[modsecurity2 설치 매뉴얼]

아이티이지
서비스 운영팀

♧ 문서 작성간에 테스트된 환경

- CentOS release 5.6 (Final) 32bit

♧ 버전 정보

- httpd-2.2.3
- mysql-5.0.77
- php-5.1.6
- mod-security-2.5.10

♧ Mod Security 란?

- Ivan Ristic이 개발한 Apache 웹서버 용 공개 웹방화벽 입니다.
- 최근 홈페이지를 통한 악성코드 유포, 피싱 사이트으로의 악용 사례 등 웹 취약점을 통한 해킹 사례가 빈번히 발생하고 있습니다.

[Apache 와 Modsecurity 호환]

Modsecurity 2.X 버전의 경우 apache 2.X 이상 버전에서만 설치 가능
Modsecurity 1.9 버전의 경우, apache 1.X, 2.X 에서 모두 설치 가능

1. Modsecurity2 다운로드
   다운로드 URL : http://www.modsecurity.org/download

2. 설치 전 필요 라이브러리 설치
   root@localhost# yum -y install pcre-* libxml2-*

```
[root@localhost ~]# yum -y install pcre-*
Failed to set locale, defaulting to C
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.tt.co.kr
 * extras: centos.tt.co.kr
 * updates: centos.tt.co.kr
```

   root@localhost# cd /[Apache 설치 파일 경로]/modules/metadata/
   root@localhost# /usr/local/apache/bin/apxs -cia mod_unique_id.c

3. Modsecurity2 설치

다운로드 받은 파일이 있는 경로로 이동합니다.

root@localhost# cd /usr/local/src

다운로드 파일 압축 해제합니다.

root@localhost# tar xvfz modsecurity-apache_2.5.10.tar.gz

```
[root@localhost ~]# cd /usr/local/src/
[root@localhost src]# ls
modsecurity-apache_2.5.10.tar.gz
[root@localhost src]# tar xvfz modsecurity-apache_2.5.10.tar.gz
```

압축 해제된 내용을 확인합니다.

```
[root@localhost src]# ll -a
total 1284
drwxr-xr-x  3 root root    4096 Jan 17 14:04 .
drwxr-xr-x 11 root root    4096 Jan 17 12:21 ..
drwxrwx---  6 1000 1000    4096 Sep 25  2009 modsecurity-apache_2.5.10
-rw-r--r--  1 root root 1290172 Oct  9  2009 modsecurity-apache_2.5.10.tar.gz
```

압축 해제된 폴더로 이동합니다.

```
[root@localhost src]# cd modsecurity-apache_2.5.10
[root@localhost modsecurity-apache_2.5.10]# ll -a
total 84
drwxrwx--- 6 1000 1000  4096 Sep 25  2009 .
drwxr-xr-x 3 root root  4096 Jan 17 14:04 ..
-rw-rw---- 1 1000 1000 22990 Sep 19  2009 CHANGES
-rw-rw---- 1 1000 1000 15128 Jul  3  2007 LICENSE
-rw-rw---- 1 1000 1000  6158 Jul 31  2008 MODSECURITY_LICENSING_EXCEPTION
-rw-rw---- 1 1000 1000   651 Mar  6  2009 README.TXT
drwxrwx--- 6 1000 1000  4096 Sep 25  2009 apache2
drwxrwx--- 3 1000 1000  4096 Sep 25  2009 doc
-rw-rw---- 1 1000 1000  1884 Sep  8  2007 modsecurity.conf-minimal
drwxrwx--- 5 1000 1000  4096 Sep 25  2009 rules
drwxrwx--- 2 1000 1000  4096 Sep 25  2009 tools
```

폴더 내에 apache2 폴더로 이동합니다.

```
[root@localhost modsecurity-apache_2.5.10]# cd apache2/
[root@localhost apache2]# ls
Makefile.in      apache2_io.c    configure.in           modsecurity.h  msc_lua.c      msc_pcre.c    msc_util.c    persist_dbm.c  re_tfns.c
Makefile.win     apache2_util.c  mlogc-src              modules.mk     msc_lua.h      msc_pcre.h    msc_util.h    persist_dbm.h  re_variables.c
acmp.c           api             mod_security2.c        msc_geo.c      msc_multipart.c msc_release.c msc_xml.c     re.c           t
acmp.h           build           mod_security2_config.h.in msc_geo.h   msc_multipart.h msc_release.h msc_xml.h     re.h           utf8tables.h
apache2.h        buildconf       mod_security2_config.hw msc_logging.c msc_parsers.c  msc_reqbody.c pdf_protect.c re_actions.c
apache2_config.c configure       modsecurity.c          msc_logging.h  msc_parsers.h  msc_test.c    pdf_protect.h re_operators.c
```

modsecurity 컴파일

root@localhost# ./configure --with-apxs=/[apache설치경로]/bin/apxs

```
[root@localhost apache2]# ./configure --with-apxs=/usr/sbin/apxs
```

modsecurity 설치

root@localhost# make && make install

```
[root@localhost apache2]# ./configure --with-apxs=/usr/sbin/apxs
checking for gawk... gawk
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking how to run the C preprocessor... gcc -E
checking for a BSD-compatible install... /usr/bin/install -c
checking whether ln -s works... yes
checking whether make sets $(MAKE)... yes
checking for ranlib... ranlib
checking for grep that handles long lines and -e... /bin/grep
checking for perl... /usr/bin/perl
checking for env... /bin/env
checking for egrep... /bin/grep -E
checking for ANSI C header files... yes
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
checking for string.h... yes
```

---------- 생 략 ----------

```
chmod 644 /usr/lib/httpd/modules/mod_security2.a
ranlib /usr/lib/httpd/modules/mod_security2.a
PATH="$PATH:/sbin" ldconfig -n /usr/lib/httpd/modules
----------------------------------------------------------------------
Libraries have been installed in:
   /usr/lib/httpd/modules

If you ever happen to want to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the `-LLIBDIR'
flag during linking and do at least one of the following:
   - add LIBDIR to the `LD_LIBRARY_PATH' environment variable
     during execution
   - add LIBDIR to the `LD_RUN_PATH' environment variable
     during linking
   - use the `-Wl,--rpath -Wl,LIBDIR' linker flag
   - have your system administrator add LIBDIR to `/etc/ld.so.conf'

See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
----------------------------------------------------------------------
chmod 755 /usr/lib/httpd/modules/mod_security2.so
```

설치가 완료되었습니다.

Apache 설치 경로에 Modsecurity2.so 파일이 생성되었는지 확인해 주시기 바랍니다.

```
[root@localhost ~]# cd /etc/httpd/modules/
[root@localhost modules]# ll |grep mod_security
-rwxr-xr-x 1 root root  949824 Jan 17 14:23 mod_security2.so
[root@localhost modules]#
```

4. Apache에 modsecurity 연동하기

vi 편집기로 apache 설정파일 내에 아래 내용을 추가합니다.

root@localhost# cd /[apache설치경로]/conf/httpd.conf
mod security
LoadModule security2_module modules/mod_security2.so
LoadFile /usr/lib/libxml2.so
Include conf/[정책설정파일명].conf

```
[root@localhost backup]# vi /etc/httpd/conf/httpd.conf

#
# This is the main Apache server configuration file.  It contains the
# configuration directives that give the server its instructions.
# See <URL:http://httpd.apache.org/docs/2.2/> for detailed information.
# In particular, see
# <URL:http://httpd.apache.org/docs/2.2/mod/directives.html>
# for a discussion of each configuration directive.
#
#
# Do NOT simply read the instructions in here without understanding
# what they do.  They're here only as hints or reminders.  If you are unsure
# consult the online docs. You have been warned.
```

---------- 생 략 ----------

```
### mod security ###

LoadModule security2_module modules/mod_security2.so
LoadFile /usr/lib/libxml2.so
Include conf/rules.conf
```

5. Modsecurity 정책 설정

Modsecurity의 경우 KISA에서 제공하는 차단 샘플 정책이 있으며, 해당 정책 파일을 참고하시기 바랍니다.

KISA 접속 URL :
http://toolbox.krcert.or.kr/MMVF/MMVFView_V.aspx?MENU_CODE=8&PAGE_NUMBER=13