IskWaf - Web Application Firewall ??? MODX 3

IskWaf — это компонент для MODX Revolution 3.x, представляющий собой простой, но гибкий межсетевой экран уровня веб-приложения (WAF)

Официальный репозиторий: https://extras.modx.com/package/iskwafwebapplicationfirewall

Modstore.pro: https://modstore.pro/packages/utilities/iskwaf

- Основные возможности
- Конфигурация
  - Системные настройки
  - Страница CAPTCHA
  - Настройка GeoIP (IP2Location)
  - CRON-задачи
- Типы правил
  - IP-правила
  - Блокировка по странам
  - User-Agent правила
  - Referrer правила
  - Request URI правила
- Система CAPTCHA
- Система отчетов
- Отказ от ответственности

???????? ????????????

???????? ????????????

- **Многоуровневые правила безопасности:**
  - IP-адрес/CIDR (с приоритетом точного IP над подсетью).
  - Страна (с исключениями для доверенных ботов).
  - User-Agent (типы: содержит, точное совпадение, регулярное выражение).
  - Referrer (типы: содержит, точное совпадение, регулярное выражение).
  - Request URI (типы: содержит, точное совпадение, регулярное выражение, начинается с; с учетом или без учета query string).
- **Интеллектуальная автоматизация правил:**
  - Автоматическое создание разрешающих правил для подсетей доверенных ботов (Google, Yandex и др.).
  - Автоматическое создание блокирующих правил для подсетей нежелательных хостеров/прокси.
  - Правила создаются на основе данных об автономной системе (ASN) через CRON.
- **Гибкие действия по правилам:** Block (403), CAPTCHA, Allow.
- **Локальная CAPTCHA:** Числовая, с заданием "первые/последние 3 цифры" из 6, сессионная.
- **Опциональные режимы проверки WAF:**
  - Проверка на каждый запрос (стандартное поведение).
  - Проверка один раз за сессию (снижает нагрузку для уже проверенных пользователей).
- **Система логирования:** Подробные логи срабатываний, настраиваемые режимы (`full`, `triggered`, `off`), автоматическая очистка старых логов. Логи также отражают, были ли правила WAF пропущены из-за сессионной проверки.
- **Анализ IP-адресов:** Определение страны, региона, города, ASN и ISP для IP-адресов из логов с помощью локальных баз IP2Location LITE (через CRON).
- **Ежедневные отчеты:** Агрегированная статистика по событиям WAF, типам правил, хитам поисковых ботов, топ-N нарушителей (в JSON), включая данные геолокации.
- **Интерфейс управления (CMP):** Вкладки для логов (с отображением страны/города), каждого типа правил и отчетов; создание, редактирование, включение/отключение, удаление правил.

IskWaf является инструментом для базовой защиты и не заменяет собой комплексные корпоративные решения безопасности или специализированные сервисы WAF. Используйте его на свой страх и риск. Рекомендуется всегда иметь актуальные резервные копии вашего сайта.

??????????????

Конфигурация

?????????? ??????????

После установки компонента необходимо настроить несколько системных параметров, страницу для CAPTCHA и подготовить окружение для баз данных GeoIP.

1. ????????? ?????????

Найдите их в разделе "Система" (значок шестеренки) -> "Системные настройки", выбрав пространство имен `iskwaf`.

Ключ	Описание	Возможные значения/Действие
`iskwaf_iskwaf_captcha_resource_id`	ID ресурса MODX для отображения страницы CAPTCHA.	Создайте новый ресурс MODX (например, с alias `captcha-verify`), убедитесь, что он **не кэшируемый**. В поле "Содержимое ресурса" поместите вызов сниппета `[[!IskWafCaptcha]]`. Укажите ID этого ресурса здесь.
`iskwaf_iskwaf_option_log`	Режим логирования WAF.	• `full`: (По умолчанию) Логируются все запросы (сработавшие правила + обычные визиты, включая те, где правила были пропущены из-за сессионной проверки). • `triggered`: Логируются только запросы, вызвавшие срабатывание правила. Опционально может логировать факт пропуска правил из-за сессионной проверки (см. код плагина). • `off`: Логирование отключено (но правила продолжают действовать).

Ключ	Описание	Возможные значения/Действие
`iskwaf_waf_check_mode`	Режим проверки правил WAF.	• `on_every_request`: (По умолчанию) Правила WAF проверяются при каждом запросе. • `once_per_session`: Правила WAF проверяются для пользователя только один раз за сессию. Если проверка пройдена, последующие запросы в той же сессии не проходят полную проверку WAF (но логи посещений могут вестись согласно настройке `iskwaf_iskwaf_option_log`).
`iskwaf_iskwaf_log_retention_days`	Количество дней хранения записей в логе `iskwaf_logs`. Старые записи удаляются CRON-скриптом.	Число (например, `7`, `30`). По умолчанию в скрипте: 7.
`iskwaf_ip2location_download_token`	Ваш персональный токен для скачивания баз данных с сайта IP2Location.	Получите токен после регистрации на lite.ip2location.com и введите его здесь.
`iskwaf_ip_analysis_limit_per_run`	Максимальное количество новых/устаревших IP для анализа за один запуск CRON-скрипта `analyze_ip2location_details.php`.	Число. По умолчанию в скрипте: 500.
`iskwaf_ip_analysis_update_interval`	Периодичность в днях для обновления информации по IP, уже существующему в таблице деталей.	Число. По умолчанию в скрипте: 30.
Автоматическое управление правилами и блокировка по странам		
`iskwaf_iskwaf_blocked_countries`	Блокируемые страны	Укажите двухбуквенные коды стран (ISO 3166-1 alpha-2) через запятую. Трафик из этих стран будет блокироваться, за исключением доверенных ботов. Пример: `CN,RU,KP`

Ключ	Описание	Возможные значения/Действие
`iskwaf_iskwaf_auto_allow_as_names`	Разрешенные имена компаний (AS Name)	Имена компаний (ASN), чьи подсети будут автоматически разрешены. Разделитель - вертикальная черта (`|`). Пример: `GOOGLE|Yandex|Microsoft`
`iskwaf_iskwaf_auto_allow_as_numbers`	Разрешенные номера AS (ASN)	Номера автономных систем (ASN), чьи подсети будут автоматически разрешены. Разделитель - вертикальная черта (`|`). Пример: `AS15169|AS13238`
`iskwaf_iskwaf_auto_block_as_names`	Блокируемые имена компаний (AS Name)	Имена компаний (ASN), чьи подсети будут автоматически заблокированы. Разделитель - вертикальная черта (`|`). Пример: `DigitalOcean|OVH`
`iskwaf_iskwaf_auto_block_as_numbers`	Блокируемые номера AS (ASN)	Номера автономных систем (ASN), чьи подсети будут автоматически заблокированы. Разделитель - вертикальная черта (`|`). Пример: `AS14061|AS16276`

???????? CAPTCHA

???????? CAPTCHA

Как указано выше, создайте ресурс MODX для отображения CAPTCHA. Он должен быть некэшируемым и содержать вызов сниппета `[[!IskWafCaptcha? &tpl=`имя_вашего_чанка_формы`]]` (параметр `&tpl` опционален, по умолчанию `iskWafCaptchaFormTpl`).

3. ????????? GeoIP (IP2Location)

Компонент IskWaf использует базы данных IP2Location LITE для определения геолокации, ASN и другой информации по IP-адресам. Сами файлы баз данных не входят в установочный пакет компонента, а скачиваются с помощью специального CRON-скрипта.

1. **Получите токен:** Зарегистрируйтесь на lite.ip2location.com и получите ваш персональный токен для скачивания. Введите его в системную настройку `iskwaf_ip2location_download_token`.
2. **PHP-библиотека IP2Location:**
   Для работы с BIN-файлами баз IP2Location необходима соответствующая PHP-библиотека. Компонент IskWaf использует PHP-файлы библиотеки, которые должны быть размещены в папке `core/components/iskwaf/lib/ip2location/src/`. Вы можете скачать "IP2Location PHP Module" (для BIN Data File) с официального сайта IP2Location и разместить содержимое его папки `src` по указанному пути.
3. **Директории для баз данных:** Убедитесь, что на сервере существуют и доступны для записи PHP следующие директории (относительно `core/components/iskwaf/`):
   - `tmp_db_download/` (для временных файлов при скачивании)
   - `geoip_db/` (для хранения распакованных BIN-файлов баз)
4. **Первоначальное скачивание баз:** После настройки токена и размещения PHP-библиотеки, запустите CRON-скрипт `ip2location_download.php` (см. ниже) один раз вручную из командной строки сервера для первоначальной загрузки баз (`IP2LOCATION-LITE-DB11.BIN` и `IP2LOCATION-LITE-ASN.BIN`).

????????? GeoIP (IP2Location)

Компонент IskWaf использует базы данных IP2Location LITE для определения геолокации, ASN и другой информации по IP-адресам. Сами файлы баз данных не входят в установочный пакет компонента, а скачиваются с помощью специального CRON-скрипта.

1. **Получите токен:** Зарегистрируйтесь на lite.ip2location.com и получите ваш персональный токен для скачивания. Введите его в системную настройку `iskwaf_ip2location_download_token`.
2. **PHP-библиотека IP2Location:**
   Для работы с BIN-файлами баз IP2Location необходима соответствующая PHP-библиотека. Компонент IskWaf использует PHP-файлы библиотеки, которые должны быть размещены в папке `core/components/iskwaf/lib/ip2location/src/`. Вы можете скачать "IP2Location PHP Module" (для BIN Data File) с официального сайта IP2Location и разместить содержимое его папки `src` по указанному пути.
3. **Директории для баз данных:** Убедитесь, что на сервере существуют и доступны для записи PHP следующие директории (относительно `core/components/iskwaf/`):
   - `tmp_db_download/` (для временных файлов при скачивании)
   - `geoip_db/` (для хранения распакованных BIN-файлов баз)
4. **Первоначальное скачивание баз:** После настройки токена и размещения PHP-библиотеки, запустите CRON-скрипт `ip2location_download.php` (см. ниже) один раз вручную из командной строки сервера для первоначальной загрузки баз (`IP2LOCATION-LITE-DB11.BIN` и `IP2LOCATION-LITE-ASN.BIN`).

Конфигурация

CRON-??????

CRON-??????

Для автоматической работы компонента настройте три CRON-задачи:

Скачивание/обновление баз GeoIP (IP2Location):

- Скрипт: `core/components/iskwaf/elements/cron/ip2location_download.php`
- Периодичность: Рекомендуется раз в месяц (например, 1-го числа каждого месяца).
- Пример команды: `/usr/bin/php /path/to/your/site/core/components/iskwaf/elements/cron/ip2location_download.php`

Анализ IP-адресов, заполнение GeoIP и авто-создание правил:

- Скрипт: `core/components/iskwaf/elements/cron/analyze_ip2location_details.php`
- Периодичность: Рекомендуется раз в 5-15 минут для оперативного создания правил.
- Пример команды: `/usr/bin/php /path/to/your/site/core/components/iskwaf/elements/cron/analyze_ip2location_details.php`

Очистка старых логов:

- Скрипт: `core/components/iskwaf/elements/cron/clear_log.php`
- Периодичность: Рекомендуется раз в сутки.
- Пример команды: `/usr/bin/php /path/to/your/site/core/components/iskwaf/elements/cron/clear_log.php`

Формирования отчетов:

- Скрипт: `core/components/iskwaf/elements/cron/reports_daily.php`
- Периодичность: Рекомендуется раз в сутки.
- Пример команды: `/usr/bin/php /path/to/your/site/core/components/iskwaf/elements/cron/reports_daily.php`

Убедитесь, что пути к PHP-интерпретатору и к скриптам указаны верно для вашего сервера.

?????????? (CMP)

Доступ к интерфейсу управления IskWaf осуществляется через главное меню менеджера MODX (обычно в разделе "Пакеты" или "Приложения").

- **Вкладка "Логи":** Просмотр всех записей лога WAF с поиском. Теперь должны отображаться колонки "Страна" и "Город" для IP-адресов, по которым есть данные.
- **Вкладки правил (IP, User-Agent, Referrer, Request URI):** Управление правилами.
- **Вкладка "Отчет":** Просмотр ежедневных сводных отчетов.

???? ??????

Типы правил

IP-???????

IP-???????

Предназначены для блокировки, разрешения или показа CAPTCHA на основе IP-адреса или CIDR-подсети посетителя.

- **Поля:** `IP/CIDR`, `Тип правила (действие)`, `Описание`, `Активно`.
- **Логика приоритета:** Точное совпадение IP имеет приоритет над CIDR-подсетью. Среди CIDR-подсетей, содержащих один и тот же IP, приоритет у более узкой (с наибольшей маской).

??????? ????????? ??? `IP/CIDR`:

- Одиночный IPv4: `192.168.1.100`
- IPv4 CIDR (подсеть): `10.0.0.0/8`
- IPv6 CIDR: `2001:db8::/32`

?????????? ?? ???????

?????????? ?? ???????

Это не отдельный тип правила в интерфейсе, а встроенный механизм WAF, который срабатывает после проверки IP-правил. Он позволяет блокировать трафик из стран, указанных в системной настройке `iskwaf_iskwaf_blocked_countries`.

- **Логика работы:** Решение о блокировке принимается в момент запроса на основе данных о геолокации IP, которые регулярно обновляются cron-скриптом.
- **Приоритет:** Эта проверка имеет более низкий приоритет, чем IP-правила. Это означает, что если для IP-адреса существует разрешающее (`allow`) правило (например, для подсети Google), посетитель будет пропущен, даже если его страна находится в черном списке.

User-Agent ???????

User-Agent ???????

Позволяют применять действия на основе строки User-Agent.

- **Поля:** `Паттерн User-Agent`, `Тип паттерна` ('contains', 'exact', 'regex'), `Тип правила (действие)`, `Описание`, `Активно`.

??????? ????????? ??? `Паттерн User-Agent`:

- Тип: `contains`, Паттерн: `AhrefsBot`
- Тип: `regex`, Паттерн: `/^EvilCorp Crawler\/[0-9\.]+/i`

Referrer ???????

Referrer ???????

Фильтруют запросы на основе HTTP Referrer.

- **Поля:** `Паттерн Referrer`, `Тип паттерна` ('contains', 'exact', 'regex'), `Тип правила (действие)`, `Описание`, `Активно`.

??????? ????????? ??? `Паттерн Referrer`:

- Тип: `contains`, Паттерн: `spam-site.com`
- Тип: `regex`, Паттерн: `/^https?:\/\/([\w-]+\.)*spammerdomain\.com/i`

Request URI ???????

Request URI ???????

Применяют действия на основе запрашиваемого URI.

- **Поля:** `Паттерн URI`, `Тип паттерна` ('contains', 'exact', 'regex', 'starts_with'), `Учитывать Query String` (да/нет), `Тип правила (действие)`, `Описание`, `Активно`.

??????? ????????? ??? `Паттерн URI`:

- Тип: `exact`, Query String: `нет`, Паттерн: `/wp-login.php`
- Тип: `starts_with`, Query String: `нет`, Паттерн: `/admin-backup/`
- Тип: `contains`, Query String: `да`, Паттерн: `eval(`

??????? CAPTCHA

??????? CAPTCHA

IskWaf использует локальную числовую CAPTCHA. Генерируется изображение с 6 цифрами, пользователю предлагается ввести первые или последние три. Прохождение запоминается в сессии. Отображается через сниппет `[[!IskWafCaptcha]]` (поддерживает `&tpl`).

??????? ???????

??????? ???????

Ежедневные сводки в `IskWafReportDaily` включают: общее количество событий WAF, блокировок, CAPTCHA, разрешений по правилам, срабатываний по типам правил, хиты поисковых ботов, топ N IP и правил (JSON). Генерируются CRON-скриптом.

Данный продукт включает в себя геолокационные данные IP2Location LITE, доступные с https://lite.ip2location.com.

This product includes IP2Location LITE data available from https://lite.ip2location.com.

?????? ??????????

Обратите внимание

- **Порядок выполнения правил:** IP-правила -> Блокировка по стране -> User-Agent -> Referrer -> Request URI. Первое сработавшее правило определяет действие.
- **Регулярные выражения:** Должны включать ограничители/флаги (например, `/badbot/i`). Тестируйте.
- **IP-адрес посетителя:** По умолчанию `$_SERVER['REMOTE_ADDR']`. Для сайтов за прокси может потребоваться адаптация.
- **Производительность:** Большое количество правил или режим логирования `full` могут влиять на производительность.
- **Ложные срабатывания:** Возможны. Регулярно проверяйте логи.

????? ?? ??????????????

IskWaf является инструментом для базовой защиты и не заменяет собой комплексные корпоративные решения безопасности или специализированные сервисы WAF. Используйте его на свой страх и риск. Рекомендуется всегда иметь актуальные резервные копии вашего сайта.