐리티  
대 표 자 : 신 용 제 (辛裕宰)  
소 재 지 : 서울시 구로구 구로6동 98-16  
(현대오피스텔 807호)  
확인유형 : 신기술기업  
평가기관 : 한국과학기술원  
유효기간 : 2005. 4. 29 ~ 2007. 4. 28

위 업체는 벤처기업육성에관한특별조치법 제 25조의 규정에 의하여 벤처기업임을 확인합니다.

2005년 4월 29일  
서울지방중소기업청장

(주)패닉시큐리티의 기술력과 사업성을  
한국과학기술원(KAIST, Korea Advanced Institute  
Of Science and Technology)으로부터  
위탁 평가 받아 신기술기업 유형으로 벤처기업 지정  
(2005년 4월 29일)

벤처기업확인서 / 서울지방중소기업청장

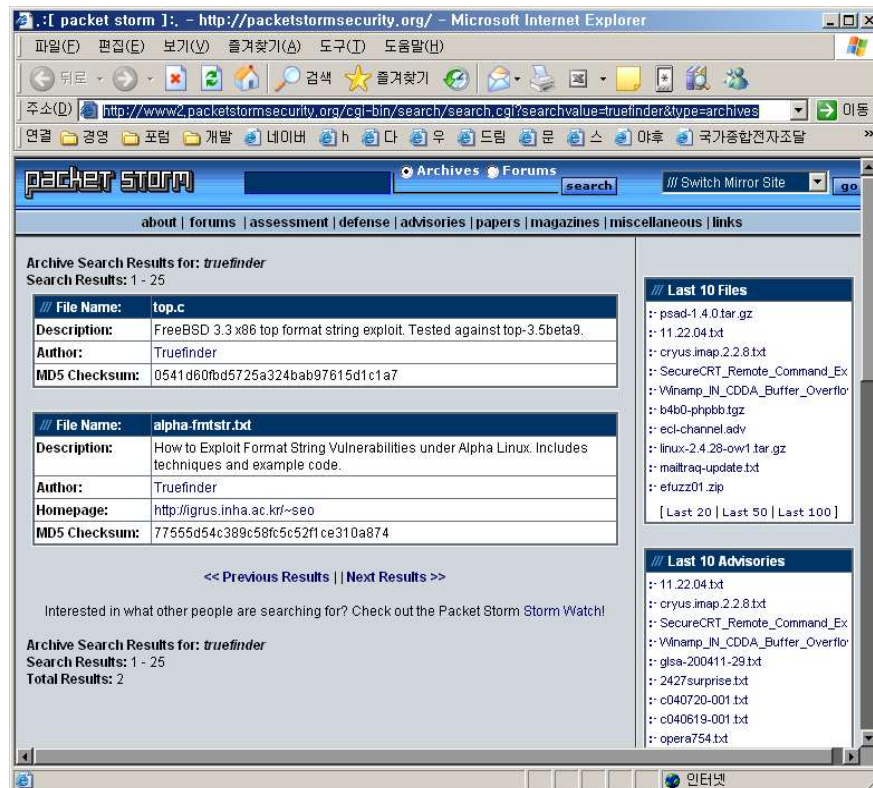
## 〈별첨 2-1〉 기술 우수성 증빙 자료



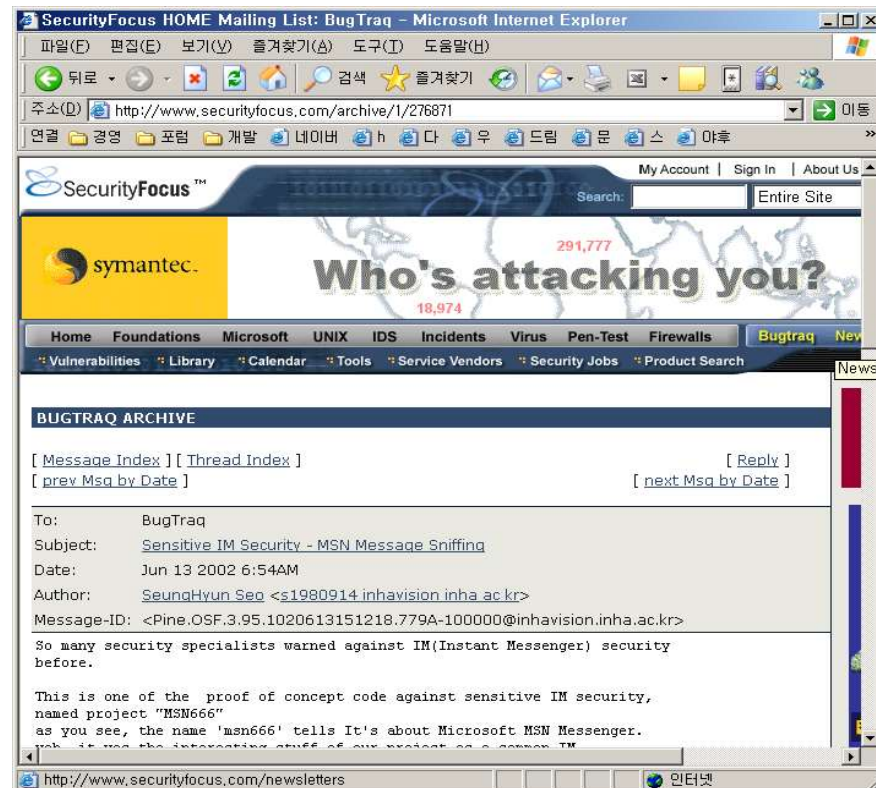
KAIST / ISC 주최 국제해킹대회 우승

## <별첨 2-2> 기술 우수성 증빙 자료

세계 취약점 포털에 신규 취약점 발표



< Packet Storm에 신규 취약점 발표 >



< SecurityFocus에 신규 공격방식 공개 >

# 감사합니다

(주)패닉시큐리티는 고객의 만족과 보안 향상을 위해  
최선의 노력을 다 하겠습니다.  
감사합니다.

<http://www.panicsecurity.com>