By Falko Timme

Published: 2007-07-05 18:08

Installing ModSecurity2 On Debian Etch

Version 1.0
Author: Falko Timme <ft [at] falkotimme [dot] com>
Last edited 06/22/2007

This article shows how to install and configure **ModSecurity** (version 2) for use with Apache2 on a Debian Etch system. ModSecurity is an Apache module that provides intrusion detection and prevention for web applications. It aims at shielding web applications from known and unknown attacks, such as SQL injection attacks, cross-site scripting, path traversal attacks, etc.

I want to say first that this is not the only way of setting up such a system. There are many ways of achieving this goal but this is the way I take. I do not issue any guarantee that this will work for you!

1 Preliminary Note

I'm assuming that Apache2 is already installed and fully functional on your Debian Etch system.

2 Installation

In Debian Sarge, ModSecurity was available as a `.deb` package in the official Debian repositories, but in Debian Etch it was removed due to some license issues. Fortunately, the original maintainer provides packages for Debian Etch in his own repository. To install these, we need to add his repository to `/etc/apt/sources.list`:

```
vi /etc/apt/sources.list
```

```
[...]
```

```
deb http://etc.inittab.org/~agi/debian/libapache-mod-security2/ etch/
[...]
```

Afterwards, we update our packages database like this:

```
apt-get update
```

Now we can install ModSecurity2 with this simple command:

```
apt-get install libapache2-mod-security2
```

That's it. The ModSecurity2 module gets enabled by default, and Apache2 is restarted automatically.

3 Configuration

Now it's time to configure ModSecurity2. The easiest way to do this is download the ModSecurity2 source package from **http://www.modsecurity.org/download/index.html** (e.g. **http://www.modsecurity.org/download/modsecurity-apache_2.1.1.tar.gz**) and unpack it. It contains a file *modsecurity.conf-minimal* with a basic configuration for ModSecurity2 which I will use here (but I have adjusted the lines *SecDebugLog* and *SecAuditLog* so that ModSecurity2 logs to the */var/log/apache2* directory, Debian's default Apache2 log directory).

We open Apache's main configuration file */etc/apache2/apache2.conf* and put the following configuration into it, right before the end where the virtual hosts are included:

```
vi /etc/apache2/apache2.conf
```

```
[...]
<IfModule mod_security2.c>
   # Basic configuration options
```

```
    SecRuleEngine On
    SecRequestBodyAccess On
    SecResponseBodyAccess Off

    # Handling of file uploads
    # TODO Choose a folder private to Apache.
    # SecUploadDir /opt/apache-frontend/tmp/
    SecUploadKeepFiles Off

    # Debug log
    SecDebugLog /var/log/apache2/modsec_debug.log
    SecDebugLogLevel 0

    # Serial audit log
    SecAuditEngine RelevantOnly
    SecAuditLogRelevantStatus ^5
    SecAuditLogParts ABIFHZ
    SecAuditLogType Serial
    SecAuditLog /var/log/apache2/modsec_audit.log

    # Maximum request body size we will
    # accept for buffering
    SecRequestBodyLimit 131072

    # Store up to 128 KB in memory
    SecRequestBodyInMemoryLimit 131072

    # Buffer response bodies of up to
    # 512 KB in length
    SecResponseBodyLimit 524288

</IfModule>
```

```
# Include the virtual host configurations:
Include /etc/apache2/sites-enabled/
```

Afterwards we restart Apache (it should restart without errors):

```
/etc/init.d/apache2 restart
```

If you haven't got any errors, ModSecurity2 is now working with a basic configuration. You can now modify/extend this basic configuration so that it fits your needs. A good starting point is the **ModSecurity2 documentation**. Also, there are more advanced rulesets in the ModSecurity2 sources that we've downloaded before (in the `rules` directory), and you can even download core rulesets from **http://www.modsecurity.org/download/index.html** (e.g. **http://www.modsecurity.org/download/modsecurity-core-rules_2.1-1.4.tar.gz**).

Christian Folini has provided a **tutorial about Remo, a GUI for creating ModSecurity rulesets**. This is another great way to create your own ModSecurity2 rulesets.

4 Links

- ModSecurity: **http://www.modsecurity.org**
- ModSecurity Documentation: **http://www.modsecurity.org/documentation/modsecurity-apache/2.1.0/html-multipage/**
- Remo - Rule Editor for ModSecurity: **http://remo.netnea.com**
- Debian: **http://www.debian.org**