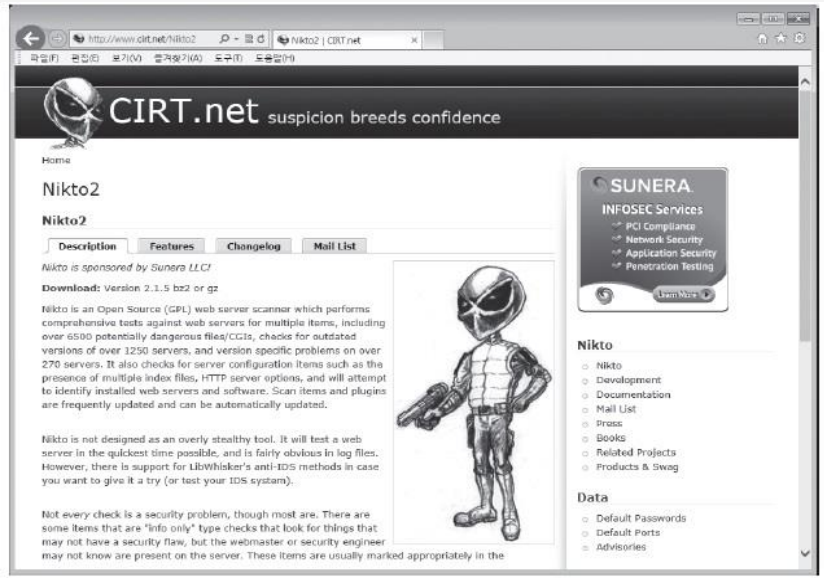
1 DB 기반 웹 스캐너

1 Nikto

- 2001년 크리스 설로가 웹 서버와 애플리케이션에 있는 취약점 데이터베이스를 만든 취약점 스캐너(wikto)
- 2000년대 초반에는 꽤 인기를 끌었지만 수많은 웹 취약점 스캐너가 나오면서 인기가 조금 시들해짐
- 공식 홈페이지 : http://www.cirt.net

1 Nikto

[Nikto 웹 사이트]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

1 Nikto

- Nikto Web Scanner is a Web server scanner that tests Web servers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received.

- The Nikto code itself is Open Source (GPL), however the data files it uses to drive the program are not.

1 Nikto

- Chris Sullo, the CFO of Open Security Foundation has written this scanner for vulnerability assessment.

1 Nikto

- Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

1 Nikto

- There are some variations of Nikto, one of which is MacNikto. MacNikto is an AppleScript GUI shell script wrapper built in Apple's Xcode and Interface Builder, released under the terms of the GPL. It provides easy access to a subset of the features available in the Open Source, command-line driven Nikto web security scanner, installed along with the MacNikto application.(wikto)

2 N-Stealth

- 웹 취약점 데이터베이스를 기반으로 하는 웹 취약점 스캐너
- 지금은 N-Stalker라는 이름으로 업데이트되고 있음
- N-Stalker Free 버전 다운로드 : http://www.nstalker.com/products/editions/free

2 N-Stealth

[N-Stealth 취약점 스캐너]

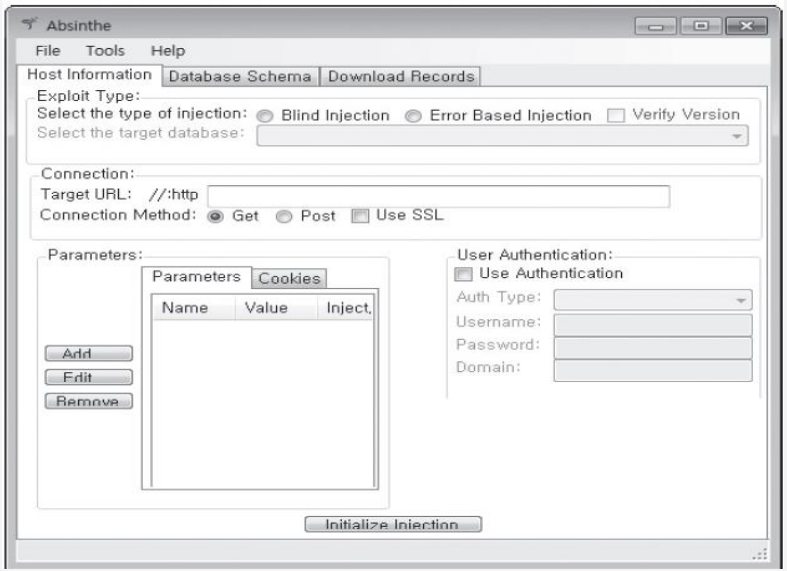
※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 특정 웹 취약점 스캐너

1 Absinthe

- 0x90이라는 유명한 해커 그룹에서 활동하던 너미시와 제론이 만든 SQL 인젝션 취약점 툴
- 소스포지사이트 (http://sourceforge.net/projects/absinthe)에서 다운로드

[Absinthe 실행 화면]

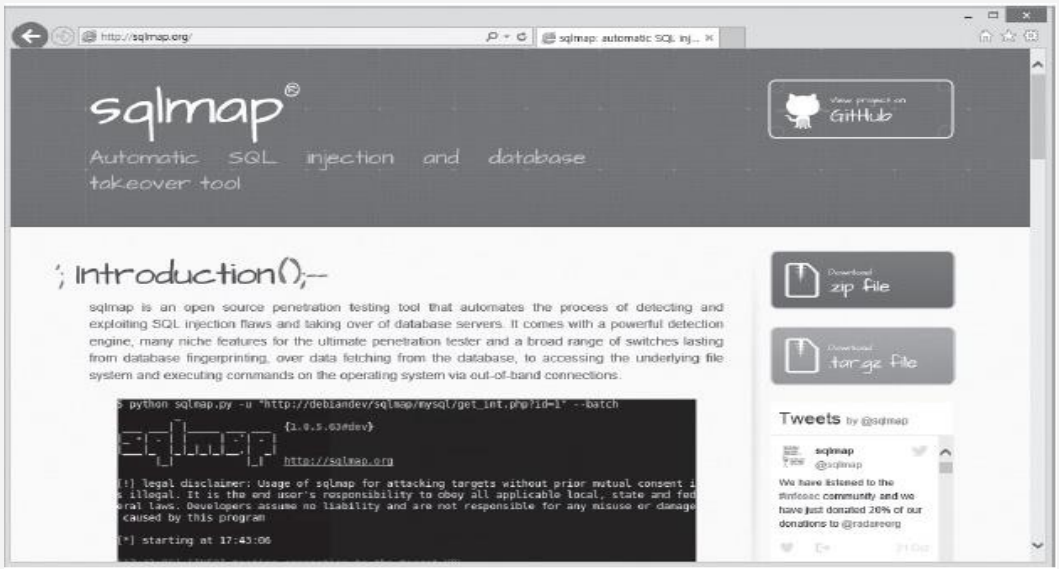


※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 Sqlmap

- 오픈 소스 툴로 최근 SQL 인젝션 자동화 공격에 많이 사용되고 있음

[Sqlmap 실행 화면]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 Sqlmap

- Sqlmap is an open source software that is used to detect and exploit database vulnerabilities and provides options for injecting malicious codes into them.
- It is a penetration testing tool that automates the process of detecting and exploiting SQL injection flaws providing its user interface in the terminal.

2 Sqlmap

- The software is run at the command line and is available to download for different operating systems: Linux distributions, Windows and Mac OS operating systems.

- In addition to mapping and detecting vulnerabilities, the software enables access to the database, editing and deleting data, and viewing data in tables such as users, passwords, backups, phone numbers, e-mail addresses, credit cards and other confidential and sensitive information.

2 Sqlmap

- Sqlmap has full support for multiple DBMSs, including MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird and SAP MaxDB
- And full support for all injection techniques: Boolean, Error, Stuck, Time, Union

2 Sqlmap

- The standard use of the software in the Unix environment will be as follows
  - sqlmap -u "http://172.16.0.0/files/file.php?id=1"
- Additional values can be combined:
  - --dbs: will display the databases.
  - --tables: will display tables in the database
  - --columns: Will display columns in the database
  - --dump: Will dump DBMS database entries

2 Sqlmap

- The help file is prompted by command
  - sqlmap -h

3 Acunetix

- 해커들이 사용하는 웹 해킹 방법으로
  웹 애플리케이션의 취약점을 찾는 휴리스틱
  웹 취약점 스캐너(휴리스틱)

- 2005년 6월에 처음 발표된 이후 지금까지
  지속적으로 발전하여 현재 가장 많이 사용되는
  상용 웹 취약점 스캐너 중 하나

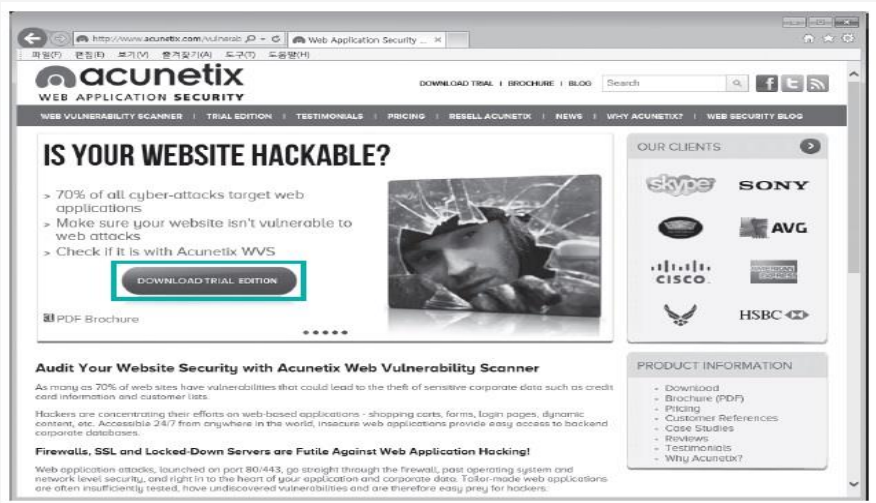
4 Acunetix 데모버전 사용하기

1. 데모버전 다운로드
   - Acunetix 홈페이지(http://www.acunetix.com/vulnerability-scanner)에 접속
   - <DOWNLOAD TRIAL EDITION>을 클릭해 정보를 입력
   - 이메일로 데모버전을 내려 받을 수 있는 경로를 알려주므로 정확히 입력해야 함

4 Acunetix 데모버전 사용하기

1 데모버전 다운로드

[Acunetix 홈페이지]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 Acunetix 데모버전 사용하기

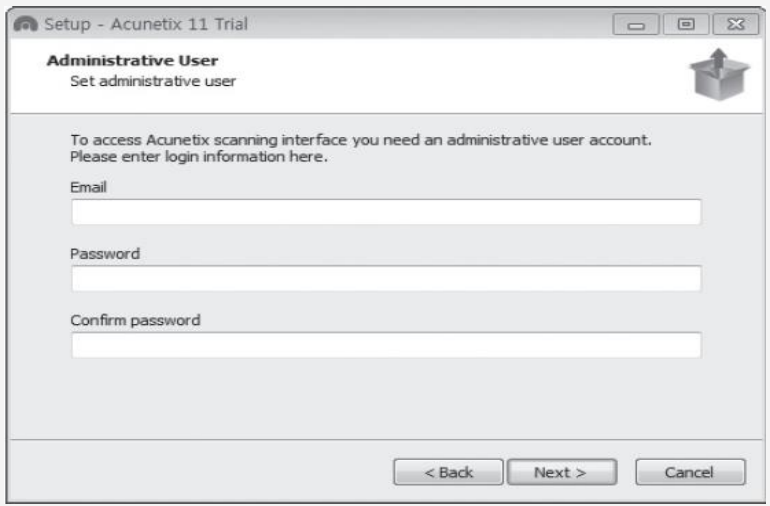
2 Acunetix 설치

- 설치 도중 관리용 계정을 요청하면 평소 사용하는 것 대신 Acunetix 관리용 계정과 패스워드를 새롭게 입력
- 설치가 끝나면 로그인 요청 화면에 설치할 때 입력한 관리용 계정 정보 입력

4 Acunetix 데모버전 사용하기

2 Acunetix 설치

[관리용 계정 정보 입력]



[관리용 계정으로 로그인 화면]

※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 Acunetix 데모버전 사용하기

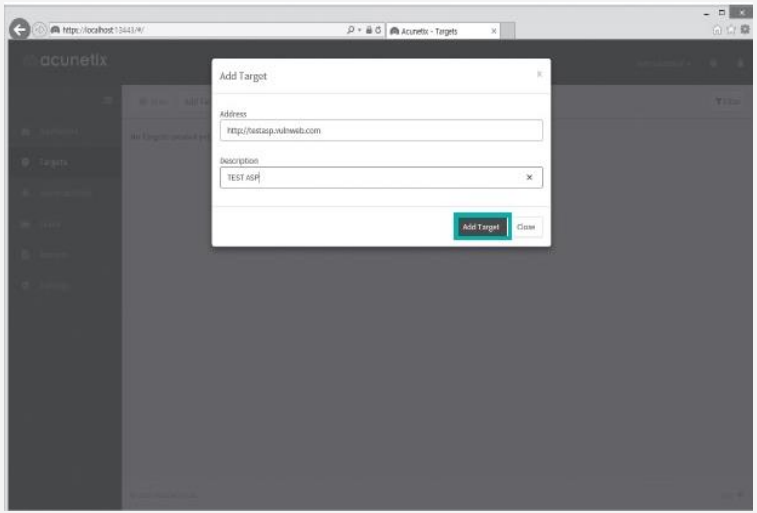
2 Acunetix 설치

- 〈Create New Target〉을 클릭하면 스캔 대상 정보를 입력할 창이 나타남
- Address에 'http://testasp.vulnweb.com', Description에 본인이 원하는 내용을 입력한 후 〈Add Target〉을 클릭

4 Acunetix 데모버전 사용하기

2 Acunetix 설치

[스캔 대상의 정보 입력]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 Acunetix 데모버전 사용하기

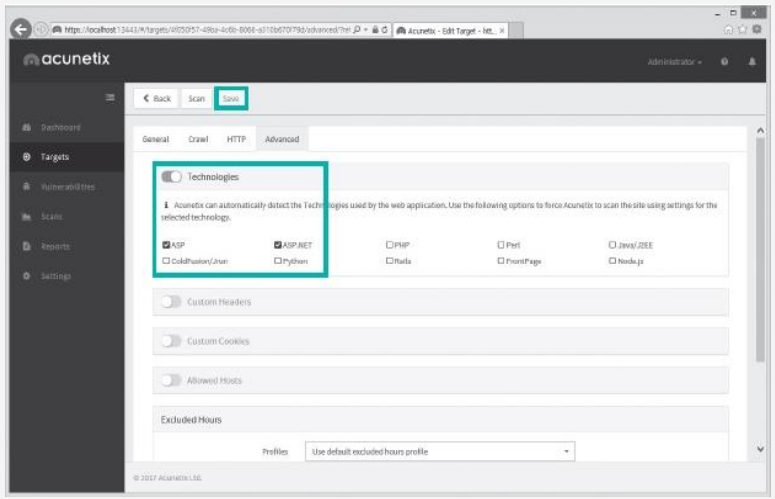
2 Acunetix 설치

- 화면 상단의 [Scan] 메뉴를 누르면 기본적인 스캔 설정 가능
- Technologies를 활성화한 다음에 'ASP'와 'ASP.NET'을 선택하고 화면 상단의 [Save]를 누름

4 Acunetix 데모버전 사용하기

2 Acunetix 설치

[옵션 설정]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 Acunetix 데모버전 사용하기

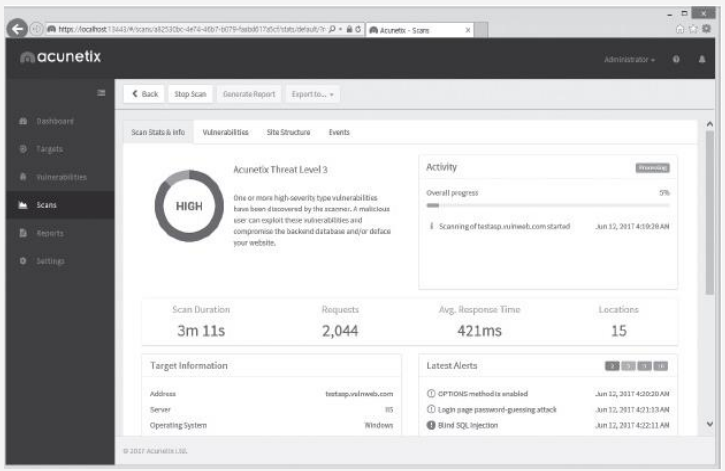
3 Acunetix 실행 결과 분석

- 저장한 후에 [Scan]을 누르면 대상 사이트에 대한 스캔 실행
- 이때 [Vulnerabilities] 메뉴를 누르면 중간 스캔 결과를 볼 수 있음

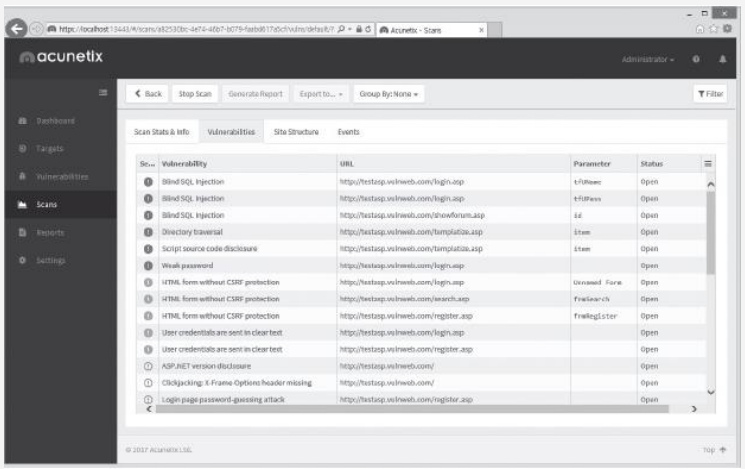
4 Acunetix 데모버전 사용하기

3 Acunetix 실행 결과 분석

[스캔 실행 화면]



[스캔 결과로 발견한 취약점 내용]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 Acunetix 데모버전 사용하기

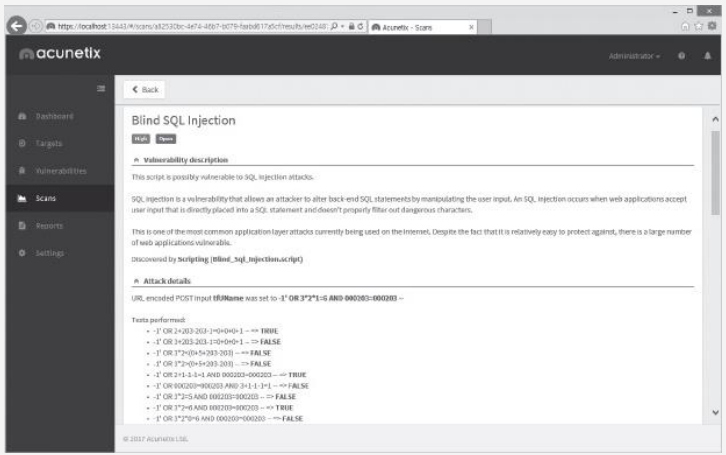
3 Acunetix 실행 결과 분석

- 특정 취약점을 선택하면 해당 취약점의 세부 내용 확인 가능
- 스캔이 완료된 후 화면 왼쪽의 [Reports] 메뉴를 선택하면 다양한 형태의 보고서를 생성

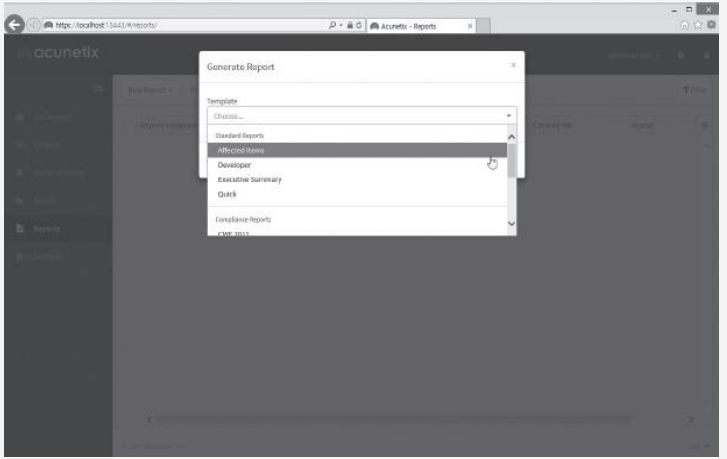
4 Acunetix 데모버전 사용하기

3 Acunetix 실행 결과 분석

[발견한 취약점의 세부 내용]



[다양한 형태의 스캔 결과 보고서]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 Acunetix 데모버전 사용하기

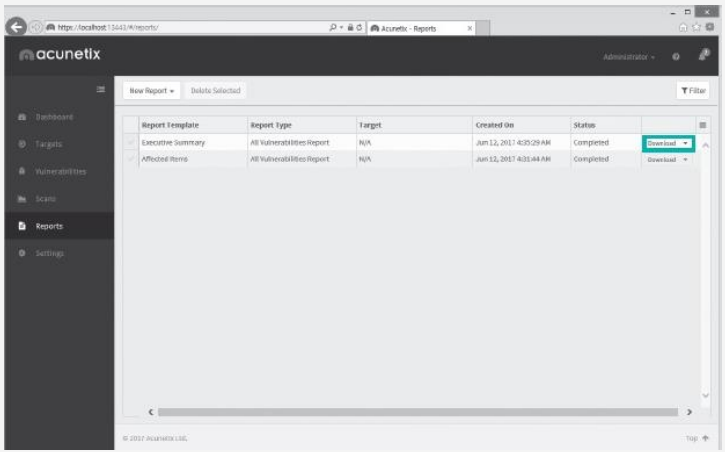
3 Acunetix 실행 결과 분석

- 생성된 보고서 목록의 가장 오른쪽에 있는 〈Download〉를 클릭하면 PDF 형태의 세부 보고서 내용을 볼 수 있음

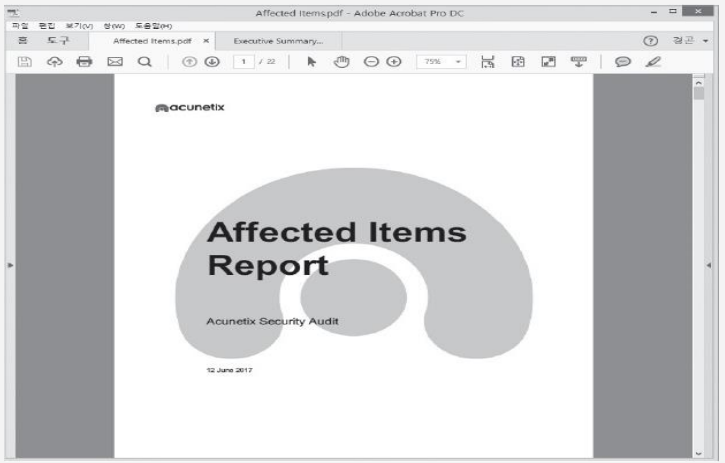
4 Acunetix 데모버전 사용하기

3 Acunetix 실행 결과 분석

[다양한 형태로 만든 보고서 목록]



[PDF 형태의 세부 보고서]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 AppScan

1 AppScan

- 워치파이어에서 만든 웹 애플리케이션 취약점 스캐너
- 2007년에 IBM이 워치파이어를 인수한 후로는 IBM에서 관리
- IBM 홈페이지 (http://www.ibm.com/developerworks/downloads/r/appscan)에서 데모버전 내려 받을 수 있음