윈도우 환경에 ModSecurity 설치하기

2008.11./인터넷침해사고대응지원센터

1. 개 요

Apache용 공개 웹방화벽인 ModSecurity를 윈도우 기반의 Apache, PHP, MySQL 통합 솔루션인 APM_Setup에 설치하는 방법을 살펴본다. 리눅스 및 유닉스 환경에서의 Apache, PHP, MySQL 등의 설치, 설정법 등에 익숙하지 않은 사용자들은 본 APM_Setup 등과 같은 통합 패키지를 설치하여 사용하는 것도 도움이 되리라 생각한다. APM_Setup은 현재 APM_Setup 6 Testing Version까지 배포된 상태이며 패키지 구성은 다음과 같다.

APM_Setup 6 Testing Version(08. 4. 18) - Apache 2.2.8 (openssl 0.9.8g) - PHP 5.2.5 - Zend Optimizer v3.3.3 - MySQL 5.0.51a - phpmyAdmin 2.11.5.1 지원 시스템 : NT계열 2000 / XP / 2003 / Vista

ModSecurity는 현재 안정화 버전으로 1.9.x와 2.1.x, 2.5.x 의 세가지 버전이 릴리즈 되어있으나 현재 1.9.x 버전은 1.9.5를 마지막으로 개발이 종료되었고, 2.1.x 버전 역시 2.1.7 버전을 마지막으로 현재는 2.5.x 버전만이 개발되고 있다.

유닉스 계열에서 Apache 1.x 버전에는 ModSecurity 1.x 버전대만 설치가 가능하며 Apache2에는 ModSecurity 1.x, 2.x 버전의 설치가 가능하다. **하지만 윈도우 계열에서 ModSecurity를 설치하기 위해서는 Apache 2.2.x 이상 버전에서만 설치가 가능하니 이점 유의해야 한다.**

윈도우 환경에 ModSecurity를 설치하기 위해서는 굳이 APM_Setup을 설치해야 하는 것이 아니라 일반적인 윈도우용 Apache를 설치하였을 때도 방법은 동일하다.

2. 윈도우에 ModSecurity 설치

설치환경은 다음과 같다.

• OS : Windows 2003 Enterprise Edition • Web Server : APM_Setup 6 Testing Version • ModSecurity : Mod_Security-2.5.6-win32

□ 프로그램 다운로드

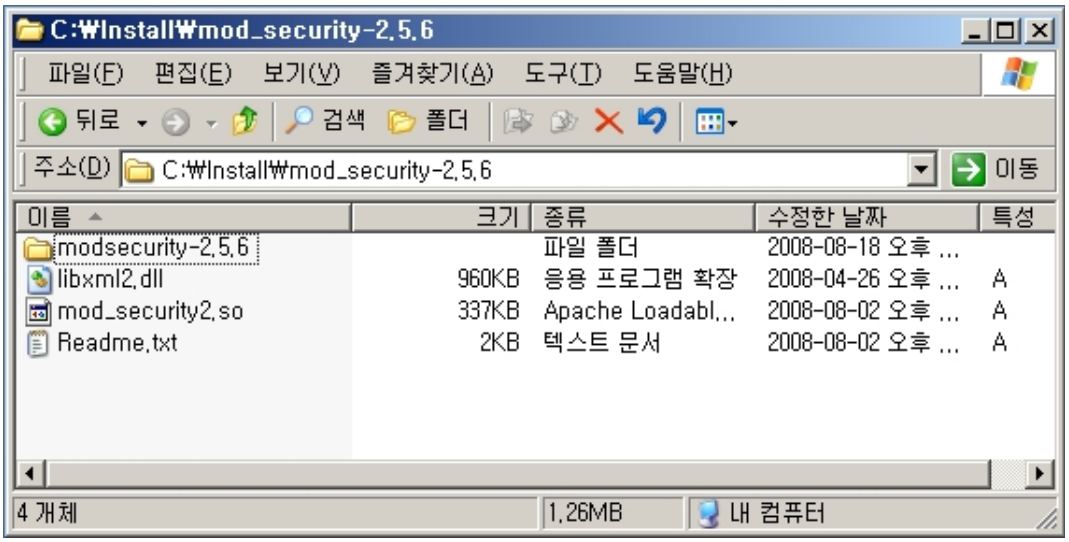
설치할 ModSecurity를 다운로드 하자. 여기서 사용할 버전은 ModSecurity-2.5.6 안정화 버전이다. 아래 사이트에서 다운로드 할 수 있다.

http://www.modsecurity.org → ModSecurity 공식 홈페이지
http://www.apachelounge.com → Windows용 Apache 및 ModSecurity를 다운로드 할 수 있다.
※ 사이트 접속이 원활하지 않을 경우 공개 웹방화벽 커뮤니티에서 다운로드

다운로드 : http://www.securenet.or.kr/main.jsp?menuSeq=501 → Mod_Security-2.5.6-win32.zip 다운

APM_Setup은 http://www.apmsetup.com 에서 다운로드 할 수 있다. 본 안내서에서 APM_Setup 6의 설치과정은 생략한다.

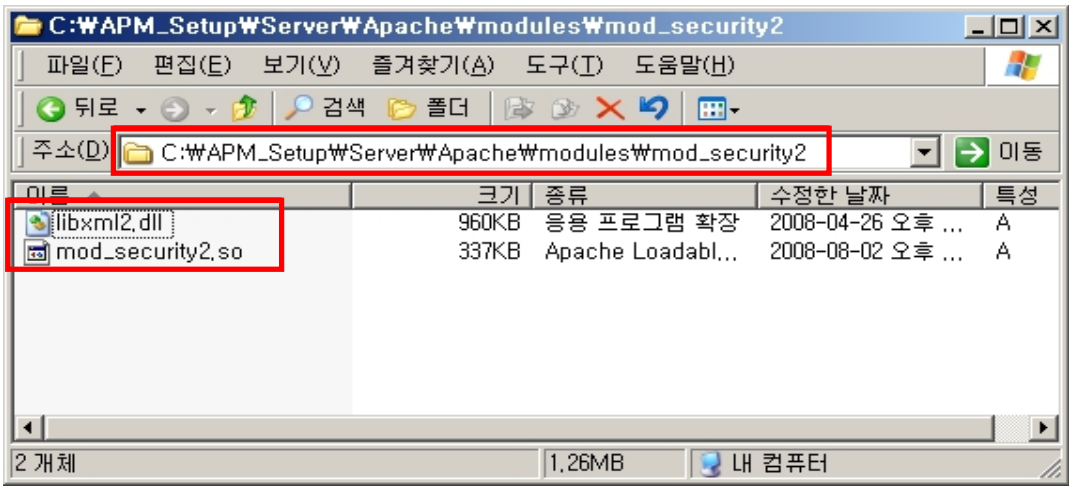
Mod_security-2.5.6-win32.zip 의 압축을 해제하면 다음과 같은 파일들이 보인다.



Readme.txt 파일에도 설치 방법이 설명되어 있으니 참고하면 되겠다.

□ 프로그램 설치 및 기본 설정

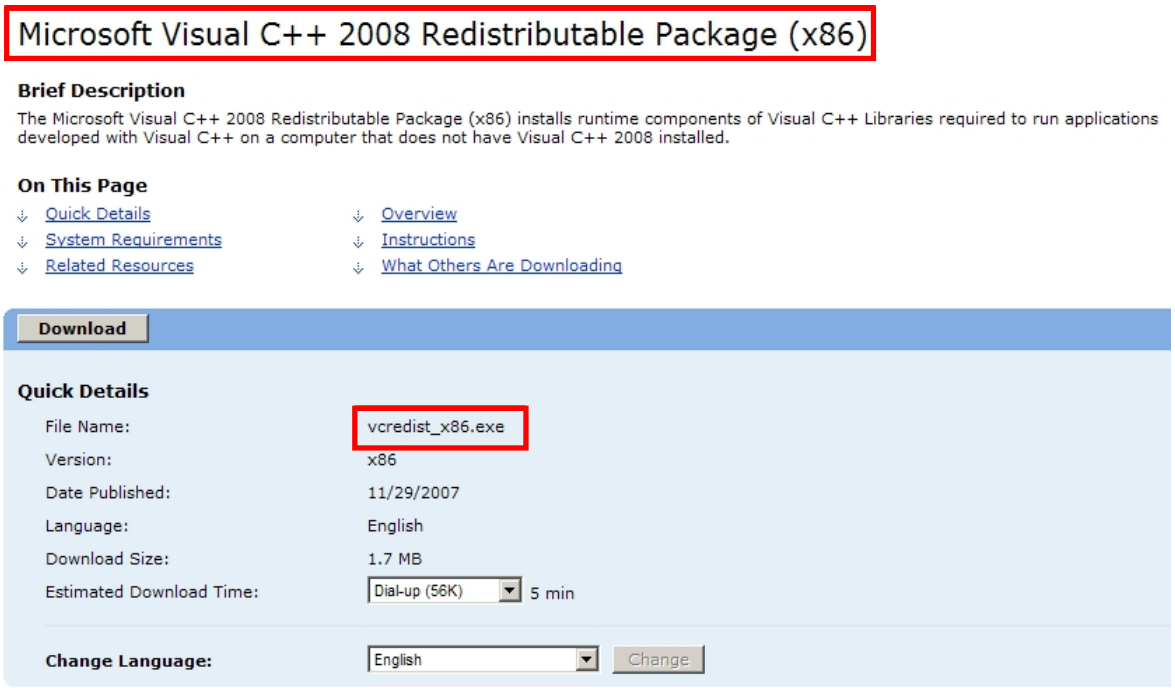
설치하는 법은 간단하다. 필요한 파일을 Copy & Paste 한 뒤 설정파일을 수정해주면 된다. 처음 압축을 해제하면 libxml2.dll 파일과 mod_security2.so 파일이 보이는데, 이 두 파일을 Apache 하위의 Modules 폴더 내에 Mod_Security2 폴더를 생성하여 복사한다.



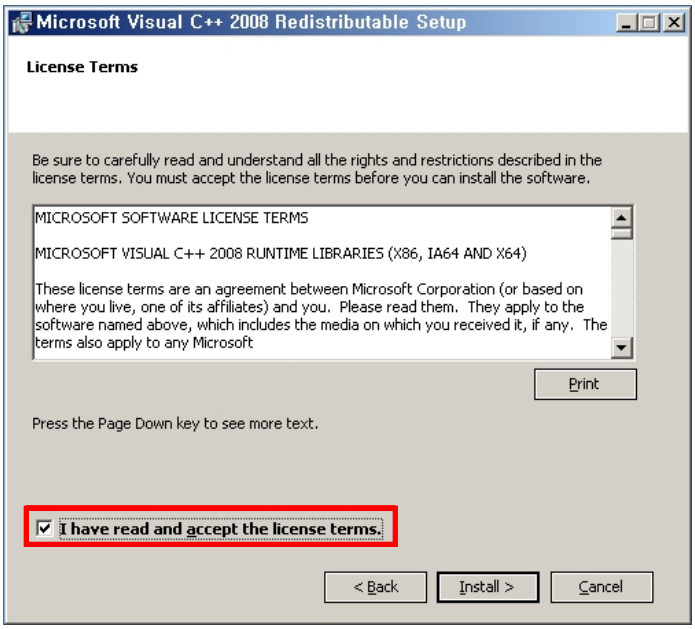
파일의 위치를 modules로 폴더가 아닌 반드시 modules/mod_security2 경로로 복사해야만 올바르게 읽어들일 수 있다.

윈도우용 Mod_Security 모듈은 Visual Studio 2008에서 개발이 되었기 때문에 VC 2008 Redistributable Package를 설치해야만 정상적으로 동작한다. 다운로드는 아래 링크를 통해 가능하다.

http://www.microsoft.com/downloads/details.aspx?FamilyID=9B2DA534-3E03-4391-8A4D-074B9F2BC1BF&displaylang=en

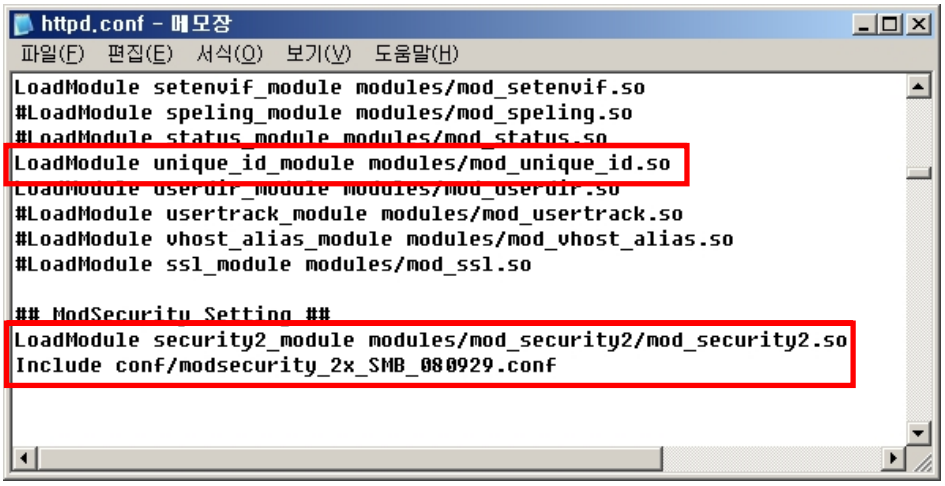


위 파일을 다운로드 한 뒤 실행하면 다음과 같은 설치 화면이 나타난다. '**I have read and accept the license terms**' 에 체크한 뒤 설치를 진행한다.



VC 2008 Package까지 설치하였다면 이제 Apache에 실제 모듈을 등록해야 한다.
Apache의 httpd.conf 파일에 다음 라인을 추가하자.

```
LoadModule unique_id_module   modules/mod_unique_id.so   // Disable 되있다면 Enable 해줘야 한다
LoadModule security2_module   modules/mod_security2/mod_security2.so   // 모듈 파일
Include conf/modsecurity_2x_SMB_080929.conf   // modsecurity 차단 샘플룰 로드
```



APM_Setup 6은 mod_unique_id.so 모듈이 기본적으로 Disable 되어있기 때문에 Enable 해줘야 한다. unique_id_module은 유닉스 환경과 마찬가지로 ModSecurity의 정상적인 필터링이 가능하게 하는 모듈이다.

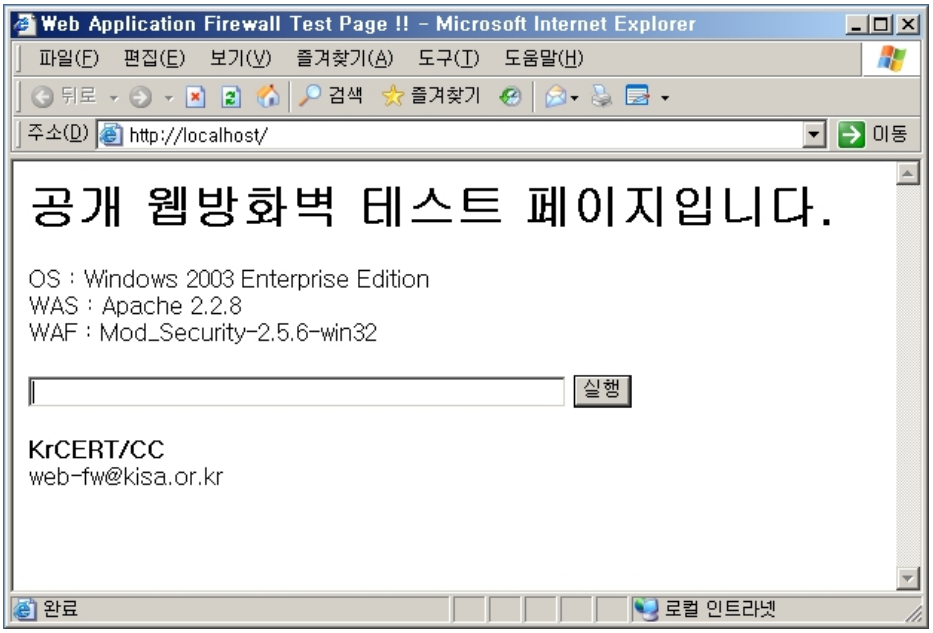
mod_security_2x_SMB_080929.conf 파일은 Rule 파일로써 공개 웹방화벽 커뮤니티를 통해 차단 샘플룰을 다운로드 할 수 있다. 커뮤니티 자료실에서 최신 버전의 샘플룰을 다운받아 원하는 위치에 복사한 뒤 Apache 설정파일에 추가해주자.

다운로드 : http://www.securenet.or.kr/main.jsp?menuSeq=501

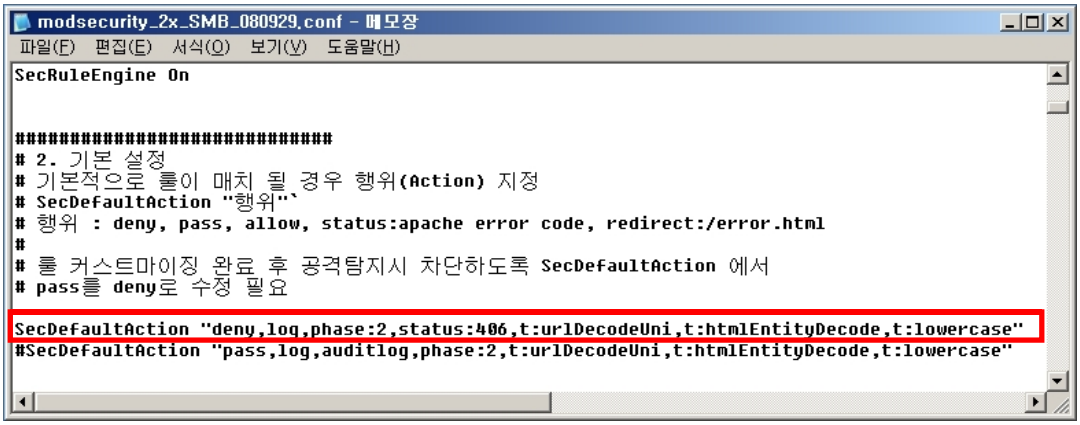
Rule 파일은 처음 압축을 해제한 위치에서 modsecurity-2.5.6/rules 폴더에 ModSecurity Core Rule이 제공된다. 그러나 Rule이 매우 상세하여 해당 Rule을 모두 적용하게 되면 웹서버의 퍼포먼스에도 영향이 발생할 수 있기 때문에 우리나라 실정에 맞는 KISA의 샘플룰을 적용하길 권장한다. 기존 유닉스 기반의 Rule 파일을 별다른 수정 없이 바로 사용할 수 있다.

□ ModSecurity 동작 확인

설치를 완료한 뒤 Rule 까지 설정을 다 끝마쳤다면 APM_Setup을 재시작하여 제대로 동작하는지를 확인해 보자. 아래 화면은 동작 확인을 위한 테스트 페이지이다.



재시작 하기 전에 KISA의 샘플룰은 배포시 탐지모드로 배포되기 때문에 실제 차단모드로 변경하여 테스트 하기 위해 아래 화면과 같이 수정해주자.

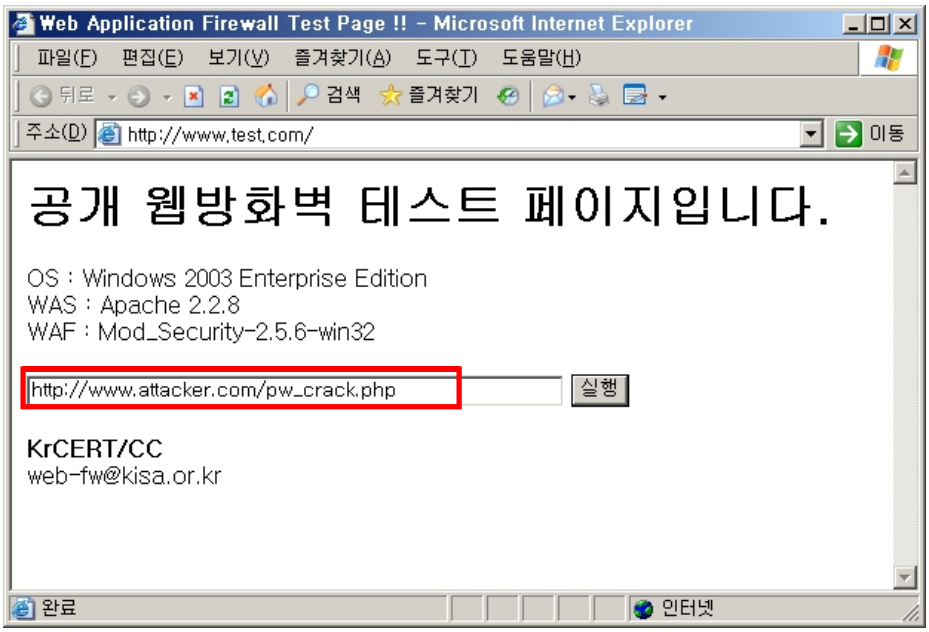


SecDefaultAction "deny,log,phase:2,status:406,t:urlDecodeUni,t:htmlEntityDecode,t:lowercase"

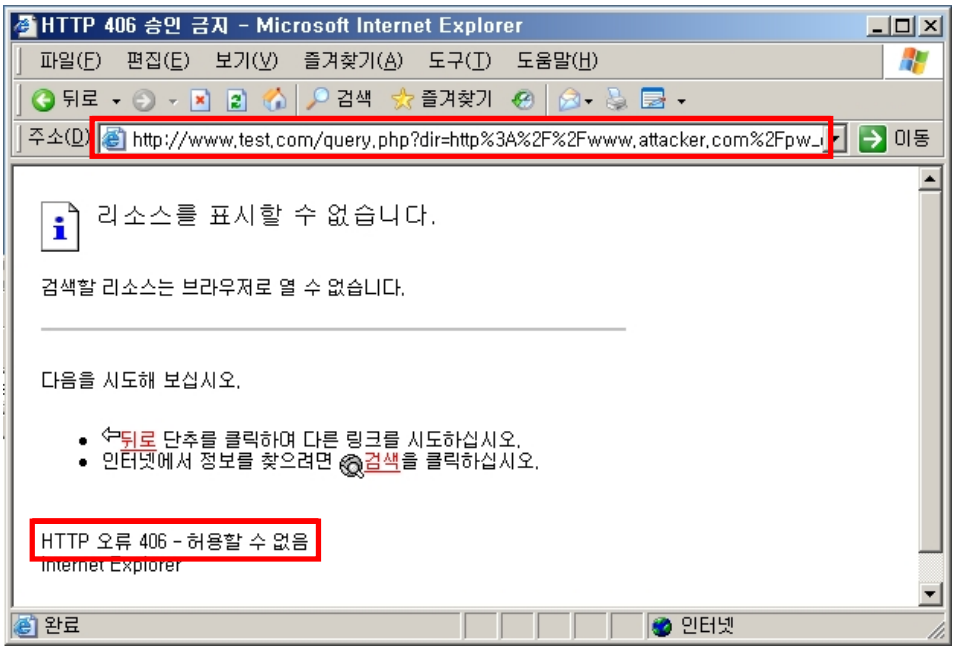
이 설정은 패턴이 일치하면 406 상태코드를 나타내며 차단하게 되는 모드이다.

실제 ModSecurity가 정상적으로 동작하는지 다음의 PHP Injection 공격구문을 입력해 보자.

☞ **http://www.attacker.com/pw_crack.php**

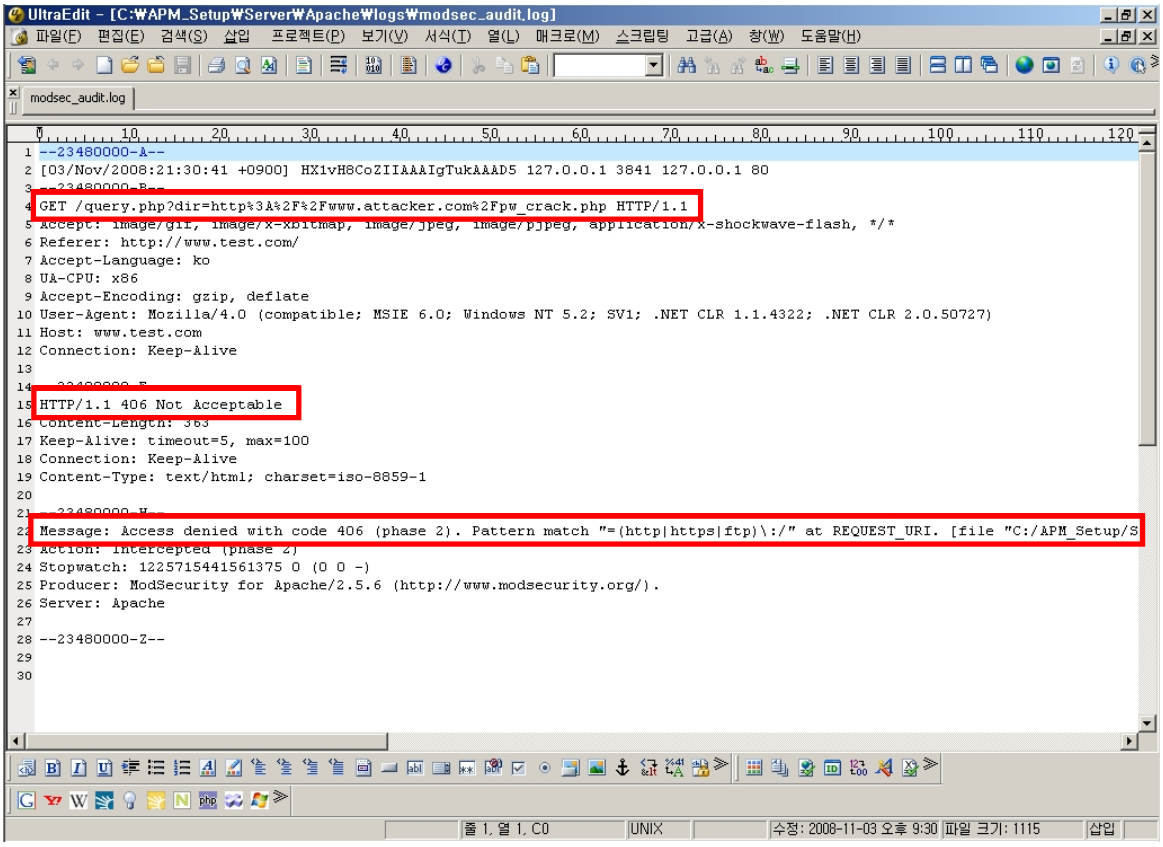


다음과 같이 'HTTP 406 승인 금지' 페이지가 나타났다.



ModSecurity가 정상적으로 동작하는 것 같으니 로그파일에는 어떻게 기록되었는지 살펴보자.

로그파일은 샘플룰 적용시 Default로 Apache 하위 logs 폴더에 modsec_audit.log 파일로 생성되도록 설정되있다. 편집기로 해당 로그파일을 열어보자.



실제 Message 항목을 보면 패턴 매치한 Rule 내용이 나타나며 정상적으로 ModSecurity가 동작하는 것까지 확인 할 수 있다.

3. 마치며..

이와 같은 방법으로 윈도우 Apache 환경에서 ModSecurity를 적용하는 법을 알아보았다. 본 안내서 서두에 언급하였듯이 윈도우 기반에서는 Apache 버전에 유의해서 설치해야만 ModSecurity가 정상적으로 동작할 수 있다.

VC Redistributable Package도 마찬가지로 설치 순서는 상관없으나 이를 생략할 경우 DLL 파일을 로드할 시 에러가 발생하여 Apache가 실행되지 않는다.

설치하는 도중 발생하는 문제점들은 이벤트뷰어(eventvwr.msc)를 이용하여 살펴볼 수 있다.

모든 솔루션이 그렇듯이 설치하자마자 최적의 상태로 동작하는 어플리케이션은 존재하지 않는다. ModSecurity도 마찬가지로 충분한 커스터마이징 작업을 통해 오탐을 줄여 나가야 한다. 설치만 한다고 모든 공격이 차단될 거라고 생각하면 오산이다. 보다 완벽한 방화벽 기능을 할 수 있도록 관리자의 지속적인 관심이 필요할 것이다.

[Reference]

http://www.modsecurity.org

http://www.apachelounge.com

http://www.apmsetup.com

http://www.krcert.or.kr/firewall2/index.jsp

http://www.securenet.or.kr/main.jsp?menuSeq=496