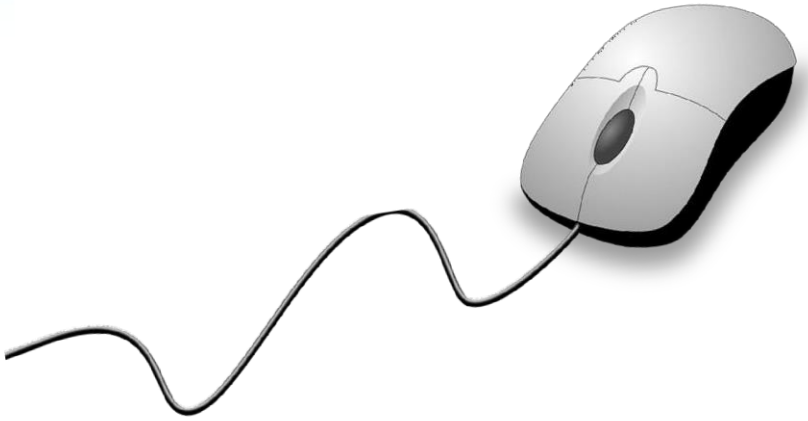
공개SW 솔루션 설치 & 활용 가이드

시스템SW > 보안



modsecurity

Open Source Web Application Firewall

제대로 배워보자

How to Use Open Source Software

Open Source Software Installation & Application Guide

OPENUP

오픈소스 소프트웨어 통합지원센터

Open Source Software Support Center

CONTENTS

1. 개요

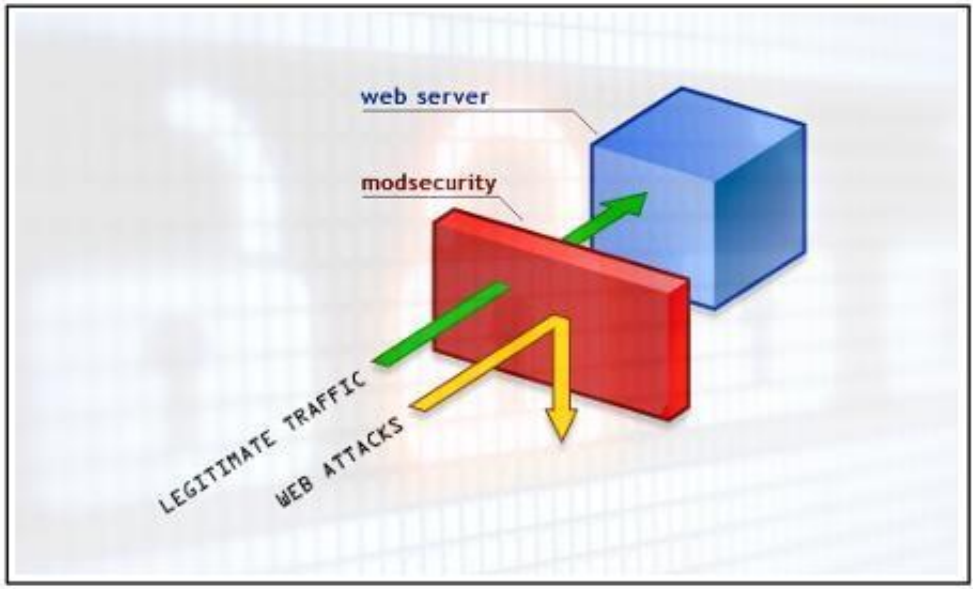
modsecurity
Open Source Web Application Firewall

소개	• ModSecurity는 웹 서비스의 공격을 효과적으로 차단할 수 있는 공개 웹 응용 프로그램 방화벽 모듈 (WAF)		
주요기능	• 웹 서비스를 통해서 공격을 시도하는 XSS, SQL Injection, Command Execute과 같은 공격을 효과적으로 차단하는 역할을 수행하는 보안 모듈이며, Apache HTTP 서버, 마이크로소프트 IIS 및 NGINX에서도 사용 가능		
대분류	• 시스템 SW	**소분류**	• 보안
라이선스 형태	• Apache License Version 2.0	**사전설치 솔루션**	• pcre, apr, apr-util, libxml2, pcre-devel, libxml2-devel, curl-devel
실행 하드웨어	• Cross-platform	**버전**	• 2.9.2 (2018년 10월 기준)
특징	• ModSecurity 는 가장 널리 알려져 있는 HTTP,HTTPS를 이용한 공격을 차단 할 수 있는 웹방화벽 • 공개SW로 무료 사용가능하며 다양한 웹 서버에서 사용 가능 • 실시간 애플리케이션 보안 모니터링 및 액세스 제어 및 전체 HTTP 트래픽 로깅		
보안취약점	• 취약점 ID : CVE-2013-5705 • 심각도 : 5.0 MEDIUM (V2) • 취약점 설명 : 웹 애플리케이션 보안을 강화하려는 Apache 모듈 인 ModSecurity에서 cunked 요청이 처리되는 방식의 결함을 발견 • 대응방안 : 2.6.6 이상으로 버전 업그레이드 • 참고 경로 : https://www.debian.org/security/2014/dsa-2991		
개발 후원사	• Trustwave : http://www.trustwave.com		
공식 홈페이지	• https://www.modsecurity.org/		

2. 기능요약

modsecurity
Open Source Web Application Firewall

- ModSecurity의 주요기능



- ModSecurity는 웹 공격에 대한 침입탐지 및 침입방지 기능을 추가해주는 아파치 웹서버 하나의 모듈로 동작
- 웹 클라이언트와 아파치 웹 서버 사이에 ModSecurity가 존재함
- 클라이언트로부터 악의적인 접속요청이 발견되면 공격차단, 로깅 등 사전에 정의된 행위 수행

3. 실행환경

modsecurity
Open Source Web Application Firewall

- 하드웨어 제약이 거의 없음
- OS 플랫폼 종류에 따른 지원

  - Unix 계열

  - 비Unix 플랫폼 : Windows (비Unix 플랫폼으로 통상 사용하지 않음)
- ModSecurity를 설치하는 쉬운 방법은 기존 OS 패키지 관리자 응용 프로그램 (Yum 또는 Aptitude)을 사용하여 기본 OS 저장소OS Repository에서 설치

  (우분투 및 윈도우 설치는 다음 URL 을 참고 : https://www.modsecurity.org/download.html)

  RHEL/CentOS Yum Repository (Jason Litka)
  Debian (Alberto Gonzalez Iniesta)
  Fedora Core (Michael Fleming)
  FreeBSD (Alex Dupre)
  Gentoo
  Apache 2.x on Windows (Steffen)
  HP-UX (Internet Express)
  Netware, Windows (Guenter Knauf)

4. 설치 및 실행

세부 목차

4.1 설치 환경 준비 및 설치 (CentOS-Source)

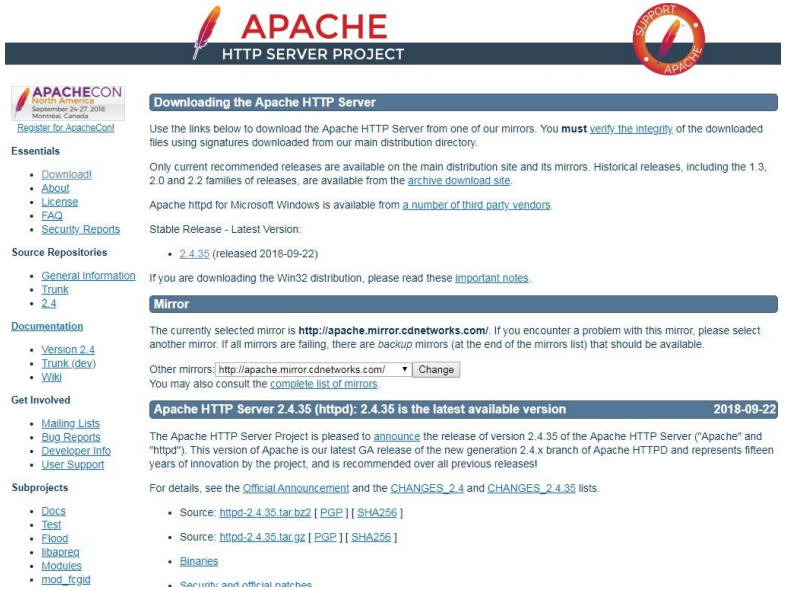
4. 설치 및 실행

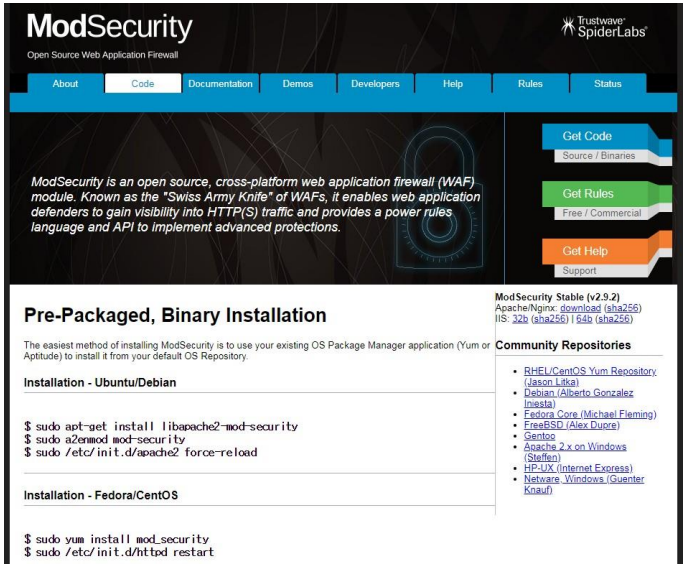
4.1 설치 환경 준비 및 설치(1/9)

- **설치 파일 버전** (18년 10월 기준 최신/안정화 권고버전 사용 및 파일 다운로드)
  - OS version: CentOS Linux release 7.5.1804 (Core)
  - Apache HTTP version : httpd-2.4.35

    Download : https://httpd.apache.org/download.cgi#apache24
  - modsecurity version : modsecurity-2.9.2

    Download : https://www.modsecurity.org/download.html





4. 설치 및 실행

4.1 설치 환경 준비 및 설치(2/9)

- **Apache HTTP 설치**

1. 설치 경로

   - Apache 설치 경로 : /app/web/apache24

2. Apache install

   - 다운로드 받은 Apache 파일의 경로에서 아래의 명령어(cli) 실행

```
# tar xvf httpd-2.4.35.tar.gz
# cd httpd-2.4.35/
# ./configure --prefix=/app/web/apache24 --with-mpm=worker --enable-mods-shared=all
# make && make install
# cd /app/web/apache24/bin
# ./apachectl –t
```

4. 설치 및 실행

4.1 설치 환경 준비 및 설치(3/9)

modsecurity
Open Source Web Application Firewall

3. Apache HTTP 기동 및 확인

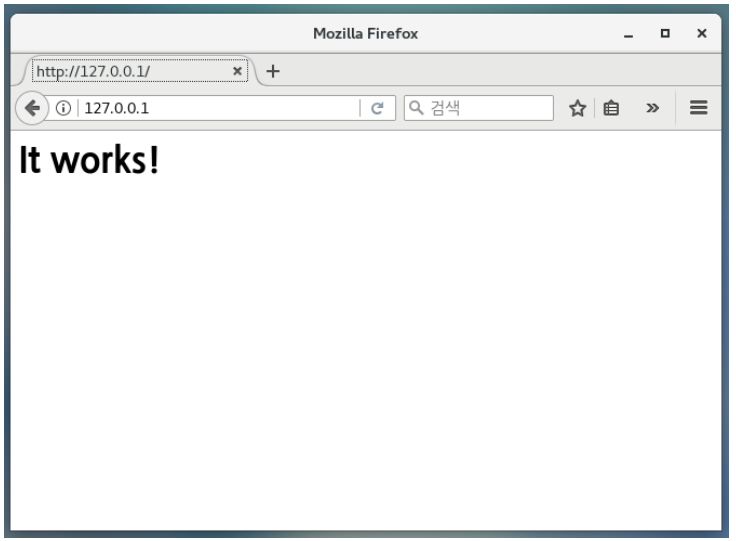
vi ../conf/httpd.conf

- ServerName {hostname} 입력

./apachectl start

ps -ef | grep httpd

curl 127.0.0.1




```
[root@centos bin]# ./apachectl start
[root@centos bin]# ps -ef | grep httpd
root     10420     1  0 14:08 ?        00:00:00 /app/web/apache24/bin/httpd -k start
daemon   10421 10420  0 14:08 ?        00:00:00 /app/web/apache24/bin/httpd -k start
daemon   10422 10420  0 14:08 ?        00:00:00 /app/web/apache24/bin/httpd -k start
daemon   10423 10420  0 14:08 ?        00:00:00 /app/web/apache24/bin/httpd -k start
root     10506  2932  0 14:08 pts/0    00:00:00 grep --color=auto httpd
[root@centos bin]# netstat -anp | grep httpd
tcp6       0      0 :::80                   :::*                    LISTEN      10420/httpd
[root@centos bin]# curl 127.0.0.1
<html><body><h1>It works!</h1></body></html>
[root@centos bin]#
```

- **ModSecurity 설치(1/6)**

1. 모듈 설치

- 다운로드 받은 파일 압축 해제

```
# tar xvf modsecurity-2.9.2.tar.gz
# cd modsecurity-2.9.2
# ./configure --with-apxs=/app/web/apache24/bin/apxs
# make && make install
# cp modsecurity.conf-recommended /app/web/apache24/conf/modsecurity.conf
# cp unicode.mapping /app/web/apache24/conf/
```

2. Apache module 확인

```
# cd /app/web/apache24/modules
# ls -lart
```

제일 하단부에 "ModSecurity2.so" so파일 추가로 생성 확인

- **ModSecurity 설치(2/6)**

3. httpd.conf 에 해당 모듈 추가

vi /app/web/apache24/conf/httpd.conf

LoadModule security2_module modules/ModSecurity2.so
LoadModule unique_id_module modules/mod_unique_id.so

- 적용 확인

./apachectl -M | grep security
security2_module (shared)

```
[root@centos bin]# ./apachectl -M | grep security
 security2_module (shared)
[root@centos bin]#
```

4. 룰셋 다운로드 및 적용

1. 2점대 버전의 룰셋 다운로드

https://github.com/SpiderLabs/owasp-modsecurity-crs/releases

- 2.2.9 버전 다운로드 (OWASP는 최소한의 웹어플리케이션 보안을 제공하기 위해 Modsecurity Core Rule Set (CRS) 프로젝트를 진행하고 있으며, OWASP TOP10을 포함한 강력한 룰셋 제공

- **ModSecurity 설치(3/6)**

2. 다운로드 파일 압축 해제 파일이동

```
# unzip owasp-modsecurity-crs-2.2.9.zip
# mv owasp-modsecurity-crs-2.2.9 modsecurity-crs
# mv modsecurity-crs /app/web/apache24/conf/
# cd /app/web/apache24/conf/modsecurity-crs
```

3. 룰셋 적용

(* 룰셋 : 광범위한 웹공격으로부터 웹 응용 프로그램을 보호하기 위한 일반적인 공격탐지 규칙의 집합)

```
# cp modsecurity_crs_10_setup.conf.example  modsecurity_crs_10_setup.conf
# for f in `ls base_rules/` ; do ln –s /app/web/apache24/conf/modsecuritycrs/base_rules/$f activated_rules/$f ; done
# ln -s /app/web/apache24/conf/modsecurity-crs/modsecurity_crs_10_setup.conf activated_rules/modsecurity_crs_10_setup.conf
```

- **ModSecurity 설치(4/6)**

vi modsecurity_crs_10_setup.conf

아래의 옵션 추가 S

ecRuleEngine On
SecAuditEngine On
SecAuditLog /app/web/apache24/logs/modsec_audit.log
SecAuditLogParts ABCFHZ
SecDataDir /tmp

```
#
SecRuleEngine On
SecAuditEngine On
SecAuditLog /app/web/apache24/logs/modsec_audit.log
SecAuditLogParts ABCFHZ
SecDataDir /tmp
```

아래의 옵션 수정

원본
SecDefaultAction "phase:1,deny,log"
SecDefaultAction "phase:2,deny,log"

수정내역
SecDefaultAction "phase:1,deny,log,auditlog"
SecDefaultAction "phase:2,deny,log,auditlog"

```
#
#SecDefaultAction "phase:1,deny,log"
#SecDefaultAction "phase:2,deny,log"

SecDefaultAction "phase:1,deny,log,auditlog"
SecDefaultAction "phase:2,deny,log,auditlog"
```

4. 설치 및 실행

4.1 설치 환경 준비 및 설치(8/9)

- **ModSecurity 설치(5/6)**

  # vi /app/web/apache24/conf/httpd.conf

  맨 아랫부분에 추가

  Include conf/modsecurity-crs/activated_rules/*.conf

  # cd /app/web/apache24/bin

  # ./apachectl –t

```
[root@centos conf]# cd ../bin
[root@centos bin]# ./apachectl -t
Syntax OK
[root@centos bin]#
```

재기동

```
[root@centos bin]# ./apachectl stop
[root@centos bin]# ./apachectl start
[root@centos bin]# ps -ef | grep httpd
root      3055     1  0 14:23 ?        00:00:00 /app/web/apache24/bin/httpd -k start
daemon    3056  3055  0 14:23 ?        00:00:00 /app/web/apache24/bin/httpd -k start
daemon    3057  3055  0 14:23 ?        00:00:00 /app/web/apache24/bin/httpd -k start
daemon    3058  3055  0 14:23 ?        00:00:00 /app/web/apache24/bin/httpd -k start
root      3141  2932  0 14:23 pts/0    00:00:00 grep --color=auto httpd
[root@centos bin]#
```

4. 설치 및 실행

4.1 설치 환경 준비 및 설치(9/9)

- **ModSecurity 설치(6/6)**

  - 로그 확인

    # cd /app/web/apache24/logs

```
[root@centos logs]# pwd
/app/web/apache24/logs
[root@centos logs]# ls
access_log  error_log  httpd.pid  modsec_audit.log
[root@centos logs]#
```

```
[root@centos logs]# cat modsec_audit.log
--3debcc15-A--
[15/Oct/2018:14:34:44 +0900] W8Qm9BejwlmDcjVf029prgAAAEs 192.168.56.101 60684 192.168.56.101 80
--3debcc15-B--
GET /?q="><script>alert(1)</script> HTTP/1.1
User-Agent: curl/7.29.0
Host: 192.168.56.101
Accept: */*

--3debcc15-F--
HTTP/1.1 200 OK
Last-Modified: Mon, 11 Jun 2007 18:53:14 GMT
ETag: "2d-432a5e4a73a80"
Accept-Ranges: bytes
Content-Length: 45
Content-Type: text/html

--3debcc15-H--
Stopwatch: 1539581684189403 2138 (- - -)
Stopwatch2: 1539581684189403 2138; combined=342, p1=340, p2=0, p3=0, p4=0, p5=2, sr=32, sw=0, l=0, gc=0
Producer: ModSecurity for Apache/2.9.2 (http://www.modsecurity.org/); OWASP_CRS/2.2.9.
Server: Apache/2.4.35 (Unix)
Engine-Mode: "ENABLED"

--3debcc15-Z--

--3debcc15-A--
[15/Oct/2018:14:35:00 +0900] W8QnBE7ivmPg8wlDIpRPcAAAAIA 192.168.56.101 60686 192.168.56.101 80
--3debcc15-B--
GET /?q="><script>alert(1)</script> HTTP/1.1
User-Agent: curl/7.29.0
Host: 192.168.56.101
Accept: */*
```

5. 기능소개

세부 목차

5.1 ModSecurity 주요기능

5. 기능소개

5.1 ModSecurity 주요기능(1/2)

modsecurity
Open Source Web Application Firewall

- ModSecurity의 주요기능은 HTTP의 포스팅 악용이나 Buffer overflow 등의 공격, 웹의 취약점을 이용한 SQL Injection / php injection 등의 공격을 drop 할 수 있는 기능을 제공하며, 설치 후 로그를 분석하여 공격형태 및 패턴을 분석하여 룰을 작성할 수 있는 아파치 모듈의 일종임

- 요청(request) 필터링 기능

  - 클라이언트로부터 웹 요청이 들어올 때, 웹서버 또는 다른 모듈들이 처리하기 전에 ModSecurity가 요청 내용을 분석하여 필터링 처리

- 우회 방지 기술 기능

  - 경로와 파라미터를 분석하기 전에 정규화 시켜 우회 공격을 차단, 즉 "//", "₩/", "./", "%00" 등 우회 공격용 스트링을 제거하고, 인코딩된 URL 디코딩 함

5. 기능소개

5.1 ModSecurity 주요기능(2/2)

modsecurity
Open Source Web Application Firewall

- HTTP 프로토콜 이해

  - 엔진이 HTTP 프로토콜을 이해하기 때문에 전문적이고 정밀한 필터링 수행 함

- POST 페이로드(payload) 분석

  - GET 방식 뿐만 아니라 POST 메소드를 사용해서 전송되는 컨텐츠도 가로채어 분석 가능

- 감사 로깅

  - POST를 포함하여 모든 요청의 모든 상세한 부분들까지 추후 분석을 위해서 로깅
  - ModSecurity에서 차단 기능을 비활성화 시킨 후, 강력한 로깅 기능만으로 침입탐지 시스템 역할 수행

- HTTPS 필터링

  - 엔진은 웹서버에 임베디드 되어 있기 때문에 복호화 한 후에 요청 데이터에 접근하여 HTTPS를 통한 공격 필터링 함

6. 활용예제

세부 목차

1. 기본 기능 설정 및 지시자
2. 기능 점검 및 활용 예제

- **ModSecurity.conf 옵션 정리**

1. SecRuleEngine On | Off | DetectionOnly

   ModSecurity 기능 활성화(enable)

   - On : ModSecurity 기능 활성화
   - Off : ModSecurity 기능 비활성화
   - DetectionOnly : 활성화는 하지만 차단하지 않고 탐지만 함

2. SecAuditEngine On | Off | RelevantOnly

   감사 로깅에 대한 설정 구성

   - On : 모든 트랜젝션 로깅
   - Off : 모든 트랜젝션 로깅하지 않음
   - DetectionOnly : Error 또는, Warning 의 트랜젝션, 그리고 SecAuditLogRelevantStatus에 정의된 상태 코드와 일치하는 트랜젝션만 로깅

3. SecAuditLog logs/modsec_audit.log

감사 로그 파일의 경로 정의

예) SecAuditLog /usr/local/apache2/logs/modsec_audit.log

4. SecAuditLogParts

로그 파일에 기록할 항목 정의 예) SecAuditLogParts ABCFHZ

- audit log header (필수)
- request header
- request body(request body가 존재하고 modsecurity가 request body를 검사하도록 설정되어 있는 경우에만)
- 보류중, response header의 중개(현재 지원 안 됨)
- response body 중간 단계(현재 modsecurity가 response body를 검사하며 감사로깅 엔진이 이를 저장하게끔 설정되어 있는 경우에만)
- 최종 response header(마지막 컨텐츠 전달 과정에서 아파치에 의해 매번 추가 되는 날짜와 서버 헤더 제외)

- 실제 response body (현재 지원 안됨)
- 감사 로그 트레일러
- 이 옵션은 C를 대체하는 옵션, multipart/form-data 인코딩이 사용되었을 때를 제외한 모든 경우엔 C와 같은 데이터 기록
- 보류중, multipart/form-data 인코딩을 사용하는 파일 업로드에 대한 정보를 포함할 때 효과가 있음
- 로그의 끝 의미 (필수)

5. SecAuditLogRelevantStatus REGEX

감사 로깅의 목적과 관련된 response 상태 코드의 값 설정

- 매개변수에는 정규표현식 들어감

  예) SecAuditLogRelevantStatus ^[45]

6. SecAuditLogType Serial | Concurrent 감사 로깅 구조의 타입 설정
   - Serial - 모든 로그는 메인 로그파일에 저장, 일시적으로 편리할 순 있지만 하나의 파일에만 기록되기 때문에 느려질 수 있음
   - Concurrent - 로그가 각 트랜잭션 별로 나누어 저장
     이 방식은 로그파일을 원격 ModSecurity Console host로 보낼 때 사용하는 방식

7. SecDefaultAction "log, auditlog, deny, status:403, phase:2, t:lowercase"
   - 룰이 매칭되면 기본적으로 취할 행동 정의
   - 룰이 특정 액션들에 대한 개별 룰을 적용하거나 다른 SecDefaultAction이 정의 되어있지 않다면 최초 지정된 SecDefaultAction의 설정 따름
   - 위의 예는 룰이 매칭 되었을 때 차단하며 로그를 남기고, 403 상태코드 페이페이지를 보여주며 필터링 단계는 "2"이며, 기본적으로 대문자는 모두 소문자로 바뀌어 필터링 됨

8. SecRequestBodyAccess On | Off

Request 값에서 Body 부분에 대한 처리 어떻게 할 것인지 구성

- On : RequestBody 접근을 시도
- Off : RequestBody 접근 시도를 하지 않음

이 지시자는 Request 값에서의 POST_PAYLOAD 검사할 때 필요

POST값을 필터링하기 위해서는 phase:2와 REQUESET_BODY 변수/로케이션, 3가지가 모두 구성 되어야만 처리가 가능

9. SecReponseBodyAccess On | Off

Response 값에서 Body 부분에 대한 처리를 어떻게 할 것인지 구성

- On : ResponseBody 접근 시도 (그러나 MIME 타입과 일치해야만 함)
- Off : ResponseBody 접근시도 하지 않음

이 지시자는 html 응답을 조사하기 위해 필요함

"phase:4"의 처리 단계와 RESPONSE_BODY 변수/로케이션, 3가지가 설정되어 있지 않으면, response body를 검사할 수 없음

10. SecResponseBodyLimit

ModSecurity가 Response Body 크기로 할당할 수 있는 메모리 최대 크기 설정

- SecRequestBodyLimit 524228 이 값을 넘어가면 서버는 500 내부 서버 오류 메시지만 표시

11. SecReponseBodyMimeType mime/type

Response 값에서 Body 값을 버퍼링할 MIME 타입 설정

- SecResponseBodyMimeType text/plain text/html // 기본값 Mime 타입은 복수로 추가

12. SecReponseBodyMimeTypesClear

ResponseBody의 버퍼링 위해 Mime 타입의 목록 지우며, 처음에 위치

- SecResponseBodyMimeType

- **ModSecurity 적용 확인**

curl --head 192.168.56.101

```
[root@centos logs]# curl --head 192.168.56.101
HTTP/1.1 403 Forbidden
Date: Mon, 15 Oct 2018 05:58:51 GMT
Server: Apache/2.4.35 (Unix)
Content-Type: text/html; charset=iso-8859-1
```

vi /app/web/apache24/conf/modsecurity-crs/modsecurity_crs_10_setup.conf
SecServerSignature "modsecurity_test" 추가

```
SecRuleEngine On
SecAuditEngine On
SecAuditLog /app/web/apache24/logs/modsec_audit.log
SecAuditLogParts ABCFHZ
SecDataDir /tmp

SecServerSignature "modsecurity_test"
```

- 아파치 재기동

curl --head 192.168.56.101 (Apache 가 아닌 modsecurity_test 가 출력되면 정상)

```
[root@centos bin]# curl --head 192.168.56.101
HTTP/1.1 403 Forbidden
Date: Mon, 15 Oct 2018 06:05:39 GMT
Server: modsecurity_test
Content-Type: text/html; charset=iso-8859-1
```

modsecurity
Open Source Web Application Firewall

- **ModSecurity 테스트를 위한 XSS 공격 테스트**

  # curl 'http://192.168.56.101/?q="><script>alert(1)</script>'

```
[root@centos bin]# curl 'http://192.168.56.101/?q="><script>alert(1)</script>'
<html><body><h1>It works!</h1></body></html>
[root@centos bin]#
```

ModSecurity 가 정상적으로 적용되었다면 403 Forbidden 응답이 표시
(Apache 웹 서버에 악의적인 요청(XSS공격)을 ModSecurity가 차단)

```
[root@centos bin]# curl 'http://192.168.56.101/?q="><script>alert(1)</script>'
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /
on this server.<br />
</p>
</body></html>
[root@centos bin]#
[root@centos bin]#
```

- **ModSecurity rule를 통한 ip 예외처리**

  적용 후 웹 서버를 재기동하면 기본 페이지가 403 에러코드로 보이게 됨

  즉 정상적인 접근도 차단

Forbidden

You don't have permission to access / on this server.

웹 서버 로그를 통해 어떤 룰을 통해서 Forbidden 이 발생하는지 확인

```
--84ff4642-H--
Message: Access denied with code 403 (phase 2). Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host. [file "/a
pp/web/apache24/conf/modsecurity-crs/activated_rules/modsecurity_crs_21_protocol_anomalies.conf"] [line "98"]
 [id "960017"] [rev "2"] [msg "Host header is a numeric IP address"] [data "192.168.56.101"] [severity "WARNI
NG"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST"] [tag
"WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [tag "http://technet.microsoft.com/en-us/magazin
e/2005.01.hackerbasher.aspx"]
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 192.168.56.1] ModSecurity: Access denied w
ith code 403 (phase 2). Pattern match "^[\\\\\\\\\\d.:]+$" at REQUEST_HEADERS:Host. [file "/app/web/apache24/co
nf/modsecurity-crs/activated_rules/modsecurity_crs_21_protocol_anomalies.conf"] [line "98"] [id "960017"] [re
v "2"] [msg "Host header is a numeric IP address"] [data "192.168.56.101"] [severity "WARNING"] [ver "OWASP_C
RS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST"] [tag "WASCTC/WASC-21"]
[tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [tag "http://technet.microsoft.com/en-us/magazine/2005.01.hackerba
sher.aspx"] [hostname "192.168.56.101"] [uri "/favicon.ico"] [unique_id "W8QzZd5v5LuHtESXuwwkXAAAAA4"]
Action: Intercepted (phase 2)
Stopwatch: 1539584869757725 1410 (- - -)
Stopwatch2: 1539584869757725 1410; combined=640, p1=561, p2=54, p3=0, p4=0, p5=25, sr=112, sw=0, l=0, gc=0
Producer: ModSecurity for Apache/2.9.2 (http://www.modsecurity.org/); OWASP_CRS/2.2.9.
Server: Apache/2.4.35 (Unix)
Engine-Mode: "ENABLED"
```

modsecurity
Open Source Web Application Firewall

- **ModSecurity rule를 통한 ip 예외처리 설정**

  반복되는 로그를 확인해보면 "ID 960017" 확인

  해당 ID는 전체적인 modsecurity 설정에서 제외시켜 줄 수 있음

  (파일명 : modsecurity_crs_21_protocol_anomalies.conf , ID : 960017)

```
--84ff4642-H--
Message: Access denied with code 403 (phase 2). Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host. [file "/a
pp/web/apache24/conf/modsecurity-crs/activated_rules/modsecurity_crs_21_protocol_anomalies.conf"] [line "98"]
 [id "960017"] [rev "2"] [msg "Host header is a numeric IP address"] [data "192.168.56.101"] [severity "WARNI
NG"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST"] [tag
"WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [tag "http://technet.microsoft.com/en-us/magazin
e/2005.01.hackerbasher.aspx"]
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 192.168.56.1] ModSecurity: Access denied w
ith code 403 (phase 2). Pattern match "^[\\\\\\\\\d.:]+$" at REQUEST_HEADERS:Host. [file "/app/web/apache24/co
nf/modsecurity-crs/activated_rules/modsecurity_crs_21_protocol_anomalies.conf"] [line "98"] [id "960017"] [re
v "2"] [msg "Host header is a numeric IP address"] [data "192.168.56.101"] [severity "WARNING"] [ver "OWASP_C
RS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST"] [tag "WASCTC/WASC-21"]
[tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [tag "http://technet.microsoft.com/en-us/magazine/2005.01.hackerba
sher.aspx"] [hostname "192.168.56.101"] [uri "/favicon.ico"] [unique_id "W8QzZd5v5LuHtESXuwwkXAAAAA4"]
Action: Intercepted (phase 2)
Stopwatch: 1539584869757725 1410 (- - -)
Stopwatch2: 1539584869757725 1410; combined=640, p1=561, p2=54, p3=0, p4=0, p5=25, sr=112, sw=0, l=0, gc=0
Producer: ModSecurity for Apache/2.9.2 (http://www.modsecurity.org/); OWASP_CRS/2.2.9.
Server: Apache/2.4.35 (Unix)
Engine-Mode: "ENABLED"
```

modsecurity
Open Source Web Application Firewall

- **ModSecurity rule를 통한 예외처리**

  - (화이트리스트) 로그를 통해 확인 한 ID 입력

    #vi /app/web/apache24/conf/modsecurity-crs/activated_rules/modsecurity_crs_21_protocol_anomalies.conf

```
SecRuleRemoveById 960017
```

    " SecRuleRemoveById 960017 "

  - 아파치 재기동 후 127.0.0.1 호출 성공 (화이트리스트 적용)

It works!

6. 활용예제

6.2 기능 점검 및 활용 예제(6/6)

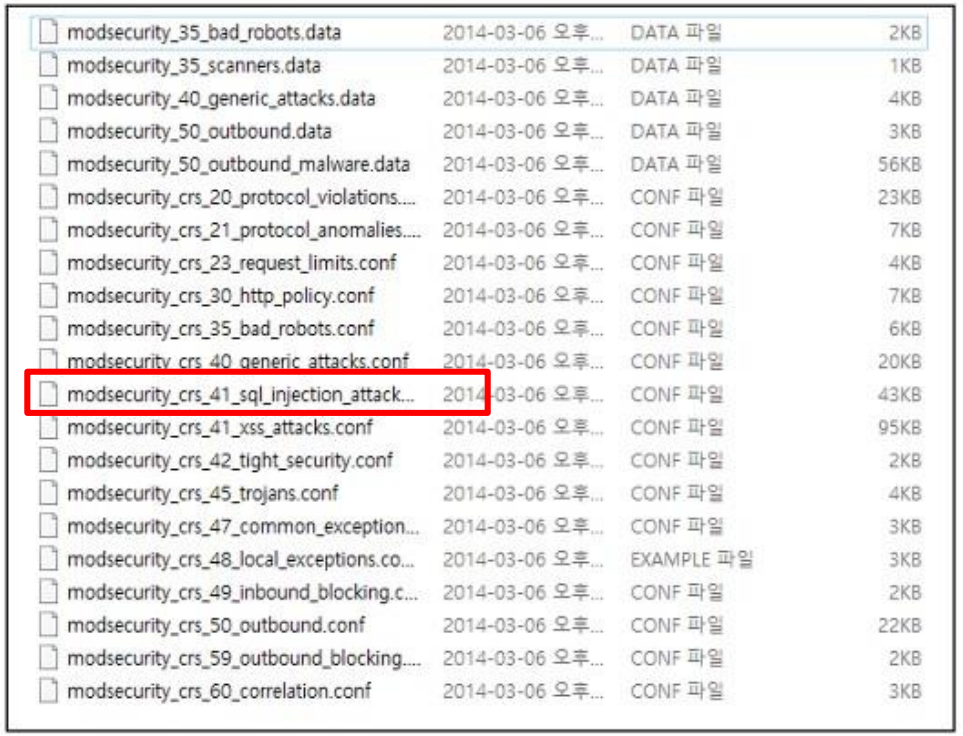
modsecurity
Open Source Web Application Firewall

- **기타 룰셋 활용**
  - 13p 내용에서 적용된 base_rules 폴더를 확인해보면 기본적으로 사용할 수 있는 다양한 룰셋들제공
  - 예를 들어 modsecurity_crs_41_sql_injection_attacks.conf 같은 경우에는 SQL Injection 공격을 차단함
    (DB에 대한 삭제, 추가, 열람시도 등 차단)

```
#
# Example Payloads Detected:
# -------------------------
# OR 1#
# DROP sampletable;--
# admin'--
# DROP/*comment*/sampletable
# DR/**/OP/*bypass blacklisting*/sampletable
# SELECT/*avoid-spaces*/password/**/FROM/**/Members
# SELECT /*!32302 1/0, */ 1 FROM tablename
# ' or 1=1#
# ' or 1=1-- -
# ' or 1=1/*
# ' or 1=1;\x00
# 1='1' or-- -
# ' /*!50000or*/1='1
# ' /*!or*/1='1
# 0/**/union/*!50000select*/table_name`foo`/**/
# -------------------------
#
SecRule REQUEST_COOKIES|!REQUEST_COOKIES:/__utm/|REQUEST_COOKIES_NAMES|ARGS

#
# --[ SQL Hex Evasion Methods ]--
#
SecRule REQUEST_COOKIES|!REQUEST_COOKIES:/__utm/|REQUEST_COOKIES_NAMES|ARGS

#
# --[ String Termination/Statement Ending Injection Testing ]--
#
# Identifies common initial SQLi probing requests where attackers insert/ap
# quote characters to the existing normal payload to see how the app/db re
#
SecRule REQUEST_COOKIES|!REQUEST_COOKIES:/__utm/|REQUEST_COOKIES_NAMES|ARGS
```



Q 아파치 2.0 라이선스란 무엇인가요?

A Apache Software Foundation(ASF)에 의해서 만들어지는 소프트웨어에 붙는License입니다. ASF에서 만들어지는 소프트웨어는 모두 공개SW Apache License V2.0이 적용됩니다. 소스코드에 대한 사용 비용을 지불하지 않으며, 수정 프로그램에 대한 소스코드의 공개를 요구하지 않기 때문에 상용SW에 무제한 사용이 가능합니다.

Q ModSecurity 의 장점이 무엇인가요?

A ModSecurity 모듈은 현재 가장 널리 알려져 있으며, 웹 서비스의 공격을 효과적으로 차단할 수 있는 웹 방화벽입니다. 아파치 웹 서버 뿐만 아니라 Nginx, 마이크로소프트 IIS 등 다양한 웹 서버에도 활용이 가능합니다.

8. 용어정리

용어	설 명
WAF	Web Application Firewall, WAF (웹 방화벽)
Apache Httpd	Apache 재단에서 만든 웹 서버로써 원래 이름이 apache httpd이기 때문에 단독으로 apache, httpd라고 부르기도 하며, 본문에서는 httpd 라고 함
CentOS	The Community Enterprise Operating System
CLI	Command Line Interface (키보드로 명령어를 입력하는 방식)
OWASP	The Open Web Application Security Project 오픈소스 웹 애플리케이션보안 프로젝트
CRS	무료 탐지 룰 : OWASP ModSecurity Core Rule Set – 무료 Commercial Rules from Trustwave SpiderLabs – 유료

Open Source Software Installation & Application Guide