WebKnight를 활용한 IIS 웹서버 보안 강화 가이드

KISA는 본 문서에서 언급한 WebKnight 및 해당 도구 개발사인 AQTRONIX와 어떠한 관계도 없으며, 국내 웹 해킹 피해 예방을 위해 공개 웹방화벽인 WebKnight를 보안 참고용으로 소개합니다.

2008. 06

KrCERT/CC 인터넷침해사고대응지원센터

KISA 한국정보보호진흥원 Korea Information Security Agency

1. 개 요

단순 홈페이지 해킹이 아닌 홈페이지 방문자들의 정보를 빼내 금전적인 이득을 취하고자 하는 홈페이지 해킹이 심각한 수준에 달하고 있다. 이는 해킹당한 업체가 피해기관이 되기도 하지만 해당 웹사이트를 신뢰하고 방문하는 수많은 네티즌들을 감염시키는 공격사이트이기도 하여 조치가 시급하다.

최근 윈도우즈 웹서버를 대상으로 발생되고 있는 해킹은 대부분 SQL Injection 공격이 그 원인이다. SQL Injection 취약점은 게시판, 공지사항 등에서 URL 인자에 대한 입력 값을 검증하지 않음으로 해서 공격이 발생되는 웹 개발과정에서의 오류라고 할 수 있다. 대형 포털, 뉴스 사이트 등 수많은 국내 사이트들이 공격을 당해 웹 방문자들을 감염시키고 있지만, 이러한 악성코드 유포지로 이용되고 있는 사이트들은 취약점이 있음을 알고 있어도 제대로 조치를 하지 못해 수차례 다시 해킹을 당하는 경우를 많이 볼 수 있다. 인터넷침해사고대응지원센터의 분석에 의하면 국내 악성코드 경유지 또는 유포지 사이트 중 약 30% 가량이 2회 이상 재발되고 있는 것으로 나타났다. 이는 SQL Injection 취약점 자체가 웹 어플리케이션의 소스 코드를 수정해야만이 근본적으로 해결될 수 있는 문제이지만 운영 중인 웹 서버의 소스 코드 수정이 쉽지 않기 때문이다.

웹 시스템 구축 이후 문제점을 수정하기 보다는 설계·개발 단계에서 보안을 고려하여 개발되는 것이 바람직하다. 인터넷침해사고대응지원센터에서는 홈페이지 개발 시 고려하여야 하는 보안사항과 웹언어별 사례, 그리고 대표적인 웹 공격에 대비할 수 있는 표준 웹 어플리케이션 보안템플릿 등을 제공하고 있으므로 이를 참고하기 바란다.

o 홈페이지 개발 보안 가이드 및 웹 어플리케이션 보안 템플릿 다운로드
http://www.krcert.or.kr 접속 > 좌측 배너 “웹 보안 4종 가이드”

이 외에도 웹서버 보안을 위한 추가적인 방안으로 MS는 IIS 보안을 위해 IISLockDown, URLScan 등의 도구를 제공하고 있다.

IISLockdown은 웹 서버를 보호하기 위한 과정을 대부분 자동화할 수 있는 도구로 서버의 용도에 따라 유형별로 다양한 보안기능을 해제하거나 보호할 수 있는 사용자 템플릿을 제공해 준다.

http://download.microsoft.com/download/iis50/Utility/2.1/NT45XP/EN-US/iislockd.exe

URLScan은 웹 사이트 관리자가 서버에서 처리 가능한 웹 요청을 제한할 수 있는 ISAPI(Internet Server Application Program Interface) 필터로써 특정 웹 요청을 제한하여 잠재적으로 유해한 웹 요청이 서버에 도달하기 이전에 차단함으로써 공격을 예방한다.

http://download.microsoft.com/download/1/9/8/198a7fdf-1057-4668-9f44-035f8faeaf95/Setup.EXE
http://www.microsoft.com/technet/security/tools/urlscan.mspx

이 외에 Windows에서 제공하는 Support Tools나 Resource Kit에도 여러 다양한 서버 보안을 위한 도구 들이 포함되어 있어 이를 잘 활용한다면 훨씬 효과적일 것이다.

하지만, 아쉽게도 IISLockdown이나 URLScan도 DB Query 문장을 필터링하지는 못하여 SQL Injection 공격의 위험에서 벗어날 수 없다.

최근 웹 공격이 심각한 수준에 이르러 국내·외 상용 웹방화벽들도 많이 출시되었다. 다양하고 정교한 웹공격을 기존의 네트워크 방화벽이나 침입탐지시스템이 방어하는 데에는 한계가 있다. 웹방화벽은 SQL Injection 등 웹 공격에 특화된 보안 솔루션이므로 웹방화벽의 도입도 검토할 필요가 있다. 그러나, 기업에서 경제적인 문제로 인해 상용 웹방화벽 도입이 어려운 경우가 많으므로 본 고에서는 공개 웹방화벽인 WebKnight를 통해 최신 여러 다양한 웹 공격으로부터 서버를 효과적으로 보호하는 방안을 살펴보고자 한다.

WebKnight는 GNU 공개 라이센스 원칙을 따르는 공개 소프트웨어로써 모든 기업이나 개인이 자유로이 사용할 수 있다. 특히, 지난해 2007년 10월 2.1로의 버전업이 이루어진 이후 IIS보안의 핵심으로 자리 잡고 있다.

또한, WebKnight는 SQL Injection을 포함한 다양한 웹공격에 대해 차단할 수 있는 프레임을 제공해 주고 있고, IIS의 각 버전(5.0, 6.0)에 따라 별다른 문제없이 운영이 가능하여 보다 효과적으로 웹서버 보안을 이룰 수 있다. 물론, WebKnight의 잘못된 설정은 정상적인 웹 요청까지 차단할 수 있으므로 충분한 최적화과정을 거쳐야 함은 웹서버 관리자의 몫임을 명심하여야 할 것이다.

본 문서는 『WebKnight를 이용한 SQL Injection 공격 차단('06.2.10)』의 개정판으로 WebKnight 2.1로 업데이트 되면서 변화된 부분과 윈도우 2003, IIS 6.0 환경에서 설치 적용하는 과정 등에 대해 중점적으로 다루었다.

2. WebKnight 개요

WebKnight는 AQTRONIX사(http://www.aqtronix.com/)에서 개발한 IIS 웹서버에 설치할 수 있는 공개용 웹 방화벽이다. WebKnight는 ISAPI 필터 형태로 동작하며, IIS 서버 앞단에 위치하여 웹서버로 전달되기 이전에 IIS 웹서버로 들어온 모든 웹 요청에 대해 웹서버 관리자가 설정한 필터 룰에 따라 검증을 하고 SQL Injection 공격 등 특정 웹 요청을 사전에 차단함으로써 웹서버를 안전하게 지켜준다. 이러한 룰은 정기적인 업데이트가 필요한 공격 패턴 DB에 의존하지 않고 SQL Injection, 디렉토리 traversal, 문자 인코딩 공격 등과 같이 각 공격의 특징적인 키워드를 이용한 보안필터 사용으로 패턴 업데이트를 최소화하고 있다. 이러한 방법은 알려진 공격 뿐만 아니라 알려지지 않은 공격에도 웹서버를 보호할 수 있다.

또한, WebKnight는 ISAPI 필터이기 때문에 다른 방화벽이나 IDS에 비해 웹서버와 밀접하게 동작할 수 있어 많은 이점이 있다. MS의 URLScan과 마찬가지로 ISAPI 필터로써 inetinfo.exe 안에서 동작하므로 오버헤드가 심하지 않다. 해킹당한 한 웹사이트에 WebKnight를 적용하여 테스트한 결과 안정적인 웹서버 운영으로 인해 웹서버 속도가 오히려 빨라진 것을 느낄 수 있었다. 하지만 다량의 웹 트래픽이 발생되는 사이트에서는 사전에 충분한 검증을 거친 후에 적용할 필요는 있다.

다음은 WebKnight의 주요 특징이다(http://www.aqtronix.com/?PageID=99 참조).

o 오픈 소스(Open Source)
WebKnight는 GNU, GPL(General Public License)를 따르는 Free 소프트웨어이다.

o Logging
기본적으로 차단된 모든 요청에 대해 로그를 남기고, 로깅 전용 모드로 운영할 경우 추가적으로 모든 허용된 요청에 대해서도 로그를 남길 수 있다. 로깅 전용 모드는 공격을 실제 차단하지 않고 로그 파일에서 공격 사실을 조사하는데 도움을 줄 수 있다.

o 최적화(Customizable)
방화벽은 어떤 작은 원인에도 최적화가 가능해야 한다. 제조사로부터 패치가 릴리즈 되기 전의 0-day(zero-day) 공격마저 무산시킬 수 있도록.

o 웹기반 어플리케이션과의 호환성
WebKnight는 Frontpage Extensions, WebDAV, Flash, Cold Fusion, Outlook Web Access, SharePoint 등과도 호환이 잘 이루어진다.

o HTTP Error Logging
WebKnight는 웹서버로부터 HTTP 에러들을 로그할 수 있도록 설정할 수 있다. 이 방법으로 '404 Not Found'와 같은 일반적인 에러나 '500 Server Error'와 같이 보다 심각한 로그들도 기록할 수

있다. 에러 로그를 이용하여 공격을 탐지하거나 깨진 링크를 발견하거나 잘못된 설정도 쉽게 발견할 수도 있다.

o SSL 보호(SSL Protection)
다른 전통적인 방화벽과는 달리 WebKnight는 ISAPI 형태로 IIS의 일부로써 동작하기 때문에 HTTPS 상의 암호화된 세션들도 모니터링 및 차단할 수 있다.

o 3rd-Party 어플리케이션 보호(Third-Party Application Protection)
WebKnight는 웹서버만 보호하는게 아니라 전자상거래 사이트 및 기타 사용자 웹사이트도 설정을 통해 보호할 수 있다.

o RFC 규약(RFC Compliant)
WebKnight는 RFC를 따름으로써 Request 값을 스캔하기 위한 기능도 포함되어 있다.

o 낮은 보유 비용(Total Cost of Ownership)
WebKnight는 윈도우즈 인스톨러 패키지와 원격 설치 스크립트로 설치가능해 사내에서 쉽게 WebKnight를 채택할 수 있다. 또한 WebKnight 설정을 바꾸기 위해 그래픽 사용자 인터페이스를 제공한다.

o 운영 중 업데이트 가능(Run-time Update)
일부 설정의 변경을 제외하고 대부분의 설정 변경은 웹서버의 재가동을 요구하지 않아, 웹 사용자들에 대한 어떠한 서비스 장애 없이 설정을 변경할 수 있다. 성능상의 이유로 매 1분마다 이러한 변경을 탐지하여 적용한다.

3. WebKnight 설치 및 제거

3.1. WebKnight 설치

WebKnight가 1.3 버전이 릴리즈 된 후 2.0 버전을 거쳐 현재 2.1 버전으로의 업데이트까지 이루어지는 동안 적지 않은 업데이트 들이 이루어졌다. 특히 2.0에서의 유니코드 등 한글처리 부분 외에 기타 버그 등이 수정 된 후 발표된 2.1은 현재 가장 안정화된 버전으로써 본 고에서도 설치 및 가이드에 안내할 버전이므로 최신 버전을 사용하길 권장한다.

WebKnight는 IIS 5.0과 6.0 양 버전에서 사용이 가능하지만 설치하는 방법에서 약간의 차이를 가지고 있다. WebKnight의 설치방법은 IIS의 버전별, 그리고 인스톨러에 따른 구분, 그리고 필터링 방법으로 나누어 살펴보겠다.

3.1.1. IIS 5.0 환경에 설치하기

o 플랫폼 : Windows 2000 SP4
o 웹서버 : IIS 5.0
o WebKnight 소스 디렉토리 : C:\Tools\WebKnight_21\
o WebKnight 기본 설치 디렉토리 : C:\Program Files\AQTRONIX WebKnight\

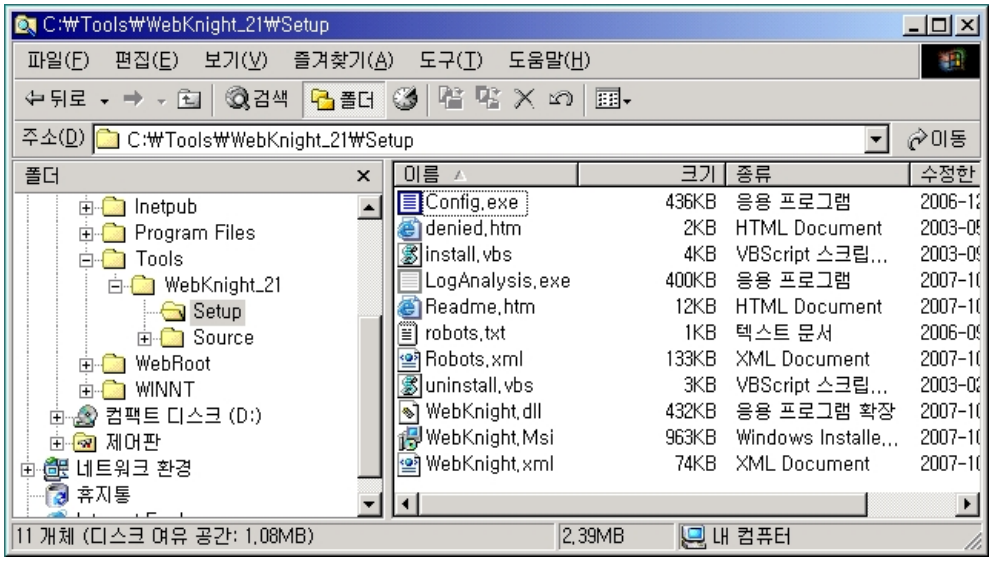
▷ 윈도우 인스톨러를 이용한 자동 설치

WebKnight를 설치하는 방법 중 가장 간단하며 기본적인 방법으로 윈도우에서 지원하는 Microsoft Installer를 이용한 설치 방법이다. 글로벌 필터를 적용하려면 이 방법으로 설치하는 것이 가장 바람직하다.

① 아래 URL에서 WebKnight 2.1을 다운로드 받는다.
http://www.aqtronix.com/downloads/WebKnight/2007.10.08/WebKnight.zip

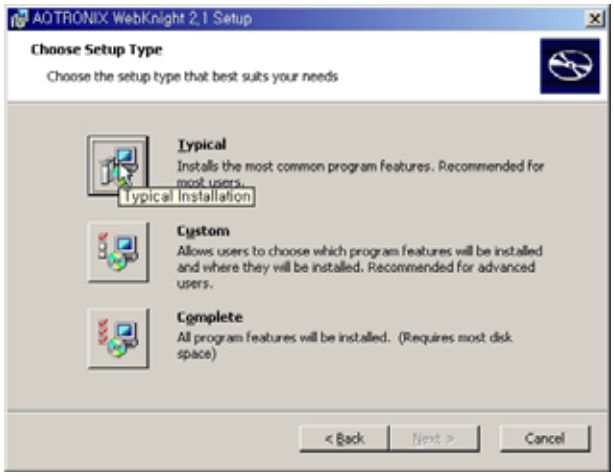
또는, KrCERT 홈페이지에서도 다운로드 받을 수 있다.
http://www.krcert.or.kr/firewall2/index3.jsp

② 압축을 해제한 뒤 Setup 폴더로 이동하면 아래와 같은 파일들이 생성된다.

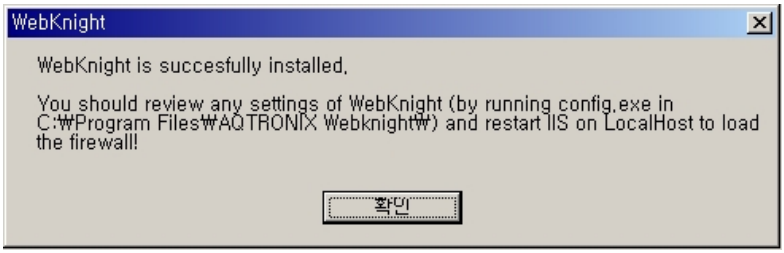


③ 위 파일 중 WebKnight.Msi 파일을 찾아 실행하면 다음 화면이 나타난다.

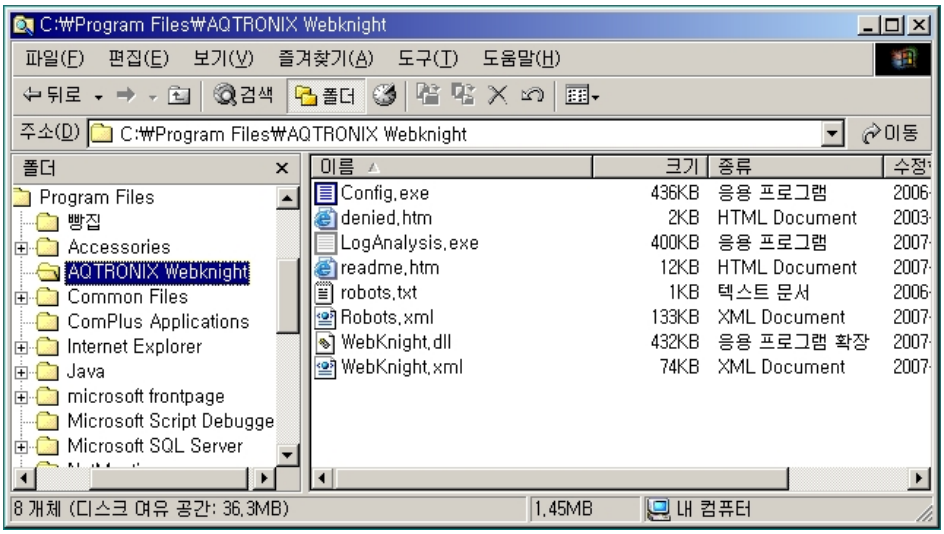
④ 라이센스 동의 후 설치 타입 선택화면이 나타나는데, “Typical"을 선택한다.



⑤ 이후 자동 설치과정이 진행되며 설치가 완료되면 다음과 같은 메시지가 나타난다.



⑥ 기본 설치를 하게 되면 C:\Program Files\AQTRONIX WebKnight\ 폴더에 WebKnight설치가 된다. WebKnight.Msi를 이용해 설치하게 되면 Default 경로로 설치가 되는 동시에 인터넷 정보 서비스에 Global Filter로 ISAPI Filter에 자동 등록되기 때문에 간편하다.

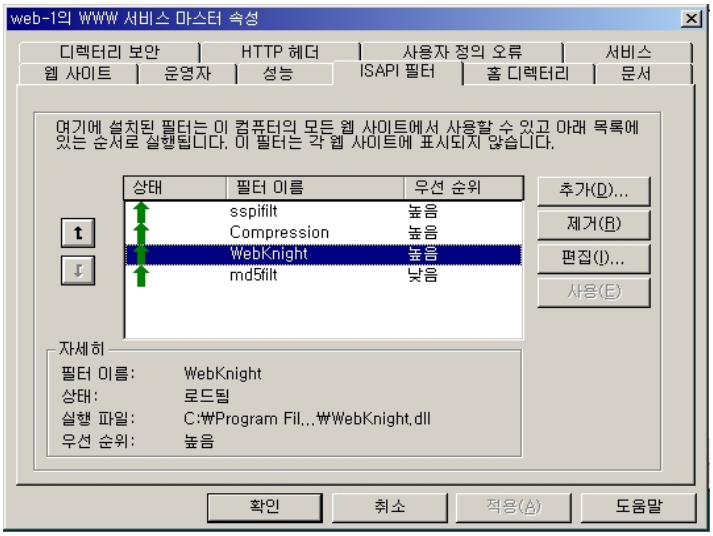


간단히 주요 파일의 특징을 살펴보자.

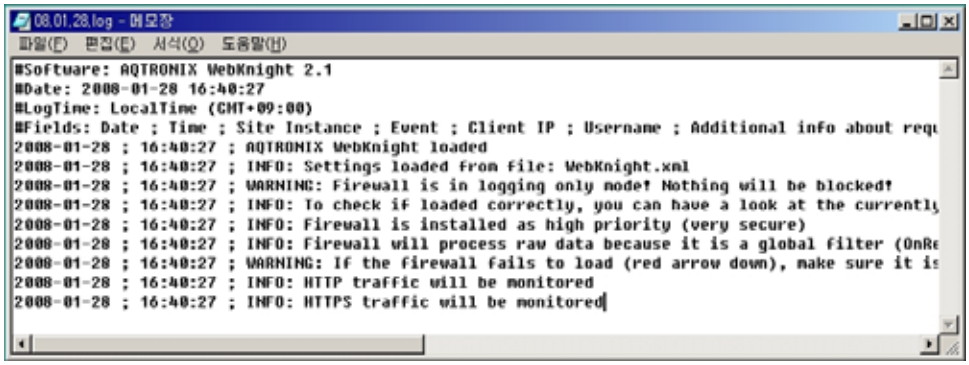
- Config.exe : WebKnight의 설정파일을 읽어들여 조작 할 수 있게 해주는 파일
- denied.htm : 설정에서 'Response Directly' 옵션을 통해 보여지는 기본 차단 메시지
- LogAnalysis.exe : 로그 분석기
- Robots.xml : User-Agent에 대한 DB 파일
- WebKnight.dll : ISAPI Filter 파일, WebKnight가 실제 동작하는 파일이다.
- WebKnight.xml : WebKnight 동작을 제어할 수 있는 설정 파일

⑦ IIS를 재시작 한다.

⑧ IIS 재시작 후에 관리자에서 정상적으로 설치가 완료되었을 경우 다음과 같이 WWW 서비스 마스터 속성에서 "ISAPI 필터" 탭에 다음과 같이 WebKnight 필터가 정상적으로 적용이 된 것을 확인할 수 있다.



⑨ 필터가 정상적으로 로드되었다면 설치폴더에 다음과 같은 로그파일이 생성되었을 것이다.



WebKnight가 정상적으로 로드되었고 Log Only모드로 동작하고 있으며 높은 우선순위로 설치 되었다는 등의 메시지가 기록되었다.

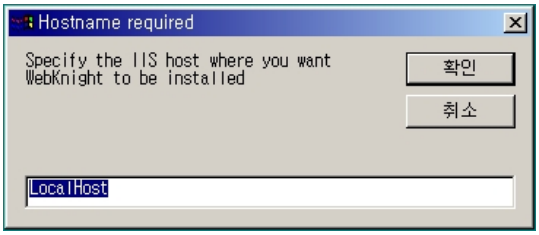
자동 인스톨러를 이용한 설치법은 이렇게 간단하며 쉽다. 다음으로 VB스크립트를 이용한 설치법을 알아보자.

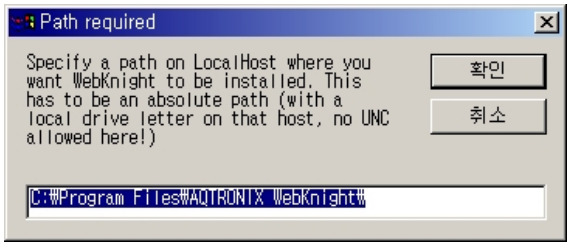
▷ VB스크립트를 이용한 자동 설치

① 앞서 과정과 마찬가지로 설치파일을 다운로드 받은 뒤 압축을 해제한다.

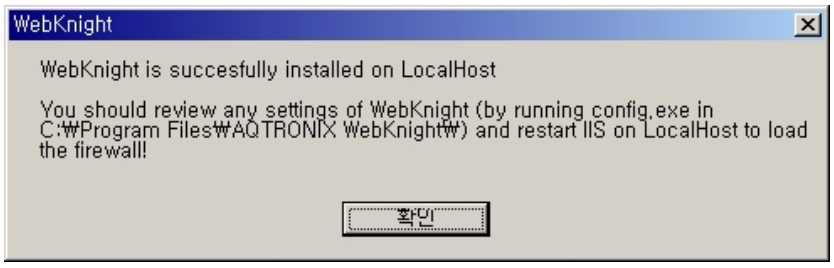
② 압축 해제 후 나타나는 파일 중에 install.vbs 파일을 실행하여 나타나는 창에 설치할 컴퓨터의 Hostname을 적어준다.

③ 이후 설치할 경로를 적어준다. Default값은 MS Installer로 설치할 때와 같다.





③ 설치 경로를 입력한 후 설치가 완료되면 다음과 같은 메시지 창이 나타나며 설치가 끝난다.



이후 부터는 “윈도우 인스톨러를 이용한 설치” 에서의 6번 과정부터 동일하게 이루어진다.
IIS를 재시작 한 뒤 필터가 정상적으로 로드 되었는지 확인하고 로드 되었다는 로그파일이 생성되었으면 설치가 끝난 것이다.

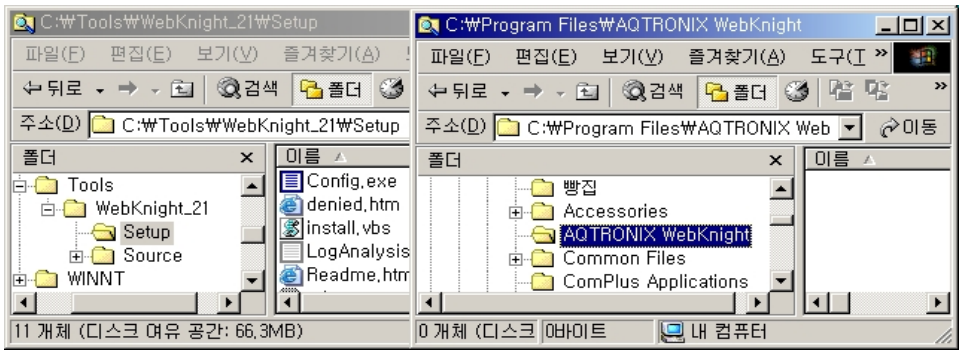
▷ 수동 설치

수동 설치는 쉽게 말하면 Copy & Paste, 복사해서 붙여넣기이다. 수동 설치는 Site Filter로 설치하기 위해 주로 사용하지만 IIS 5.0에선 수동 설치를 통한 Global Filter 설치법을 알아보겠다.

※ IIS의 버전별 Architecture의 차이로 인해 IIS 5.0에서는 Site Filter 설치가 불가하며 IIS 6.0에만 가능하다.

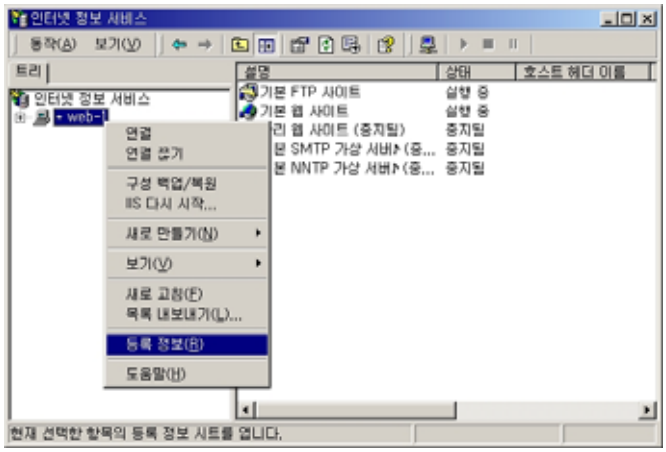
■ 글로벌 필터로 수동 설치

① 압축 해제 후 생성되는 Setup 폴더를 C:\Program Files\AQTRONIX WebKnight와 같은 서버 내의 로컬 폴더를 생성하고 여기에 복사한다.



② 인터넷 정보 서비스를 실행한다.

③ 서버 이름에서 우측 마우스를 클릭하여 “등록정보”를 선택한다.

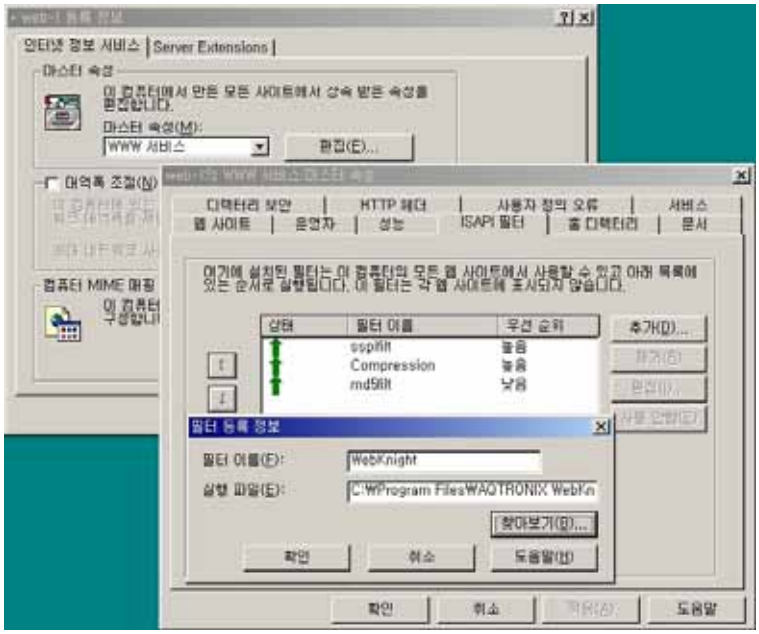


④ 마스터 속성 리스트에서 “WWW 서비스”를 선택하고, “편집” 버튼을 누른다.

⑤ “ISAPI 필터” 탭을 선택하고 “추가” 버튼을 클릭한다.

⑥ “필터 등록 정보”가 나타나면 필터 이름과 실행 파일 경로를 입력한다.

예) 필터 이름 : WebKnight, 실행 파일 경로 : C:\Program Files\AQTRONIX WebKnight\WebKnight.dll



⑦ "확인" 버튼을 누르고 대화상자를 빠져 나간다.

⑧ IIS를 재시작한다.

3.1.2. IIS 6.0 환경에 설치하기

o 플랫폼 : Windows 2003 Enterprise Edition
o 웹서버 : IIS 6.0
o WebKnight 소스 디렉토리 : C:\Tools\WebKnight_21\
o WebKnight 기본 설치 디렉토리 : C:\Program Files\AQTRONIX WebKnight\
o WebKnight Site Filter 디렉토리
- C:\Program Files\AQTRONIX WebKnight\KISA_1\
- C:\Program Files\AQTRONIX WebKnight\KISA_2\

IIS 6.0 에서는 IIS 5.0 환경과는 다르게 별도의 과정이 더 필요하다. 일반적인 설치 방법은 IIS 5.0 에서의 3가지 방법과 동일하나 그 이후에 추가 작업이 이행되어야 한다.

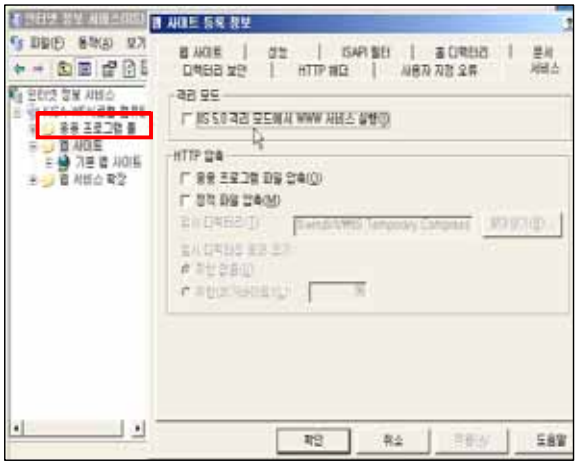
IIS 6.0 부터는 Application Pool(응용프로그램 풀)이 추가 되어 각각의 독립적인 “작업자 프로세스

모드"로 구동하게 된다. 그 외에도 COM+ 컴포넌트나 .NET Framework 등 여러 응용프로그램을 지원하게 되면서 5.0과는 구조적으로 많은 변화가 이루어졌으며 이에 따라 WebKnight를 적용하는 방법 또한 조금의 차이점이 생기게 됐다. 따라서 IIS 6.0 에서의 설치 방법은 Global Filter 설치와 Site Filter 설치로 구분지어 알아보자.

> **※ IIS Architecture에 따라 발생하는 WebKnight 필터링 차이**
> **IIS가 5.0에서 6.0으로 업그레이드되면서 내부 Architecture가 바뀌었다. IIS 6.0부터 작업자 프로세스 기반으로 동작하게 되면서 WebKnight 적용 시 Global Filter를 설정하지 못하게 되었고, 이로 인해 POST Data에 대한 필터링이 불가능하게 되었다. 그러므로 POST method를 통한 입력값까지 검증하기 위해서 IIS 5.0 격리모드로 사용해야 한다.**

■ Global Filter 설치 - IIS 5.0 Isolation Mode

IIS 6.0을 5.0 격리모드로 전환하는 것으로 "웹 사이트" 등록정보에서 "서비스" 탭의 "IIS 5.0 격리모드에서 WWW 서비스 실행" 에 체크한 뒤 IIS를 재시작하게 되면 IIS 6.0이 5.0 형태로 전환되면서 "응용 프로그램 풀"이 사라진다.



위와 같이 격리모드로 전환 후에는 "IIS 5.0 환경에 설치하기"의 절차와 설치법이 동일하다. 단지 이와 같은 격리모드로 전환할 경우에는 IIS 6.0에서 지원되는 기능을 사용할 수 없기 때문에 최초 개발시 환경이나 적용 대상 웹 어플리케이션의 플랫폼 등을 충분히 검토한 후에 전환하여야만 문제 없이 동작할 수 있을 것이다.

■ Global Filter 설치 - IIS 6.0 with Application Pool

기본적인 "윈도우 인스톨러를 이용한 설치"와 "VB Script를 이용한 설치", "수동 설치"를 통해 설치할 경로를 지정하고 파일을 복사한 뒤 필터를 등록하는 절차까지 동일하다. 단지 필터를 등록하

는 위치는 IIS 5.0에서의 '서버 이름'이 아닌 '웹 사이트'의 등록정보에서 ISAPI 필터 탭에 등록하면 된다. Default로 "C:\Program Files\AQTRONIX WebKnight\" 에 설치하였다고 가정하자.

① IIS 6.0에서 수동 설치를 제외한 두가지 방법으로는 자동으로 ISAPI 필터에까지 등록이 된다. 하지만 "알수 없음" 으로 표시되며 로드가 되지 않는다.

② WebKnight를 설치한 폴더로 이동하여 Config.exe를 실행한 뒤 webknight.xml 을 불러온다.

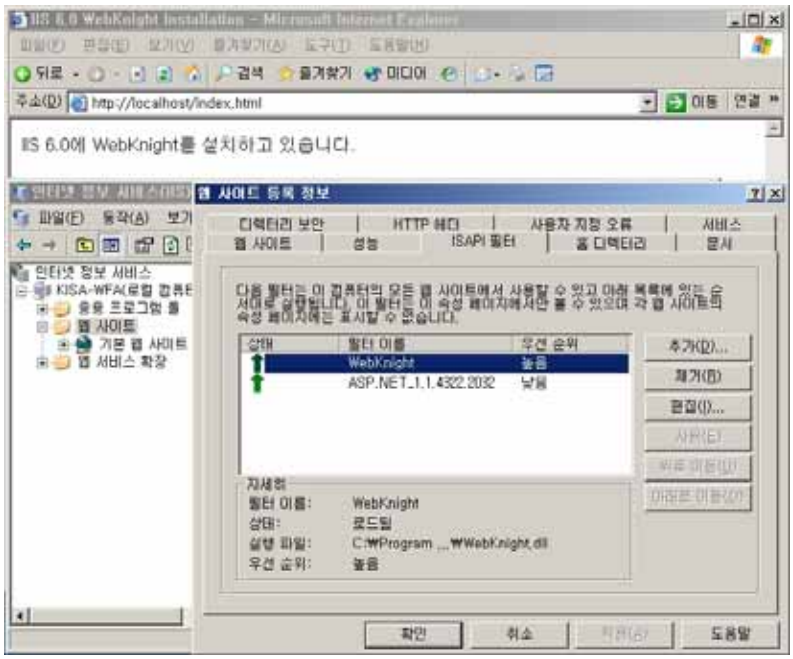
③ "Global Filter Capabilities" 섹션으로 이동한 뒤 "Is Installed As Global Filter" 옵션을 체크해제하고 저장한다.

④ WebKnight 설치폴더의 등록정보에서 "보안"탭에 "Network Service" 계정을 추가한 뒤 "쓰기" 권한을 부여해 준다.

※ 이 과정을 거치지 않으면 WebKnight.dll이 정상적으로 로드되지 않으며 쓰기권한을 부여하지 않았을 경우 로그파일이 생성되지 않는다.

⑤ IIS를 재시작한다.

⑥ 웹페이지를 Refresh 하거나, 새 브라우저를 통해 관리 대상 웹사이트를 브라우징 해줘야만 필터가 정상적으로 로드된다.



이와 같은 IIS 6.0 의 Global Filter의 설치 방법은 적용될 웹사이트가 모두 DefaultAppPool 또는, 한가지의 공통된 AppPool을 적용하고 있을 때 정상 작동한다. 이에 대한 자세한 설명은 Site Filter 설치법에서 다루도록 하겠다.

■ Site Filter 설치

Site Filter로 설치시에는 수동설치 하여야만 한다. 윈도우 인스톨러나 스크립트를 이용해 설치하면 Default로 Global Filter로 설치되기 때문에 Site Filter로 두 번 작업해야 하는 경우가 생겨 더 번거롭기만 하다. 수동 설치를 이용한 Site Filter 설치법을 알아보자.

① 압축 해제 후 생성되는 Setup 폴더를 C:\Program Files\AQTRONIX WebKnight\KISA_1 과 같은 서버내의 로컬 폴더를 생성하여 복사한다.(단, 각 WebKnight 설치를 위한 유일한 폴더를 가져야 한다.)

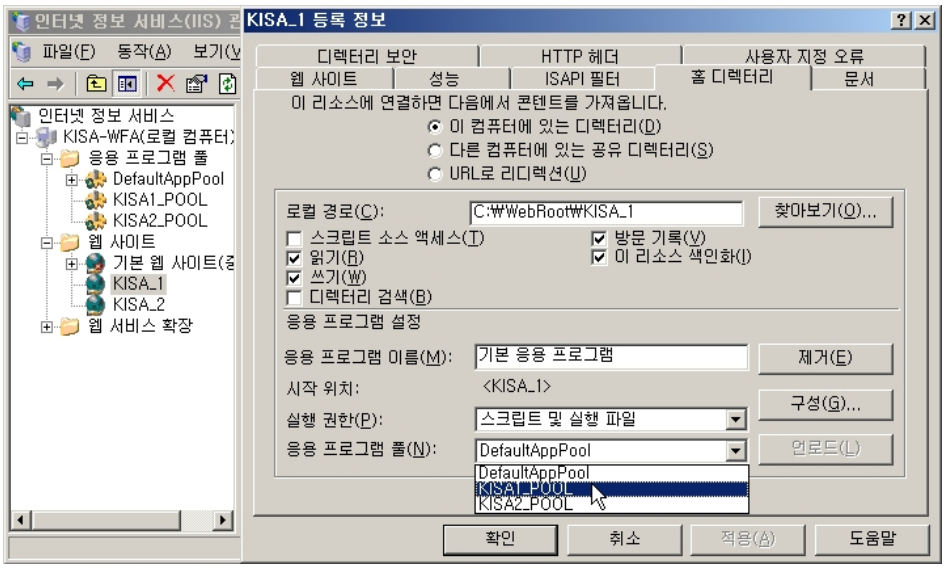
② 그 후 각 WebKnight의 Config.exe를 실행하여 WebKnight.xml을 불러온 뒤 “Global Filter Capabilities" 섹션에서 ”Is Installed As Global Filter" 옵션의 체크를 해제하고 저장한다. 또는 저장된 하나의 xml파일을 각 폴더에 일괄적으로 덮어쓰기 한다.

③ 각 WebKnight 폴더의 등록정보에서 "보안“ 탭에 ”NETWORK SERVICE" 계정을 추가하고 “쓰기” 권한을 부여해준다.

④ 인터넷 정보 서비스를 실행한다.

⑤ 각 개별 사이트의 “등록정보”를 클릭하여 “ISAPI 필터“ 탭에서 WebKnight필터를 등록한다.
ex) 필터 이름: WebKnight, 실행 파일 경로: C:\Program Files\AQTRONIX WebKnight\KISA_1\WebKnight.dll)

⑥ 그리고 “응용 프로그램 풀“에서 각각의 사이트 별로 풀(Pool)을 생성하여 매칭시킨다.



※ 주의 : 만약 AppPool을 동일하게 사용하게 되면 필터를 각 사이트별로 등록했더라도 정상적으로 사이트 필터링을 적용할 수 없다.

⑦ IIS를 재시작한다.

⑧ IIS 재시작 후 웹페이지를 브라우징 해주면 WebKnight가 로딩되었다는 로그가 생성되면서 정상작동 하게 된다.

3.2. WebKnight 제거

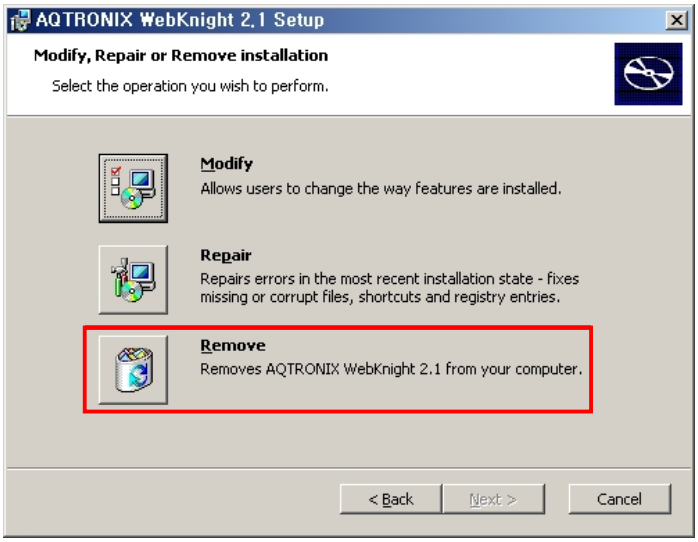
만일 WebKnight를 제거하고자 할 경우 설치방법과 마찬가지로 3가지 방법 중 하나를 선택하면 된다. WebKnight를 제거한 후에는 반드시 IIS를 재시작 해준다.

▷ 윈도우즈 인스톨러를 이용한 자동 제거

설치시 이와 같은 방법으로 설치하였다면 제거도 같은 방법으로 하면 된다. 설치 원본 파일중에 WebKnight.msi를 실행하면 아래 그림과 같은 화면이 뜨는데 “Remove"를 선택해주면 자동으로 필터까지 제거해 준다. 그동안 생성된 로그 파일은 삭제되지 않는다.

디폴트 경로에 설치되어 있는 경우도 마찬가지로 제거하면 된다.

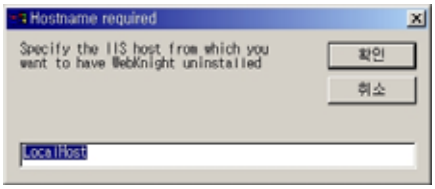
Default) C:\Program Files\AQTRONIX WebKnight\



▷ VB 스크립트를 이용한 자동 제거

VB스크립트를 이용하여 설치하였을 경우엔 Uninstall.vbs를 실행하여 제거하면 된다.
디폴트 경로에 설치되어 있는 경우도 마찬가지로 제거하면 된다.

Default) C:\Program Files\AQTRONIX WebKnight\

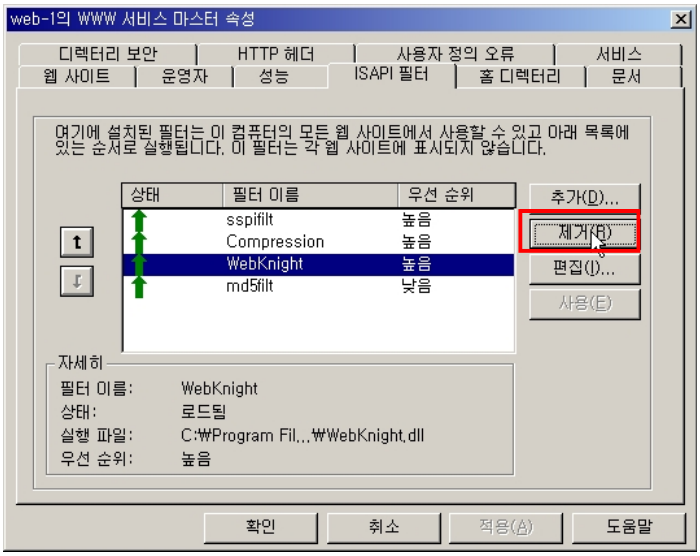


< 제거할 호스트명 >

< 제거 완료 >

▷ 수동 제거

수동 설치과정과 마찬가지로 인터넷 정보 서비스를 열고 글로벌 필터 또는 사이트 필터에 따라 서버 이름 또는 사이트 이름을 선택한 후 "등록정보"에서 "ISAPI 필터" 탭을 선택하여 WebKnight 항목을 선택한 후 "제거" 버튼을 누르면 된다.



상기와 같이 WebKnight를 제거한 후 변경사항을 반영하기 위해서는 IIS를 재가동하여야 한다.

4. 설정 최적화

4.1. Config과 LogAnalysis를 이용한 최적화

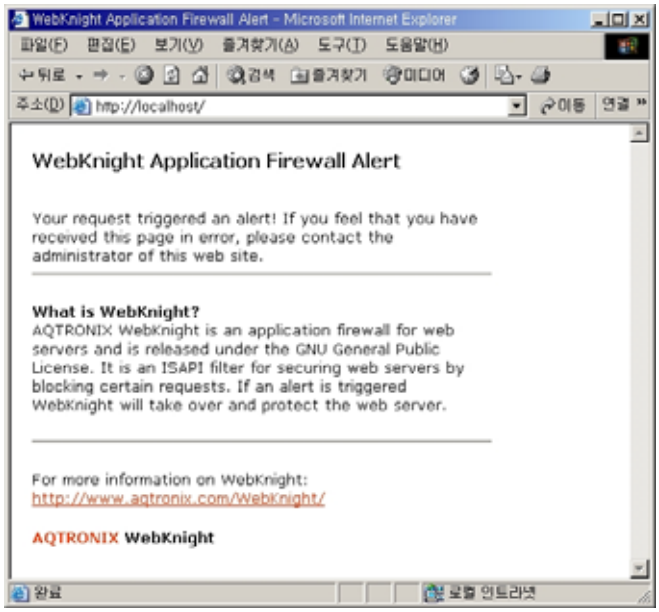
WebKnight는 SQL Injection 공격차단, 허용하지 않는 파일 또는 확장자에 대한 접속 차단 등 웹 공격에 대해 대단히 다양한 차단기능을 제공해 주고 있다. 또한 기본적으로 이러한 차단기능이 설정되어 설치와 동시에 적용이 되는데 이 차단기능이 정상적인 웹 접속을 차단할 수도 있다. 따라서 설치이후 자신의 웹사이트 환경에 맞게 적절하게 최적화하는 과정을 반드시 거쳐야 한다. 실제 설치보다는 최적화에 많은 노력과 시간을 들여야만 한다. 설정과정을 통해 오히려 웹 공격의 다양한 패턴을 익힐 수 있는 기회도 될 수 있을 것이다.

먼저, WebKnight 설치 이후 해당 웹사이트에 접속해서 정상적으로 웹요청 및 응답이 이루어지는지 확인을 하고, 접속이 차단될 경우 WebKnight의 로그를 참조하여 어떠한 룰에 의해 요청이 차단되었는지 찾아 이 룰을 수정하여야 한다.

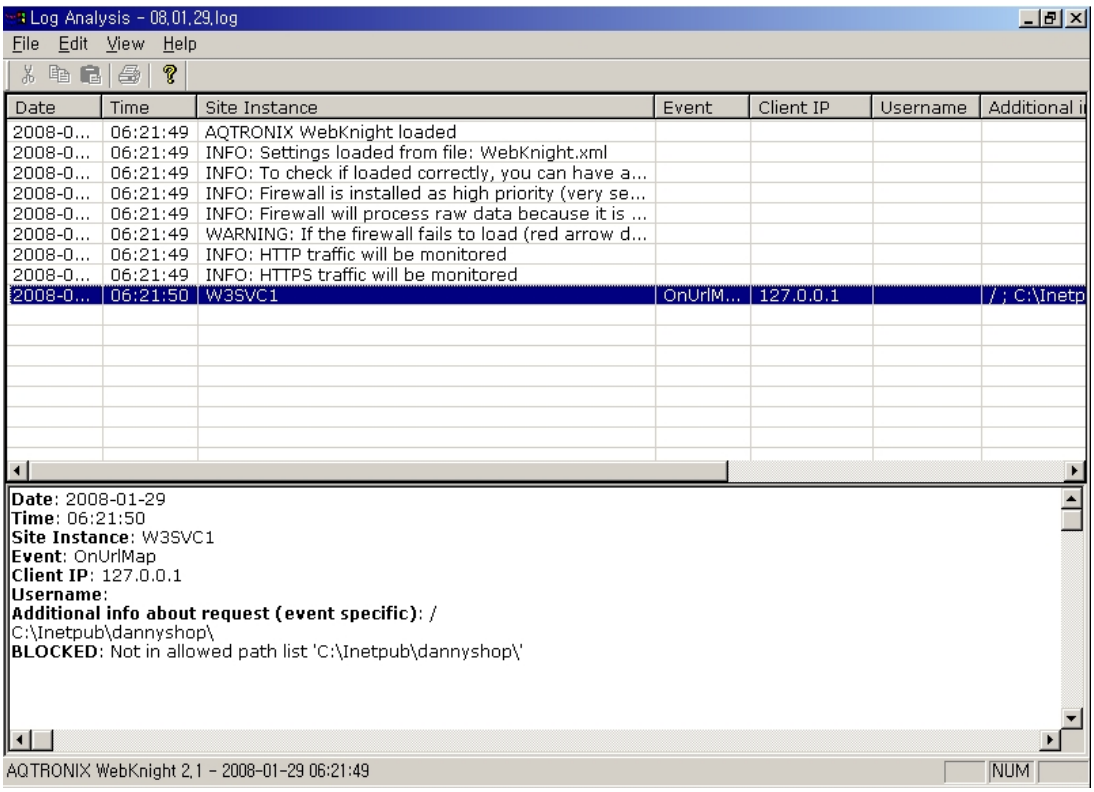
디폴트 설치시 로그파일의 위치와 설정프로그램, 설정 파일은 다음과 같다.

- o 로그파일 : C:\Program Files\AQTRONIX WebKnight\LogFiles\YYMMDD.log
- o 설정프로그램 : C:\Program Files\AQTRONIX WebKnight\Config.exe
- o 설정 파일 : C:\Program Files\AQTRONIX WebKnight\WebKnight.xml
- o WebAgents Database : C:\Program Files\AQTRONIX WebKnight\Robots.xml

설정파일은 차단 정책(룰)파일 이라고도 부른다. WebKnight를 설치 후 기본 룰이 적용된 상태에서 웹사이트 접속 시 다음과 같은 경고 화면이 뜰 수 있다.



이 화면은 WebKnight에서 필터 룰에 의해 차단을 시킨 후 접속자에게 보내는 기본 경고화면이다. 정상적인 웹 요청을 했는데도 불구하고 이와 같이 차단된다면 로그파일을 열어 “BLOCKED" 메시지를 확인하고 어느 룰에서 차단되었는지 찾아 설정파일에서 이를 수정해야 한다. WebKnight는 2.0 버전부터 로그분석기를 제공해주고 있는데 설치폴더 내에 LogAnalysis.exe를 실행하면 자동으로 로그 파일들을 불러오거나 선택할 수 있고 로그를 분석하는데 좀 더 용이하게 해준다.



위의 화면을 보면 정상적인 웹 접속이 차단되어 로그파일을 분석해 보니 다음과 같은 로그가 남았다.

2008-01-29 ; 06:21:50 ; W3SVC1 ; OnUrlMap ; 127.0.0.1 ; ; / ; C:\Inetpub\dannyshop\ ;
BLOCKED: Not in allowed path list 'C:\Inetpub\dannyshop\'

기본적인 로그파일의 각 필드는 다음과 같다.

Time ; Site Instance ; Event ; Client IP ; Username ; Additional info about request(event specific)

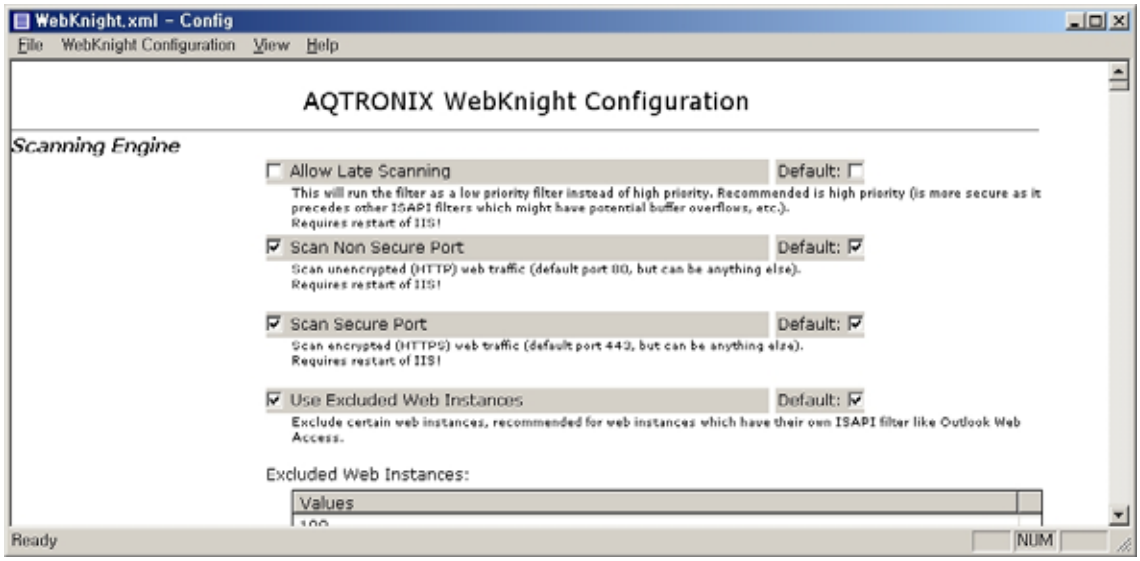
이 외에도 룰 설정의 "Logging" 섹션에서 추가적으로 항목을 구성할 수 있다.

위의 로그를 보면 "C:\Inetpub\dannyshop" 이라는 폴더에 대한 접속이 허용되지 않도록 설정이 되어 있어 차단된 것이다. 이처럼 White List 필터링 방식으로 허용할 사항들만 키워드를 등록하여 사용할 수도 있다. 불필요한 폴더로의 접근은 거부하는 등 웹서버에 대한 보안을 강화시킬 수 있는 옵션이 다양하게 구현돼 있다.

다음 FAQ에는 WebKnight의 설치와 환경설정, 로그파일 분석시 자주 발생될 수 있는 문제와 궁금증에 대해 질의·응답식으로 정리되어 있으므로 참고하기 바란다.

http://www.aqtronix.com/?PageID=114

로그파일 해석 시 기본 설정의 로그 시간대는 GMT/UTC로 한국 시간대인 GMT+09 보다 9시간 늦으므로 로그 분석 시 이를 감안하여야 한다.(설정에서 "USE GMT"를 체크하지 않음으로써 시스템 시간과 동기화시킬 수 있다.)



Config.exe를 통해 WebKnight의 다양한 필터링 기능을 설정할 수 있는데 다음과 같은 설정을 할 수 있다. 룰 설정 시 웹서버 관리자가 유의해야 할 사항도 포함되었으니 "확인 사항"을 참고하기 바란다.

구 분	기 능	확인 사항
Scanning Engine	암호화 포트(HTTPS), 비암호화 포트(HTTP)에 대한 모니터링, 웹 인스턴스나 IP에 대한 제외여부 등 설정	
Incident Response Handling	필터가 일치했을 경우 WebKnight의 응답방식을 제어한다. Default로 정의된 파일을 보여줄 것인지 사용자 정의 파일로 바꿀 것인지 로그만 남길 것인지 등의 제어가 가능	최초 설치시 "Log Only" 모드로 룰 최적화
Logging	로깅 여부, 로그 시간대, 로그 항목(클라이언트 IP, 사용자 명 등) 등을 설정	Use GMT: Disable Client Error, Server Error: Disable
Connection	IP를 모니터링하거나 차단, 요청의 제한 등을 설정	
Authentication	시스템의 인증 및 계정, 패스워드 설정 등에 대해 설정하고 Brute force에 대해서 거부하는 등의 동작	
Request Limits	컨텐츠 길이, URL 길이, 쿼리스트링 길이 등을 제한	
URL Scanning	URL Encoding 공격, 상위 경로(../), URL 백슬래쉬(\), URL 인코딩(%), 특정 URL 스트링 등 URL 관련 모니터링 및 차단	"URL Denied Sequences" 항목 확인 필요
Mapped Path	Directory Traversal 공격, 백슬래쉬(\) 등 허용하지 않을 문자 및 로컬 시스템내의 허용할 경로 정의	"Allowed Paths"에서 웹App가 있는 위치 확인 및 지정 필요

구 분	기 능	확인 사항
Requested File	차단시킬 파일의 문자열과 키워드 목록, 차단·허용할 파일 확장자 등을 정의	정상적인 요청이 차단될 수 있으므로 반드시 확인필요
Robots	자동화된 로봇, 봇 에이전트 등에 대한 차단 동작을 설정	추가로 Robots.xml이 있다.
Headers	서버 헤더 정보 변경, 특정 헤더 차단 및 헤더에서의 악의적인 동작 등에 대한 차단 등 설정	
Referer	외부의 불필요한 링크나 트래픽에 대한 제한, 특정 도메인에 대한 제한 등에 설정	
User Agent	웹서버로 접속하는 브라우저 등의 Agent에 대해 차단 및 허용 여부를 설정	Robots.xml을 통해 세부설정 가능
Methods	허용 또는 차단할 Method를 결정(예 : GET, HEAD, POST은 허용하고 DELETE, PUT 등은 차단)	
Querystring	특정 query 스트링(xp_cmdshell, cmd.exe 등) 차단, query 스트링에서 SQL Injection 차단 등 설정	
Global Filter Capabilities	글로벌 필터 적용 여부, POST 값에서의 특정 스트링(xp_cmdshell, cmd.exe 등) 차단 등을 결정	POST 값에 대한 필터링 여부와 IIS버전에 따른 옵션 해제
SQL Injection	SQL Injection 공격에 이용되는 키워드 정의 (‘, ;, ’select’, ‘insert’ ‘xp_’ 등)	공격에 이용될 수 있는 수십개의 키워드가 정의되어 있으나 확장저장프로시져의 사용 유무 등을 고려하여 추가/삭제 필요
Web Applications	WebDAV, IISADMPWD 등 웹어플리케이션의 허용유무 결정	기본적으로 모두 사용하지 않는 것으로 설정되어 있음

※ : WebKnight 2.x 로 업데이트 되면서 추가된 사항

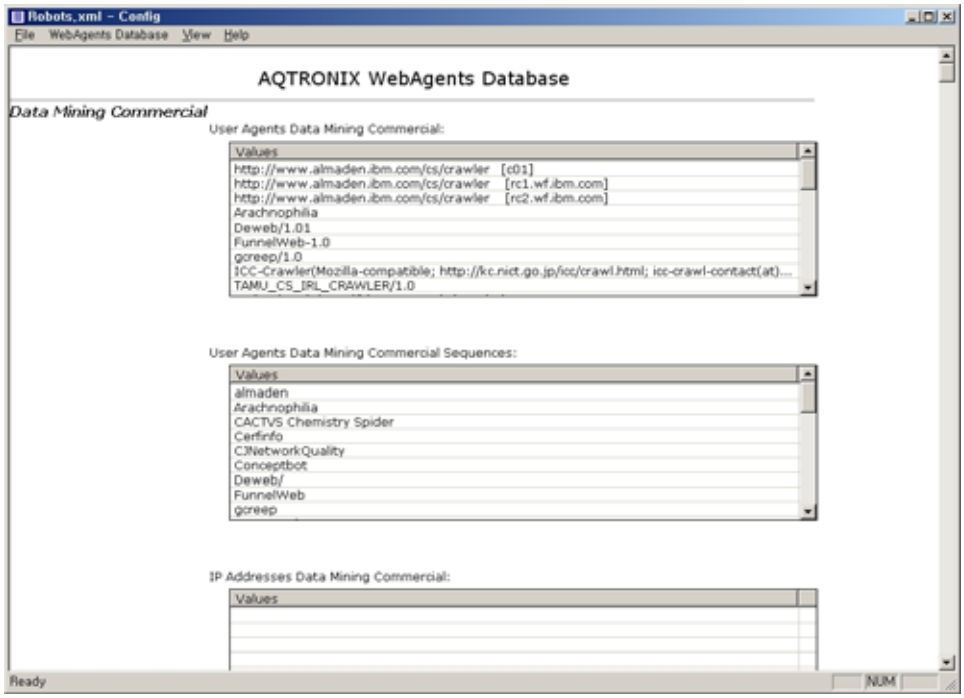
위 대부분의 옵션은 IIS의 재시작 없이 바로 적용이 되지만 일부 항목은 재시작이 필요한 옵션이 있으므로 각 옵션 하단의 코멘트를 확인하여 IIS나 Firewall의 재시작이 필요한 경우엔 재시작을 해줘야만 정상 적용이 된다. 만약 최초 설치했을 때의 설정으로 돌아가고 싶다면 WebKnight.xml 파일을 삭제한 뒤 IIS를 재시작 해주면 최초 Default 설정을 갖는 WebKnight.xml 파일이 새로 생성된다.

참고로, 앞서 설치과정에서 설명했듯이 IIS 6.0에서는 POST Method를 사용하는 인자 값 필터링을 위해서 IIS5.0 격리모드로 설정해야 한다.

4.2. Robots.xml

WebKnight 2.0부터 지원되는 기능 중에 Robots.xml을 이용한 User-Agent의 감시 기능이 있다.

WebKnight 설치폴더에 함께 포함되어 있는 Robots.xml파일은 WebAgents Database 파일로써 악성 봇이나 사용자가 지정한 Agent 들에 대하여 차단할 수 있다.



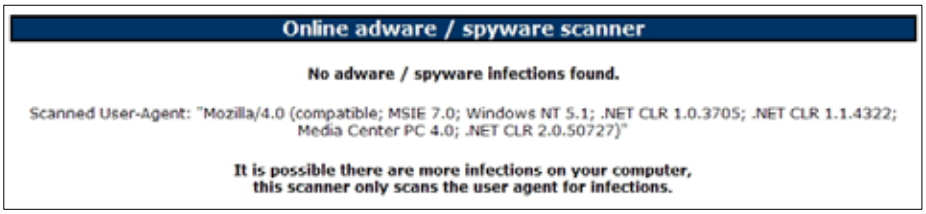
이러한 Robots.xml 파일은 수시로 업데이트 되기 때문에 AQTRONIX 홈페이지에서 최신 Robots.xml 파일을 다운받아 업데이트 하는게 좋다. Robots.xml 파일에 의해 차단이 될 경우엔 다음과 같은 로그가 남는다.

BLOCKED: User Agent not allowed

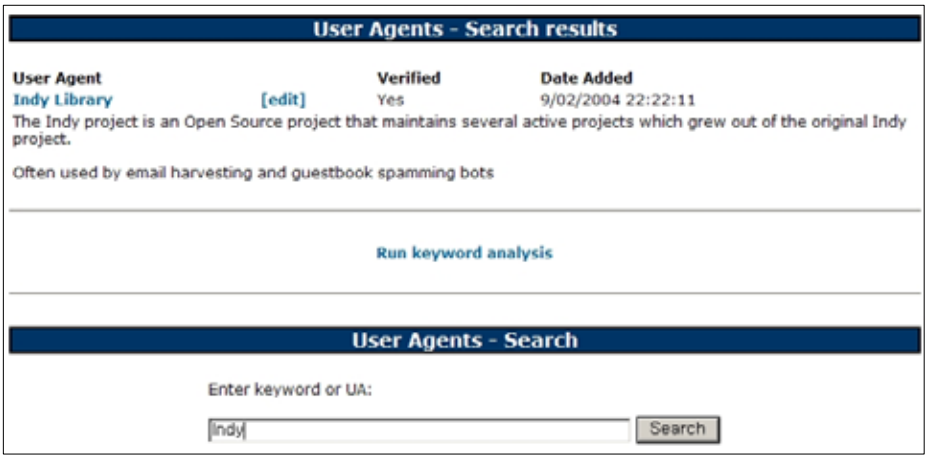
BLOCKED: '[token]' not allowed in User Agent

자신의 Agent나 차단된 Agent가 어떤 특성을 가지고 있는지 알고 싶을 때에는 아래의 URL에서 확인할 수 있다.

o 자신의 Agent 확인
http://www.aqtronix.com/research/agents/?Action=ScanUserAgent



o Agent 검색
http://www.aqtronix.com/research/agents/?Action=ShowSearch



사용자가 Agent를 추가할 수도 있으며 적당한 카테고리에 “Insert Item" 을 이용하여 키워드를 입력하면 된다.

현재 Robots.xml 파일의 DataBase 현황은 다음과 같다.('08. 6. 19 기준)

총 27가지로 분류되어 데이터 채집 및 e-mail주소 수집, 방명록 스패머 등의 알려진 악성 봇이나 Agent 들의 Database를 제공하여 주기 때문에 홈페이지를 수시로 확인하여 업데이트를 해주는 것이 좋다.

o Robots.xml 업데이트
http://www.aqtronix.com/downloads/WebKnight/Robots/Robots.xml

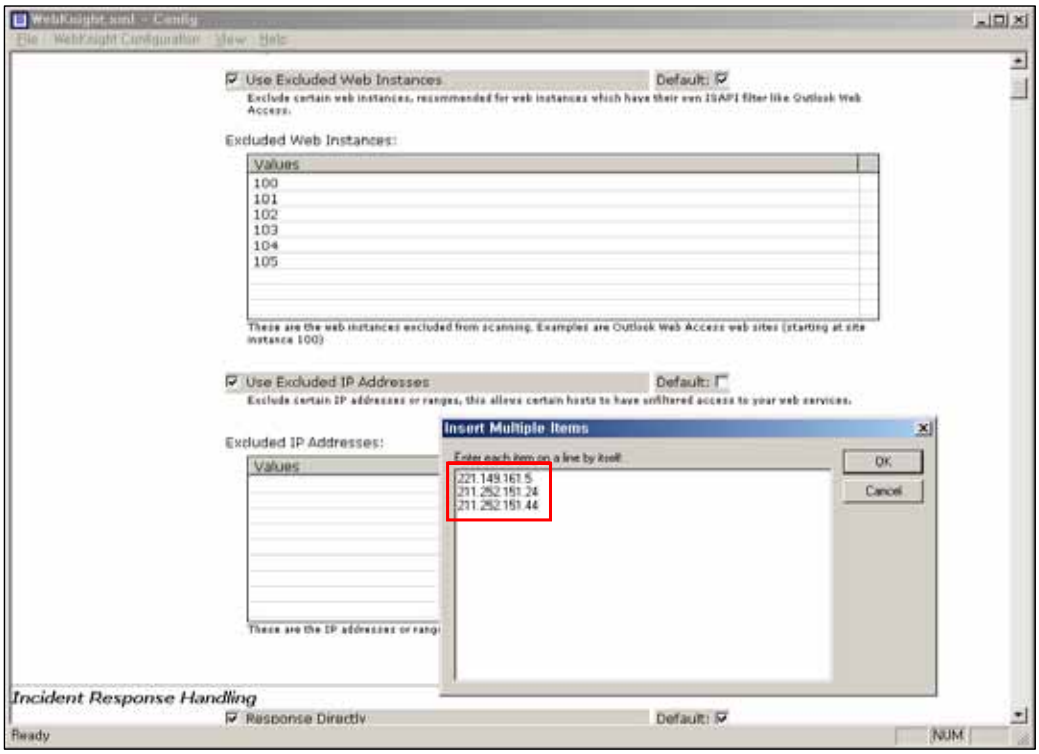
4.3 트래픽 감사 예외 IP 설정

외부에서 취약점 점검이나 모의 해킹 등을 수행 할 때에는 점검 트래픽과 공격트래픽이 거의 유사하기 때문에 공격으로 탐지되어 차단된다. 그러므로 이러한 진단작업을 진행하기에 앞서, 감사 예외 IP로 설정하면 지정된 IP에 대해서는 차단조치하지 않기 때문에 정상적인 점검이 가능하다. 단, 예외 IP처리 기능은 버전 2.1이상에서만 지원된다.

다음은 본 설정방법을 설명하기 위한 예시 IP 목록이며 아래의 IP들에 대해 감사 예외 IP로 설정하는 방법을 알아본다.

① 221.149.161.5	② 211.252.151.24	③ 211.252.151.44

이 IP 목록을 WebKnight 설정 파일에서 Scanning Engine - Use Excluded IP Addresses 옵션을 Enable 한 뒤 아래 화면과 같이 등록해주면 된다. 또한 하나의 IP가 아니라 범위로 지정하고자 한다면 221.149.161.5/24 와 같이 CIDR표기법으로 설정하면 된다.

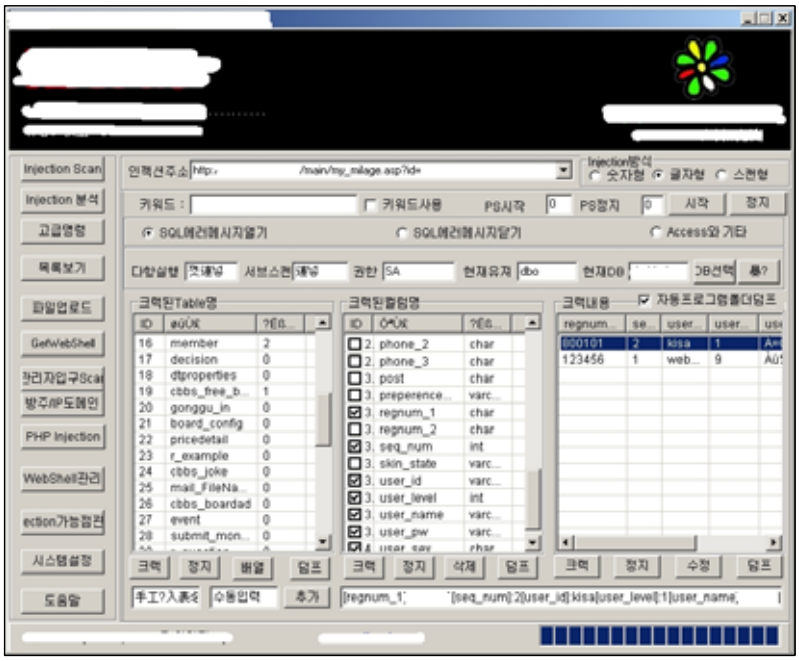


※ 이 기능은 WebKnight 2.1 이상 버전에서만 가능하기 때문에 하위 버전 사용자는 2.1 버전으로 업그레이드 해야만 사용할 수 있다.

5. 모의 공격 및 공격차단 확인

WebKnight의 설정 최적화를 완료 하였다면 얼마나 효과적으로 웹 공격에 대해 차단 해 주는지 확인해 볼 필요가 있다.

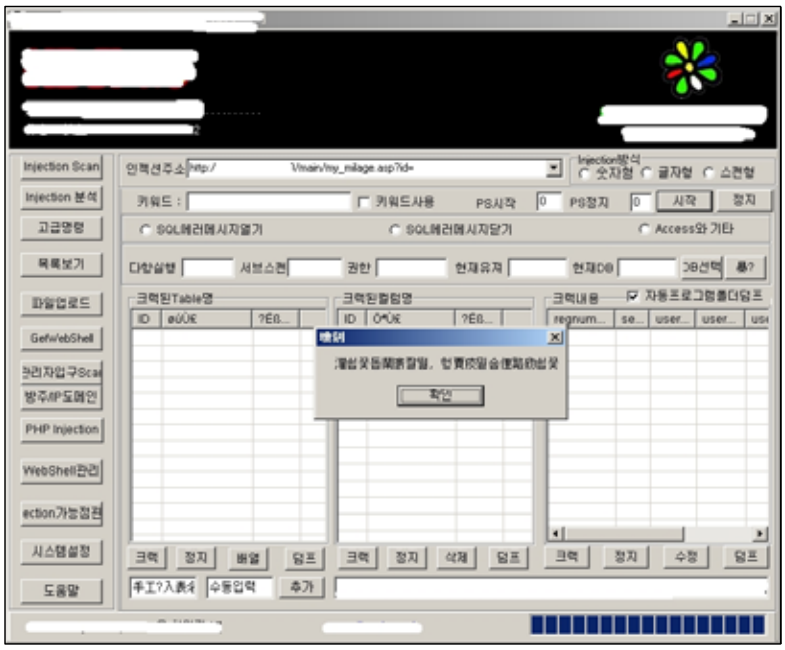
다음 그림은 WebKnight 설치 이전에 해당 웹서버가 SQL Injection 공격에 취약하여 공격툴에 의해 DB 접근이 가능하고 DB 계정 및 테이블이 노출되고 있는 화면이다.



그러나, WebKnight의 설치 이후 동일한 공격툴을 이용하여 테스트한 결과 공격은 실패하였으며, 다음과 같은 로그파일이 생성되었다.

```
16:29:38 ; W3SVC1 ; OnPreprocHeaders ; x.x.x.x ; ; HEAD ; /main/my_milage.asp ;
id=;create%20table%20t_XXX(XXX%20varchar(200)) ;
BLOCKED: Possible SQL injection in querystring ; HTTP/1.1 ; Mozilla/3.0 (compatible; Indy Library) ;
BLOCKED: User Agent not allowed ; BLOCKED: 'indy library' not allowed in User Agent
16:29:39 ; W3SVC1 ; OnPreprocHeaders ; x.x.x.x ; ; HEAD ; /main/my_milage.asp ;
id=%20And%201=1 ; HTTP/1.1 ; Mozilla/3.0 (compatible; Indy Library) ;
BLOCKED: User Agent not allowed ; BLOCKED: 'indy library' not allowed in User Agent
```

WebKnight는 SQL Injection이 가능한 문자열을 발견하였기 때문에 차단되었고 자동화 툴이 "Indy Library"라는 Agent를 사용하기 때문에 차단이 되었다. 다음은 차단된 공격 툴 화면이다.



이러한 SQL Injection 공격이외에도 취약한 CGI 공격, Directory Traversal 공격 등 다양한 웹 공격이 차단되는 것을 확인할 수 있었다.

WebKnight의 설치가 끝나고 제대로 동작하는지 테스트가 끝났다면 앞에서 언급한 것처럼 주기적으로 로그를 확인하면서 정상적인 서비스가 차단 되는지 오탐지 분석을 해야 한다. 또한 이러한 로그 분석을 통해 관리자는 여러 웹 공격 시도로부터의 적절한 대응 능력을 갖출 수 있어야 할 것이다.

지금까지 공개 웹방화벽인 WebKnight를 이용한 IIS 웹서버의 보안 강화에 대해 소개하였다. WebKnight를 실제 운용되고 있는 취약한 웹서버에 적용시켜 본 결과 훌륭한 공격 차단효과를 확인할 수 있었는데, 상용 웹 보안도구의 도입이 여의치 않은 중소규모의 웹사이트에서 유용하게 활용 할 수 있다.

웹 보안의 기본은 안전하게 코딩된 웹 프로그램에 있음을 명심하여야 할 것이다.
홈페이지 개발보안 가이드, 표준 웹어플리케이션 보안 템플릿 등을 참고하여 웹 어플리케이션 설계단계에서부터 안전하게 개발하는 것이 가장 우선시 되어야 할 것이고, 부가적인 보안 조치로 WebKnight를 활용하기 바란다.