Judul : *Membangun Web Application Firewall Dengan Modsecurity Sebagai Upaya Pengamanan Website*

Penulis : *Muhammad Romadi Siregar (175410054)*

MANUAL PENELITIAN DAN PENGGUNAAN PROGRAM

1. Kebutuhan

Untuk mewujudkan simulasi keadaan server pada jaringan internet, digunakan beberapa aplikasi, di antaranya :

a. VMWare Fusion

VMWare Fusion adalah aplikasi yang menyediakan virtualisasi, digunakan untuk membuat server virtual di dalam komputer lokal. Aplikasi ini dapat diganti dengan VirtualBOX atau aplikasi penyedia virtualisasi yang lain.

b. Sistem Operasi Linux CentOS 6.5

Linux CentOS digunakan oleh semua server virtual yang dibuat pada penelitian ini.

c. Bind / Named

Aplikasi Bind atau Named sebagai DNS server, digunakan untuk membentuk nama domain dari setiap server virtual. Dengan menggunakan penamaan server, maka konfigurasi virtualhost apache identik dengan konfigurasi yang digunakan pada jaringan internet.

d. Apache

Apache merupakan web server yang digunakan pada penelitian.

e. Modsecurity

Modsecurity adalah web application firewall sebagai objek dari penelitian.

f. CMS Wordpress (dengan plugin) dan Joomla

Pada penelitian ini diteliti kelemahan tentang *File Upload*, *PHP Code Injection* dan *PHP Object Injection.* Dipilih beberapa plugin dari wordpress dan joomla yang mengandung kelemahan untuk diteliti.

Tabel 1 Kebutuhan Konfigurasi

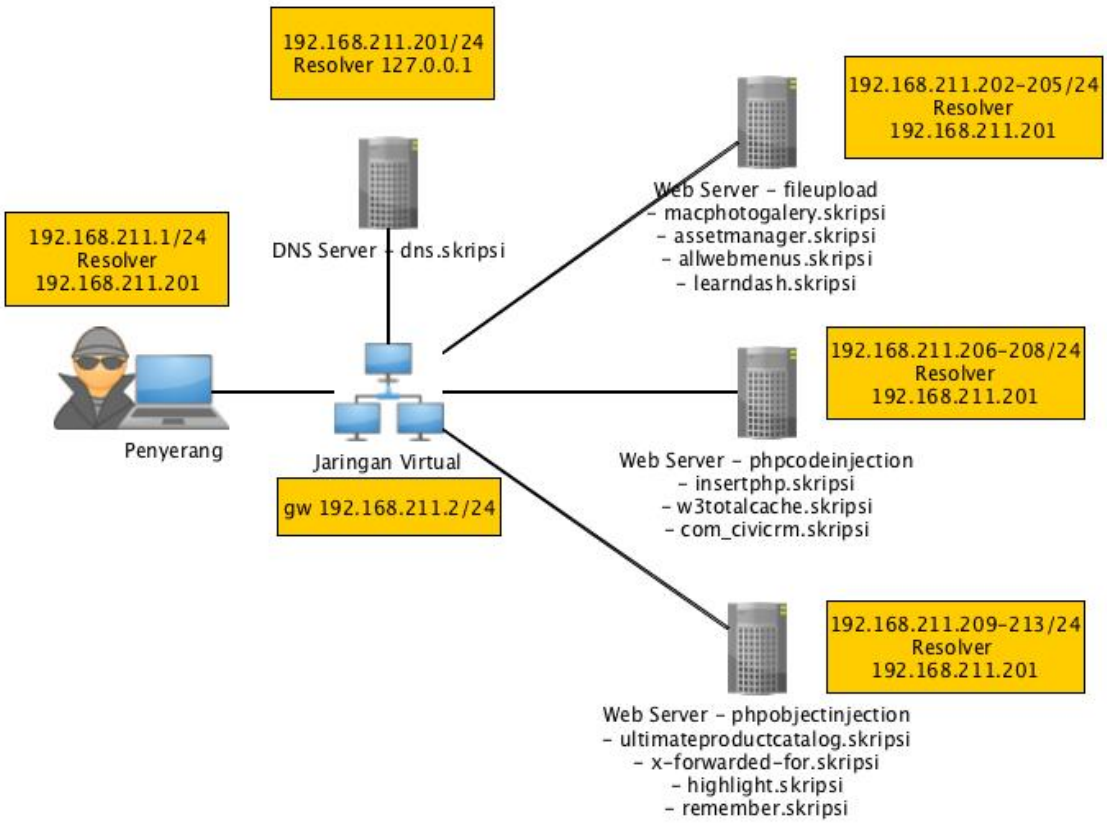
Nama	**Jenis Kelemahan**	**Kebutuhan Konfigurasi**
Wordpress Plugin Mac Photo Gallery 2.7	*File Upload*	Wordpress 3.6+
Wordpress Plugin Asset Manager 0.2	*File Upload*	Wordpress 2.7+
Wordpress Plugin AllWebMenus < 1.1.9	*File Upload*	Wordpress 2.3+
Wordpress Plugin LearnDash 2.5.3	*File Upload*	Wordpress 3+
Wordpress Plugin Insert PHP < 3.3.1	*PHP Code Injection*	Wordpress 4.7.0+
Wordpress Plugin W3 Total Cache 0.9.2.3	*PHP Code Injection*	Wordpress 3.2+
Joomla Component com_civicrm 4.2.2	*PHP Code Injection*	Joomla 2.5
Wordpress Plugin Ultimate Product Catalog <= 4.2.24	*PHP Object Injection*	Wordpress 3.5.0+
Joomla! 1.5 < 3.4.5 'x-forwarded-for'	*PHP Object Injection*	Joomla 3.0.2
Joomla! 3.0.2 – 'highlight.php'	*PHP Object Injection*	Joomla 3.0.2
Joomla! 3.0.3 – 'remember.php'	*PHP Object Injection*	Joomla 3.0.3

g. Program Penyerang

Program penyerang digunakan untuk membuat simulasi serangan. Dengan program ini akan diketahui contoh log serangan yang kemudian akan dianalisis pada variabel apa saja yang mungkin

dijadikan filter. Program ini juga digunakan untuk pengujian filter ketika filter sudah diterapkan.

2. Skema Jaringan



Gambar 1 Skema Jaringan

Pada penelitian ini, satu server mewakili sebuah kelemahan, sehingga penamaan server disesuaikan dengan nama kelemahan. Berikut merupakan tabel lengkap konfigurasi alamat ip jaringan.

Tabel 2 Konfigurasi Domain dan Alamat IP

Nama Domain	Alamat IP
ns1.skripsi	192.168.211.201
macphotogallery.skripsi	192.168.211.202
assetmanager.skripsi	192.168.211.203
allwebmenus.skripsi	192.168.211.204
learndash.skripsi	192.168.211.205

insertphp.skripsi	192.168.211.206
w3totalcache.skripsi	192.168.211.207
com-civicrm.skripsi	192.168.211.208
ultimateproductcatalog.skripsi	192.168.211.209
x-forwarded-for.skripsi	192.168.211.210
highlight.skripsi	192.168.211.211
remember.skripsi	192.168.211.212
nginx	192.168.211.213

*top level domain *(tld)* : "skripsi".

Terdapat 13 server virtual yang digunakan pada penelitian ini.

3. Installasi

Server virtual dengan Sistem Operasi Linux CentOS yang telah terinstall kemudian dilengkapi dengan aplikasi yang dibutuhkan. Ada dua jenis server yang mempunyai cara installasi berbeda. Berikut merupakan perintah shell yang dijalankan di dalam server :

a. DNS Server

```
yum install bind bind-utils -y
chkconfig named on
```

b. MySQL Server

```
yum install mysql-server -y
mysql_secure_installation
chkconfig mysqld on
```

c. Web Server

```
rpm -Uvh
http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-
6-8.noarch.rpm
```

```
yum install httpd php php-mysql mod_security -y
chkconfig httpd on
```

4. Konfigurasi

a. Komputer / Laptop Penyerang

Untuk dapat menterjemahkan nama domain dari server virtual maka perlu melakukan setting resolver pada komputer/laptop yang digunakan sebagai penyerang. Resolver harus mengarah ke server DNS. Hal ini dilakukan dengan menambahkan IP DNS server pada list DNS server yang digunakan. Pada penelitian konfigurasi DNS berada pada file "/etc/resolv.conf".

```
nameserver 192.168.211.201
nameserver 192.168.43.1
```

IP 192.168.211.201 merupakan alamat dari DNS Server pada jaringan virtual.

b. DNS Server

- **File named.conf (/etc/named.conf)**

```
options {
      listen-on port 53 { 127.0.0.1;192.168.211.201; };
      listen-on-v6 port 53 { ::1; };
      directory     "/var/named";
      dump-file     "/var/named/data/cache_dump.db";
      statistics-file "/var/named/data/named_stats.txt";
      memstatistics-file "/var/named/data/named_mem_stats.txt";
      allow-query     { localhost; };
      recursion yes;

      dnssec-enable yes;
      dnssec-validation yes;

      /* Path to ISC DLV key */
```

```
      bindkeys-file "/etc/named.iscdlv.key";

      managed-keys-directory "/var/named/dynamic";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
      type hint;
      file "named.ca";
};

// Tambahan untuk TLD .skripsi
zone "skripsi." {
      type master;
      file "/etc/named/db.skripsi";
      allow-transfer { any;};
      allow-query { any;};
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

- **File db.skripsi (/etc/named/db.skripsi)**

```
$TTL 604800
@   IN SOA skripsi. root.skripsi. (
      2     ; Serial
      604800      ; Refresh
      86400 ; Retry
      2419200     ; Expire
```

```
     604800 ); Negative Cache TTL
;

@   IN NS ns1.skripsi.
@   IN NS ns2.skripsi.
ns1       IN A 192.168.211.201
ns2       IN A 192.168.211.201

;Web Server File Upload
macphotogallery         IN A 192.168.211.202
assetmanager            IN A 192.168.211.203
allwebmenus             IN A 192.168.211.204
learndash               IN A 192.168.211.205

;Web Server PHP Code Injection
insertphp               IN A 192.168.211.206
w3totalcache            IN A 192.168.211.207
com-civicrm             IN A 192.168.211.208

;Web Server PHP Object Injection
ultimateproductcatalog  IN A 192.168.211.209
x-forwarded-for         IN A 192.168.211.210
highlight               IN A 192.168.211.211
remember                IN A 192.168.211.212
nginx                 IN A 192.168.211.213
```

c. Web Server

- **MySQL Server**

```
create database wpdb;
create user 'wp'@'localhost' identified by 'skripsipwd';
grant all privileges on wpdb.* to 'wp'@'localhost'
identified by 'skripsipwd';
flush privileges;
```

- **VirtualHost Apache**

  DocumentRoot berada di "/var/www/html/wordpress" untuk cms wordpress dan "/var/www/html/joomla" untuk joomla.

```
<VirtualHost *:80>
    ServerAdmin webmaster@<Nama_Domain>
    DocumentRoot /var/www/html/wordpress
    ServerName <Nama_Domain>
    ErrorLog logs/<Nama_Domain>-error_log
    CustomLog logs/<Nama_Domain>-access_log common
</VirtualHost>
```

Nama domain dan DocumentRoot menyesuaikan. Contoh :

```
<VirtualHost *:80>
    ServerAdmin webmaster@assetmanager.skripsi
    DocumentRoot /var/www/html/wordpress
    ServerName assetmanager.skripsi
    ErrorLog logs/assetmanager.skripsi-error_log
    CustomLog logs/assetmanager.skripsi-access_log common
</VirtualHost>
```

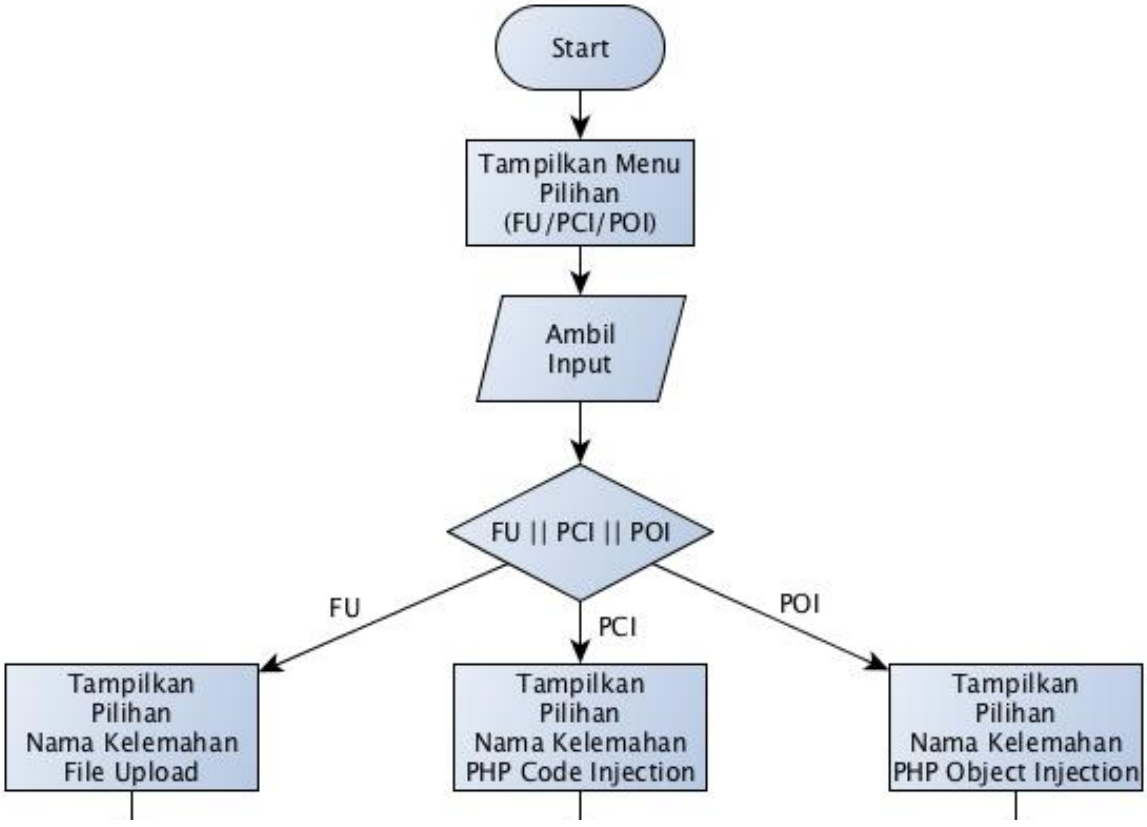
- **ModSecurity (/etc/httpd/conf.d/mod_security.conf)**

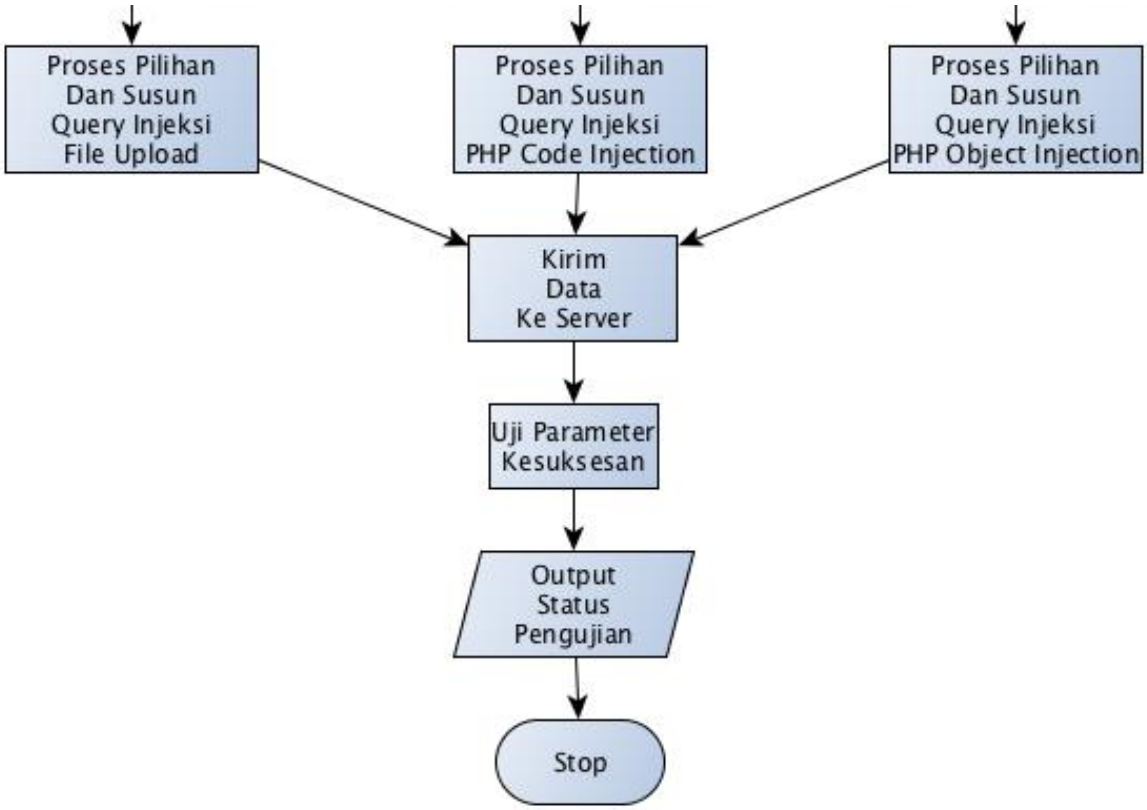
```
LoadModule security2_module modules/mod_security2.so


<IfModule !mod_unique_id.c>
LoadModule unique_id_module modules/mod_unique_id.so
</IfModule>
<IfModule mod_security2.c>
# ModSecurity Core Rules Set configuration
Include modsecurity.d/*.conf
Include modsecurity.d/activated_rules/*.conf
```

```
# Default recommended configuration
SecRuleEngine On
SecRequestBodyAccess On
SecRule REQUEST_HEADERS:Content-Type "text/xml" \
"id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=XML"
SecRequestBodyLimit 13107200
SecRequestBodyNoFilesLimit 131072
SecRequestBodyInMemoryLimit 131072
SecRequestBodyLimitAction Reject
SecRule REQBODY_ERROR "!@eq 0" \
"id:'200001', phase:2,t:none,log,deny,status:400,msg:'Failed to parse request
body.',logdata:'%{reqbody_error_msg}',severity:2"
SecRule MULTIPART_STRICT_ERROR "!@eq 0" \
"id:'200002',phase:2,t:none,log,deny,status:44,msg:'Multipart request body \
failed strict validation: \
PE %{REQBODY_PROCESSOR_ERROR}, \
BQ %{MULTIPART_BOUNDARY_QUOTED}, \
BW %{MULTIPART_BOUNDARY_WHITESPACE}, \
DB %{MULTIPART_DATA_BEFORE}, \
DA %{MULTIPART_DATA_AFTER}, \
HF %{MULTIPART_HEADER_FOLDING}, \
LF %{MULTIPART_LF_LINE}, \
SM %{MULTIPART_MISSING_SEMICOLON}, \
IQ %{MULTIPART_INVALID_QUOTING}, \
IP %{MULTIPART_INVALID_PART}, \
IH %{MULTIPART_INVALID_HEADER_FOLDING}, \
FL %{MULTIPART_FILE_LIMIT_EXCEEDED}'"

SecRule MULTIPART_UNMATCHED_BOUNDARY "!@eq 0" \
"id:'200003',phase:2,t:none,log,deny,status:44,msg:'Multipart parser detected a
possible unmatched boundary.'"

SecPcreMatchLimit 1000
SecPcreMatchLimitRecursion 1000

SecRule TX:/^MSC_/ "!@streq 0" \
```

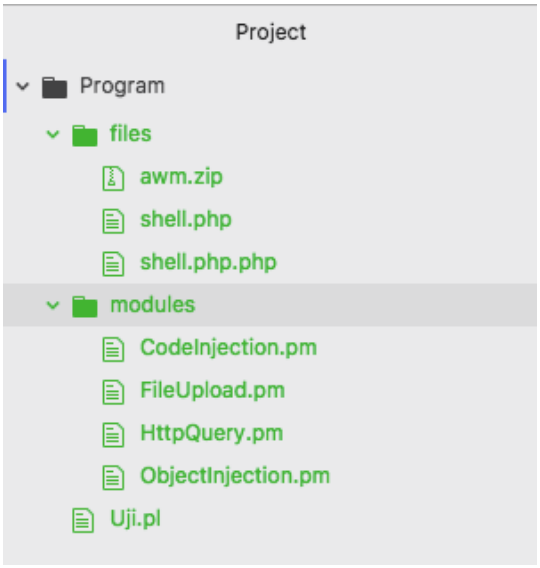
```
"id:'200004',phase:2,t:none,deny,msg:'ModSecurity internal error
flagged: %{MATCHED_VAR_NAME}'"

SecResponseBodyAccess Off
SecDebugLog /var/log/httpd/modsec_debug.log
SecDebugLogLevel 9
SecAuditEngine On
SecAuditLogRelevantStatus "^(?:5|4(?!04))"
SecAuditLogParts ABCJDEFHKZ
SecAuditLogType Serial
SecAuditLog /var/log/httpd/modsec_audit.log
SecArgumentSeparator &
SecCookieFormat 0
SecTmpDir /var/lib/mod_security
SecDataDir /var/lib/mod_security
</IfModule>
```

5. Program Penyerang





Gambar 2 Flowcart Program Penyerang



Gambar 3 Struktur File Program Penyerang

6. Langkah Pengambilan Data

a. DNS Server harus dalam keadaan sudah berjalan.

b. Jalankan server yang mengandung salah satu kelemahan.

c. Jalankan program penyerang dan memilih jenis penyerangan yang sesuai pada komputer/laptop penyerang.

```
 Program : master ✘ : perl Uji.pl
MENU UTAMA PENGUJIAN
--------------------
PILIHAN MODE
1. Normal (Penyerangan)
2. Uji Filter (Pengujian Filter)
Masukkan Mode : 1
1. File Upload
2. PHP Code Injection
3. PHP Object Injection
Masukkan Pilihan : 1


MENU TEST FILE UPLOAD
1. Mac Photo Gallery (Wordpress)
2. Asset Manager (Wordpress)
3. All Web Menus (Wordpress)
4. Learn Dash (Wordpress)
5. Mac Photo Gallery (Wordpress on nginx)
```

Gambar 4 Menu Program Penyerang

d. Konfirmasi pengujian berhasil memanfaatkan kelemahan.

```
 Program : master ✘ : perl Uji.pl
MENU UTAMA PENGUJIAN
--------------------
PILIHAN MODE
1. Normal (Penyerangan)
2. Uji Filter (Pengujian Filter)
Masukkan Mode : 1
1. File Upload
2. PHP Code Injection
3. PHP Object Injection
Masukkan Pilihan : 1


MENU TEST FILE UPLOAD
1. Mac Photo Gallery (Wordpress)
2. Asset Manager (Wordpress)
3. All Web Menus (Wordpress)
4. Learn Dash (Wordpress)
5. Mac Photo Gallery (Wordpress on nginx)
Masukkan Pilihan : 2
```

```
[-] Upload shell.php
Pengujian berhasil! Shell ada di : http://assetmanager.skripsi
/wp-content/uploads/assets/temp/shell.php
  Program : master  : _
```

Gambar 5 Penyerangan Berhasil

e. Masuk ke server dengan ssh untuk mengetahui semua elemen permintaan pengujian dari sisi server.

```
[root@assetmanager ~]# cat /var/log/httpd/modsec_audit.log
--5415520b-A--
[11/Aug/2018:11:52:47 +0700] W25rn38AAAEAAAaGB3EAAAAA 192.168.
211.1 50863 192.168.211.203 80
--5415520b-B--
POST /wp-content/plugins/asset-manager/upload.php HTTP/1.1
TE: deflate,gzip;q=0.3
Connection: TE, close
Host: assetmanager.skripsi
User-Agent: Mozilla/8.0 (Program Penguji)
Content-Length: 173
Content-Type: multipart/form-data; boundary=xYzZY
```

```
--5415520b-C--
--xYzZY
Content-Disposition: form-data; name="Filedata"; filename="she
ll.php"
Content-Type: text/plain

<?php
echo "<pre>";
passthru("cat /etc/passwd");
?>

--xYzZY--
```

Gambar 6 Isi File modsec_audit.log

f. Menyusun rule yang paling efisien memanfaatkan pengetahuan dari audit log pada tahap sebelumnya.

```
SecRule REQUEST_METHOD "post" "chain, id:777001, phase:2, t:lowercase, deny,
log, msg:'AKAKOMSEC: Percobaan exploit assetmanager diblok.'"
SecRule REQUEST_FILENAME "/wp-content/plugins/asset-manager/upload.php" "chain"
SecRule &REQUEST_HEADERS:Cookie "@eq 0" "chain"
SecRule FILES_NAMES|FILES ".php"
```

Gambar 7 Filter akakom_assetmanager.conf

g. Menyimpan dan mengaktifkan rule yang telah dibuat secara spesifik untuk satu kelemahan pada satu file.

```
[root@assetmanager activated_rules]# pwd
/etc/httpd/modsecurity.d/activated_rules
[root@assetmanager activated_rules]# ll
total 4
-rw-r--r-- 1 root root 300 Aug  9 09:10 akakom_assetmanager.co
nf
[root@assetmanager activated_rules]# /etc/init.d/httpd restart
Stopping httpd:                                            [
OK  ]
Starting httpd: httpd: Could not reliably determine the server
's fully qualified domain name, using 127.0.0.1 for ServerName
                                                           [
OK  ]
[root@assetmanager activated_rules]#
```

Gambar 8 Penambahan Filter

Filter yang akan diaktifkan diletakkan pada folder "/etc/httpd/modsecurity.d/activated_rules/". Diperlukan reload apache untuk mengaktifkan filter. Pada penelitian ini digunakan perintah restart httpd.

```
/etc/init.d/httpd restart
```

h. Jalankan program penguji dan memilih jenis pengujian yang sesuai, dilakukan seperti pada tahap 3.

i. Konfirmasi pengujian tidak berhasil.

j. Konfirmasi dengan melihat log pada server untuk menunjukkan rule dapat menangkal pemanfaatan kelemahan pada aplikasi web.

7. Filter Yang Dihasilkan

Semua filter yang berhasil dibuat pada penelitian ini disertakan pada listing program.