



보안공부닷컴
<http://www.boangongbu.com>

Acunetix Web Vulnerability Scanner 맞보기

작성날짜: 2010년 5월 21일 금요일

메일주소: boangongbu@naver.com

【실전으로 배워보는 인터넷보안】

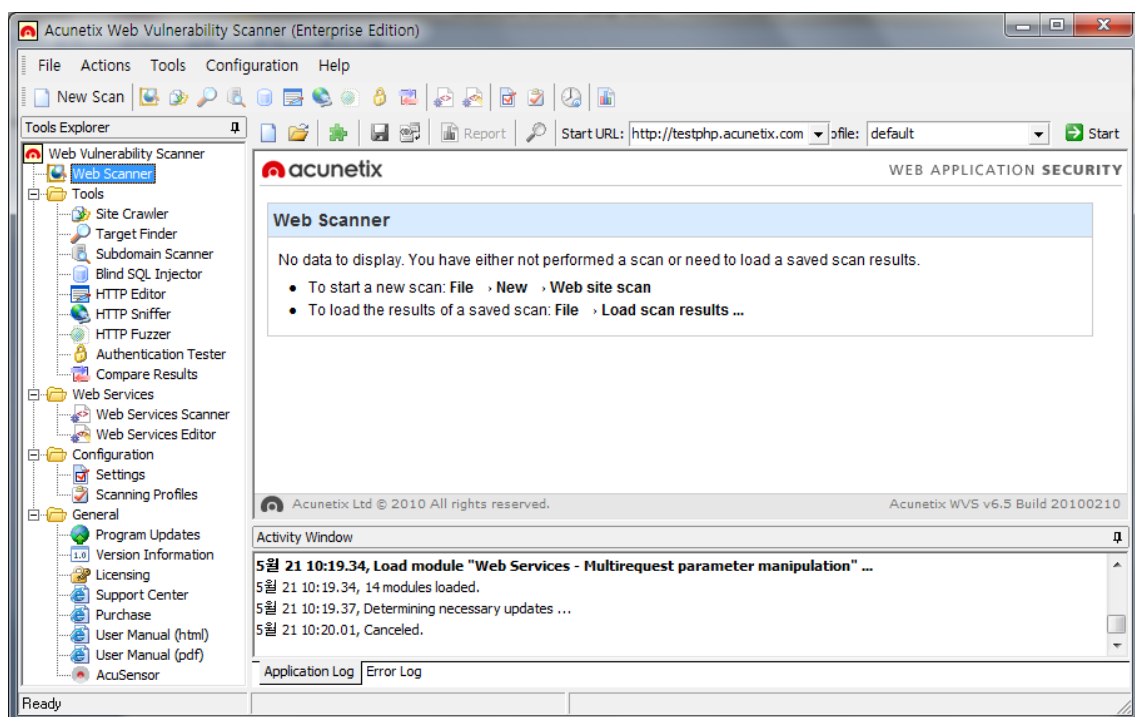
Acunetix Web Vulnerability Scanner 모르시는분들이 있을지 모르겠지만. 보안에 관심이있거나 보안업계에 몸을 담고있다면 모르시는분이 없으리라고 믿구있구요. 해커의 컴퓨터라면 거의 다 깔려있을법한 아큐네틱스. 그럼 아래에 간략한 사용법을 소개해드리도록 하겠습니다.

다운로드: http://rapidshare.com/files/356407862/2010_02_10_01_webvulnscan65.exe

크랙파일: <http://rapidshare.com/files/356414045/web.vulnerability.scanner.6.5.patch.rar>

위 링크에서 설치파일과 크랙파일을 받으시구요. 먼저 프로그램을 설치하고 크랙파일을 설치폴더에 위치한다음 patch 를 클릭하면 크랙은 완료.

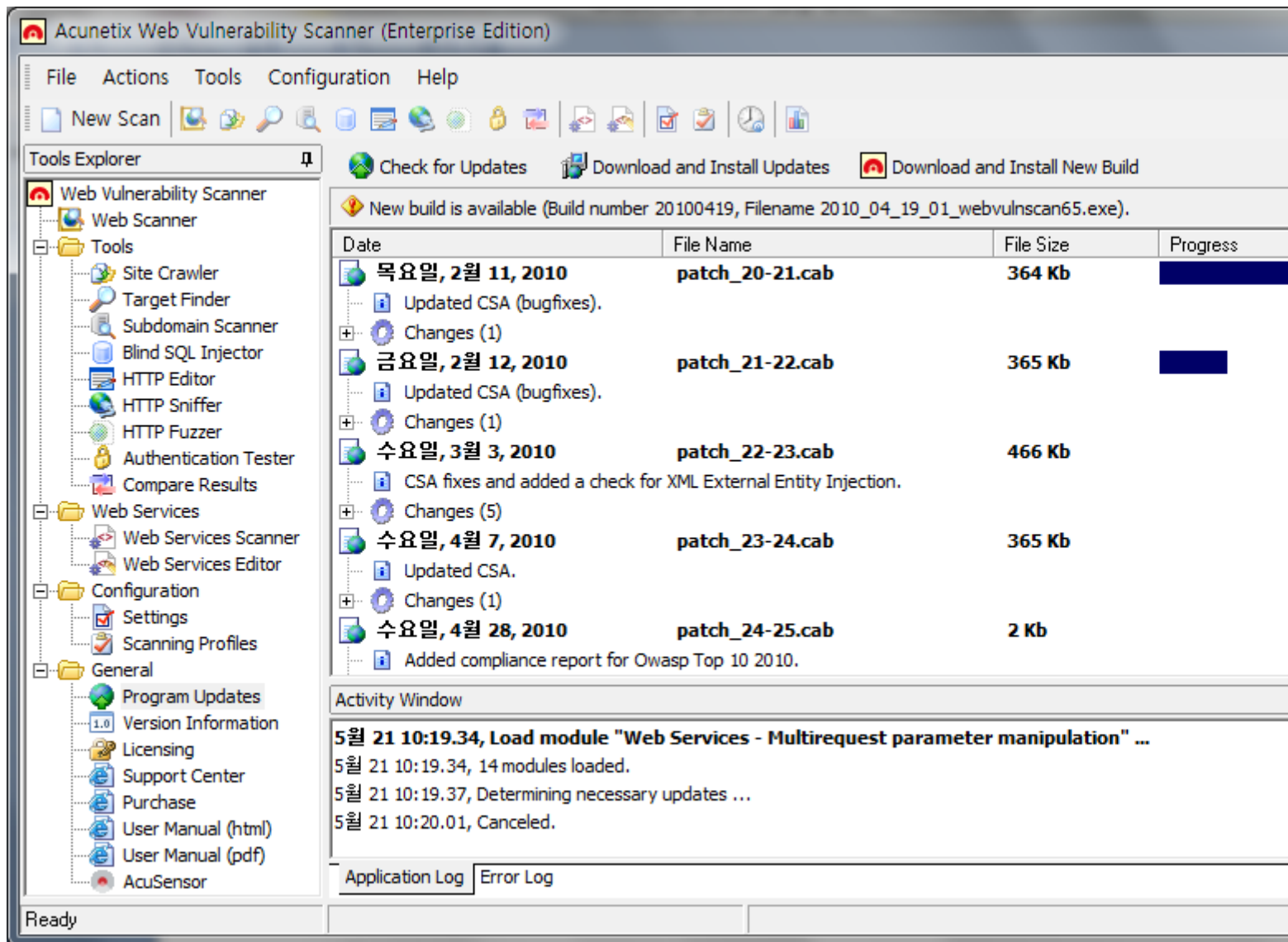
프로그램을 실행하면 아래와 같은 프로그램창을 확인가능.



제일 처음 해야될건 프로그램 업그레이드.

메뉴바에서 "Help" -> "Check for updates" 를 실행하여 업데이트파일 존재여부를 확인.

만약 업데이트 가능한 파일들이 존재한다면 아래처럼 파일리스트가 보여질꺼구요.

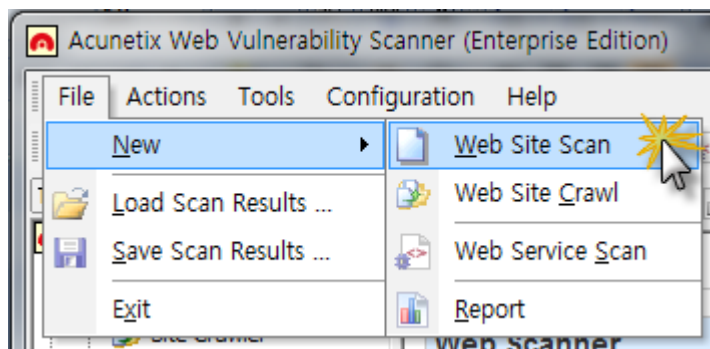


“Download and Install Updates” 를 실행하여 이들을 설치.

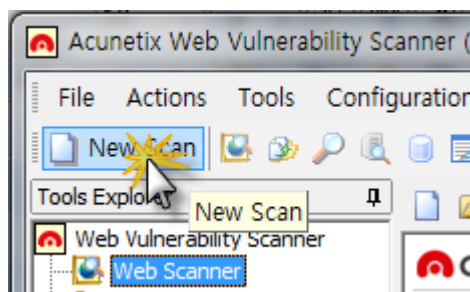
옆메뉴에서 “Download and Install New Build” 버튼이 활성화 되었을시는 새로운 프로그램이 발표되었다는 얘기구요. 우선 새로운 버전의 크랙파일이 공개되었는지를 확인하고 업그레이드하는 것을 추천. 만약 그렇지 않다면 업그레이드후 프로그램이 실행안되는 불상사가 발생. (아큐네틱스는 프로그램 업그레이드가 빈번하다.)

그럼 타겟을 하나 잡고 스캔을 해보도록 하겠습니다.

【실전으로 배워보는 인터넷보안】

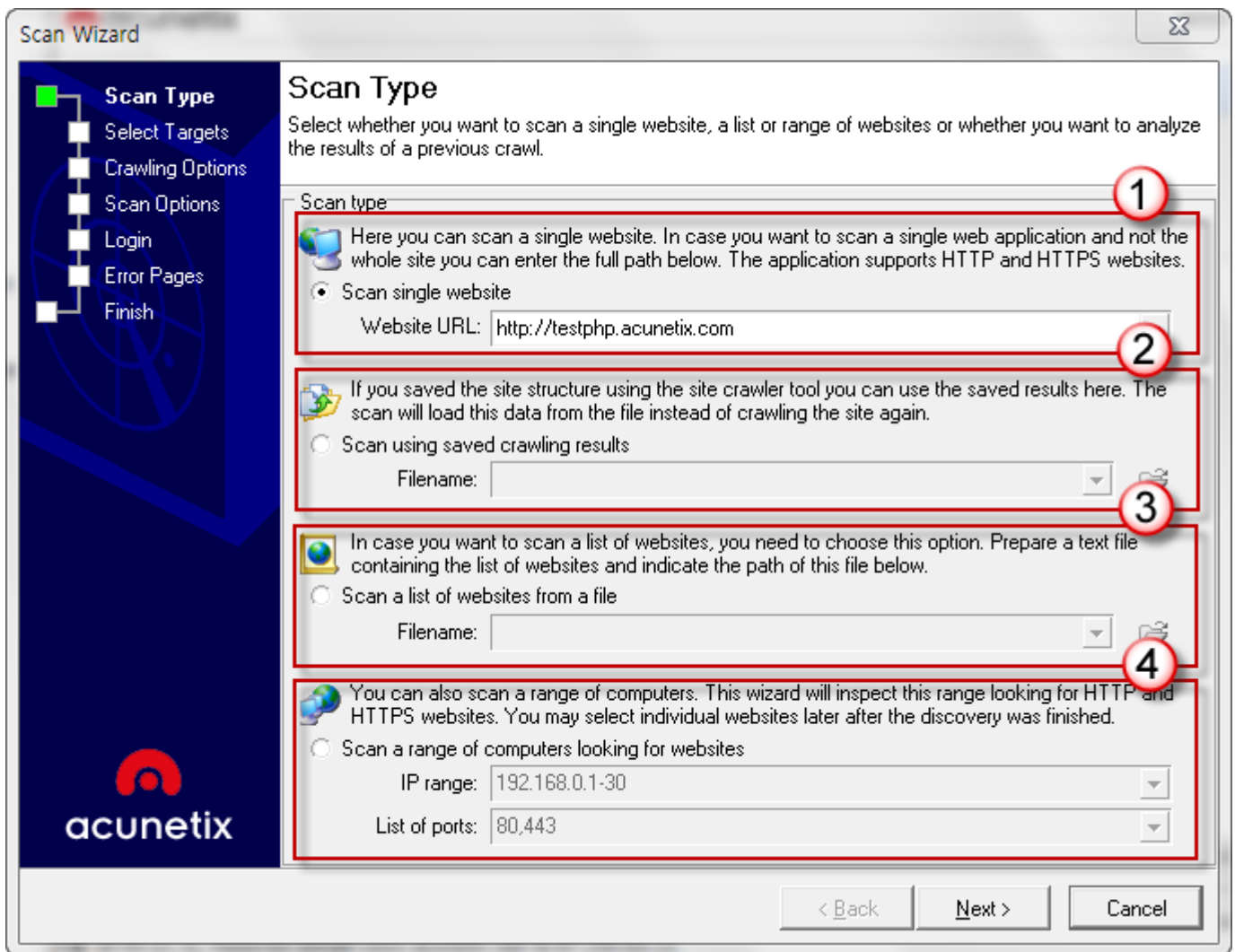


메뉴바에서 “File -> New -> Web Site Scan” 을 클릭 혹은.



퀵바에서 “New Scan”을 클릭

그럼 아래와 같은 창이 뜰건데요.



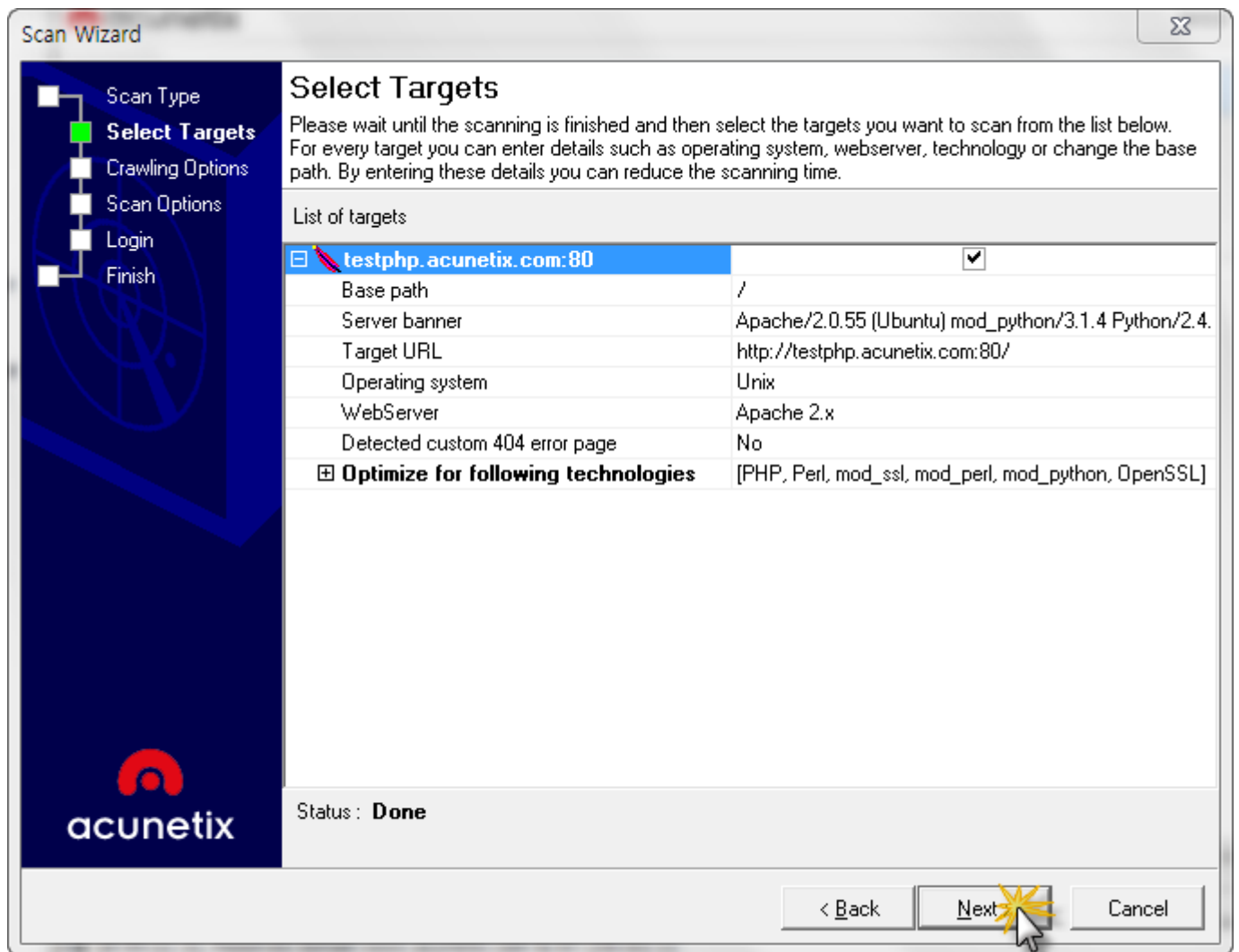
1번: 특정타겟 웹사이트의 도메인을 입력.

2번: “Site Crawler” 프로그램으로 스캔가능한 웹사이트주소를 수집하였고 또 이를 저장하였을시 해당파일을 선택하여 다수스캔이 가능. (Site Crawler툴은 뒤에서 설명드릴꺼구요)

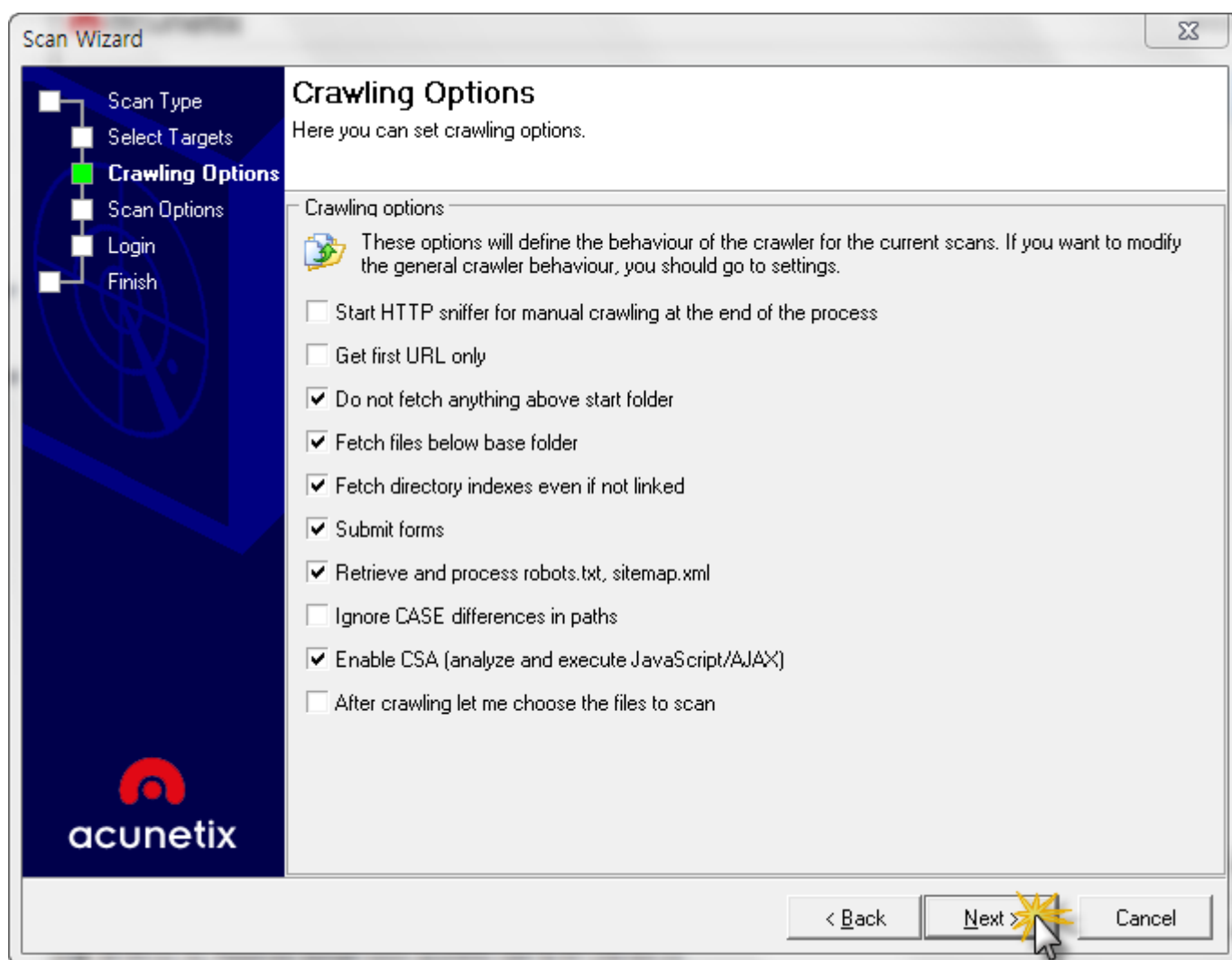
3번: 텍스트파일에 저장된 웹사이트들을 스캔하려고 할시. 이를 선택.

4번: 직접 특정 아이피대역을 입력하여 스캔을 하려고 할시 4번을 선택.

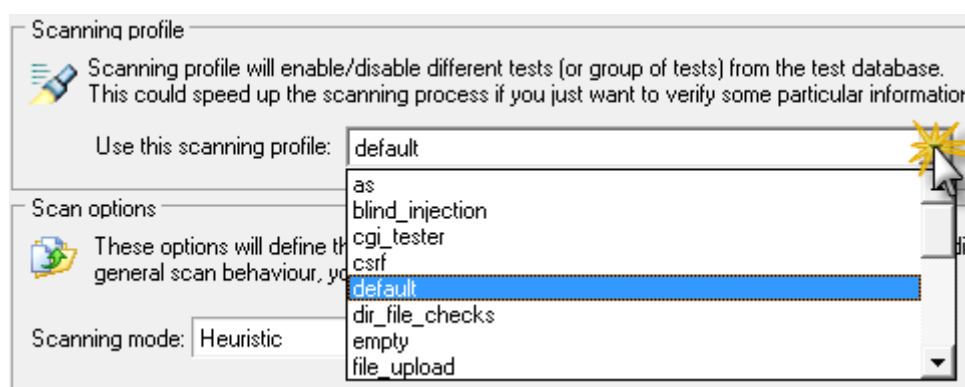
선택완료후 “Next”를 클릭하여 다음페이지로 이동함.



이 페이지에서는 타겟 웹사이트의 간략한 정보를 보여줌. 상관말고 "Next"

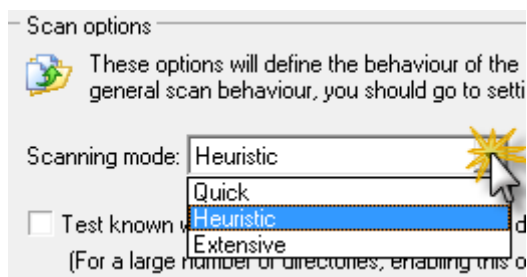


스캔시 각종 옵션들인데 그냥 상관없이 "Next"

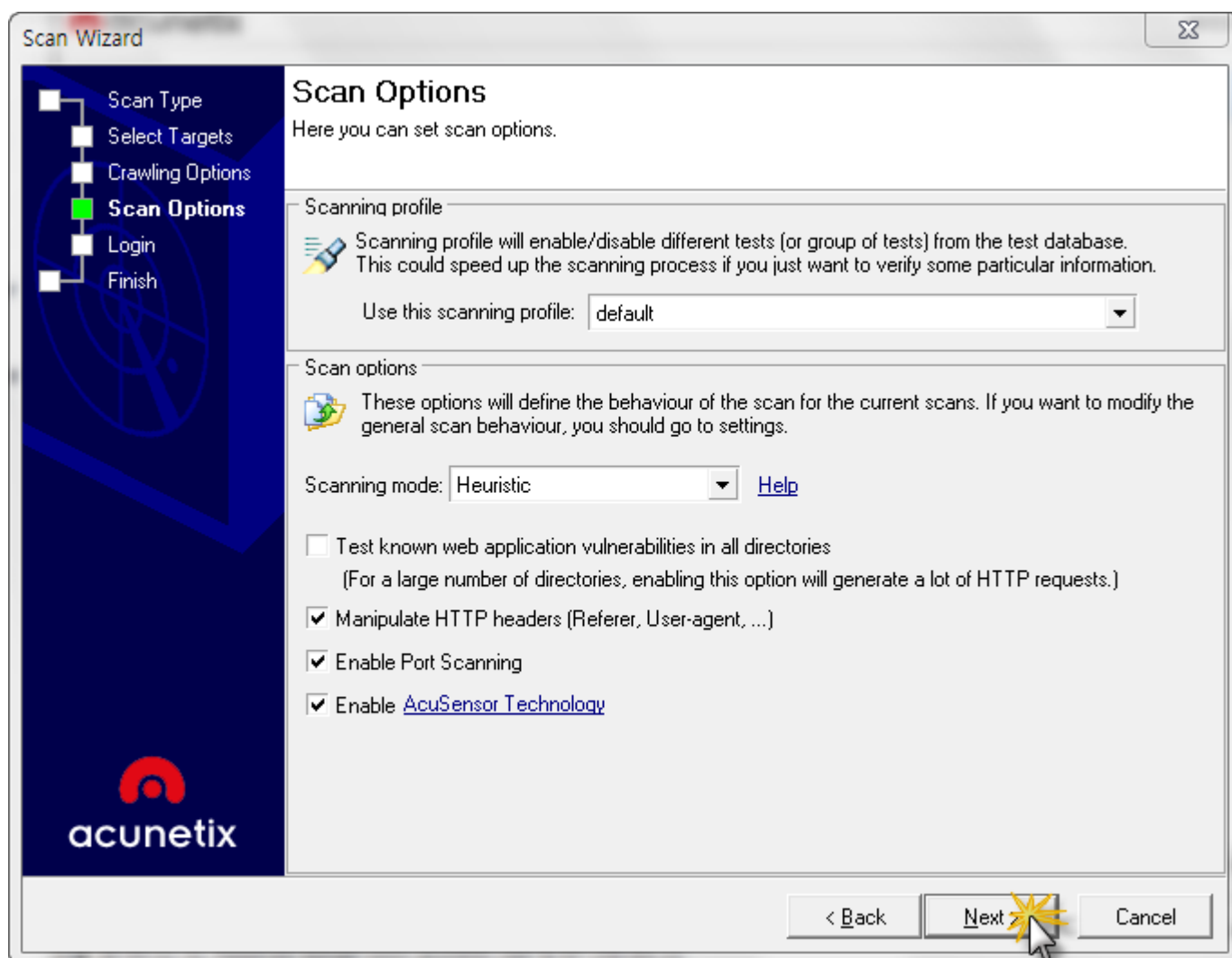


여기선 특정 버그만 스캔할지 여부를 선택. 역시 디폴트로 설정.

【실전으로 배워보는 인터넷보안】



여기는 스캔속도설정, 빠르게? 일반? 아니면 느리게? 스캔결과에 정확도에 영향주는거니깐 그냥 일반적으로 "Heuristic" 그대로 두시면 되구요.

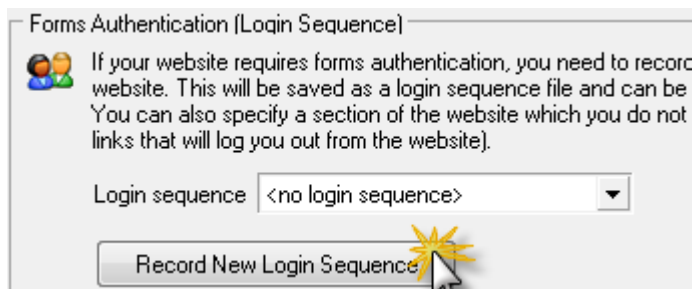


역시 "Next"

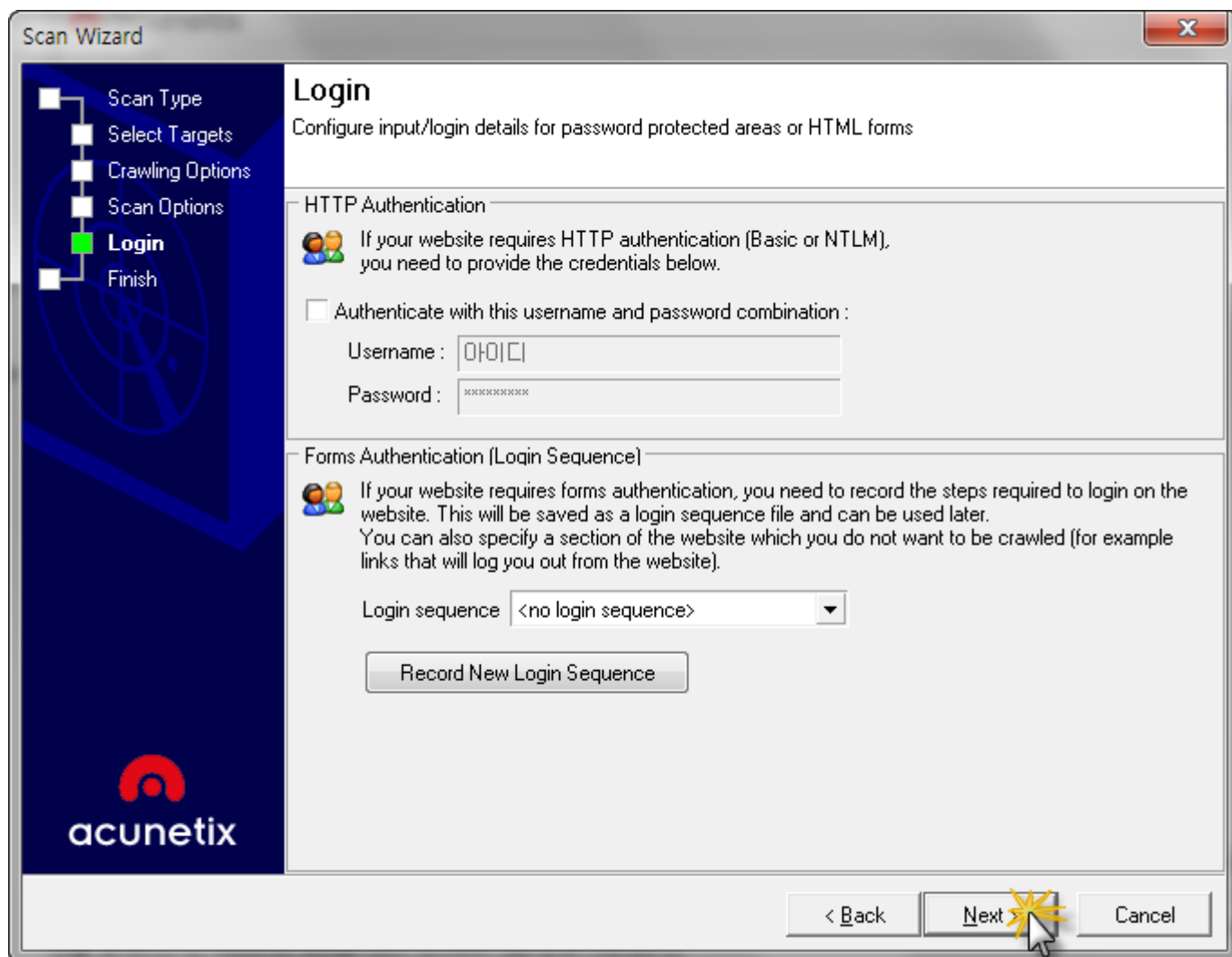
【실전으로 배워보는 인터넷보안】



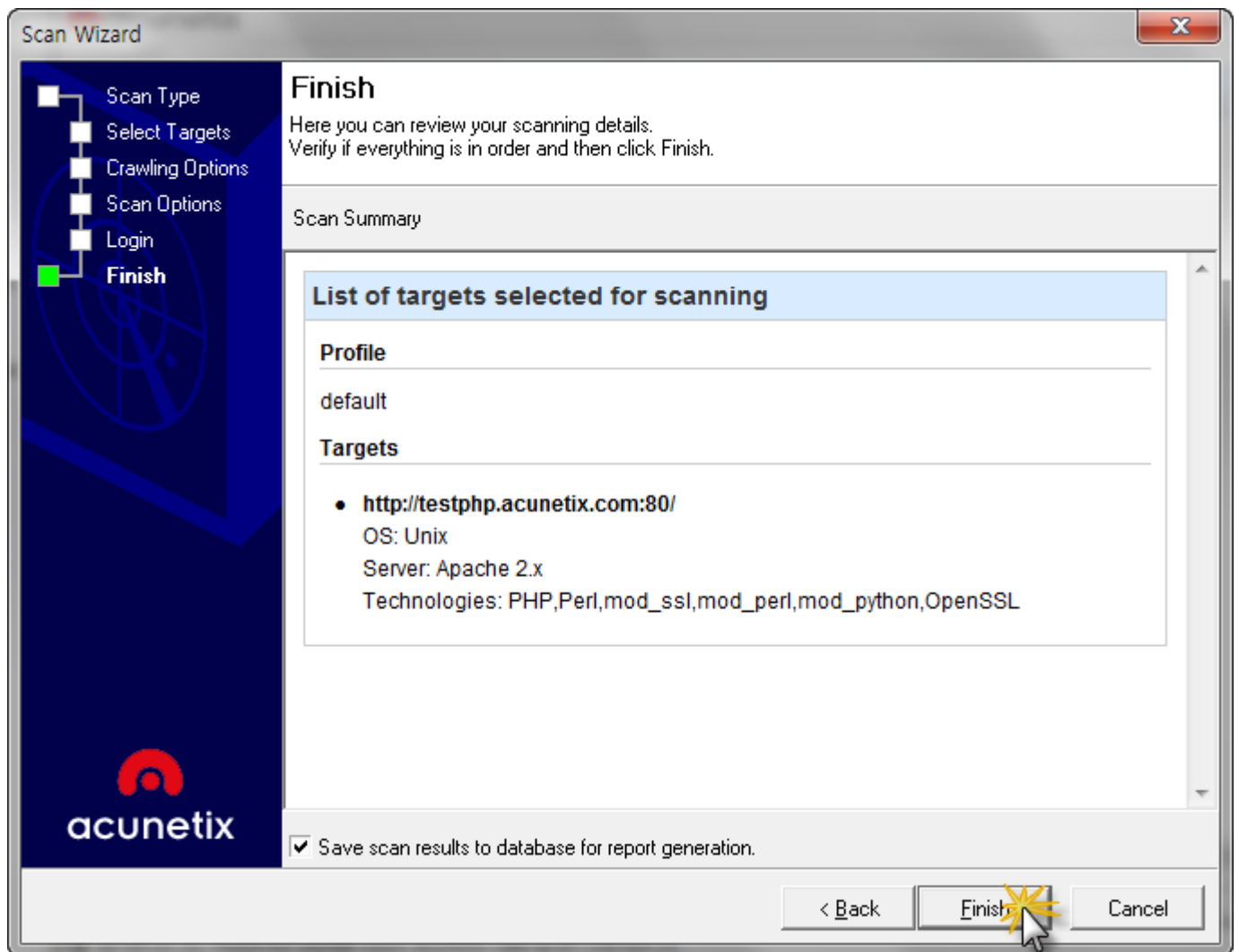
그다음 페이지로 넘어왔을 때 로그인에 필요한 사이트라면 설정해야될 옵션들이죠.
HTTP인증이 필요한 웹페이지라면 체크를 하시고 아이디 하고 패스워드를 입력.



만약 웹로그인이 필요하다면 위에 버튼을 클릭하면 오픈되는 웹사이트에서 로그인하시고 세션을 저장.

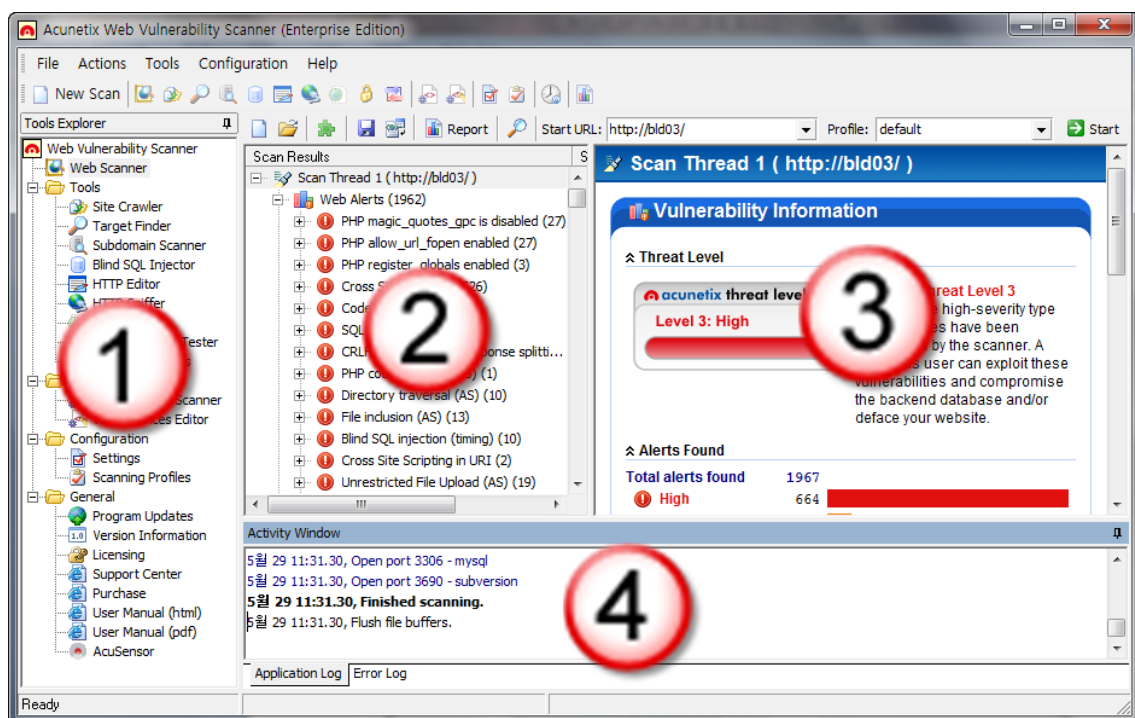


저장이 끝났다면 저장된 세션을 선택하고 "Next" 클릭.



여기까지 오면 설정 완료. 그냥 "Finish" 를 클릭하시면 스캔이 시작됩니다.

【실전으로 배워보는 인터넷보안】

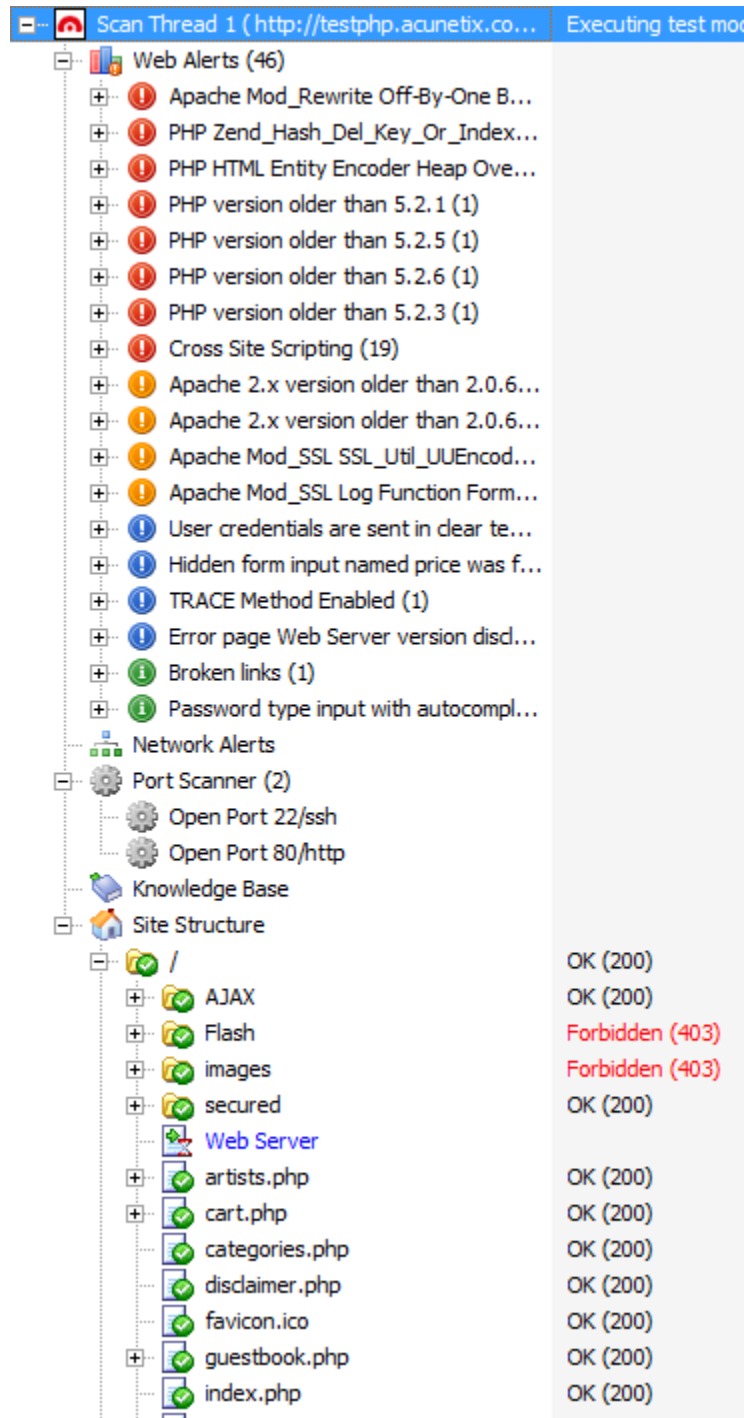


스캔이 시작되면 위에 상태로 보여지는데요.

- 1) 여러가지 보조용 해킹툴
- 2) 웹사이트 파일리스트와 존재하는 버그들
- 3) 위험레벨
- 4) 현재 진행상태

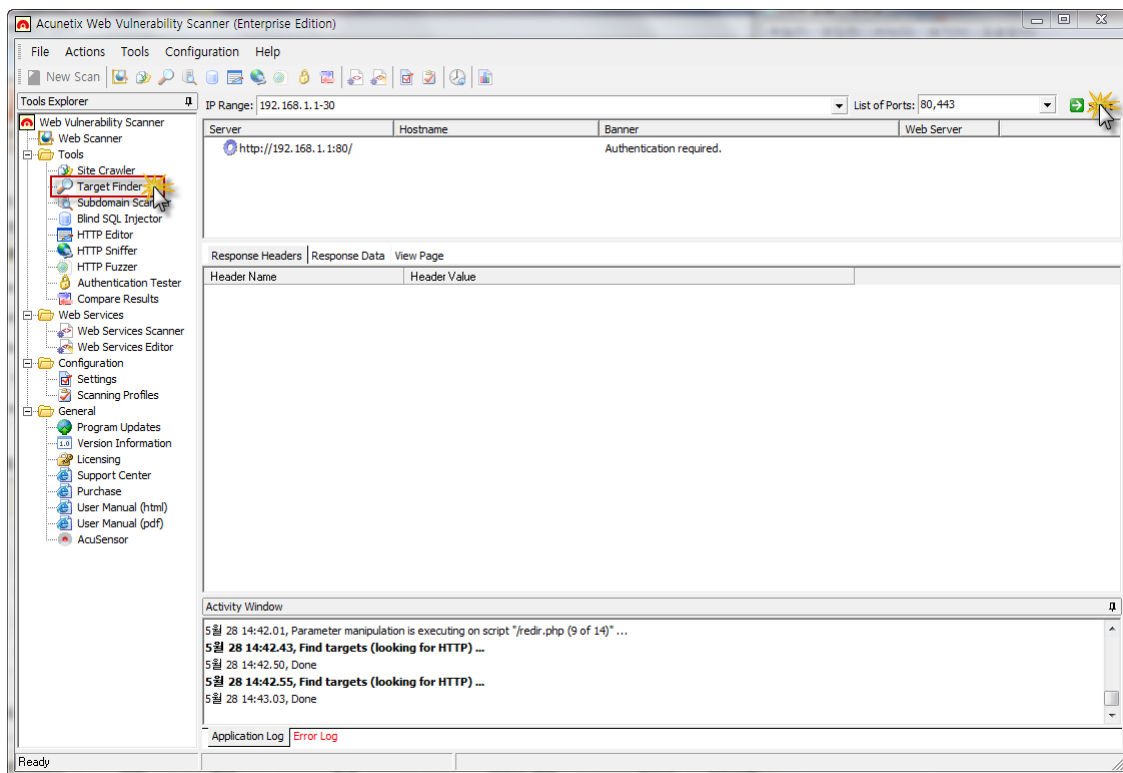
스캔이 완료되었다면 2번창에서는 아래와 유사한 정보를 확인가능.

【실전으로 배워보는 인터넷보안】

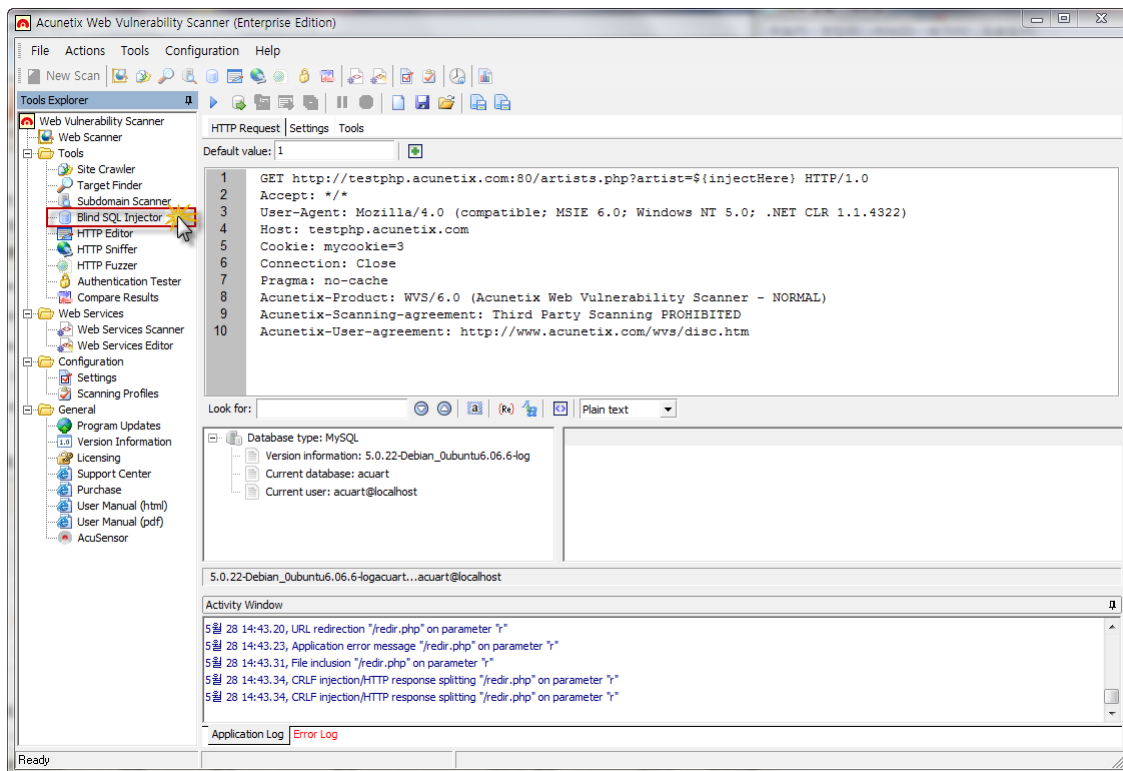


현재 존재하는 버그들을 그 위험도에 따라 색상별로 정리가 됨. 그리고 스캔옵션 설정시 포트스캔설정도 체크를 하였다면 현재 서버에 오픈된 포트가 아래에 보여짐. (개인적으로 이 옵션은 닫아두는 것을 추천함.) 그리고 그 아래에는 사이트 폴더와 파일구조를 확인할수있구요 이는 실정 해킹에 많은 도움이 되죠.

【실전으로 배우보는 인터넷보안】



왼쪽 프로그램리스트에서 “Target Finder” 는 일정한 IP대역에 대한 스캔을 통하여 현재 웹 서버가 실행중인 아이피를 확인.



【실전으로 배워보는 인터넷보안】

“Blind SQL Injection” 툴은 SQL인젝션 버그가 존재하는 페이지에 대한 침투테스트를 도와주는 기능이구요. 위에 화면처럼 현재 서버에 사용된 디비서버 유형과 버전. 그리고 현재 웹사이트에 사용된 디비유저등 정보를 확인하실수있구요.

그외에도 다른기능들이 있지만 다음기회에 소개해드리는거로 하구요 일단 여기까지만 아셔도 자신이 운영하고 있는 웹사이트에 대한 보안체킹이 가능하니깐 한번씩은 프로그램을 다운받으셔서 웹서버의 보안상태를 점검해보시는 것을 추천합니다.

더욱 상세한 정보는 아큐네틱스 공식홈페이지(<http://www.acunetix.com>) 을 확인하시거나 매뉴얼 파일을 다운받아 보시는 것을 추천드립니다.

매뉴얼 파일: <http://www.acunetix.com/vulnerability-scanner/wvsmanual.pdf>

그리고 마지막으로 acunetix 는 유료 프로그램이기에 여건이 되시는분들은 최대한 정품을 사용하시길 바랍니다. ^^

그럼 다음강좌에서 봐요~