install modsecurity for yourÂ platform

- modsecurity.org/download

get rules from gotroot applicable to your modsecurityÂ version

- download from http://gotroot.com/ into /etc/apache2/modsecurity/ for example
  - recommended confs: apacheN-rules, exclude, jitp, proxy, recons, rootkits, rules, useragents

create a config for apache to load the modsecurityÂ module

[+]

#these settings work with modsecurity version 1.9.4 #on gentoo this configfile is named: /etc/apache2/modules.d/99_mod_security.conf for example, #on gentoo edit /etc/conf.d/apache2 and add -D SECURITY to APACHE2_OPTS #check your paths for the Include below to use the rules from gotroot LoadModule security_module modules/mod_security.so SecFilterEngine On # Action to take by default SecFilterDefaultAction "deny,log,status:403" SecServerSignature "Apache2" # Make sure that URL encoding is valid SecFilterCheckURLEncoding On SecFilterCheckUnicodeEncoding Off SecFilterCheckCookieFormat On # Should mod_security inspect POST payloads SecFilterScanPOST On # Only allow bytes from this range SecFilterForceByteRange 1 255 # The audit engine works independently and # can be turned On of 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 DynamicOrRelevant SecAuditEngine RelevantOnly # The name of the audit log file SecAuditLog logs/audit_log SecFilterDebugLog logs/modsec_debug_log SecFilterDebugLevel 0 Include conf/modsecurity/*.conf

restart apache

implement more TikiSecurity