보안공부닷컴
http://www.boangongbu.com

개나소나 다하는 SQL인젝션 공격

작성날짜: 2010년 4월 27일 화요일

메일주소: boangongbu@naver.com

SQL인젝션 공격에 대해서 많이 들어들 보셨을겁니다. 2002년부터 시작된 이런 공격 방식은 아직도 보안에 무신경한 웹개발자들이나 서버관리자들땜에 많이 먹히고 있다는 사실이 정말 안타깝기만 할뿐이죠. 여러 대형 사이트들도 이렇게 단순한 공격에 무너지는 것을 보면 문제의 심각성을 알수있죠. (조선닷컴, 옥션, 신세계백화점 등등….)

어떻게 되어 이런공격이 가능한지는 현재 인터넷에 많은 문서들이 떠돌고있구요. 하지만 이런 단순한 공격을 해커라는 분들이 어떻게 진행을 하는가에는 상세한 문서가 없는거 같더라구요. 이번 계기로 <보안공부닷컴> 에서 한번 만들어 보도록 하겠습니다.

보안공부닷컴은 실전위주로 진행을 하기에 각설하고 타겟을 잡고 공격부터 들어갑니다. ^^

필요한 프로그램:

웹버그스캐너: N-Stealth, Watchfire AppScan, WebInspect, nikto, webscarab, Acunetix, JSky 등

인젝션공격툴: pangolin, NBSI, SQL map, SQL ninja 등.

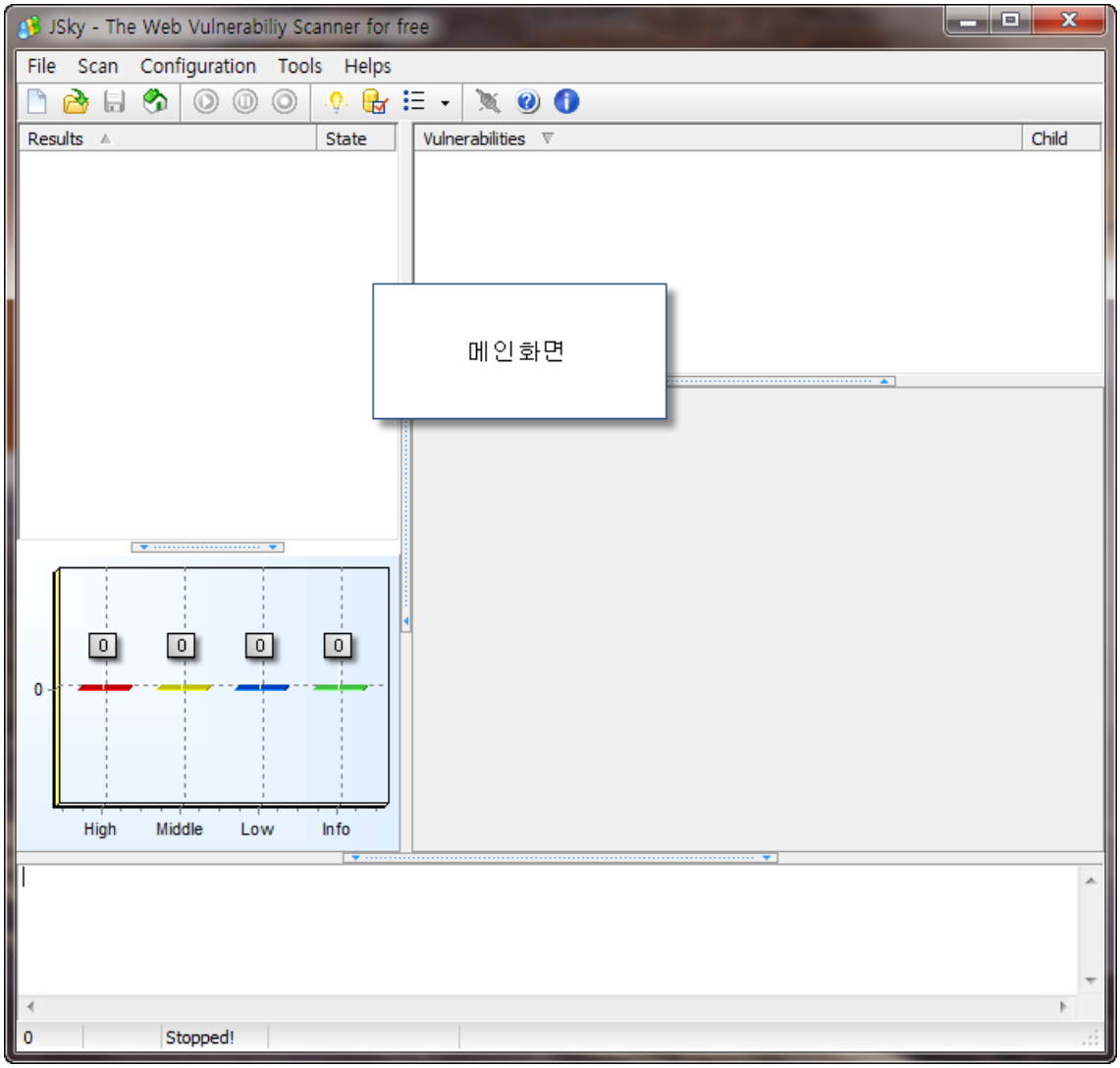
본 문서에서는 초보자가 사용하기 편한 웹버그 스캐너 JSky 와 인젝션 공격툴 Pangolin 을 사용해 보도록 하겠습니다. 이 두 프로그램은 동일한 개발자에 의하여 만들어졌으며 얼마전 모 유명 백신 프로그램 일본 공식사이트에 대한 공격에 Pangolin 이 사용되었다는 것이 밝혀지면서 유명세를 타게 되었죠?

먼저 보안공부닷컴에서 이 두 프로그램을 다운받은다음 압축을 풀고 준비를 합니다.

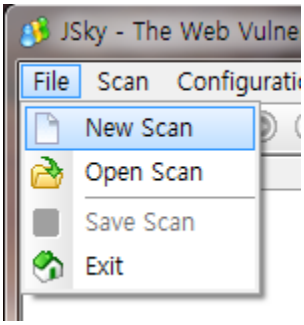
준비가 되셨다면 일단 타겟을 잡아야겠죠?

구글에 접속하여 검색창에 inurl: view.asp?id 를 입력후 검색버튼을 클릭합니다. 물론 여기에서 사용된 검색자 view.asp?id 는 제가 임의로 지정한거구요 자주 사용하는 파일명 혹은 변수를 대입하여 다른 검색자를 사용해 보셔도 무관합니다.

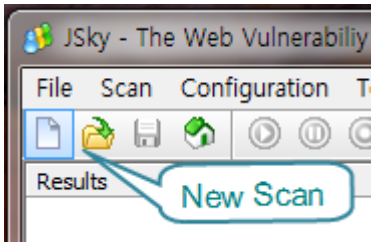
검색되어 나온 사이트들 중에 하나를 골라서 스캔을 해보도록 하겠습니다. 먼저 Jsky를 실행합니다. 그럼 아래와 같은 프로그램 메인창이 뜰거구요.



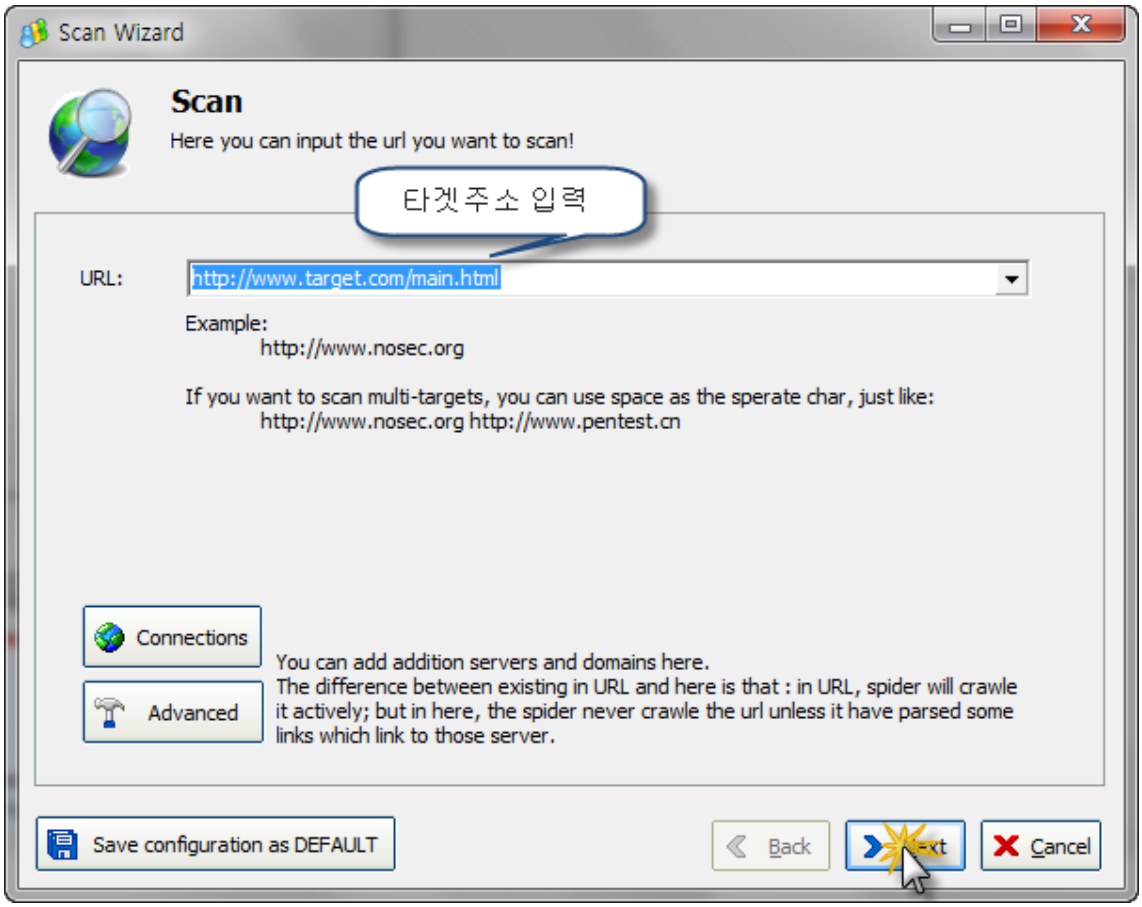
타겟을 지정해줍니다.



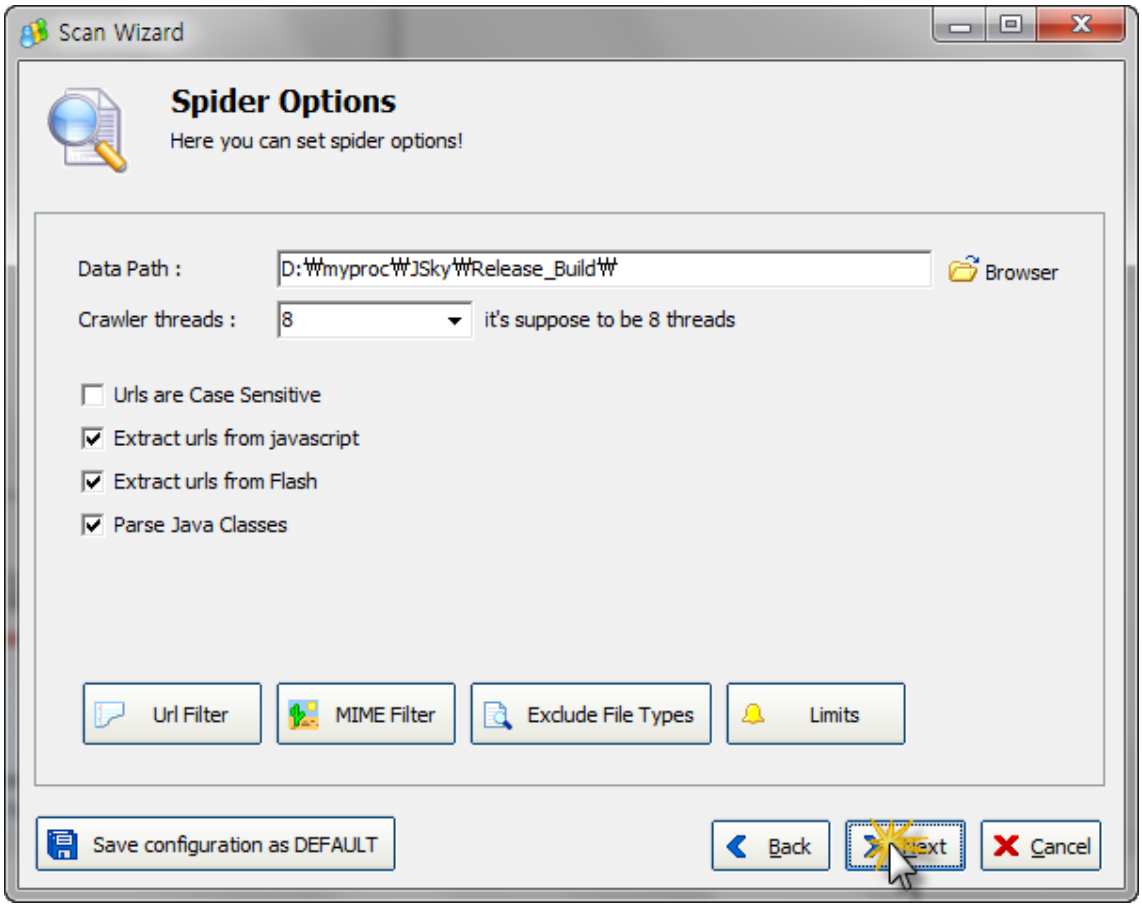
File메뉴에서 New Scan 을 실행하거나 혹은 메뉴바에서 New Scan 아이콘을 클릭합니다.



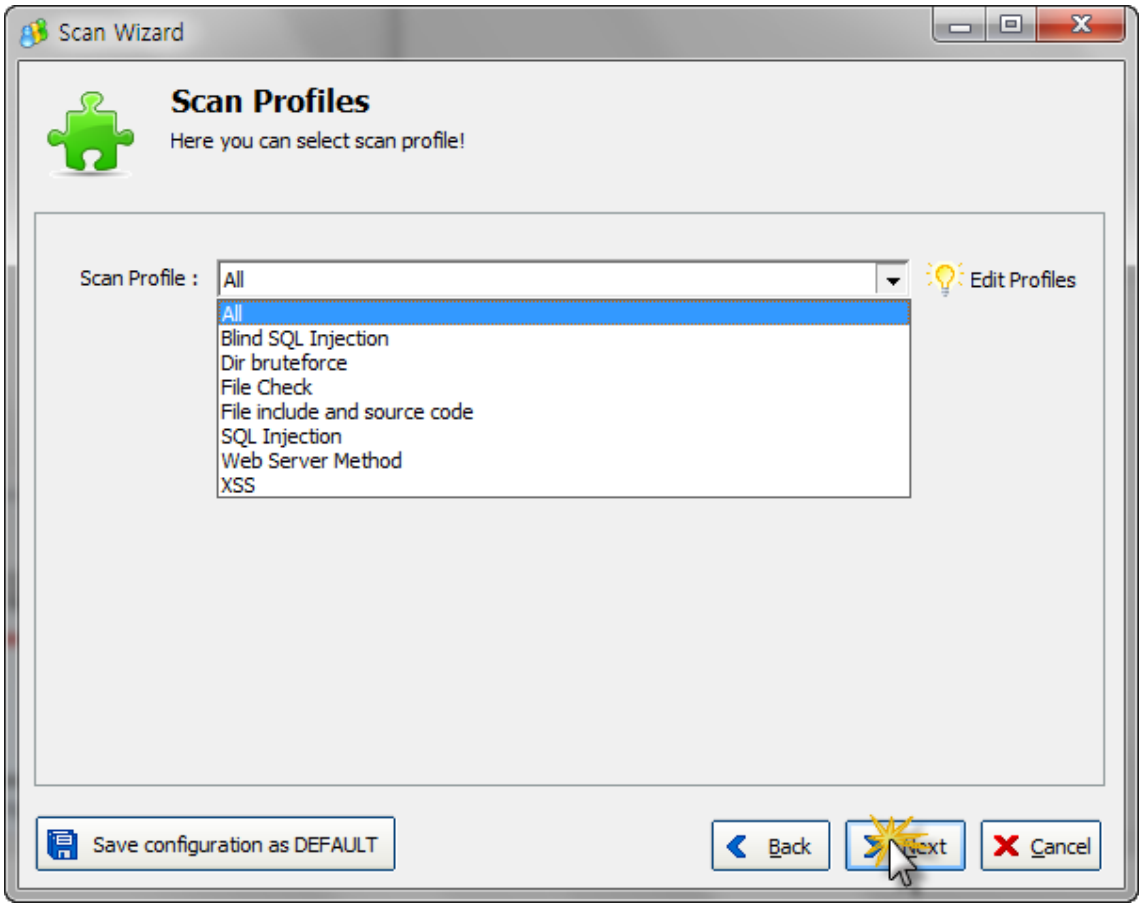
그다음 나오는 창에서 타겟 주소를 입력하구요. Next 를 클릭합니다.



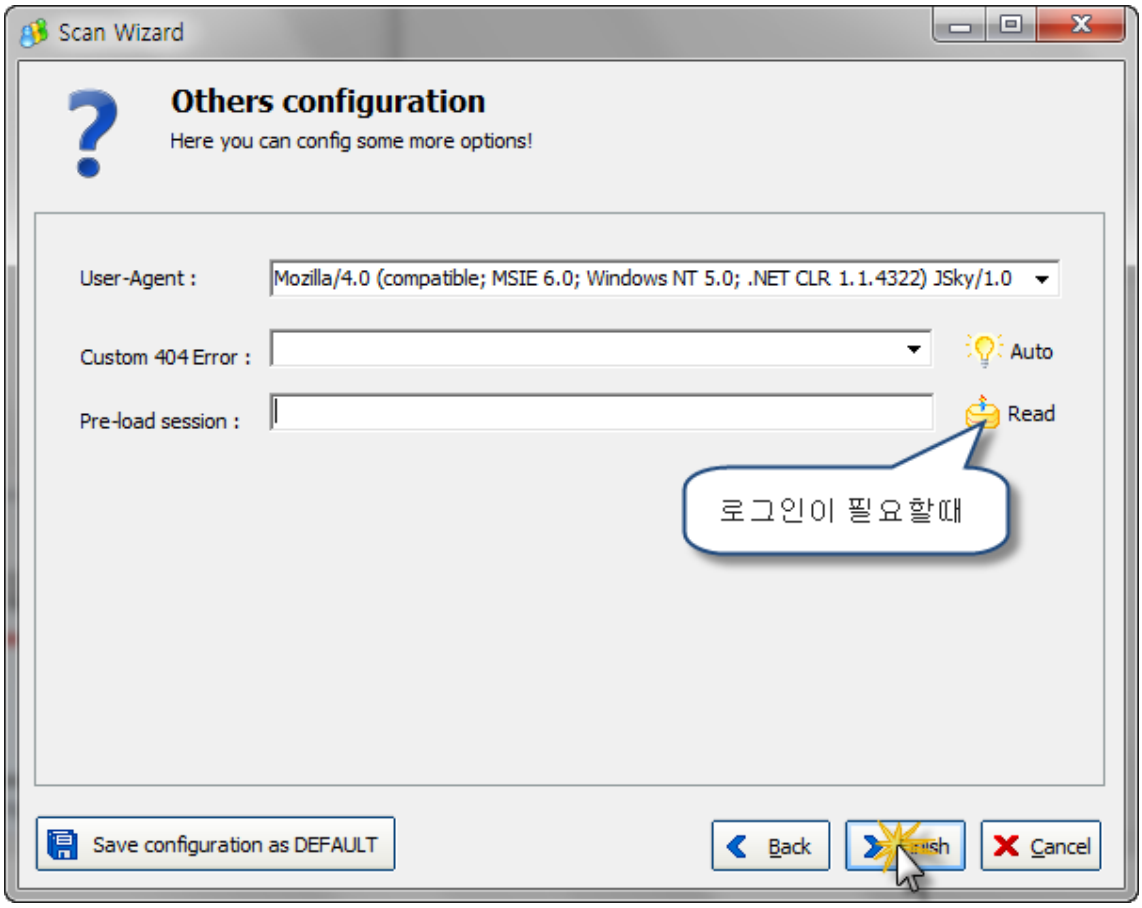
여기서 주의할껀 일부사이트에서는 iframe 같은 코드로 메인 페이지를 포함하였을시 꼭 실제 메인페이지 주소를 찾아서 입력을 해주야 한다는 것을 아셔야하는데요. 이는 보통 메인페이지 소스를 확인해보면 파일명을 알수있구요



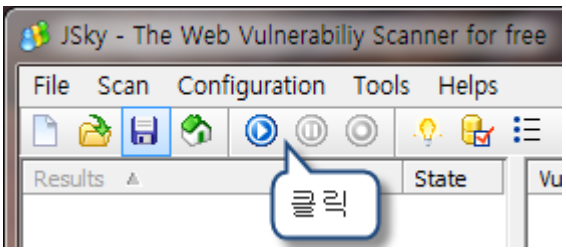
그리고 다음페이지에 건너오면 스캔후 저장할 데이터의 위치와 자바스크립에서 웹사이트구조를 찾아낼것인가 와 플래쉬에서 주소를 찾아낼것인가 등 여러가지 설정을 하는곳인데요 일단 여기서는 디폴트로 놔두시고요 역시 Next~



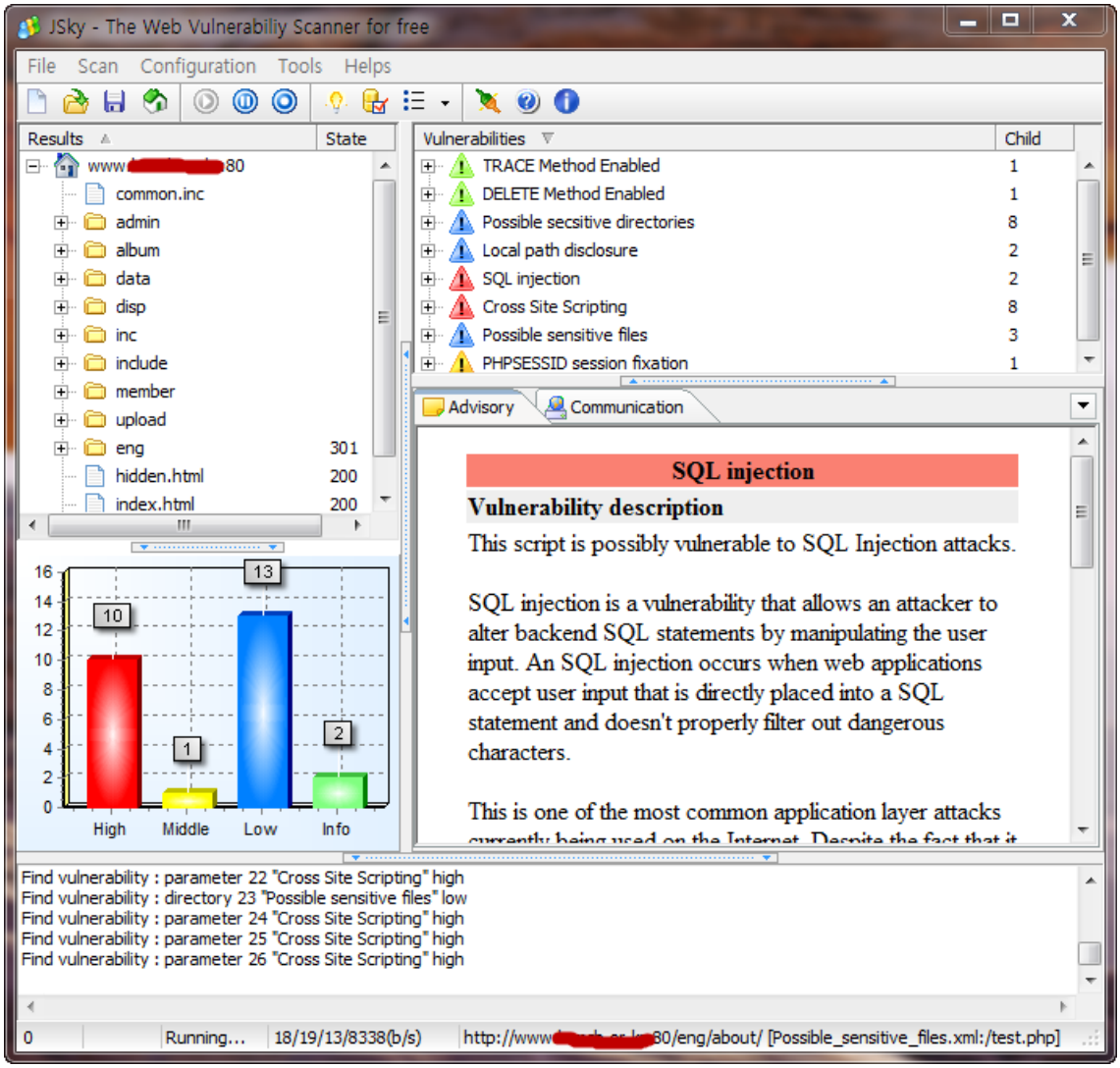
아, 그다음페이지 스캔할 버그들을 선택하는 페이지 인데요 뭐 여러가지가 있지만 일단 전부 ALL 그대로 Next 를 클릭.



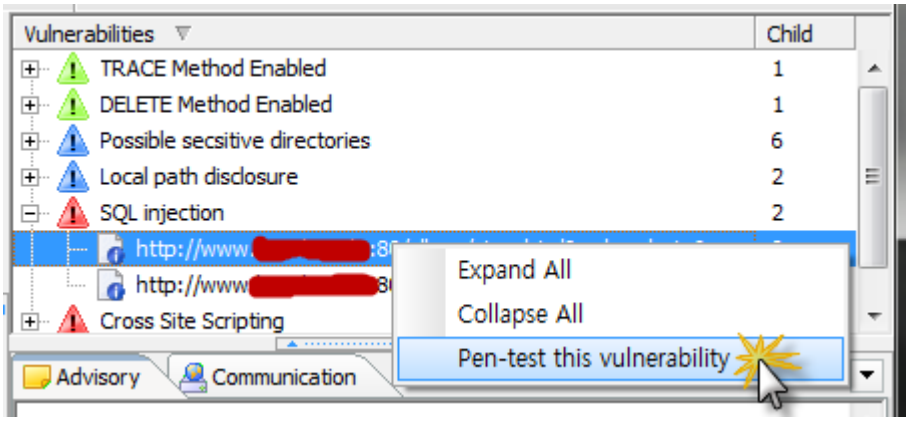
아, 여기는 패킷을 보낼시 웹서버한테 전송되는 클라이언트 정보와 세션정보를 입력하는 곳입니다. 만약 로그인을 해야만 접속이 가능한 페이지라면 우에 Read버튼을 클릭하여 사이트에 접속을 하신후 스캔을 하셔야 더욱 많은 버그를 찾아낼수있습니다.



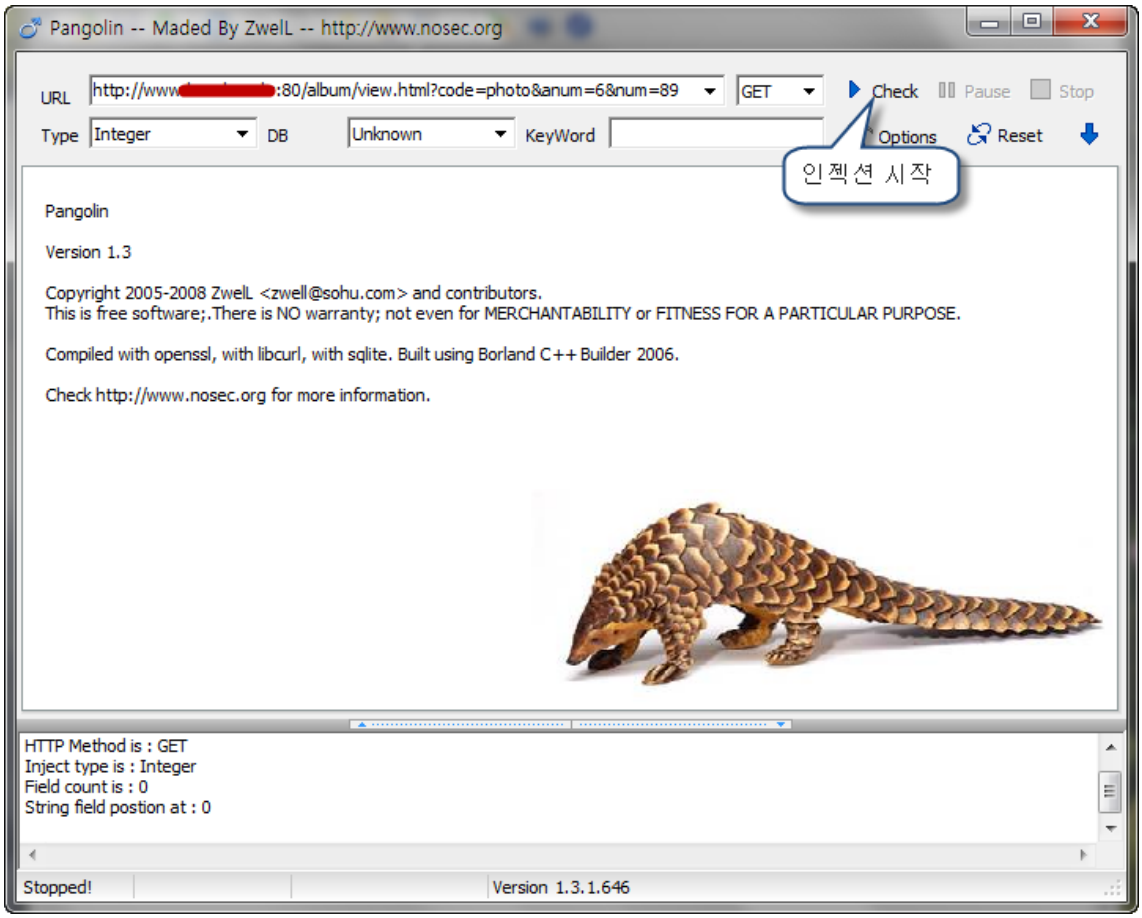
설정이 끝났으면 실행 아이콘을 클릭하여 스캔을 시작!



스캔이 끝나고나면 위와같이 버그의 위험도별로 웹사이트에 존재하는 버그가 나뉘어 지거고 왼쪽에는 사이트구조가 그대로 보여지죠. 이는 해킹시 아주 유용하게 사용되기도 하죠.

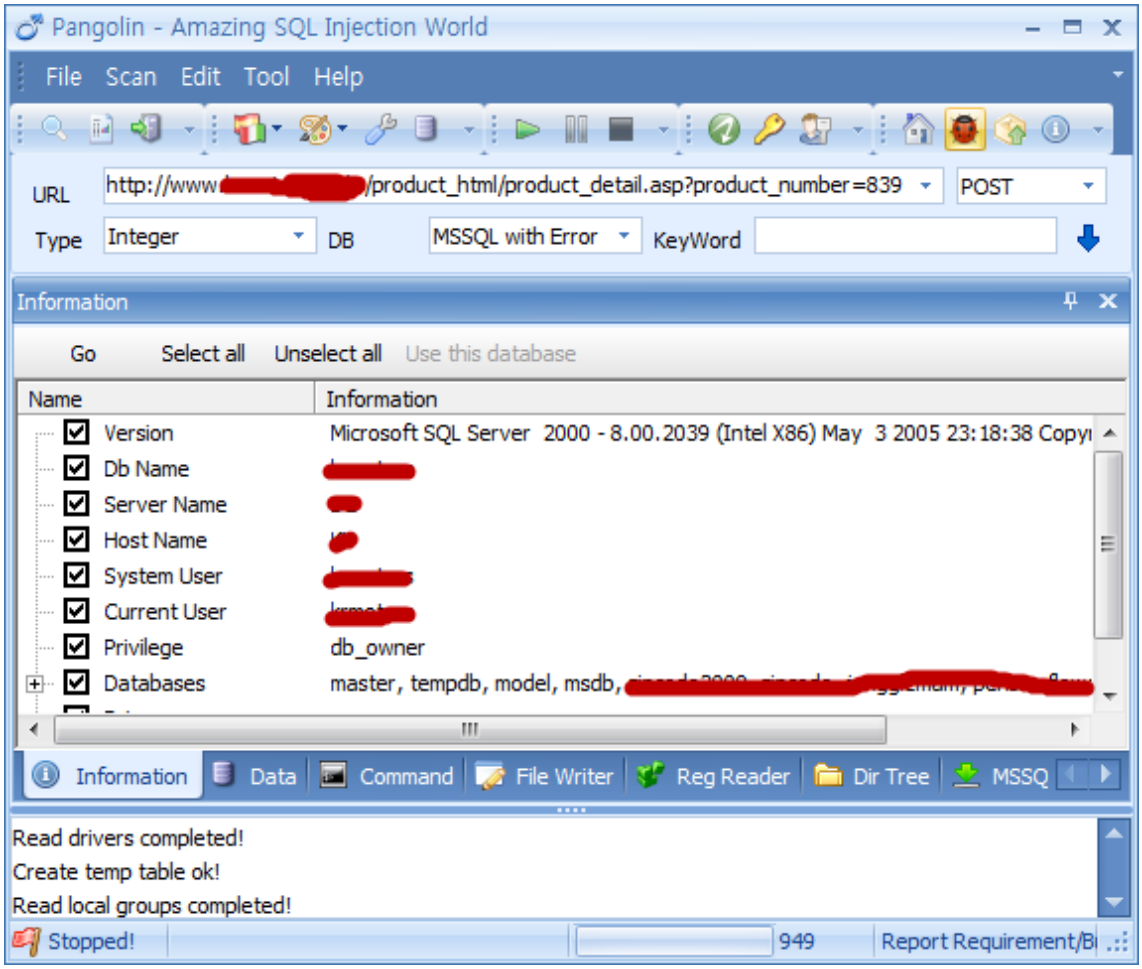


SQL Injection 파트에 + 를 클릭하면 버그가 존재하는 페이지 리스트를 확인할수있구요 임의의 페이지 위에 마우스 오른쪽버튼을 클릭하여 Pen-test this vulnerability 를 실행하면 스캐너에 포함된 인젝션 공격툴 pangolin을 불려내게 됩니다.

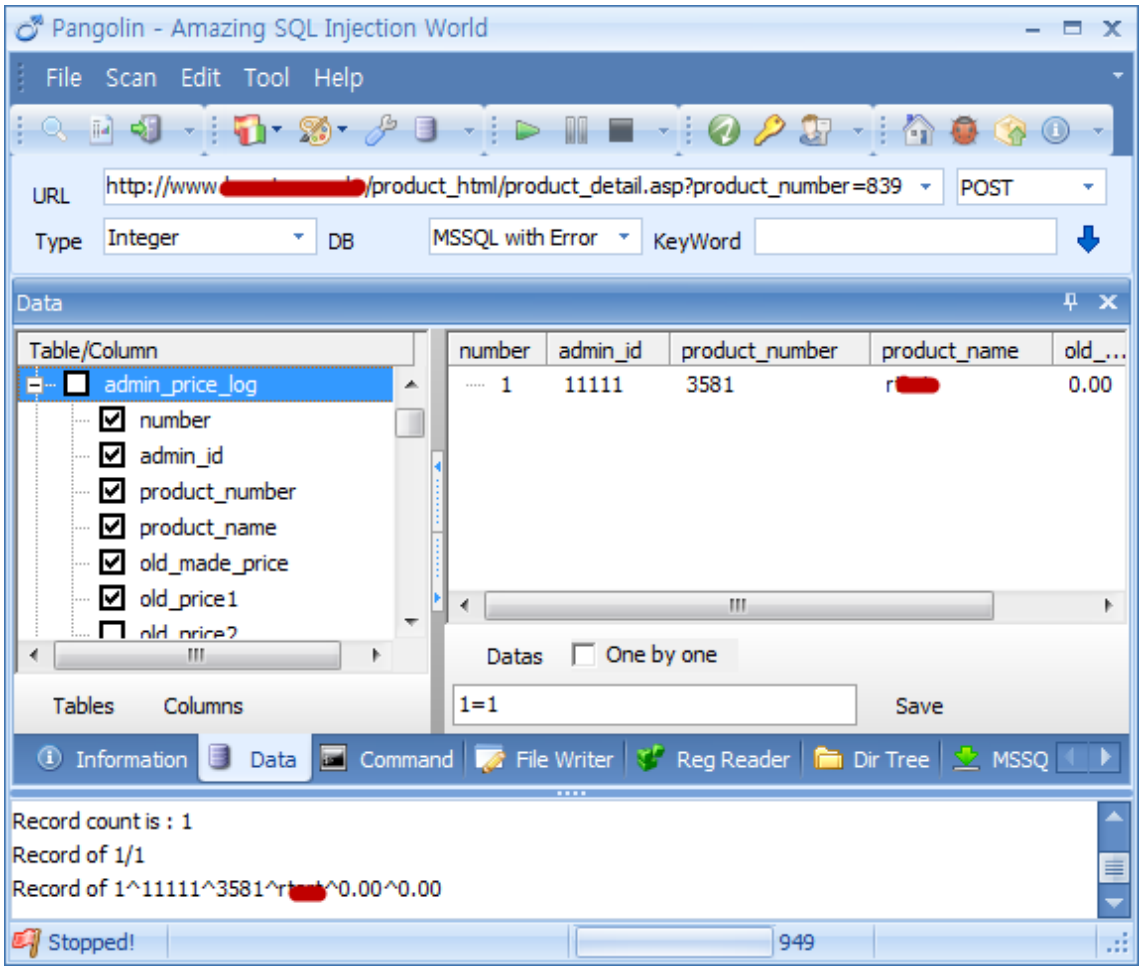


하지만 기본으로 내장된 버전은 오래된 버전이라 기능상 많이 낙후된거구요 현재 최신으로 배포된 무료버전을 받아서 주소를 입력한다음 실행 버튼을 클릭하면 아래와같이 공격이 가

가능한 것을 확인하실수있습니다.



위와 같이 디비서버 버전, 디비명 등 민감한 정보를 한눈에 확인 하실수있구요. 디비내의 정보를 확인하고싶으면 Data 탭으로 이동하여 Tables 버튼을 클릭.



그러면 위처럼 디비구조가 그대로 노출될꺼구요 테이블내에 입력된 정보를 확인하시려면 확인 하고싶은 컬럼을 선택하시고 옆에 Datas 버튼을 클릭하면 위처럼 정보확인 가능.

여기서 사용된 pangolin이라는 프로그램은 현재 유료버전이고 위에처럼 무료버전을 사용할 수있지만 php+mysql 인젝션 oracle환경 인젝션등 기능을 사용못하게 나오는거라 제한이 좀 있구요. Jsky에 포함된 버전은 비록 asp + mssql 인젝션공격에 조금 제한이 있지만 php + mysql 환경에 대한 인젝션도 지원을 한다는 장점이 있죠. 각 버전사이의 차이점은 직접 사용해보시면서 확인하시구요.

이런 방법으로 웹사이트에 가입시 입력한 나의 정보가 어느날 갑자기 이상한 사이트에 남겨져 있거나 불법적인 목적으로 사용되게 되는거죠.

다음번 강좌에서는 다른 유용한 프로그램들로 찾아뵙도록 하겠습니다. 꾸벅~ (__)