Variables

modsecurity	freewaf	OpenWAF	描述
ARGS		ARGS	所有的请求参数，包含 ARGS_GET 和 ARGS_POST，table 类型，但只检验 value，不检验 NAME
	REQUEST_ARGS		包含 uri 参数，请求体及请求头 cookies，table 类型
ARGS_COMBINED_SIZE		ARGS_COMBINED_SIZE	请求参数总长度,只包含 key 和 value 的长度,不包含& = 等符号
ARGS_GET	URI_ARGS	ARGS_GET	querystring 参数，table 类型
ARGS_GET_NAMES		ARGS_GET_NAMES	querystring 参数 key 值，table 类型
ARGS_NAMES		ARGS_NAMES	uri 参数名称及 post 参数名称，table 类型
ARGS_POST		ARGS_POST	post 参数，table 类型
ARGS_POST_NAMES		ARGS_POST_NAMES	post 参数 key 值，table 类型
AUTH_TYPE			身份验证方法，反向代理时，若在后端服务器中验证，则该信息不可用
DURATION		DURATION	处理事务用时，dynamic
ENV			环境变量
FILES		FILES	从请求体中得到的原始文件名(带有文件后缀名)，table 类型
FILES_COMBINED_SIZE			
FILES_NAMES		FILES_NAMES	上传文件名称，table 类型
FULL_REQUEST			包含请求行，请求头，请求体
FULL_REQUEST_LENGTH			
FILES_SIZES			单个文件的大小,table 类型
FILES_TMPNAMES			临时文件名称 table 类型
FILES_TMP_CONTENT			上传文件的内容
GEO		GEO	OpenWAF 中值为数组，包含 code3,code,id,continent,name
		GEO_CODE3	request.GEO.code3 3 个字母长度的国家缩写
		GEO_CODE	request.GEO.code 2 个字母长度的国家缩写
		GEO_ID	request.GEO.id 国家 ID
		GEO_CONTINENT	request.GEO.continent 国家所在大洲
		GEO_NAME	request.GEO.name 国家全称
HIGHEST_SEVERITY			
INBOUND_DATA_ERROR			
MATCHED_VAR	MATCHED_VAR	MATCHED_VAR	最新匹配中的变量
MATCHED_VARS	MATCHED_VARS	MATCHED_VARS	单条规则中匹配中的所有变量
MATCHED_VAR_NAME	MATCHED_VAR_NAME	MATCHED_VAR_NAME	最新匹配中的变量名称
MATCHED_VARS_NAMES	MATCHED_VARS_NAMES	MATCHED_VARS_NAMES	单条规则中匹配中的所有变量名称
MODSEC_BUILD			
MULTIPART_CRLF_LF_LINES			
MULTIPART_FILENAME			
MULTIPART_NAME			
MULTIPART_STRICT_ERROR			
MULTIPART_UNMATCHED_BOUNDARY			
OUTBOUND_DATA_ERROR			
PATH_INFO			
PERF_COMBINED			
PERF_GC			
PERF_LOGGING			
PERF_PHASE1			
PERF_PHASE2			
PERF_PHASE3			
PERF_PHASE4			
PERF_PHASE5			
PERF_RULES			
PERF_SREAD			
PERF_SWRITE			
QUERY_STRING	QUERY_STRING	QUERY_STRING	未解码参数
REMOTE_ADDR	REMOTE_ADDR	REMOTE_ADDR	客户端地址
REMOTE_HOST		REMOTE_HOST	域名
REMOTE_PORT		REMOTE_PORT	端口号,number 类型
REMOTE_USER		REMOTE_USER	身份验证的用户名
REQBODY_ERROR			
REQBODY_ERROR_MSG			
REQBODY_PROCESSOR			
REQUEST_BASENAME	REQUEST_BASENAME	REQUEST_BASENAME	the filename part of REQUEST_FILENAME (e.g., /test.php)
REQUEST_BODY	REQUEST_BODY	REQUEST_BODY	请求体
REQUEST_BODY_LENGTH			
REQUEST_COOKIES	REQUEST_COOKIES	REQUEST_COOKIES	cookies，table 类型
REQUEST_COOKIES_NAMES		REQUEST_COOKIES_NAMES	cookies 名称，table 类型
REQUEST_FILENAME		REQUEST_FILENAME	relative request URL (e.g., /html/rules/test.php)

REQUEST_HEADERS	REQUEST_HEADERS	REQUEST_HEADERS	请求头，table 类型
REQUEST_HEADERS_NAMES		REQUEST_HEADERS_NAMES	请求头 key 值，table 类型
REQUEST_LINE	REQUEST_LINE	REQUEST_LINE	请求行
REQUEST_METHOD	METHOD	REQUEST_METHOD	请求方法
REQUEST_PROTOCOL	PROTOCOL	REQUEST_PROTOCOL	http 请求协议版本,(e.g., HTTP/1.1)
	HTTP_VERSION	HTTP_VERSION	http 请求协议版本(e.g., 1.1)
	URI	URI	仅有路径，既不带域名，也不带参数
		URL	SCHEME 与 HTTP_HOST 与 URI 的拼接，(e.g., http://www.example.com/index.php)
REQUEST_URI	REQUEST_URI	REQUEST_URI	带参数，但不带有域名 (e.g., /index.php? p=X).
REQUEST_URI_RAW			modsec 表示带有 query string，但不带有域名 (e.g., http://www.example.com/index.php?p=X).
RESPONSE_BODY		RESPONSE_BODY	响应体
RESPONSE_CONTENT_LENGTH			
RESPONSE_CONTENT_TYPE			
RESPONSE_HEADERS	RESPONSE_HEADERS	RESPONSE_HEADERS	响应头，table 类型
RESPONSE_HEADERS_NAMES			
RESPONSE_PROTOCOL			
RESPONSE_STATUS	STATUS	RESPONSE_STATUS	响应状态码
RULE			
SCRIPT_BASENAME			
SCRIPT_FILENAME			
SCRIPT_GID			
SCRIPT_GROUPNAME			
SCRIPT_MODE			
SCRIPT_UID			
SCRIPT_USERNAME			
SDBM_DELETE_ERROR			
SERVER_ADDR		SERVER_ADDR	服务器地址
SERVER_NAME		SERVER_NAME	服务器名称
SERVER_PORT		SERVER_PORT	服务器端口号,number 类型
SESSION		SESSION	
SESSIONID			
STREAM_INPUT_BODY			
STREAM_OUTPUT_BODY			
TIME		TIME	hour:minute:second
TIME_DAY		TIME_DAY	1–31
TIME_EPOCH		TIME_EPOCH	seconds since 1970
TIME_HOUR		TIME_HOUR	0–23
TIME_MIN		TIME_MIN	0–59
TIME_MON		TIME_MON	modsec:0–11 OpenWAF:1-12
TIME_SEC		TIME_SEC	0–59
TIME_WDAY		TIME_WDAY	0–6
TIME_YEAR		TIME_YEAR	four-digit ex:1997
TX	TX	TX	临时变量
UNIQUE_ID		UNIQUE_ID	唯一标识
URLENCODED_ERROR			
USERID		USERID	用户 ID
USERAGENT_IP			
WEBAPPID			
WEBSERVER_ERROR_LOG			
XML			
		SCHEME	http or https
		HTTP_HOST	域名+端口（80 省略）
		SESSION_DATA	SESSION 信息
		BYTES_IN	接收信息长度
		CONNECTION_REQUESTS	当前连接请求数
		HTTP_USER_AGENT	agent 头字段
		RAW_HEADER	请求头,带请求行
		RAW_HEADER_TRUE	请求头，不带请求行
		TIME_LOCAL	时间，如：26/Aug/2016:01:32:16 -0400
		ORIGINAL_DST_ADDR	服务器地址，应用代理模式为 WAF 地址，透明模式为后端服务器地址
		ORIGINAL_DST_PORT	服务器端口号
		POLICYID	策略 ID
		HTTP_REFERER	请求头中的 referer
		GZIP_RATIO	压缩等级
		IP_VERSION	IPv4 or IPv6
		HTTP_COOKIE	cookie 头字段

Transformation functions

modsecurity	freewaf	OpenWAF	描述
base64Decode	base64_decode	base64_decode	base64 解码
sqlHexDecode	sql_hex_decode	sql_hex_decode	
base64DecodeExt			
base64Encode	base64_encode	base64_encode	base64 编码
cmdLine			
compressWhitespace	compress_whitespace	compress_whitespace	压缩空格
cssDecode			Decodes characters encoded using the CSS 2.x escape rules syndata.html#characters
escapeSeqDecode			
hexDecode	hex_decode	hex_decode	
hexEncode	hex_encode	hex_encode	
htmlEntityDecode	html_decode	html_decode	
jsDecode			Decodes JavaScript? escape sequences
length	length	length	
lowercase	lowercase	lowercase	
md5	md5	md5	
none			
normalisePath	normalise_path	normalise_path	
normalisePathWin			
parityEven7bit			
parityOdd7bit			
parityZero7bit			
removeNulls		remove_nulls	移除空字符\0
removeWhitespace	remove_whitespace	remove_whitespace	移除空白字符\s 包含水平定位字符（'\t'）、归位键('\r')、换行('\n')、垂直定位字符('\v')或翻页('\f')
replaceComments	replace_comments	replace_comments	modsec 表示用一个空格代替注释内容/* ... */, --, #，OpenWAF 表示用一个空格代替注释内容/*...*/
removeCommentsChar	remove_comments_char	remove_comments_char	去掉/*,*/,--,#
removeComments	remove_comments	remove_comments	modsec 支持去掉/*...*/,--,#，OpenWAF 支持去掉/*...*/
replaceNulls			
urlDecode	uri_decode	uri_decode	modsec: Decodes a URL-encoded input string. OpenWAF:Unescape str as an escaped URI component.
urlDecodeUni		uri_decode_uni	uri_decode_uni 与 uri_decode 一样
urlEncode		uri_encode	
utf8toUnicode			
sha1	sha1	sha1	
trimLeft	trim_left	trim_left	去除左侧空格
trimRight	trim_right	trim_right	去除右侧空格
trim	trim	trim	去除左右两侧空格
		counter	计数，相当于 modsec 中&符号

Operators

modsecurity	freewaf	OpenWAF	描述
beginsWith		begins_with	开始于
contains	CONTAINS	contains	子字符串
containsWord		contains_word	包含(带字边界)
detectSQLi		detect_sqli	SQL 注入检验，目前 OpenWAF 与 modsec 用的都是同一个源文件
detectXSS		detect_xss	跨站脚本检验，目前 OpenWAF 与 modsec 用的都是同一个源文件
endsWith		ends_with	终止于
fuzzyHash			ssdeep 的 hash 值
eq	EQUALS	equal	等于
ge	GREATER_EQ	greater_eq	大于等于
geoLookup			
gsbLookup			
gt	GREATER	greater	大于
inspectFile			
ipMatch		ip_utils	ip 段,支持子网掩码，支持单 ip，支持以'-'为间隔符的 ip 段
ipMatchF			ipMatchF 为 ipMatchFromFile 的简称
ipMatchFromFile			
le	LESS_EQ	less_eq	小于等于
lt	LESS	less	小于
pm		"-"	modsecurity 中 pm 为不区分大小写的 contains，且不支持正则 OpenWAF 无 pm，因为 OpenWAF 中 pattern 支持数组
pmf		pf	pmf 为 pmFromFile 的简称 pf 为 patternFromFile，与 pattern 互斥（不可同时出现） pf 支持各类 operators 如 regex,contains 等
pmFromFile		pf	
rbl			
rsub			
rx	REGEX	regex	正则匹配
streq		equal	字符串相等
strmatch	str_find	str_match	字符串匹配 modsecurity 使用 Boyer-Moore-Horspool 算法 比正则匹配效率高
validateByteRange			
validateDTD			
validateHash			
validateSchema			
validateUrlEncoding		validate_url_encoding	检测%xx，其中 xx 为 16 进制
validateUtf8Encoding			
verifyCC			
verifyCPF			
verifySSN			
within			
		num_range	pattern 可为 123 或"12-45"
		str_range	pattern 可为"ab"或"01:42:00-04:32:00"

Action

modsecurity	freewaf	OpenWAF	描述
accuracy			
allow		allow	跳过当前 phase 的 rule
append			
auditlog			
block			
capture		"-"	与正则一起使用时，捕获变量，存入集合 默认生效
chain	match		"与"
ctl			
deny	DENY	deny	阻断请求
deprecatevar			
drop			
exec			
expirevar			
id		id	规则 ID
initcol			
log			
logdata			
maturity			
msg			
multiMatch			各个 transform 前后进行 operator 操作，暂不支持
noauditlog			
nolog		nolog	不记录日志
pass		pass	继续执行下一条规则
pause			
phase		phase	modsec 中为 1-5 OpenWAF 中为 access/header_filter/body_filter,支持数组
prepend			
proxy			
redirect		redirect	重定向
rev		charactor_version	特征规则版本
sanitiseArg		sanitise_arg	将相应参数由‘*’(位数不变)代替，支持字符串和数组
sanitiseMatched			
sanitiseMatchedBytes			
sanitiseRequestHeader			
sanitiseResponseHeader			
severity		severity	严重等级
setuid			
setrsc			
setsid			
setenv			
setvar		setvar	
skip			
skipAfter			
status		meta	
t		transform	
tag		tag	
ver		release_version	特征库版本
xmlns			暂不支持
	ACCEPT		
	SCORE		
	IGNORE		
		policy	执行其他策略
		robot	进行人机识别，添加动作 CHAIN 后可取消
		add_resp_headers	添加/修改/删除 响应头