
공개 웹 방화벽

WebKnight 3.1 사용설명서

2013. 12

제·개정 이력

순번	날자	변경 내용	작성자	비고
1	2013. 5	개정	이재춘	WebKnight를 활용한 IIS 웹서버 보안 강화 안내서(2008) 다음버전
2	2013.12	WebKnight 3.1 버전 추가사항 변경	이재춘	

KISA는 본 문서의 WebKnight 및 해당 도구 개발사인 AQTRONIX社와 어떠한 관계도 없으며, 국내의 영세한 업체들의 웹 해킹 피해 예방을 위해 공개 웹 방화벽인 WebKnigt를 보안 참고용으로 소개합니다.

따라서 관련 문의나 기타 지원 요청은 AQTRONIX社에 직접 연락을 주시길 바랍니다.

[목 차]

1. 개요	1
2. WebKnight 소개	3
3. WebKnight 설치 및 제거	6
3.1. WebKnight 설치	6
3.2. WebKnight 제거	10
4. 웹나이트(WebKnight) 운영	11
4.1. WebKnight 기본동작	11
4.2. WebKnight 설정관리자(Config.exe)	14
5. KISA 웹 취약점 점검과 차단정책 설정	21
5.1. 웹 취약점 점검 소개	21
5.2. 웹 취약점 점검 결과보고서 설명	22
5.3. WebKnight 차단정책 설정	21

1. 개요

과거에는 해커의 공격이 웹 사이트 자체를 대상으로 하여 그 피해가 웹 서비스에 한정되었으나, 최근 들어 조직 전체를 장악하기 위한 진입점으로 악용하는 사례가 많아지고 있다. 해커는 장악한 웹 사이트를 개인정보, 민감정보 등 중요한 정보를 탈취를 위한 공격 거점 및 추가 공격을 목적으로 악성코드 유포에 이용하는 등 웹 사이트의 보안취약점을 악용한 공격이 지속적으로 발생하고 있다. 따라서 이러한 침해사고를 예방하기 위해서는 웹 사이트에 대한 보안을 더욱 강화할 필요가 있다.

웹 사이트의 보안취약점은 아래 2가지 방법으로 조치할 수 있다.

첫 번째는 웹서버, WAS 등 운영환경의 설정이나 해당 서버의 소프트웨어 업데이트하는 방법이다. 업데이트나 환경설정을 통한 보안취약점 조치는 비교적 간단한 방법으로 해결할 수 있는 부분이며, 기존에 배포된 많은 가이드라인 및 솔루션 제조사들을 통해 안전한 설정 방법을 확인할 수 있다.

두 번째는 사이트 소스코드 자체를 수정하는 방법이다. 소스코드 수정은 SQL 인젝션, 크로스사이트스크립팅 등 심각한 보안취약점들을 근본적으로 해결할 수 있으나, 비용과 인력 등이 많이 소요되기 때문에, 중소기업의 기업들이 수행하는 것은 쉽지 않다. 또한, 대기업이라 할지라도 빈번히 갱신하여야 하는 웹 환경에서 매번 시큐어코딩을 적용하는 것은 매우 어려운 일이다.

위와 같이 소스코드에 대한 수정이 어려운 환경에서 웹 방화벽(WAF : Web Application Firewall)은 웹 취약점 공격을 방어하기 위한 효과적인 대안이 될 수 있다. 웹 방화벽은 상용 웹 방화벽부터 공개 웹 방화벽까지 다양한 제품들이 출시되어 있으나, 공공기관이나 대기업 등은 상용 웹 방화벽 사용을 권장한다.

대표적인 공개 웹 방화벽은 KISA의 캐슬(CASTLE), ATRONIX社의 WebKnight, TrustWave社의 ModSecurity등이 있으며, 본 문서에서는 WebKnight 설치·사용 방법을 설명한다.

한국인터넷진흥원에서는 영세기업을 대상으로 무료 웹 방화벽에 대해 안내뿐 아니라, 홈페이지 원격 취약점 점검 또한 무료로 제공하고 있다.

자신의 웹 사이트에 맞는 웹 취약점 점검을 한 후, 그에 따른 웹 방화벽 정책을 설정 할 경우 보다 나은 웹 보안 환경을 구축 하는 데 도움이 될 것이다.

WebKnight는 GNU 공개 라이선스 원칙을 따르는 공개 소프트웨어로써 모든 기업이나 개인이 자유로이 사용할 수 있다.

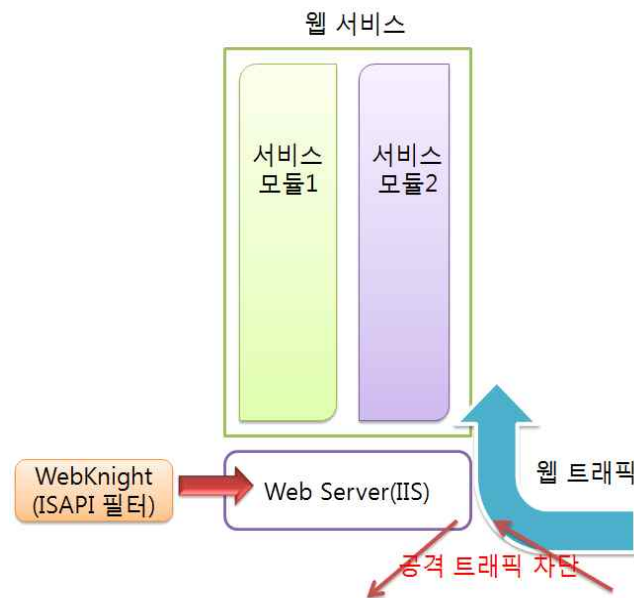
또한, WebKnight는 SQL Injection을 포함한 다양한 웹 공격에 대해 차단할 수 있는 프레임を提供해 주고 있고, IIS의 각 버전에 따라 별다른 문제없이 운영이 가능하여 보다 효과적으로 웹 서버 보안을 이룰 수 있다.

하지만, WebKnight의 잘못된 설정은 정상적인 웹 요청까지 차단할 수 있으므로 충분한 최적화 과정을 거쳐한다.

2. WebKnight 소개

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 보안 필터 사용으로 패턴 업데이트를 최소화하고 있다. 이러한 방법은 알려진 공격뿐만 아니라 알려지지 않은 공격에도 웹서버를 보호할 수 있다.



또한, WebKnight는 ISAPI 필터이기 때문에 다른 방화벽이나 IDS에 비해 웹서버와 밀접하게 동작 할 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 발생하는 사이트에서는 사전에 충분한 검증을 거친 후에 적용할 필요는 있다.

WebKnight 3.1은 2013년 7월 31일 기준으로 업데이트 되었으며, 관리자 기능이 웹 사이트 빌트인 형태로 추가되는 등 일부 기능이 추가되었다.

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

□ WebKnight 특징

○ 오픈 소스(Open Source)

WebKnight는 GNU, GPL(General Public License)를 따르는 Free 소프트웨어이다.

○ 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.

○ 최적화(Customizable)

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

○ 웹기반 어플리케이션과의 호환성

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

○ 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.

○ SSL 보호(SSL Protection)

다른 전통적인 방화벽과는 달리 WebKnight는 ISAPI 형태로 IIS의 일부로써 동작하기 때문에 HTTPS 상의 암호화된 세션들도 모니터링 및 차단할 수 있다.

○ 3rd-Party 어플리케이션 보호(Third-Party Application Protection)

WebKnight는 웹서버 보호뿐만 아니라 전자상거래 사이트 및 기타 사용자 웹사이트도 설정을 통해 보호할 수 있다.

○ RFC 규약(RFC Compliant)

WebKnight는 RFC를 따름으로써 Request 값을 스캔하기 위한 기능도 포함되어 있다.

- 낮은 보유 비용(Total Cost of Ownership)

WebKnight는 윈도우즈 인스톨러 패키지와 원격 설치 스크립트로 설치 가능해 사내에서 쉽게 WebKnight를 채택할 수 있다. 또한 WebKnight 설정을 바꾸기 위해 그래픽 사용자 인터페이스를 제공한다.

- 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.

□ WebKnight 3.0 이상 버전에서 추가된 특징

- 관리자 웹 인터페이스(Admin Web Interface)

관리 및 통계 등 웹 관리자 기능 추가하였다.

- 필터확장(ISAPI Extension)

IIS 5에서 원시 데이터 추가 필터 기능 추가, 아직 IIS 7에서는 지원하지 않는다.

- 사용자 에이전트(User-Agent)

비트 웹 코드 탐지, 특수 공백 및 스푸핑 탐지와 같은 기능이 사용자 에이전트에 일부 추가되어 검색을 제공된다

- 엔진향상(Improved Engine)

기본 정책에 일부 규칙을 추가하였으며, 사용자가 이 기능은 제외가능 하다.

- 64bit IIS에서 동작하는 32bit Webknight(32-bit on 64bit IIS)

64bit IIS에서 32bit용 Webknight 버전이 설치 가능하다.

- 웹사이트 별 설정(Settings per website)

웹 사이트 별로 설정이 가능하다

3. WebKnight 설치 및 제거

3.1. WebKnight 설치

안내서 설치환경

- 플랫폼 : Windows 2008 R2(윈도우 2008 x64)
- 웹서버 : IIS 7.0
- WebKnight 소스 디렉토리 : C:\Users\Administrator\Desktop\WebKnight
- WebKnight 기본 설치 디렉토리 : C:\Program Files\AQTRONIX WebKnight

① 아래 URL에서 WebKnight 3.1을 다운로드 받는다.

<http://www.aqtronix.com/?PageID=136>

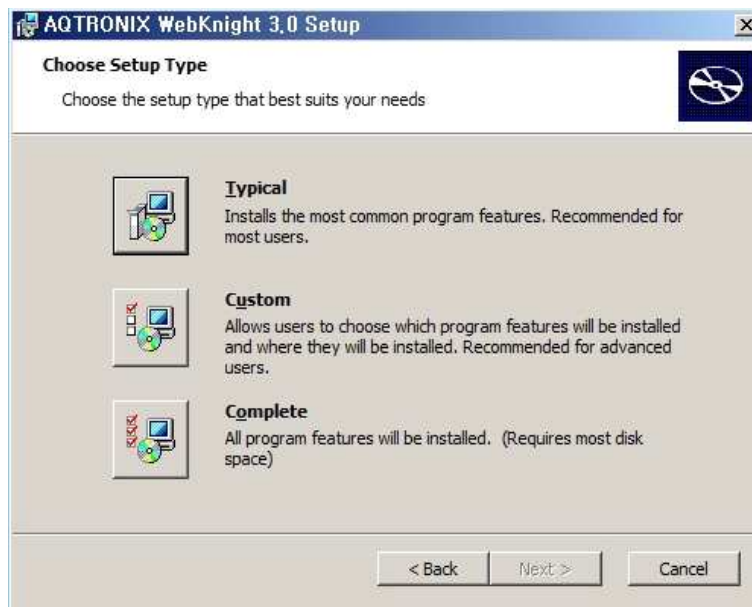
② 압축을 해제한 뒤 Setup폴더로 이동하면 아래와 같은 파일들이 생성된다.

이름	수정된 날짜	유형	크기
Config	2013-04-01 오전...	응용 프로그램	659KB
default	2013-03-28 오후...	ASP 파일	7KB
denied	2003-05-29 오후...	HTML 문서	2KB
GUI	2013-02-12 오전...	XSL 스타일시트	5KB
install	2010-12-28 오후...	VBScript 스크립...	7KB
ISAInstall	2012-11-30 오전...	VBScript 스크립...	9KB
ISAUninstall	2012-11-30 오전...	VBScript 스크립...	9KB
LogAnalysis	2013-04-01 오전...	응용 프로그램	669KB
Readme	2013-04-15 오전...	HTML 문서	15KB
robots	2012-02-26 오후...	ASP 파일	2KB
robots	2006-09-13 오후...	텍스트 문서	1KB
Robots	2013-04-01 오전...	XML 문서	345KB
uninstall	2010-12-28 오후...	VBScript 스크립...	5KB
WebKnight.32bit.dll	2013-04-04 오후...	응용 프로그램 확장	662KB
WebKnight.dll	2013-04-04 오후...	응용 프로그램 확장	845KB
WebKnight	2013-04-15 오후...	Windows Installer...	321KB
WebKnight	2013-04-04 오후...	XML 문서	100KB

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



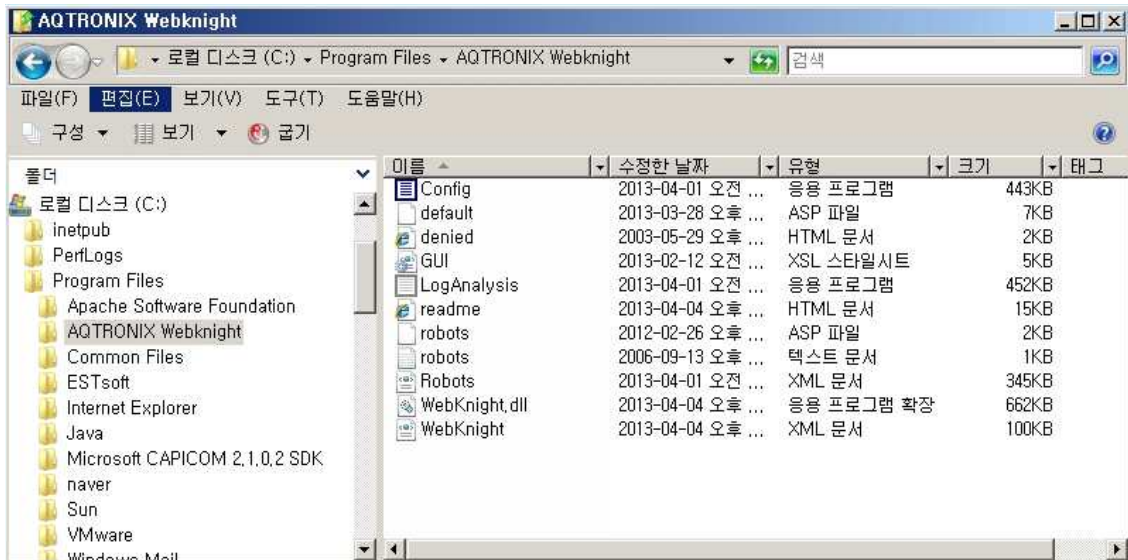
- ④ 라이선스 동의 후 설치 타입 선택화면이 나타나는데, "Typical"을 선택한다.



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



- ⑥ 기본 설치를 하게 되면 C:\Program Files\AQTRONIX Webknight\ 폴더에 WebKnight 설치가 된다. WebKnight.msi를 이용해 설치시 Default 경로로 설치가 되는 동시에 IIS에서 ISAPI Filter에 자동 등록된다.



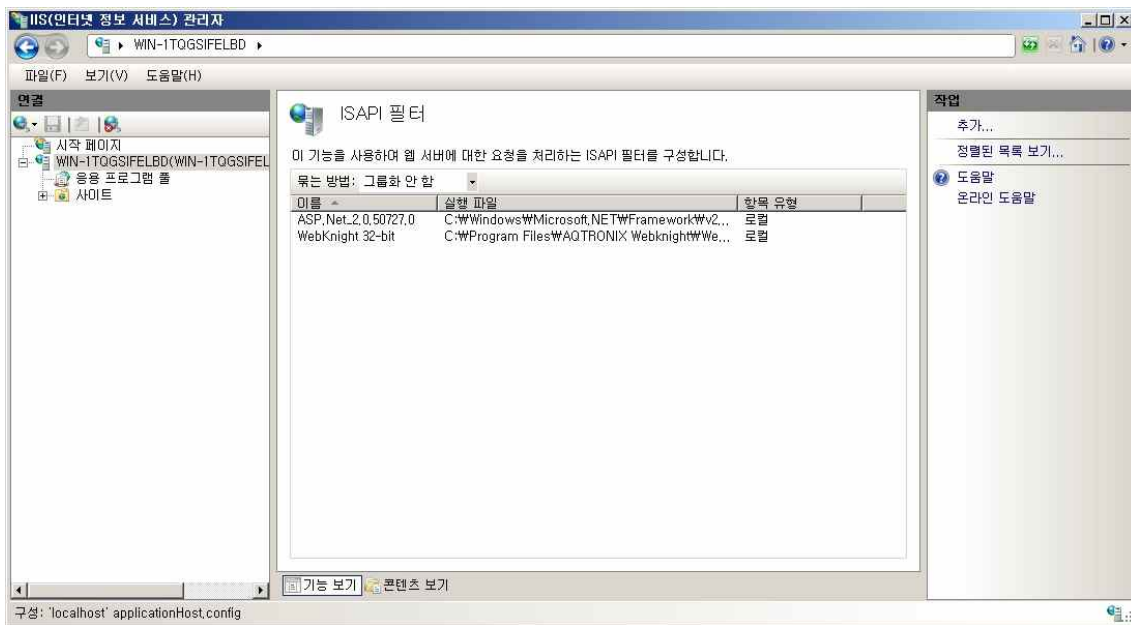
간단히 주요 파일의 특징은 아래와 같다

□ 주요파일 특징

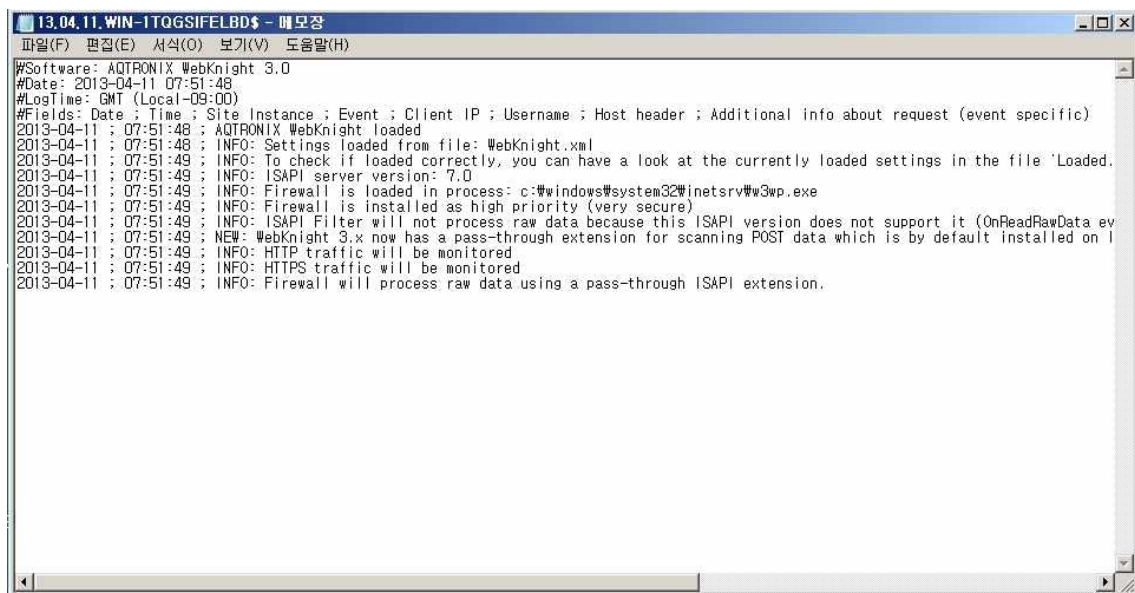
- Config.exe : WebKnight의 설정파일을 읽어 조작 할 수 있게 해주는 파일
- denied.htm : 설정에서 'Response Directly' 옵션을 통해 보이는 기본 차단 메시지
- LogAnalysis.exe : 로그 분석기
- Robots.xml : User-Agent에 대한 DB 파일
- WebKnight.dll : ISAPI Filter 파일, WebKnight가 실제 동작하는 파일
- WebKnight.xml : WebKnight 동작을 제어할 수 있는 설정 파일

- ⑦ IIS를 재시작 한다.

- ⑧ IIS 재시작 후에 관리자에서 정상적으로 설치가 완료되었을 경우 다음과 같이 IIS관리자에서 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 설치되었다는 등의 메시지가 기록되었다.

⑩ IIS 7.0 이상 환경에서 설치 시 (WebKnight.dll ISAPI필터)



IIS 7.0 이상의 환경에서는 Global Filter 기능을 지원하지 않기 때문에 체크를 해제해야 한다. 이로 인해, OnReadRawData 이벤트를 확인할 수 없어 POST 메소드의 Body에 포함된 공격을 탐지할 수 없는 한계가 있다.

3.2 WebKnight 제거

WebKnight를 제거한 후에는 반드시 IIS를 재시작 해준다.

설치 원본 파일 중에 WebKnight.msi를 실행하면 아래 그림과 같은 화면이 뜨는데 "Remove"를 선택해주면 자동으로 필터까지 제거해 준다. 그동안 생성된 로그 파일은 삭제되지 않는다.



4. WebKnight 운영

4.1. WebKnight 기본동작

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.

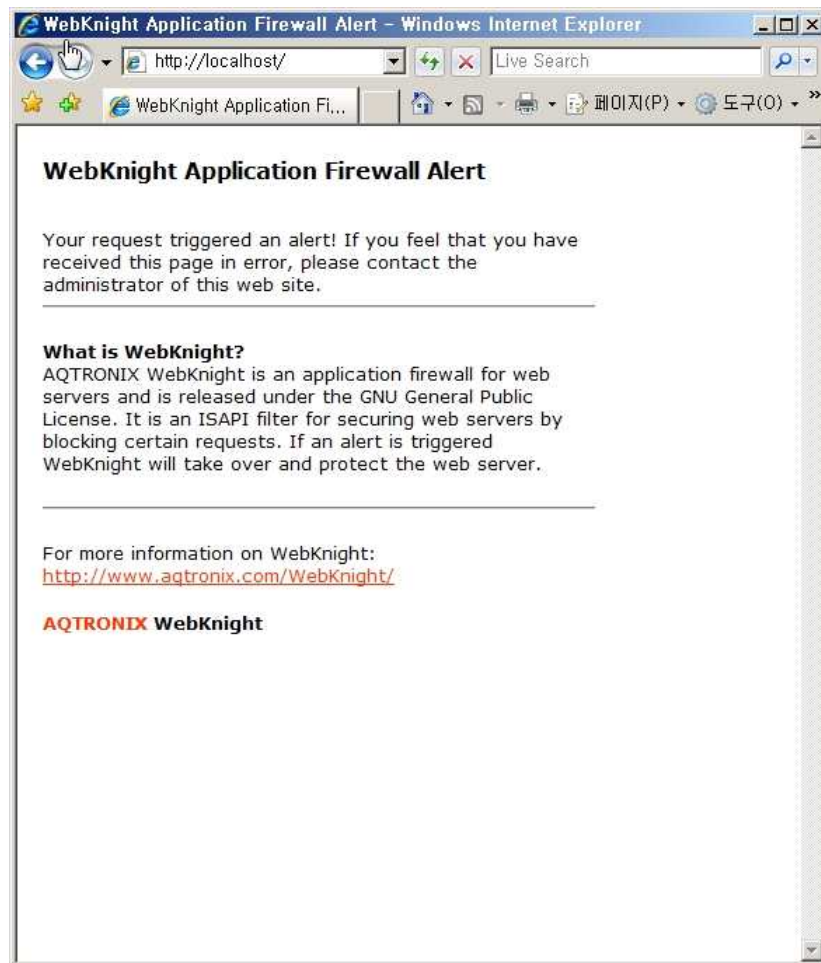
먼저, WebKnight 설치 이후 해당 웹사이트에 접속해서 정상적으로 웹 요청 및 응답이 이루어지는지 확인을 하고, 접속이 차단될 경우 WebKnight의 로그를 참조하여 어떠한 룰에 의해 요청이 차단되었는지 찾아 이 룰을 수정하여야 한다.

디폴트 설치 시 로그파일의 위치와 설정프로그램, 설정 파일은 다음과 같다.

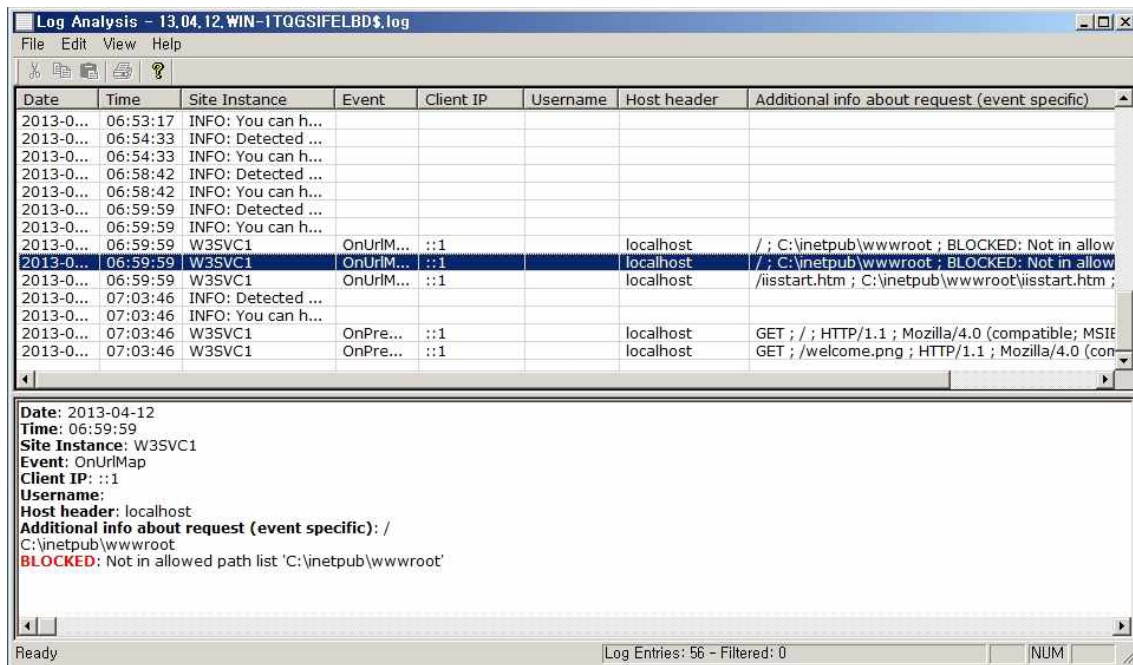
□ 주요프로그램

- 로그파일 : C:\Program Files\AQTRONIX WebKnight\LogFiles\YYMMDD.log
- 설정프로그램 : C:\Program Files\AQTRONIX WebKnight\Config.exe
- 설정 파일 : C:\Program Files\AQTRONIX WebKnight\WebKnight.xml
- 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 로그분석기를 제공하고 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.

2013-04-12 ; 06:59:59 ; W3SVC1 ; OnUrlMap ; ::1 ; ; localhost ; / ; C:\inetpub\wwwroot ; BLOCKED: Not in allowed path list 'C:\inetpub\wwwroot'

기본적인 로그파일의 각 필드는 다음과 같다.

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

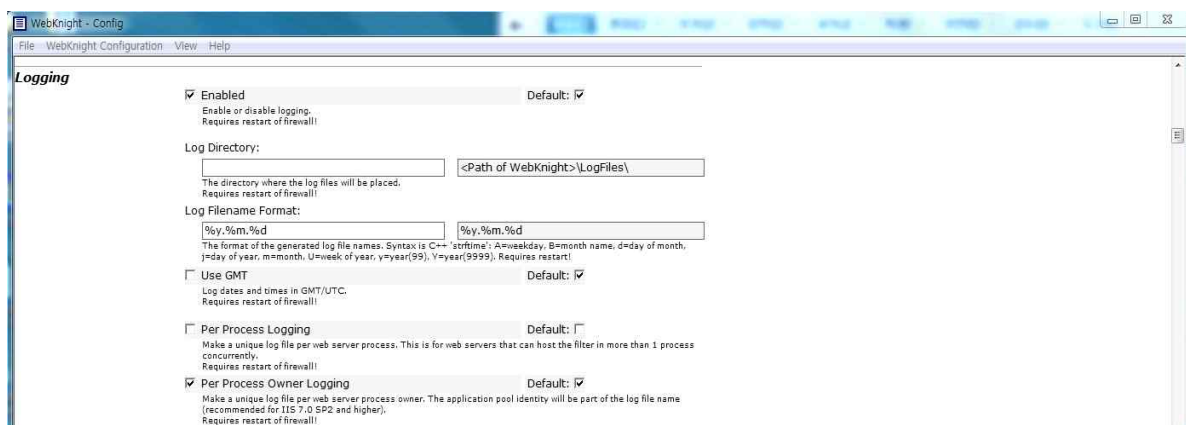
이 외에도 룰 설정의 "Logging" 섹션에서 추가적으로 항목을 구성할 수 있다.

위의 로그를 보면 "C:\inetpub\wwwroot" 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 분석 시 자주 발생할 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 9 시간 늦으므로 로그 분석 시 이를 감안하여야 한다.(설정에서 "USE GMT"를 체크하지 않음으로써 시스템 시간과 동기화시킬 수 있다.)

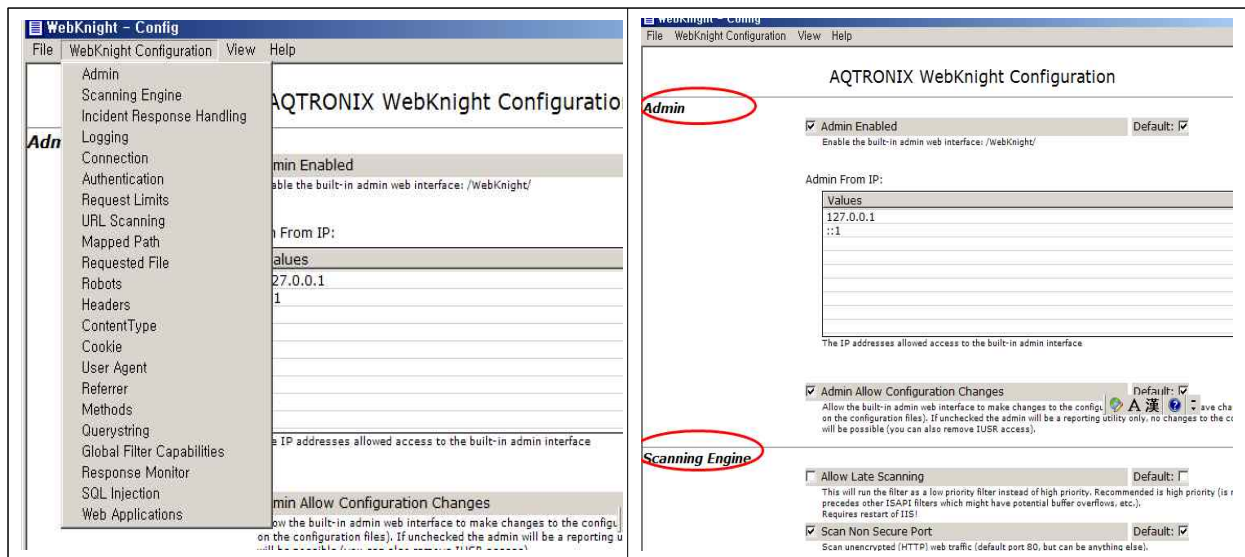


4.2. WebKnight 설정관리자(Config.exe)

설정 파일은 WebKnight.xml로 XML 파일 형태로 작성이 되며, WebKnight 설치시 인스톨 되는 설정관리자(Config.exe)를 사용하면 각종 정책을 보다 쉽게 관리할 수 있다.



WebKnight.xml 파일을 Config.exe로 실행할 경우 WebKnight Configuration에 각각의 정책 항목을 볼 수 있다.



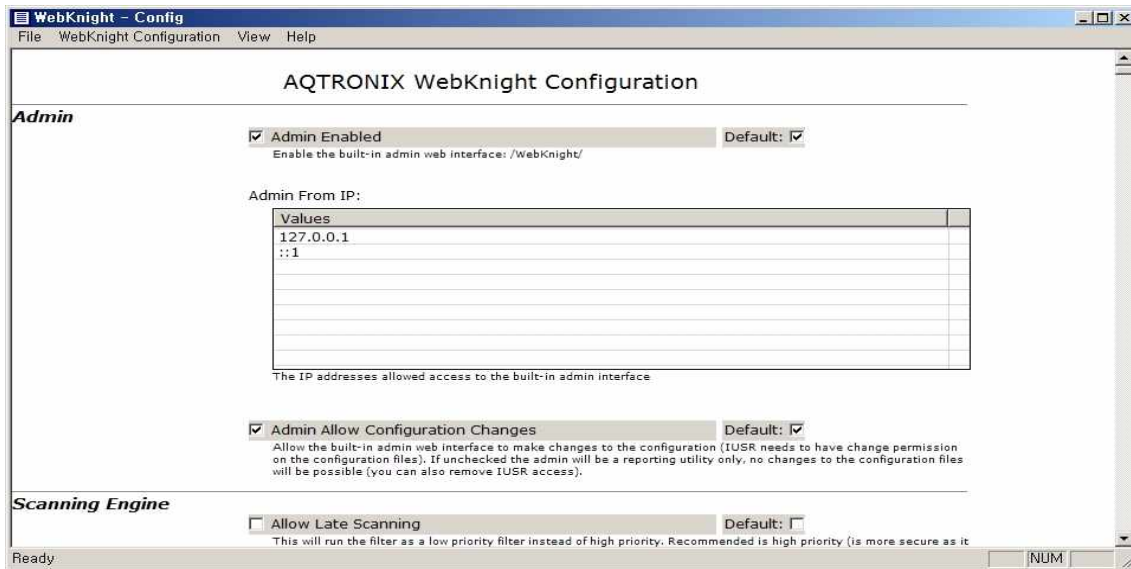
WebKnight는 대응방법, 로깅, 로봇차단, 메소드 차단 등 다양한 설정기능들이 존재한다. 세부 정책항목은 다음과 같다.

구 분	기 능	비 고
Admin	WebKnight 3.1 에서 추가된 기능으로 관리 및 통계를 지원하는 웹 인터페이스	Default 설정 시 : /127.0.0.1/WebKnight/ 에서 확인가능
Scanning Engine	암호화 포트(HTTPS), 비암호화 포트(HTTP)에 대한 모니터링, 웹 인스턴스나 IP에 대한 제외여부 등 설정	
Incident Response Handling	탐지가 되었을 때 응답처리 방식, Default로 정의된 파일을 보여줄 것인지 사용자 정의파일로 바꿀 것인지 로그만 남길 것인지 등의 제어가 가능	최초 설치 시 "Log Only" 모드로 를 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	"URL Denied Sequences"

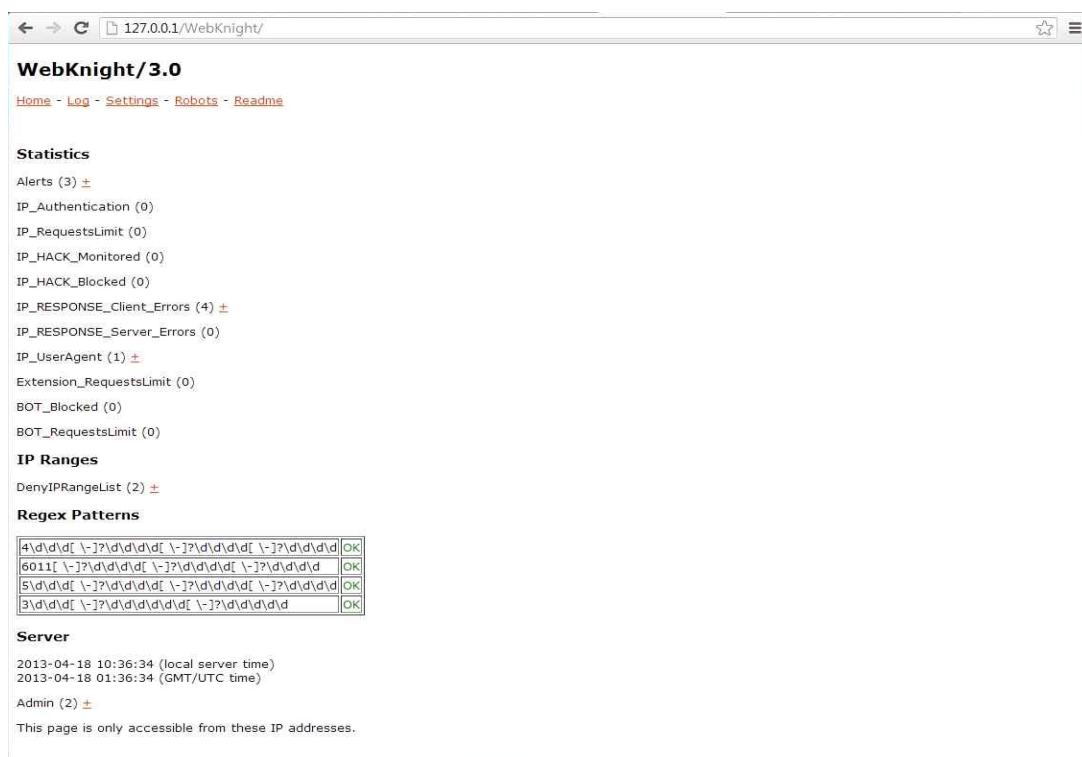
	차단	항목 확인 필요
Mapped Path	Directory Traversal 공격, 백슬래쉬(₩) 등 허용하지 않을 문자 및 로컬 시스템내의 허용할 경로 정의	"Allowed Paths"에서 웹App가 있는 위치확인 및 지정 필요
Requested File	차단시킬 파일의 문자열과 키워드 목록, 차단.허용할 파일 확장자 등을 정의	정상적인 요청이 차단될 수 있으므로 반드시 확인필요
Robots	자동화된 로봇, 봇 에이전트 등에 대한 차단 동작을 설정	추가로 Robots.xml이 있다.
Headers	서버 헤더 정보 변경, 특정 헤더 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 확장 저장 프로시저의 사용 유무 등을 고려하여 추가/삭제 필요
Web Applications	WebDAV, IISADMPWD 등 웹 어플리케이션의 허용유무 결정	기본적으로 모두 사용하지 않는 것으로 설정되어 있음

4.2.1 WebKnight 관리자 웹 인터페이스

WebKnight 3.1 에서는 관리자 웹 인터페이스가 추가되었다. 이에 따라, 설정관리자(Config.exe)에서 웹 관리자 인터페이스를 사용할지 결정할 수 있다.

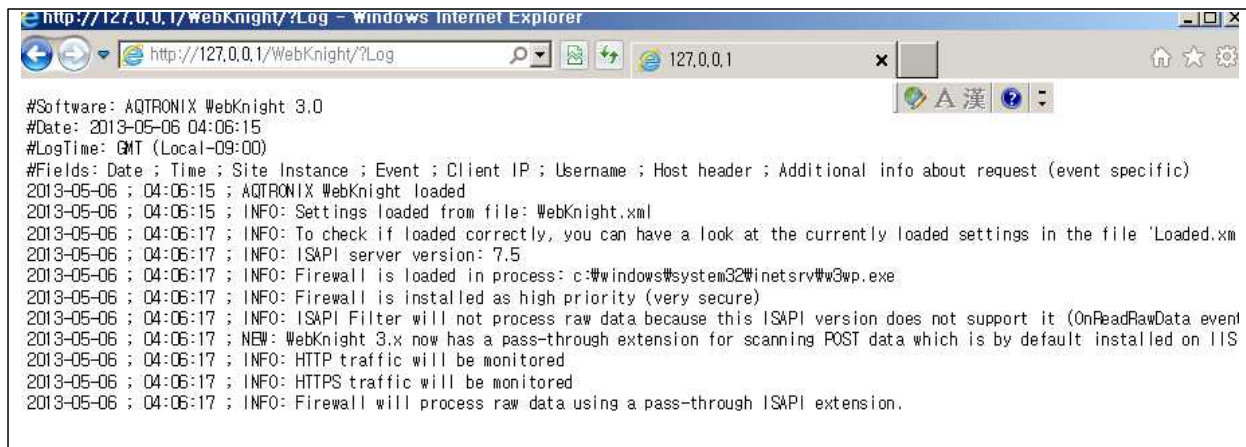


위의 그림과 같이 설정파일에서 Enable 시킬 경우 웹 관리자를 통하여 정책 및 로그 등을 웹 인터페이스를 통하여 확인 가능하다. Default 설정시 /127.0.0.1/WebKnight/에서 웹 관리자 페이지를 볼 수 있다.



웹 관리자 인터페이스에서는 설정한 정책, Log, 설정 세팅, Robots 등을 확인 가능하다.

Log 메뉴는 LogAnalysis.exe 실행없이 웹 UI에서 직접 로그파일을 볼 수 있다.



Settings 메뉴는 아래 그림과 같이 구성된다.

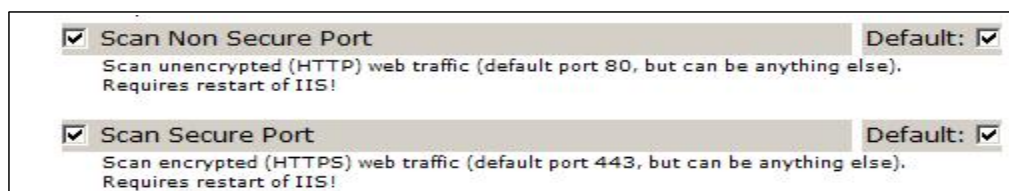


이중, Configured settings의 경우 정책을 설정하는 페이지이며, Loaded settings는 기저장된 설정 파일(Loaded.xml)을, Reload settings는 이전의 설정파일(WebKnight.xml)을 읽어오는 페이지이다. Clear cache의 경우 중간에 저장된 설정파일을 삭제한다.

4.2.2 트래픽 감사 설정

설정 메뉴 중 'Scanning Engine'은 트래픽 엔진이 탐지할 곳을 설정할 수 있는 메뉴이다.

최초 설치시 설정되어 있는 Scan Non Secure Port, Scan Secure Port 항목을 체크하여 HTTP/HTTPS 트래픽을 모두 탐지하도록 해야지만, 보다 안전하게 운영할 수 있다.



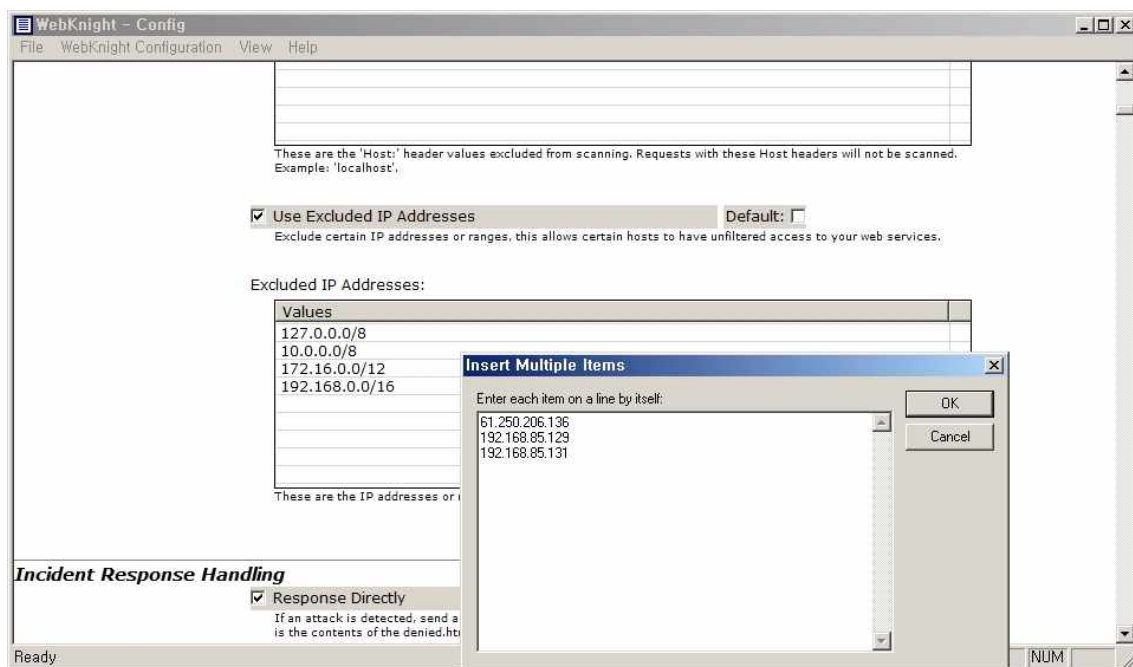
만약, 트래픽을 감사할 필요가 없는 신뢰된 사이트가 존재하거나 취약점 점검, 모의해킹 등을 수행할 목적으로 차단해지가 필요할 경우, 위의 전체 감사기능을 끄는 것이 아니라 일

부 IP만 예외 처리하는 것이 가능하다.

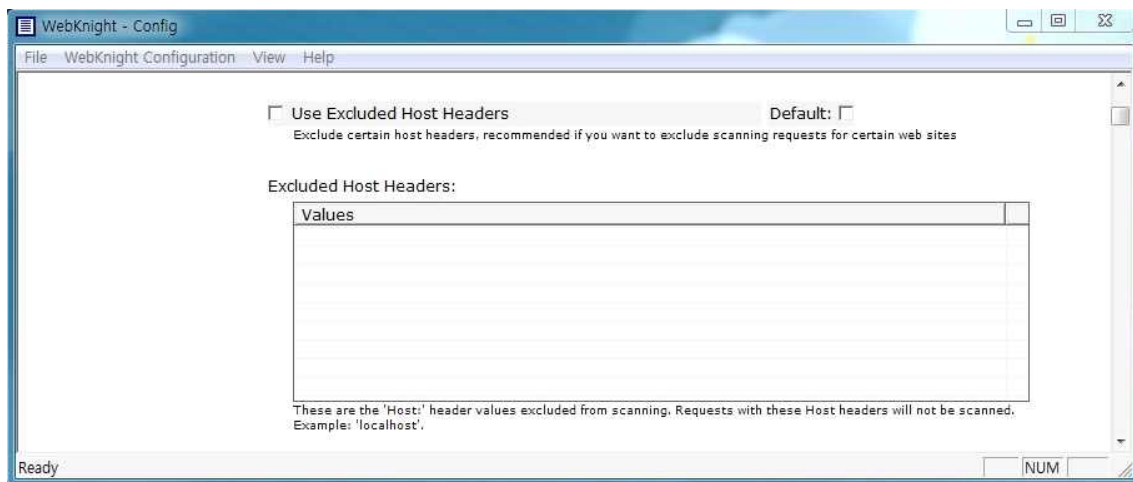
다음은 본 설정방법을 설명하기 위한 예시 IP 목록이며 아래의 IP들에 대해 감사 예외 IP로 설정하는 방법을 알아본다.

61.250.206.136	192.168.85.129	192.168.85.131
----------------	----------------	----------------

이 IP 목록을 WebKnight 설정 파일(Config.exe)에서 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.



이외에도, WebKnight 3.1 부터는 특정 IP 대역에 대한 예외처리 뿐 아니라, user-agent 등 헤더의 파일을 보고 예외처리 할 수 있는 기능이 추가되었다.



그 외 특정 공격에 대하여 차단정책을 설정하는 방법은 5장에서 다룬다.

5. KISA 웹 취약점 점검과 차단정책 설정

5.1 웹 취약점 점검소개

한국인터넷진흥원에서는 영세기업들이 안전한 홈페이지 운영을 지원하고자 웹사이트 원격 취약점 점검을 무료로 제공하고 있다.

툴박스 홈페이지(<http://toolbox.krcert.or.kr>)에서 무료 웹 취약점 점검을 신청한 이후 점검 결과를 바탕으로 자신의 웹사이트 중 취약한 부분에 대하여 맞춤형 설정을 할 경우, 더 안전하게 웹 사이트 운영이 가능하다.

KISA

로그인 | 회원가입 | 아이디찾기 | 비밀번호찾기 | 전체보기 | 검색어를 입력하세요 | 검색

무료 원격 웹취약점 점검 | 웹사이트 보안 도구 | DDoS 사이버대피소 | 보안정보 | 이용안내

웹사이트 보안강화 웹 보안 툴박스에서 시작하세요
웹사이트 개발자/관리자를 위한 보안 서비스 사이트

웹 취약점 원격점검 서비스 [바로 신청하기](#)

공지사항 (+ 더보기)

- 툴박스 홈페이지 점검 안내 04/17
- 툴박스 홈페이지 서버 점검 안내 04/05
- [안내] 회원가입 시 본인확인방법 변경안내 04/04
- 툴박스 관련 문의 전화번호 안내 03/21
- 웹셀[웹서버 악성코드] 탐지기술 공유 03/13

점검 FAQ (+ 더보기)

- 점검신청은 어떻게 하나요? 08/18
- 점검 제외 대상은 무엇입니까? 08/18
- email.txt 업로드는 어떻게 하나요? 08/18
- 취약점 점검 시 사용하는 IP 12/20
- XSS 또는 Cross Site Scripting 취약점 12/20

WHISTL/CASTLE (+ 더보기)

- 64bit 휘슬 실행 시 xterm 오류 발생 문제 10/18
- 휘슬 예약 설정 및 점검 토큰 저장 방법 안내 08/25
- 기존 담당자가 퇴사하여 휘슬 점검결과를 받음 08/18
- 휘슬 업데이트시 장애로 업데이트가 되지 않음 08/18
- 휘슬을 사용하고 싶은데 어떻게 신청하나요? 08/18

공개웹방화벽 (+ 더보기)

- 웹나이트 정책 설정 안내서 01/25
- AQTRONIX WebKnight 2.4 01/05
- WebKnight 2.3버전용 차단 샘플들 [10.04.23] 04/23
- AQTRONIX WebKnight 2.3 04/22
- ModSecurity 2.5.12 유닉스용 설치파일 03/25

CASTLE 홈페이지 해킹 방지 도구

WHISTL 웹셀 탐지 프로그램

공개 웹 방화벽

웹 취약점의 이해와 대응방법

웹보안 강화도구의 이해와 활용

KrCERT/CC 인터넷침해대응센터

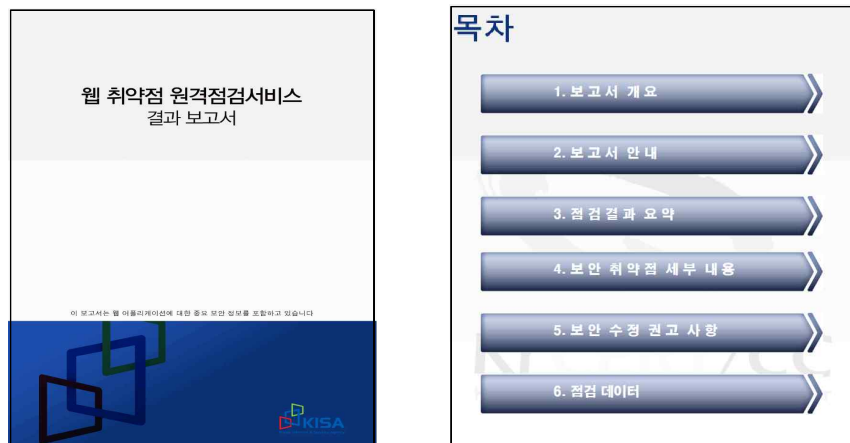
KISA

무료 원격 웹 취약점 점검 신청의 경우, 취약점 점검 신청자 본인이 해당 사이트 운영자인지 확인을 하여 검증이 이루어지기 때문에 해당 사이트 url에 해당하는 E-Mail로 신청하거나 사이트 관련 사업자 증명서 등을 보유해야 한다.

5.2 웹 취약점 점검 결과보고서 설명

① 결과보고서 템플릿

웹사이트 원격 취약점점검을 받은 이용자분들은 점검이 완료된 후 점검 결과보고서를 받게 되며, 웹 취약점 결과보고서는 취약점 종류, URI에 포함된 취약점 개수, 조치방법 등을 포함하고 있다.




② 점검 결과 요약

3.5 보안 취약점이 많은 URL(문제 개수) TOP 5	
URL	문제 개수
http://www. .asp	3
http://www .asp	3
http://www asp	1
http://www .asp	1
http://www. asp	1
3.6 취약점 별 결과 요약	
경고 그룹	문제 개수
링크 인젝션(크로스 사이트 요청 위조 유도)	16
애플리케이션 오류	17
크로스 사이트 스크립팅(XSS)	10
SQL 인젝션	2

3.5항, 3.6항의 내용을 통해 웹사이트의 취약점 현황을 파악할 수 있다. 3.5항 URL의 문제 개수는 해당 URL의 잠재한 취약점 항목의 개수를 의미하며, 3.6항의 취약점 별 결과요약의 문제개수는 취약점 항목별 HTTP 요청 시 포함된 취약한 파라미터의 개수를 의미한다.

③ 보안 취약점 세부 내용

웹 취약점 세부내용은 위험도, 영향 받는 URL, 분류, 취약점 원인, 점검환경, 요청/응답내용으로 구성되어 있다. 위험도는 발견된 취약점의 피해영향에 따라 "상", "중", "하", "참고"로 구분되며, 영향 받는 URL은 취약점이 발견된 페이지를 의미한다. 분류는 조치 방법이 소스코드 수정 사항인지 환경설정 사항인지를 의미한다. 점검환경은 취약점이 발견된 파라미터와 점검문자열을 설명한다. 요청/응답내용은 취약점 점검을 위해 사용자 브라우저에서 요청한 내용과 웹서버가 응답한 내용을 포함하고 있다.

4.2.5 크로스 사이트 스크립팅(XSS)	
위험도	상
영향 받는 URL	http:// .asp
분류	개발자 수정
취약점 원인	테스트에서 응답에 스크립트를 포함시켰습니다. 이것은 페이지가 사용자의 브라우저에 로드되면 실행됩니다. 애플리케이션이 크로스 사이트 스크립팅(XSS)에 취약함을 의미합니다.
점검 환경	 [브라우저로 확인하기] 점검을 위해 아래와 같이 변형하여 적용되었습니다. <div style="border: 1px solid red; padding: 5px; margin: 10px 0;"> 파라메타 값을 colz=colz → colz=>"><img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert(208153)> 으로 변경 </div>
요청/응답내용	<pre>GET .asp?colz=>"><img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert(208153)>&txt=&page= HTTP/1.0 Cookie: ASPSESSIONIDAQCRBAQ=APODKGMCPJCHGHAHJKCBHFAM Accept: */* Accept-Language: en-US User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32) Host: Referer: .asp?IDXNo=240 HTTP/1.1 200 OK Content-Length: 41714 Connection: close</pre>

WebKnight 차단정책 설정을 위해 유심히 확인해야 될 내용은 파라메타 값 변경 부분이다. 웹 취약점 점검은 정상적인 파라메타 값을 비정상적인 값으로 변경시켜 취약여부에 대해 확인하는 방법을 사용하기 때문이다.

위의 웹 취약점 내용은 입력 값에 대한 적절한 필터링이 되지 않아 발생하는 XSS(크로스 사이트 취약점) 취약점 예시이다.

보고서에 기록된 요청/응답내용 부분을 확인하여 실제 점검내용이 정·오탐 여부 확인과 취약점에 대한 상세내용을 확인하는데 참고할 수 있으며, 또한, 한국인터넷진흥원에서는 해

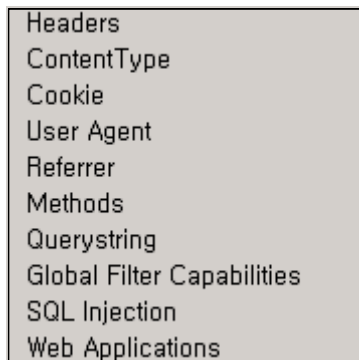
당 내용에 대한 정탐/오탐 여부에 대해 자세한 기술지원을 하고 있다.

□ 웹 취약점 점검 및 관련 기술지원 기술 문의

- o Tel : 02-405-5665
- o E-Mail : toolboxadmin@krcert.or.kr

5.3. WebKnight 차단정책 설정

WebKnight는 차단정책 설정 시 4.2의 “세부정책항목”에서 설명된 옵션들을 사용한다. 이 중 아래 그림의 메뉴들이 주로 차단정책에 활용할 수 있는 메뉴들이다.



WebKnight에서는 정규식을 지원하지 않기 때문에, 차단정책을 설정할 경우 차단될 문자열과 특수문자로 조합으로 설정해야 한다.

여기서는 5.2절의 웹 점검결과보고서를 바탕으로 취약점 차단하는 방법을 설명한다.

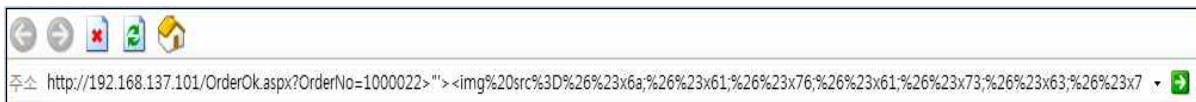
5.3.1 XSS 취약점 차단 정책 예

① WebKnight 설치 전 취약점 확인

- ▶ 1단계) 웹취약점 결과보고서에서 URL, 파라미터, 점검 문자열을 식별한다.

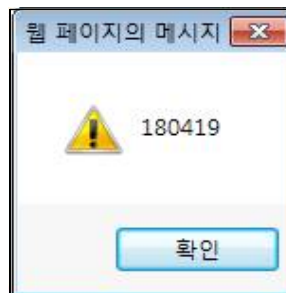
구분	내 용
URL	http://192.168.137.101/OrderOk.aspx
파라미터	OrderNo
점검문자열	>"' <img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert(180419)
디코딩	>"'

▶ 2 단계) 웹 브라우저를 이용하여 취약점이 존재하는지 테스트한다.



▶ 3 단계) 테스트 결과를 확인한다.

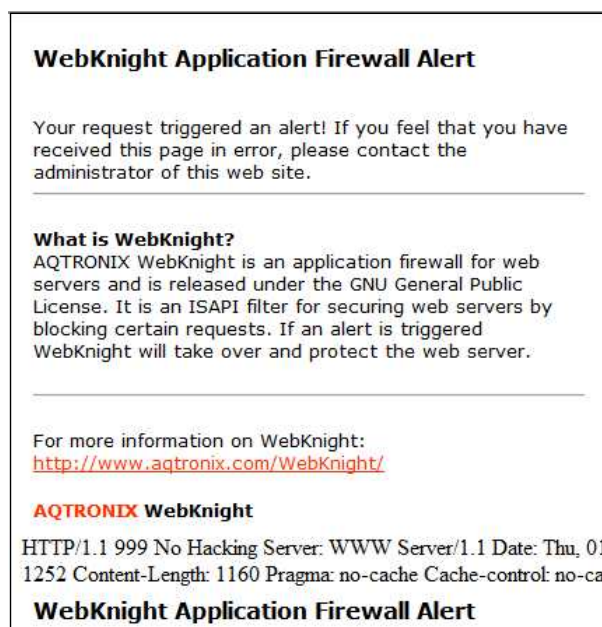
아래와 같이 스크립트가 정상적으로 실행되는 것을 확인할 수 있으며, 홈페이지에 XSS 취약점이 존재한다고 판단할 수 있다.



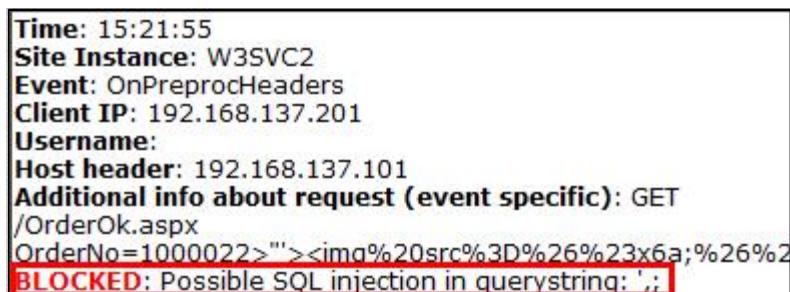
② WebKnight 설치 후 취약점 확인

설치 후 점검문자열이 정상적으로 차단되는지 테스트한다. 기본차단정책으로 아래와 같이 공격이 차단된 것을 확인할 수 있다. 하지만 차단정책으로 방어가 되는 않는 취약점들은 추가적인 차단정책 설정이 필요하다.

- ▶ 1단계) 동일한 문자열로 테스트한다.
- ▶ 2단계) WebKnight에 아래와 같은 차단 메시지가 출력되는지 확인한다.



- ▶ 3단계) WebKnight 설치 폴더에서 LogAnalysis.exe를 실행한 후 차단로그를 확인한다.



차단로그를 확인한 결과 SQL인젝션 차단정책에 설정되어 있는 '(SingleQuotation),;(Semicolon)으로 차단되었다. 차단은 되었지만 XSS 공격이 SQL인젝션 차단정책으로 차단되었기 때문에, 정확한 차단을 위해 추가적인 차단정책을 설정해야 한다.

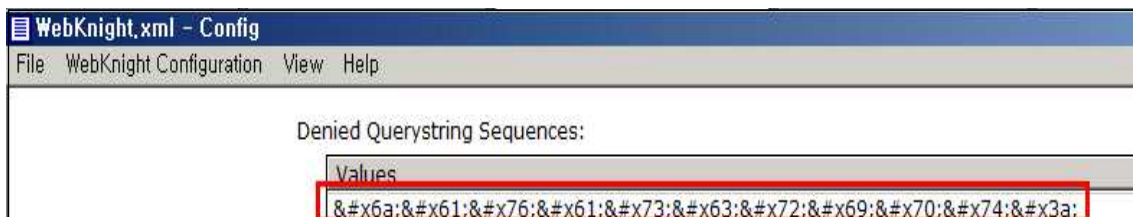
▶ 4 단계) 점검 문자열을 분석한다.

아래의 점검문자열을 방어하기 위해서는 OrderNo 파라미터의 뒤에 추가적으로 붙은 문자열을 정책으로 설정하는 것이 핵심이다. <img[SPACE]를 차단문자열로 설정할 수 있지만 웹사이트에 따라서 오차단의 여지가 발생할 수 있기 때문에, javascript: 문자열의 html 인코딩 문자열을 방어정책으로 설정을 하였다. 실제로 XSS 공격은 javascript에서 제공하는 다양한 기능을 이용하기 때문에 근본적으로 javascript:를 사용하지 못하도록 차단하는 것이다. javascript: 문자열은 이미 기존에 차단정책으로 설정되어 있지만 html 인코딩으로 인해 차단을 못하는 경우이다

취약점 점검 문자열
>""><img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert(180419)

방어 문자열
javascript:

▶ 4단계) 차단정책 설정을 위해 Config.exe를 실행시킨 후 QueryString 부분에 정책을 설정한다.



▶ 5단계) LogAnalysis.exe를 실행한 후 차단정책이 적절히 동작하는지 확인한다.

```
Time: 09:18:44
Site Instance: W3SVC2
Event: OnPreprocHeaders
Client IP: 192.168.137.201
Username:
Host header: 192.168.137.101
Additional info about request (event specific): GET
/OrderOk.aspx
OrderNo=1000022>""><img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;
BLOCKED: Possible SQL injection in querystring: ';
BLOCKED: '&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;' not allowed in querystring
```

[XSS 차단정책 결과 로그확인]

추가 설정한 차단문자열로 점검문자열이 정상적으로 차단되는 것을 확인할 수 있다. 차단 정책 설정 후에는 반드시 서비스 이용에 문제가 없는지 로그분석을 통해 충분한 테스트를 수행해야 한다. 차단정책이 오차단 등 서비스 이용에 문제를 야기한다면, 다른 정책을 고려해야 한다.

POST 메소드를 사용하여, Request 데이터를 전달 시 게시판에 입력된 내용들이 Body에 포함되어 전달됩니다. 게시판에 작성한 글들은 HTML 인코딩 후 전달되기 때문에 이 부분을 고려하여 차단정책을 설정해야 한다. WebKnight에서 지원하는 디코드 엔진은 URL 인코딩만 해당되기 때문에 HTML 인코딩을 디코딩하여 차단하지 않음을 참고해야 한다.

③ WebKnight 설치 후 이행점검을 통해 취약점이 확인된 경우

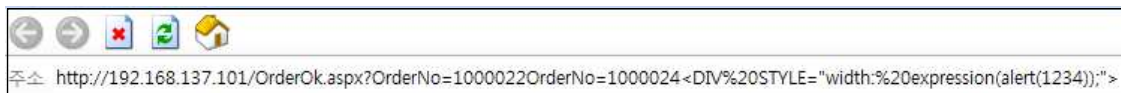
결과보고서에 있는 취약점에 대해 기본방어정책이나 추가정책을 수립하여도 이행점검을 통해 추가적인 취약점이 발견될 수 있기 때문에, 이행점검은 반드시 받아야 한다.

이행점검을 통해 발견된 취약점은 역시 차단정책으로 설정해야 합니다.

▶ 1단계) 취약점 결과보고서에서 URL, 파라미터, 점검문자열을 식별한다.

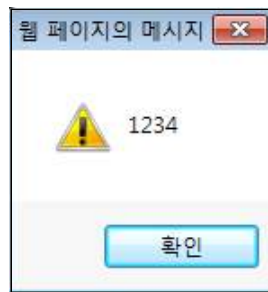
구분	내 용
URL	http://192.168.137.101/OrderOk.aspx
파라미터	OrderNo
점검문자열	<DIV%20STYLE="width:%20expression(alert(1234));">

▶ 2 단계) 웹 브라우저를 이용하여 취약점이 존재하는지 테스트한다.



▶ 3 단계) 테스트 결과를 확인한다.

WebKnight의 기본차단정책으로 처음 점검문자열은 차단했지만 다른 패턴의 점검문자열이 시도된 결과 아래와 같이 스크립트가 정상적으로 실행되어 홈페이지에 XSS 취약점이 존재한다고 판단할 수 있다.



▶ 4 단계) 점검 문자열을 분석한다.

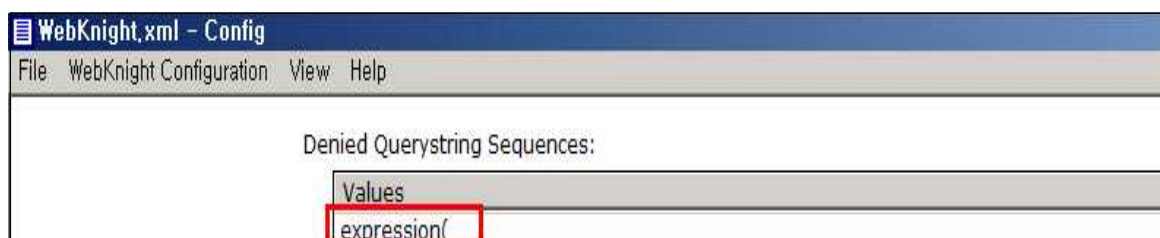
아래의 점검문자열을 방어하기 위해서는 OrderNo 파라미터의 뒤에 추가적으로 붙는 문자열을 정책으로 설정하는 것이 핵심이다. <div[SPACE] 혹은 STYLE="를 차단정책으로 설정할 수 있지만 오차단이 발생할 수 있어 expression(를 차단정책으로 설정하였다. expression은 MS사에서 제공하는 Dynamic Properties로 CSS 환경에서 동적콘텐츠를 제공하기 위해 제공하는 기능이다. 해당 속성을 사용하여 CSS 파일에 악성URL을 삽입하는 것으로 악용되기도 합니다.

취약점 점검 문자열
<DIV%20STYLE="width:%20expression(alert(1234));">

방어 문자열
expression(

▶ 5 단계) WebKnight의 Querystring 영역에 차단정책을 설정한다.

차단할 문자열을 아래와 같이 등록한다.



▶ 6 단계) 차단정책이 적절히 동작하는지 확인한다.

정상적으로 차단이 되었는지 아래와 같이 테스트를 실행합니다. 점검문자열이 포함된 요청 시 정상적으로 차단된 것을 확인할 수 있습니다.



그리고 WebKnight에 포함된 LogAnalysis.exe 도구를 사용하여, 차단로그를 확인한다. 아래 처럼, 정상적으로 차단이 된 것을 확인할 수 있다.

```
Time: 09:45:30
Site Instance: W3SVC2
Event: OnPreprocHeaders
Client IP: 192.168.137.201
Username:
Host header: 192.168.137.101
Additional info about request (event specific): GET
/OrderOk.aspx
OrderNo=1000022<DIV%20STYLE="width:%20expression(alert(1234));">
WARNING: SQL keyword found in querystring (1 more will block request)
BLOCKED: 'expression()' not allowed in querystring
```

역시, 차단정책 설정 후에는 반드시 서비스 이용에 문제가 없는지 로그분석을 통해 충분한 테스트를 수행해야 한다. 차단정책이 서비스 이용에 문제가 생긴다면 다른 차단정책을 고려해야 한다.