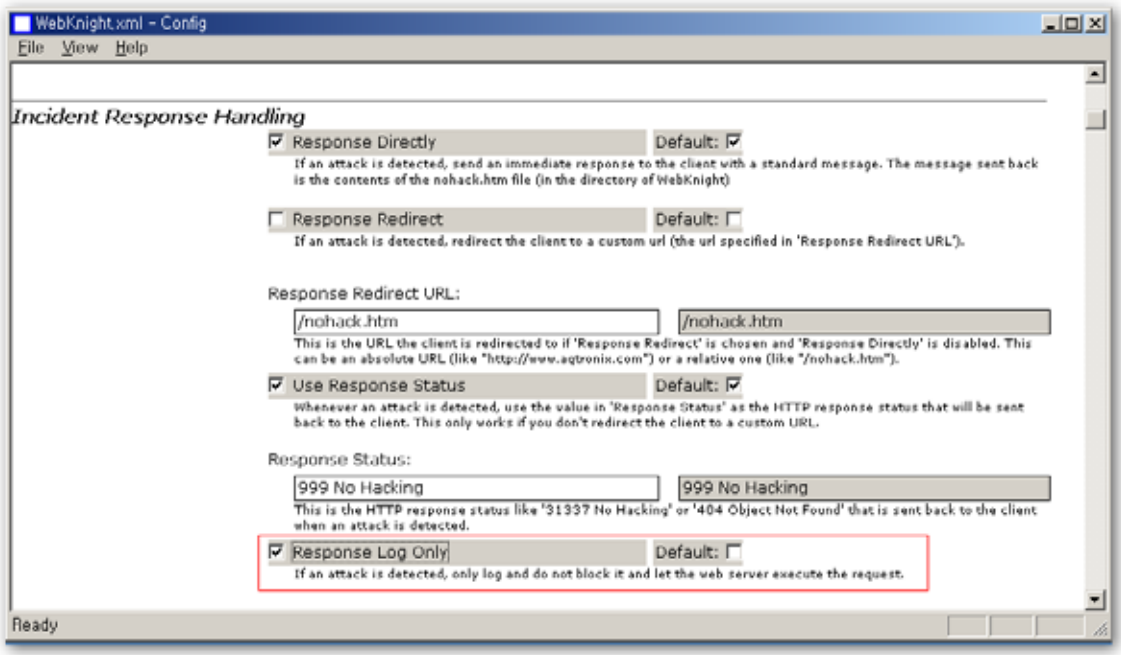
WebKnight 설치・운영 FAQ

Q. WebKnight 설치 후 정상적인 서비스 접속이 차단되고 WebKnight 경고창이 뜹니다.

A. WebKnight의 기본 설정은 상당히 엄격하게 되어 있어 정상적인 웹접속 요청이 차단될 수 있습니다. 따라서, 설치 후 WebKnight 설정을 로깅모드로 전환한 후 룰을 최적화 시키는 과정이 필요합니다.

먼저, Config.exe를 실행하여 「Incident Response Handling」 섹션의 "Response Log Only"를 enable 합니다. 이는 패턴이 일치하더라도 실제 차단시키지는 않고 로그만 남기도록 하는 것입니다. 로그파일에서 "BLOCKED" 메시지를 확인하여 정상적인 웹요청이 차단된 경우 해당 룰을 수정 또는 제거하시기 바랍니다. 일정시간동안 정상적인 웹요청이 차단되지 않음을 확인한 후 다시 이 부분을 disable하여 공격발생시 로그뿐만 아니라 실제 차단하도록 하십시오.

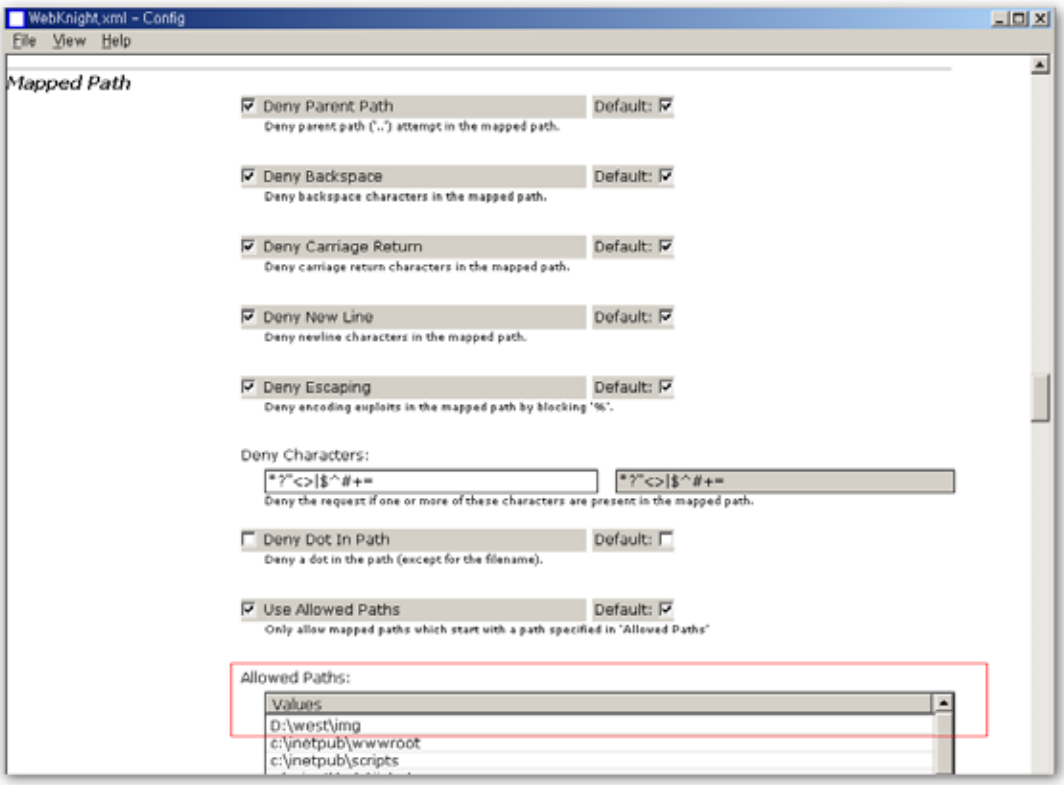


Q. WebKnight 설치 후에 홈페이지의 글자는 보이는데, 그림파일들은 보이지 않고 엑스(X) 형태의 박스로 뜹니다.

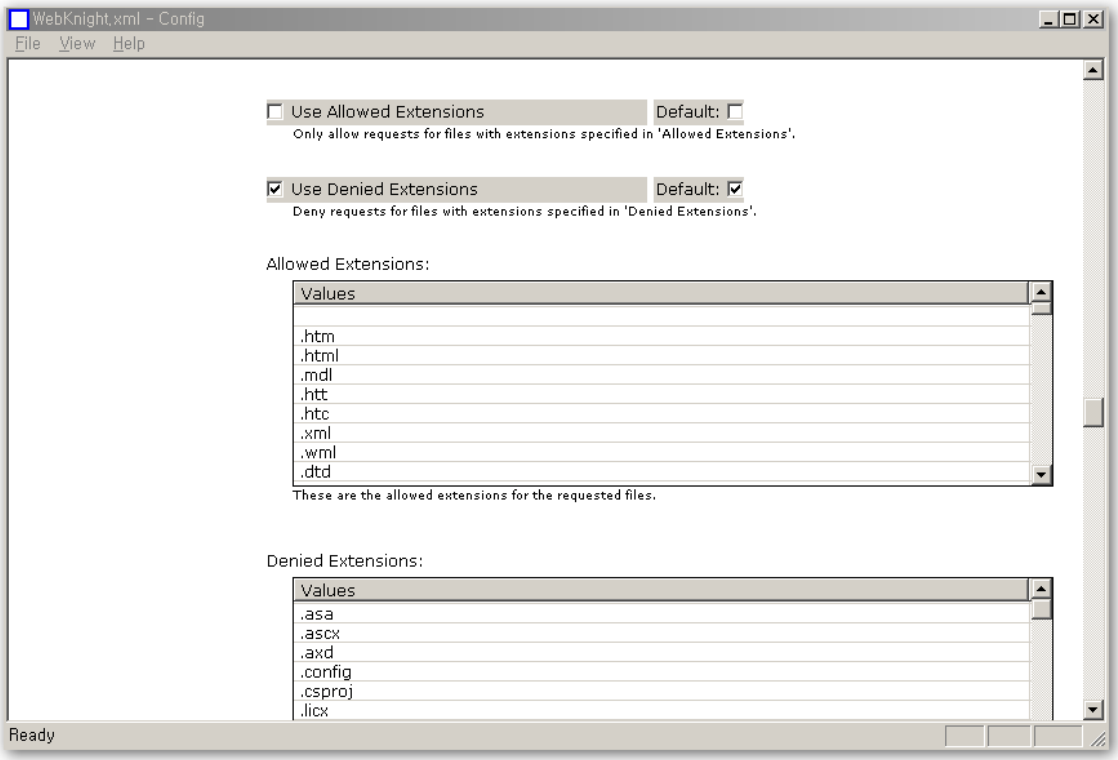
A. 그림파일들이 보이지 않는 것은 그림파일이 접근허용하지 않은 폴더에 위치하고 있거나, 허용하지 않는 확장자를 사용하고 있어 차단되었을 가능성이 높습니다. 허용하지 않는 Path를 사용할 경우 로그파일에 아래와 같은 차단로그가 기록됩니다.

05:41:52 ; W3SVC31 ; OnUrlMap ; xxx.xxx.98.86 ; ; /west/img/bb/abc.jpg ; D:₩west₩img₩bb₩abc.jpg ; BLOCKED: Not in allowed path list 'D:₩west₩img₩bb₩abc.jpg' ;

이 경우 「Mapped Path」 섹션의 "Allowed Paths" 리스트에서 그림파일이 위치한 Path를 등록하시기 바랍니다. WebKnight는 웹을 통해 접근을 허용하는 Path를 지정하고 그 이외의 폴더로 접근하고자 할 경우 모두 차단하고 있습니다. 이는 ../.. 등을 통해 웹 홈디렉토리 상위 폴더로 접근하고자 하는 다운로드 공격을 차단하기 위함입니다.



특정 파일이 열리지 않을 경우 해당 파일의 확장자가 차단되고 있는지 확인할 필요도 있습니다. WebKnight의 기본 설정은 차단하는 확장자를 지정하고 그 이외의 확장자를 가진 파일은 허용하고 있습니다. 차단된 파일의 확장자가 「Requested File」 섹션의 "Denied Extentions"에 포함되어 있는지 확인하십시오.



Q. WebKnight 설치 후 웹 접속 속도가 상당히 느려졌습니다.

A. 속도가 느려질 경우 룰 설정이 정상적인지 확인해 볼 필요가 있습니다. 가령 앞의 질의와 같이 일부 파일의 Path가 허용되지 않은 경우도 그림파일을 호출하기 위해 속도가 느려질 수가 있습니다. 일반적으로 중소규모의 웹사이트에서 정상적으로 WebKnight가 설치된 경우 다소의 접속지연은 있지만, 체감할 정도는 아닙니다. 로그파일 분석을 통해 룰을 다시 최적화시켜 보시기 바랍니다.

Q. WebKnight를 설치하였는데, ISAPI 필터에서 webknight.dll이 load되지 않았습니다. 정상적으로 설치되었는지 어떻게 확인할 수 있습니까?

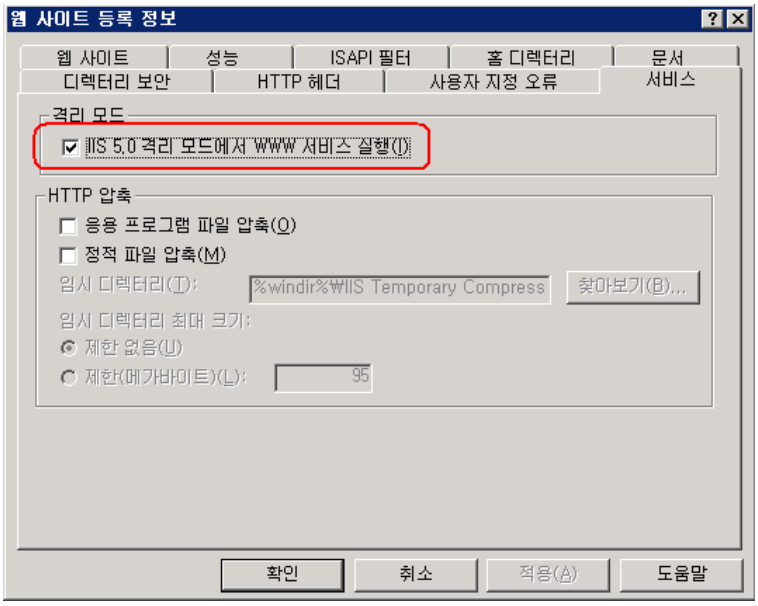
A. WebKnight 최초 설치 후에는 IIS 웹서버를 재가동(Reload)하여야 WebKnight가 load됩니다. 간혹, WebKnight가 정상적으로 운용이 되는데도 불구하고, ISAPI 필터에서 load되지 않았다고 나오거나 "알수 없음"으로 나오기도 합니다(특히, IIS 6.0에서 이러한 현상이 자주 나타나는 듯 합니다.). WebKnight가 로드되었을 경우 아래와 같이 로그파일에 "AQTRONIX WebKnight loaded"라고 로그를 남깁니다. 또한, 정상적으로 WebKnight가 운용되고 있는지는 로그파일에 차단

로그가 쌓이는지 확인하거나, 실제 공격하여 공격이 차단되는지 확인함으로써 정상 동작 여부를 확인할 수도 있습니다.

```
#Software: AQTRONIX WebKnight 1.3
#Date: 2006-10-18 00:39:22
#LogTime: GMT (Local-09:00)
#Fields: Time ; Site Instance ; Event ; Client IP ; Username ; Additional info about request (event specific)
00:39:22 ; AQTRONIX WebKnight loaded
00:39:22 ; INFO: Settings loaded from WebKnight.xml file
00:39:22 ; INFO: To check if WebKnight is loaded correctly, you can have a look at the currently loaded settings in the file 'Loaded.xml' (start config.exe and open this file).
00:39:22 ; INFO: Firewall is installed as high priority (very secure)
```

Q. IIS 6.0에서 글로벌 필터로 WebKnight가 설치되지 않습니다.

A. IIS 6.0에서 글로벌 필터로 구동하기 위해서는 “IIS 5.0 격리 모드”로 IIS를 구동하여야 합니다. IIS 6.0은 기본적으로 “작업자 프로세스 모드”로 구동이 되고 있는데 “IIS 5.0 격리 모드”로 변경할 경우에는 동일 환경의 테스트 서버에서 정상적으로 동작하는지 검증을 거치는 것이 바람직합니다. “IIS 5.0 격리 모드”로 변경하면 IIS의 재시작이 필요합니다.



Q. WebKnight 디폴트 설정으로 돌아가기 위해서는 어떻게 해야 하나요?

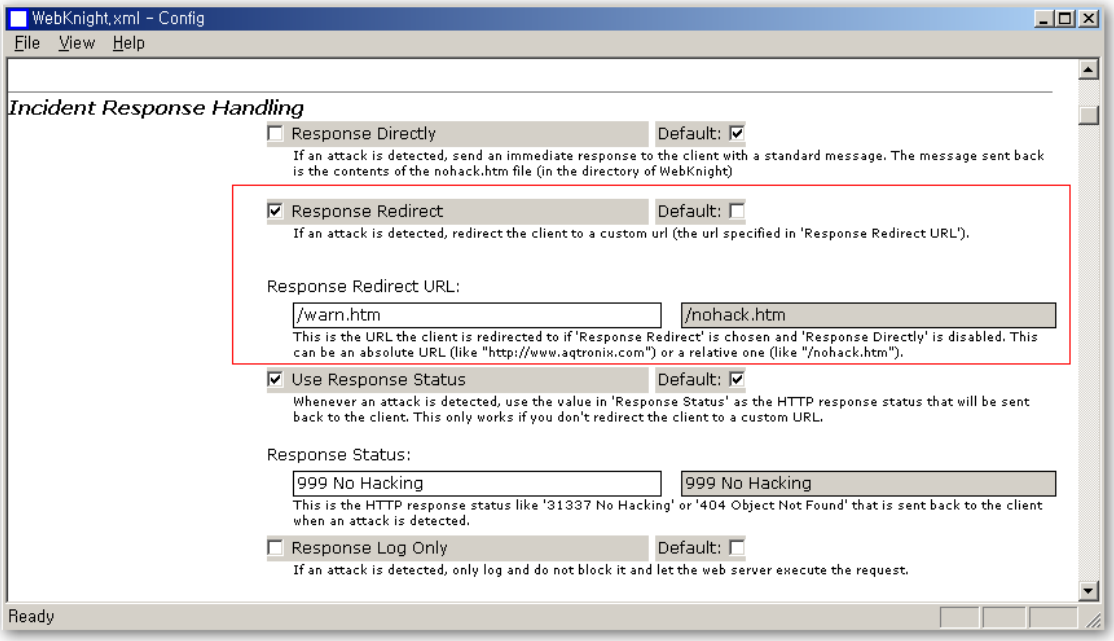
A. WebKnight 설치 폴더의 webknight.xml 파일을 삭제하고 웹서버를 재가동하면 됩니다. 웹서버 재가동시 디폴트 설정을 가진 webknight.xml 파일이 새로 생성됩니다.(http://www.aqtronix.com/?PageID=99#faq 참조)

Q. WebKnight 설정을 변경하였는데, 변경된 설정내용을 저장하였다가 이후에 다시 불러올 수 있나요?

A. Config.exe를 실행하여 "File" → "Save AS"를 통해 현재 WebKnight의 설정을 다른 이름으로 저장해 둘 수 있습니다. 추후 이 설정파일을 다시 사용하려면 이 파일을 webknight.xml로 파일 이름을 바꾸면 됩니다.

Q. WebKnight에 의해 차단될 경우 사용자들에게 "WebKnight Application Firewall Alert"이라는 제목의 경고창이 보여 주는데, 이 경고창을 보여주지 않거나 보여지는 화면을 바꿀 수 있습니까?

A. WebKnight는 공격 탐지시 기본적으로 WebKnight 설치 폴더에 있는 nohack.htm 파일을 띄워 줍니다. 공격자에게 WebKnight 설치 사실을 숨기거나 정상적인 접속이 차단될 경우 관리자에게 문의하게 하기 위하여 이 파일의 내용을 변경하거나 다른 파일이 띄워지게 할 수 있습니다. 경고창을 변경하기 위해서는 2가지 방법을 사용할 수 있습니다. 첫 번째 방법은 "Response Directly"를 enable 시키고 nohack.html 파일의 내용을 수정하는 것입니다. 두 번째 방법은 "Response Directly"를 disable, "Response Redirect"를 enable 시키고, "Response Redirect URL" 부분을 리다이렉션 하고자 하는 URL(절대경로 또는 상대경로)로 변경해 주는 것입니다.



Q. Config.exe를 통해서 룰 설정을 변경하였는데 반영되지 않는 듯 합니다.

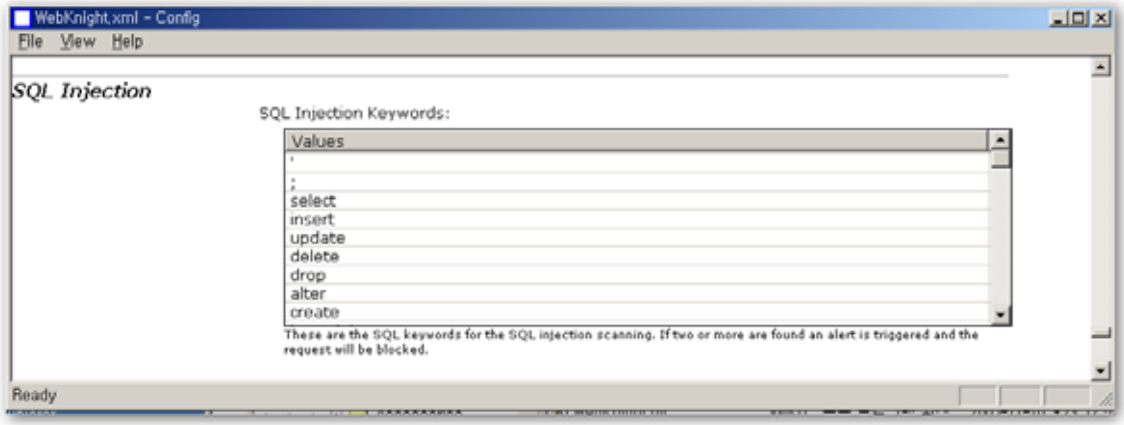
A. WebKnight는 자동으로 매 1분마다 변경된 설정 내역을 감지하여 반영합니다. 따라서, 룰 설정이 변경되더라도 변경내역이 실시간으로 반영되지 않을 수 있으나, 약 1분 이후에는 반영된 것을 확인하실 수 있을 것입니다.

Q. 룰 설정을 변경한 후에는 반드시 IIS 웹서버를 재가동하여야 합니까?

A. 대부분의 룰 설정은 IIS의 재가동이 필요없습니다. 하지만, 일부 변경시에는 IIS 웹서버 재가동이 필요한데, 이 경우에는 각 설정 부분의 주석에 재가동이 필요하다고 명기되어 있습니다.

Q. SQL Injection 공격 차단을 위한 패턴은 어디에 추가할 수 있습니까?

A. 「SQL Injection」 섹션에서 "SQL Injection Keywords"에 공격 키워드를 추가·삭제할 수 있습니다. WebKnight에서는 여기에 등록된 키워드 중 2개 이상이 발견될 경우 차단하고 경고창을 띄웁니다.


WebKnight.xml - Config
File View Help
SQL Injection
SQL Injection Keywords:
Values
'
;
select
insert
update
delete
drop
alter
create
These are the SQL keywords for the SQL injection scanning. If two or more are found an alert is triggered and the request will be blocked.
Ready