

Protect your dynamic webapps using <http://www.modsecurity.org/>

On gentoo

```
emerge mod_security
```

Then setup /etc/apache2/conf/modules.d/99_mod_security.conf

Most important is, you will only want to filter your dynamic content, not the static pages, so make sure the 'SecFilterEngine' directive is set to 'DynamicOnly'.

For protecting Tikiwiki these are useful:

```
SecFilter "tiki-install.php" SecFilter "tiki-edit_templates.php"
```

The modsecurity rules at gotroot got updated on aug12 2005, check them out:

http://www.gotroot.com/mod_security+rules

also see the autoupdater script there: "Downloading the rules automatically" at the bottom of the page...

Take a look at the example below for inspiration:

This script should work with modsecurity 1.8.6 and apache2.

```
LoadModule security_module extramodules/mod_security.so # Examples below are taken from the
online documentation # Refer to: # http://www.modsecurity.org/documentation/quick-examples.html
# Turn the filtering engine On or Off SecFilterEngine On SecFilter DynamicOnly # Action to take by
default SecFilterDefaultAction "deny,log,status:403" SecServerSignature "Apache2" # Make sure
that URL encoding is valid SecFilterCheckURLEncoding On SecFilterCheckUnicodeEncoding Off
SecFilterCheckCookieFormat Off # Should mod_security inspect POST payloads SecFilterScanPOST
Off # Only allow bytes from this range SecFilterForceByteRange 1 255 # The audit engine works
independently and # can be turned On or Off on the per-server or # on the per-directory basis. "On"
will log everything, # "DynamicOrRelevant" will log dynamic requests or violations, # and
"RelevantOnly" will only log policy violations SecAuditEngine RelevantOnly # The name of the audit
log file SecAuditLog logs/audit_log SecFilterDebugLog logs/modsec_debug_log SecFilterDebugLevel
0 # SecFilterSelective REQUEST_METHOD "^POST$" chain # SecFilterSelective HTTP_CONTENT-
TYPE "!(^application/x-www-form-urlencoded$|^multipart/form-data;)" SecFilterSelective
HTTP_Transfer-Encoding "!" # Prevent OS specific keywords SecFilter /etc/passwd SecFilter
/etc/shadow # Prevent path traversal (..) attacks SecFilter "\.\/" # Weaker XSS protection but allows
common HTML tags SecFilter "<[:space:]*script" # Prevent XSS attacks (HTML/Javascript
injection) SecFilter "<(,|n)+>" # Very crude filters to prevent SQL injection attacks SecFilter
"delete[:space:]]+from" SecFilter "insert[:space:]]+into" SecFilter "select.+from"
SecFilterSelective COOKIE_sessionid "!(^([0-9]{1,9}))$" ... # Require HTTP_USER_AGENT and
HTTP_HOST headers SecFilterSelective "HTTP_USER_AGENT|HTTP_HOST" "^$" SecFilterSelective
"HTTP_ACCEPT" "^$" log,pass ... # Forbid file upload #SecFilterSelective "HTTP_CONTENT_TYPE"
multipart/form-data # Only watch argument p1 #SecFilterSelective "ARG_p1" 555 # Watch all
arguments except p1 #SecFilterSelective "ARGS"!ARG_p2" 666 # Only allow our own test utility to
send requests (or Mozilla) #SecFilterSelective HTTP_USER_AGENT "!(mod_security|mozilla)" # Do
not allow variables with this name #SecFilterSelective ARGS_NAMES 777 # Do now allow this
```

variable value (names are ok) #SecFilterSelective ARGS_VALUES 888 # Test for a POST variable parsing bug, see test #41 #SecFilterSelective ARG_p2 AAA # Stop spamming through FormMail # note the exclamation mark at the beginning # of the filter - only requests that match this regex will # be allowed # # SecFilterSelective "ARG_recipient" "!@webkreator.com\$" # # when allowing upload, only allow images # note that this is not foolproof, a determined attacker # could get around this· # # SecFilterInheritance Off # SecFilterSelective POST_PAYLOAD "!image/(jpeg|bmp|gif)" # # WEB-ATTACKS ps command attempt SecFilterSelective THE_REQUEST "/bin/ps" # WEB-ATTACKS /bin/ps command attempt SecFilterSelective THE_REQUEST "ps\x20" # WEB-ATTACKS wget command attempt SecFilter "wget\x20" # WEB-ATTACKS uname -a command attempt SecFilter "uname\x20-a" # WEB-ATTACKS /usr/bin/id command attempt SecFilter "/usr/bin/id" # WEB-ATTACKS id command attempt SecFilter "\id" # WEB-ATTACKS echo command attempt SecFilter "/bin/echo" # WEB-ATTACKS kill command attempt SecFilter "/bin/kill" # WEB-ATTACKS chmod command attempt SecFilter "/bin/chmod" # WEB-ATTACKS chgrp command attempt SecFilter "/chgrp" # WEB-ATTACKS chown command attempt SecFilter "/chown" # WEB-ATTACKS chsh command attempt SecFilter "/usr/bin/chsh" # WEB-ATTACKS tftp command attempt SecFilter "tftp\x20" # WEB-ATTACKS /usr/bin/gcc command attempt SecFilter "/usr/bin/gcc" # WEB-ATTACKS gcc command attempt SecFilter "gcc\x20-o" # WEB-ATTACKS /usr/bin/cc command attempt SecFilter "/usr/bin/cc" # WEB-ATTACKS cc command attempt SecFilter "cc\x20" # WEB-ATTACKS /usr/bin/cpp command attempt SecFilter "/usr/bin/cpp" # WEB-ATTACKS cpp command attempt SecFilter "cpp\x20" # WEB-ATTACKS /usr/bin/g++ command attempt SecFilter "/usr/bin/g\+\+\ " # WEB-ATTACKS g++ command attempt SecFilter "g\+\+\x20" # WEB-ATTACKS bin/python access attempt SecFilter "bin/python" # WEB-ATTACKS python access attempt SecFilter "python\x20" # WEB-ATTACKS bin/tclsh execution attempt SecFilter "bin/tclsh" # WEB-ATTACKS tclsh execution attempt SecFilter "tclsh8\x20" # WEB-ATTACKS bin/nasm command attempt SecFilter "bin/nasm" # WEB-ATTACKS nasm command attempt SecFilter "nasm\x20" # WEB-ATTACKS /usr/bin/perl execution attempt SecFilter "/usr/bin/perl" # WEB-ATTACKS perl execution attempt SecFilter "perl\x20" # WEB-ATTACKS nt admin addition attempt SecFilter "net localgroup administrators /add" # WEB-ATTACKS traceroute command attempt SecFilter "traceroute\x20" # WEB-ATTACKS ping command attempt SecFilter "/bin/ping" # WEB-ATTACKS netcat command attempt SecFilter "nc\x20" # WEB-ATTACKS nmap command attempt SecFilter "nmap\x20" # WEB-ATTACKS xterm command attempt SecFilter "/usr/X11R6/bin/xterm" # WEB-ATTACKS X application to remote host attempt SecFilter "\x20-display\x20" # WEB-ATTACKS lsof command attempt SecFilter "lsof\x20" # WEB-ATTACKS mail command attempt SecFilter "/bin/mail" # WEB-ATTACKS mail command attempt SecFilter "mail\x20" # WEB-ATTACKS /bin/ls command attempt SecFilterSelective THE_REQUEST "/bin/ls" # WEB-ATTACKS /etc/inetd.conf access SecFilter "/etc/inetd\conf" log,pass # WEB-ATTACKS /etc/motd access SecFilter "/etc/motd" log,pass # WEB-ATTACKS /etc/shadow access SecFilter "/etc/shadow" log,pass # WEB-ATTACKS conf/httpd.conf attempt SecFilter "conf/httpd\conf" log,pass # WEB-ATTACKS .htgroup access SecFilterSelective THE_REQUEST "\.htgroup" log,pass # WEB-ATTACKS .htgroup access SecFilterSelective THE_REQUEST "tiki\install\php" log,pass # WEB-CGI bash access SecFilterSelective THE_REQUEST "/bash" log,pass # WEB-CGI perl.exe command attempt SecFilterSelective THE_REQUEST "/perl\exe\?" # WEB-CGI perl.exe access SecFilterSelective THE_REQUEST "/perl\exe" # WEB-CGI perl command attempt SecFilterSelective THE_REQUEST "/perl\?" # WEB-CGI zsh access SecFilterSelective THE_REQUEST "/zsh" # WEB-CGI csh access SecFilterSelective THE_REQUEST "/csh" # WEB-CGI tcsh access SecFilterSelective THE_REQUEST "/tcsh" # WEB-CGI rsh access SecFilterSelective THE_REQUEST "/rsh" # WEB-CGI ksh access SecFilterSelective THE_REQUEST "/ksh" # WEB-CGI swc access SecFilterSelective THE_REQUEST "/swc" # WEB-CGI AltaVista Intranet Search directory traversal attempt SecFilterSelective THE_REQUEST "/query\?mss=\.\." # WEB-CGI test.bat access SecFilterSelective THE_REQUEST "/test\bat" log,pass # WEB-CGI input.bat access SecFilterSelective THE_REQUEST "/input\bat" log,pass # WEB-CGI input2.bat access SecFilterSelective THE_REQUEST "/input2\bat" log,pass # WEB-CGI envout.bat access SecFilterSelective THE_REQUEST "/envout\bat" log,pass # WEB-CGI echo.bat arbitrary command execution attempt SecFilterSelective THE_REQUEST "/echo\bat" chain SecFilter "&" # WEB-CGI

echo.bat access SecFilterSelective THE_REQUEST "/echo\bat" log,pass # WEB-CGI hello.bat
arbitrary command execution attempt SecFilterSelective THE_REQUEST "/hello\bat" chain SecFilter
"&" # WEB-CGI hello.bat access SecFilterSelective THE_REQUEST "/hello\bat" log,pass # WEB-CGI
tst.bat access SecFilterSelective THE_REQUEST "/tst.bat" log,pass # WEB-CLIENT Outlook EML
access SecFilterSelective THE_REQUEST "\.eml" # WEB-CLIENT XMLHttpRequest attempt
SecFilter "file:\/\/" # WEB-CLIENT readme.eml download attempt SecFilterSelective THE_REQUEST
"/readme\eml" # WEB-CLIENT readme.eml autoload attempt SecFilter
"window\open(\"readme\eml\" # WEB-CLIENT Javascript document.domain attempt SecFilter
"document\domain(\" # WEB-CLIENT Javascript URL host spoofing attempt SecFilter "javascript:\/\/"
WEB-IIS unicode directory traversal attempt SecFilter "\.\.\xc0\xaf\.\." # WEB-IIS unicode
directory traversal attempt SecFilter "\.\.\xc1\x1c\.\." # WEB-IIS unicode directory traversal
attempt SecFilter "\.\.\xc1\x9c\.\." # WEB-IIS unicode directory traversal attempt SecFilter
"\.\.\x255c\.\." # WEB-MISC cross site scripting attempt SecFilter "" # WEB-MISC cross site
scripting \(\img src=javascript\) attempt SecFilter "img src=javascript" # WEB-MISC Cisco IOS HTTP
configuration attempt SecFilterSelective THE_REQUEST "/exec/" # WEB-MISC Netscape Enterprise
DOS SecFilter "REVLOG / " # WEB-MISC Netscape Enterprise directory listing attempt #SecFilter
"INDEX " # WEB-MISC iPlanet GETPROPERTIES attempt SecFilter "GETPROPERTIES" # WEB-
MISC weblog view source attempt SecFilterSelective THE_REQUEST "\.js\x70" # WEB-MISC
Tomcat directory traversal attempt SecFilterSelective THE_REQUEST "\x00\.jsp" # WEB-MISC
Tomcat view source attempt SecFilterSelective THE_REQUEST "\x252ejsp" # WEB-MISC ftp attempt
SecFilter "ftp.exe" log,pass # WEB-MISC xp_enumdsn attempt SecFilter "xp_enumdsn" # WEB-
MISC xp_filelist attempt SecFilter "xp_filelist" # WEB-MISC xp_availablemedia attempt SecFilter
"xp_availablemedia" # WEB-MISC xp_cmdshell attempt SecFilter "xp_cmdshell" # WEB-MISC nc.exe
attempt SecFilter "nc.exe" log,pass # WEB-MISC wsh attempt SecFilter "wsh.exe" log,pass # WEB-
MISC rcmd attempt SecFilter "rcmd.exe" log,pass # WEB-MISC telnet attempt SecFilter
"telnet.exe" log,pass # WEB-MISC net attempt SecFilter "net.exe" log,pass # WEB-MISC tftp
attempt SecFilter "tftp.exe" log,pass # WEB-MISC xp_regread attempt SecFilter "xp_regread"
log,pass # WEB-MISC xp_regwrite attempt SecFilter "xp_regwrite" log,pass # WEB-MISC
xp_regdeletekey attempt SecFilter "xp_regdeletekey" log,pass # WEB-MISC WebDAV search access
SecFilter "SEARCH " log,pass # WEB-MISC .htpasswd access SecFilter "\.htpasswd" # WEB-MISC
Lotus Domino directory traversal SecFilterSelective THE_REQUEST "\.\." # WEB-MISC WebDAV
propfind access SecFilter "xmlns:a=\"DAV\">" log,pass # WEB-MISC Allaire JRUN DOS attempt
SecFilterSelective THE_REQUEST "servlet\.\.\.\.\." # WEB-MISC ICQ Webfront HTTP DOS
SecFilterSelective THE_REQUEST "\?\?\?\?\?\?\?\?\?" # WEB-MISC cd.. SecFilter "cd\.\." # WEB-
MISC ///cgi-bin access SecFilterSelective THE_REQUEST "///cgi-bin" # WEB-MISC /cgi-bin/// access
SecFilterSelective THE_REQUEST "/cgi-bin///" # WEB-MISC /~root access SecFilterSelective
THE_REQUEST "/~root" # WEB-MISC /~ftp access SecFilterSelective THE_REQUEST "/~ftp" #
WEB-MISC cat%20 access #SecFilter "cat\x20" # WEB-MISC get32.exe access SecFilterSelective
THE_REQUEST "/get32.exe" # WEB-MISC whisker HEAD/. SecFilter "HEAD\." # WEB-MISC long
basic authorization string SecFilter "Authorization: Basic " # WEB-MISC http directory traversal
SecFilter "\.\." # WEB-MISC sadmind worm access SecFilter "GET x HTTP/1.0" # WEB-MISC mod-
pysql administration access SecFilterSelective THE_REQUEST "/admin/" log,pass # WEB-MISC
Phorecast remote code execution attempt SecFilter "includedir=" # WEB-MISC .history access
SecFilterSelective THE_REQUEST "\.history" # WEB-MISC .bash_history access SecFilterSelective
THE_REQUEST "\.bash_history" # WEB-MISC /~nobody access SecFilterSelective THE_REQUEST
"/~nobody" # WEB-MISC SecureSite authentication bypass attempt SecFilter "secure_site, ok" #
WEB-MISC Apache Chunked-Encoding worm attempt SecFilter "CCCCCCC:
AAAAAAAAAAAAAAAAAAAAA" # WEB-MISC Transfer-Encoding: chunked SecFilter "chunked" # WEB-
MISC webalizer access #SecFilterSelective THE_REQUEST "/webalizer/" log,pass # WEB-MISC
robots.txt access SecFilterSelective THE_REQUEST "/robots.txt" log,pass # WEB-MISC robot.txt
access SecFilterSelective THE_REQUEST "/robot.txt" log,pass # WEB-MISC Linksys router default
password login attempt (\:admin\) SecFilter "Authorization: Basic OmFkbWlu" # WEB-MISC
Linksys router default password login attempt (admin\:admin\) SecFilter "YWRtaW46YWRtaW4" #

WEB-MISC perl post attempt SecFilterSelective THE_REQUEST "/perl/" chain SecFilter "POST" #
WEB-MISC TRACE attempt SecFilter "TRACE" # WEB-PHP squirrel mail spell-check arbitrary
command attempt SecFilterSelective THE_REQUEST "/squirrelspell/modules/check_me\.mod\.php"
chain SecFilter "SQSPELL_APP\" # WEB-PHP squirrel mail theme arbitrary command attempt
SecFilterSelective THE_REQUEST "/left_main\.php" chain SecFilter "cmdd=" # WEB-PHP PHP-Wiki
cross site scripting attempt SecFilterSelective THE_REQUEST "" SecFilter "delete[:,space:]]+from"
SecFilter "insert[:,space:]]+into" SecFilter "select.+from"