Cloudflare Web Application Firewall Review

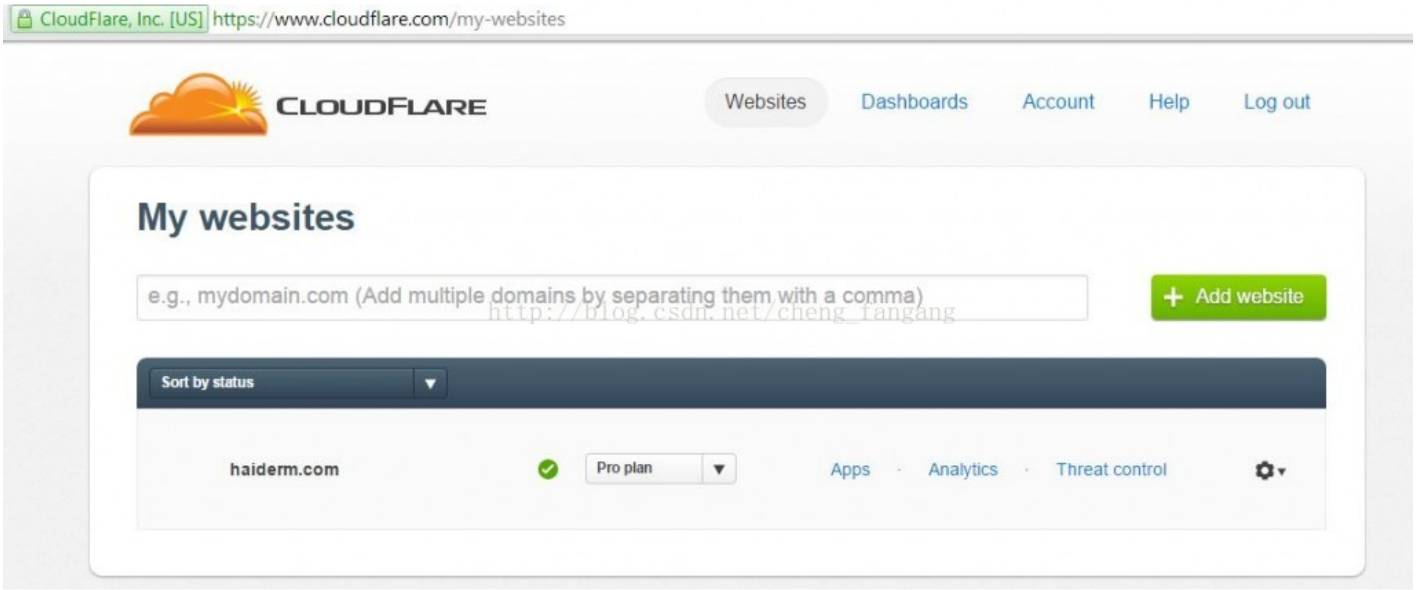
转载

天天向上_好好学习 于 2015-04-07 13:22:19 发布 1405 收藏
分类专栏： firewall 安全

firewall 同时被 2 个专栏收录

8 篇文章 0 订阅
订阅专栏

安全
63 篇文章 0 订阅
订阅专栏


CloudFlare, Inc. [US] https://www.cloudflare.com/my-websites

My websites

e.g., mydomain.com (Add multiple domains by separating them with a comma)

haiderm.com Pro plan

Cloudflare Web Application Firewall Review

Hi, I hope most of you are familiar with Cloudflare, in short, CloudFlare protects and accelerates any website online. Check more details about their features Cloudflare Overview. I'm a fan of cloudflare right from the start. Cloudflare has a free account , pro and business account, For over an year i was using cloudflare as a free member and enjoying all the benefits it offers free of cost. One of my personal favorite is that its a reverse proxy, so from security point of view, you can't tell the IP address of the server my website is hosted on. Some time back i participated in Cloudflare Bug Bounty, I found a XSS vulnerability in cloudflare core infrastructure which was effecting all cloudflare based websites, here is the writeup. They awarded me Cloudflare Pro account for lifetime. Cloudflare pro, apart from other cool features, also offers Web Application Firewall. I've been using it for about 6 months now so i decided to write Cloudflare Web Application Firewall Review and let everyone know about its features.

Cloudflare Web Application Firewall Interface

Cloudflare WAF has an online easy to use interface, which users can access from their cloudflare account, Users have complete control over the working of WAF, which is explained later in this post. Users can do the following (but not limited to) operations.

- Users can Turn Off/On firewall on single click

- Rulesets can be changed.
- Particular action can be decided for a particular rule, either, block, challenge, or just log the activity u3on triggering a user.
- View IP address, user activity, and rules they triggered.
- How many times a specific rule is triggered and who triggered it.

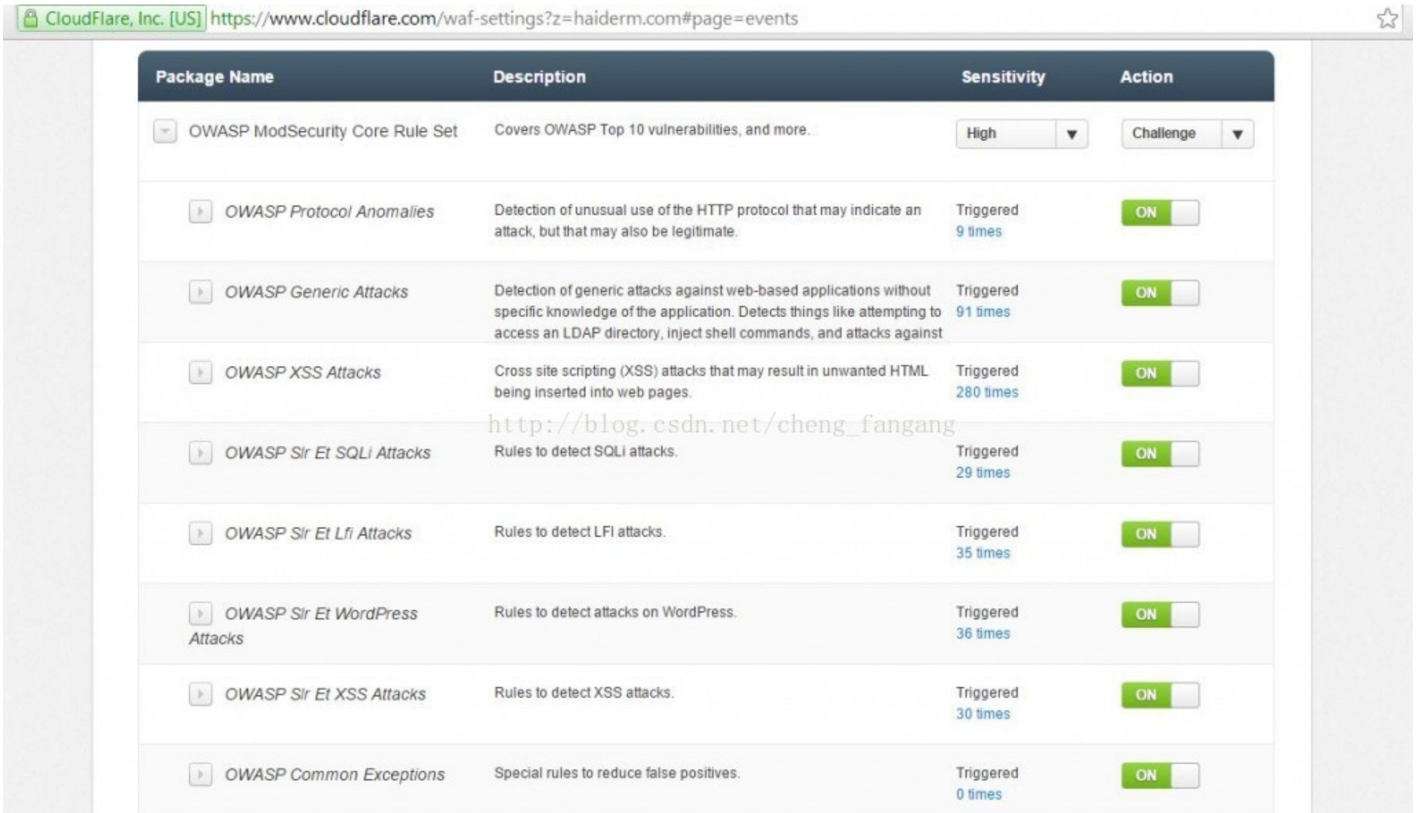
Cloudflare Web Application Firewall Rulesets

Cloudflare Web Application firewall is based on two types of rulesets , which are then divided over several rulesets, users have the ability to select rulesets that they want to enable or disable, also the action that firewall should take after a particular ruleset is triggered. Two main rule sets are as follow:-

OWASP ModSecurity Core Rule Set

OWASP ModSecurity Core Rule Set is opensource rule set developed by ModSecurity and OWASP, The OWASP ModSecurity CRS provides protections if the following attack/threat categories:

- Protecting HTTP protocol violations.
- IP looks for blacklisted IP's from 3rd party.
- HTTP DOS Protection
- Common Web attack protection
- BOT/Crawler detection
- Scanning for malicious file uploads
- Tracking sensitive data like credit card leaks
- Detecting trojan horses
- Application defects and misconfiguration detection
- Error Detection



CloudFlare, Inc. [US] https://www.cloudflare.com/waf-settings?z=haiderm.com#page=events

Package Name	Description	Sensitivity	Action
OWASP ModSecurity Core Rule Set	Covers OWASP Top 10 vulnerabilities, and more.	High ▼	Challenge ▼
OWASP Protocol Anomalies	Detection of unusual use of the HTTP protocol that may indicate an attack, but that may also be legitimate.	Triggered 9 times	ON
OWASP Generic Attacks	Detection of generic attacks against web-based applications without specific knowledge of the application. Detects things like attempting to access an LDAP directory, inject shell commands, and attacks against	Triggered 91 times	ON
OWASP XSS Attacks	Cross site scripting (XSS) attacks that may result in unwanted HTML being inserted into web pages.	Triggered 280 times	ON
OWASP Slr Et SQLi Attacks	Rules to detect SQLi attacks.	Triggered 29 times	ON
OWASP Slr Et Lfi Attacks	Rules to detect LFI attacks.	Triggered 35 times	ON
OWASP Slr Et WordPress Attacks	Rules to detect attacks on WordPress.	Triggered 36 times	ON
OWASP Slr Et XSS Attacks	Rules to detect XSS attacks.	Triggered 30 times	ON
OWASP Common Exceptions	Special rules to reduce false positives.	Triggered 0 times	ON

Cloudflare Web Application Firewall Modsecurity core ruleset

Cloudflare’s own ruleset

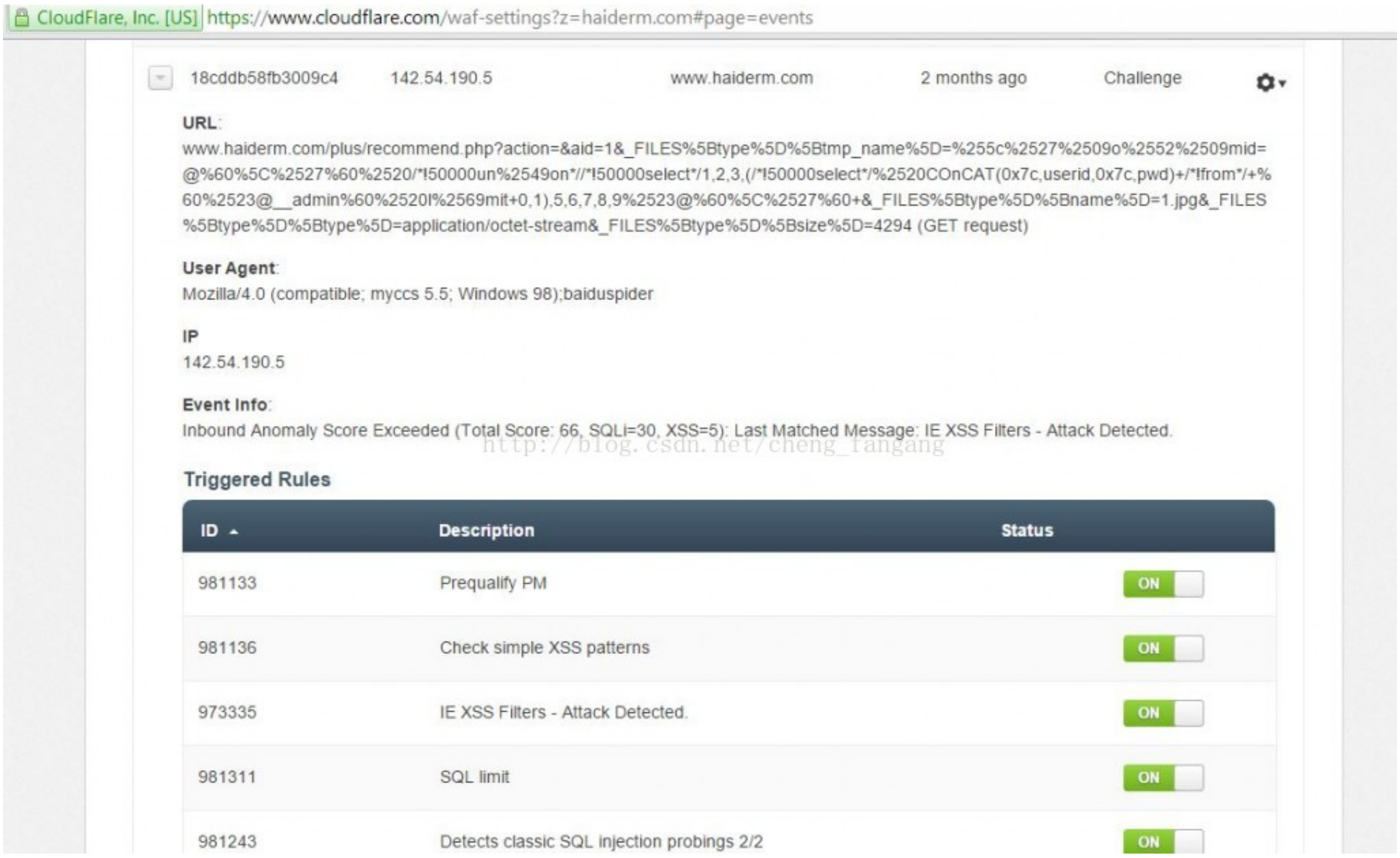
Cloudflare Ruleset is developed in-house by cloudflare. This ruleset contains several other rulesets for particular applications which contains the following.

- ***CloudFlare Atlassian*** This ruleset provides specific protections against vulnerabilities within Atlassian applications and services.
- ***CloudFlare Plone*** This ruleset should only be enabled if the Plone CMS is used for this domain. It contains additional rules that complement the technology-specific protections provided by similar rules in the OWASP ruleset.
- ***CloudFlare Miscellaneous*** CloudFlare Miscellaneous contains rules to deal with known malicious traffic or patch flaws in specific web applications.
- ***CloudFlare Php*** This ruleset should only be enabled if PHP is used for this domain. It contains additional rules that complement the technology-specific protections provided by similar rules in the OWASP ruleset.
- ***CloudFlare Whmcs*** This ruleset should only be enabled if WHMCS is used for this domain. It contains additional rules that complement the technology-specific protections provided by similar rules in the OWASP ruleset.
- ***CloudFlare WordPress*** This ruleset should only be enabled if the WordPress CMS is used for this domain. It contains additional rules that complement the technology-specific protections provided by similar rules.
- ***CloudFlare Joomla*** This ruleset should only be enabled if the Joomla CMS is used for this domain. It contains additional rules that complement the technology-specific protections provided by similar rules in the OWASP ruleset.
- ***CloudFlare Drupal*** This ruleset should only be enabled if the Drupal CMS is used for this domain. It contains additional rules that complement the technology-specific protections provided by similar rules in the OWASP ruleset.

- ***CloudFlare Flash*** This ruleset should only be enabled if Adobe Flash content is used for this domain. It contains additional rules that complement the technology-specific protections provided by similar rules.
- ***CloudFlare Specials*** CloudFlare Specials contains a number of rules that have been created to deal with specific attack types.

Cloudflare WAF events

Cloudflare WAF generates events when they are triggered, user can view those events their rulesets, why they were triggered, including the POST or GET request. This is particularly interested for people in Information security because you can see what attacks are common now adays, which services are being attacked and what are the payloads being used. I personally saw some interesting attacks. For example this one



CloudFlare, Inc. [US] https://www.cloudflare.com/waf-settings?z=haiderm.com#page=events

18cddb58fb3009c4 142.54.190.5 www.haiderm.com 2 months ago Challenge

URL:

```
www.haiderm.com/plus/recommend.php?action=&aid=1&_FILES%5Btype%5D%5Btmp_name%5D=%255c%2527%2509o%2552%2509mid=
@%60%5C%2527%60%2520/*!50000un%2549on*//*!50000select*/1,2,3,(/*!50000select*/%2520COnCAT(0x7c,userid,0x7c,pwd)+/*!from*/+%
60%2523@__admin%60%2520I%2569mit+0,1),5,6,7,8,9%2523@%60%5C%2527%60+&_FILES%5Btype%5D%5Bname%5D=1.jpg&_FILES
%5Btype%5D%5Btype%5D=application/octet-stream&_FILES%5Btype%5D%5Bsize%5D=4294 (GET request)
```

User Agent:

Mozilla/4.0 (compatible; myccs 5.5; Windows 98);baiduspider

IP

142.54.190.5

Event Info:

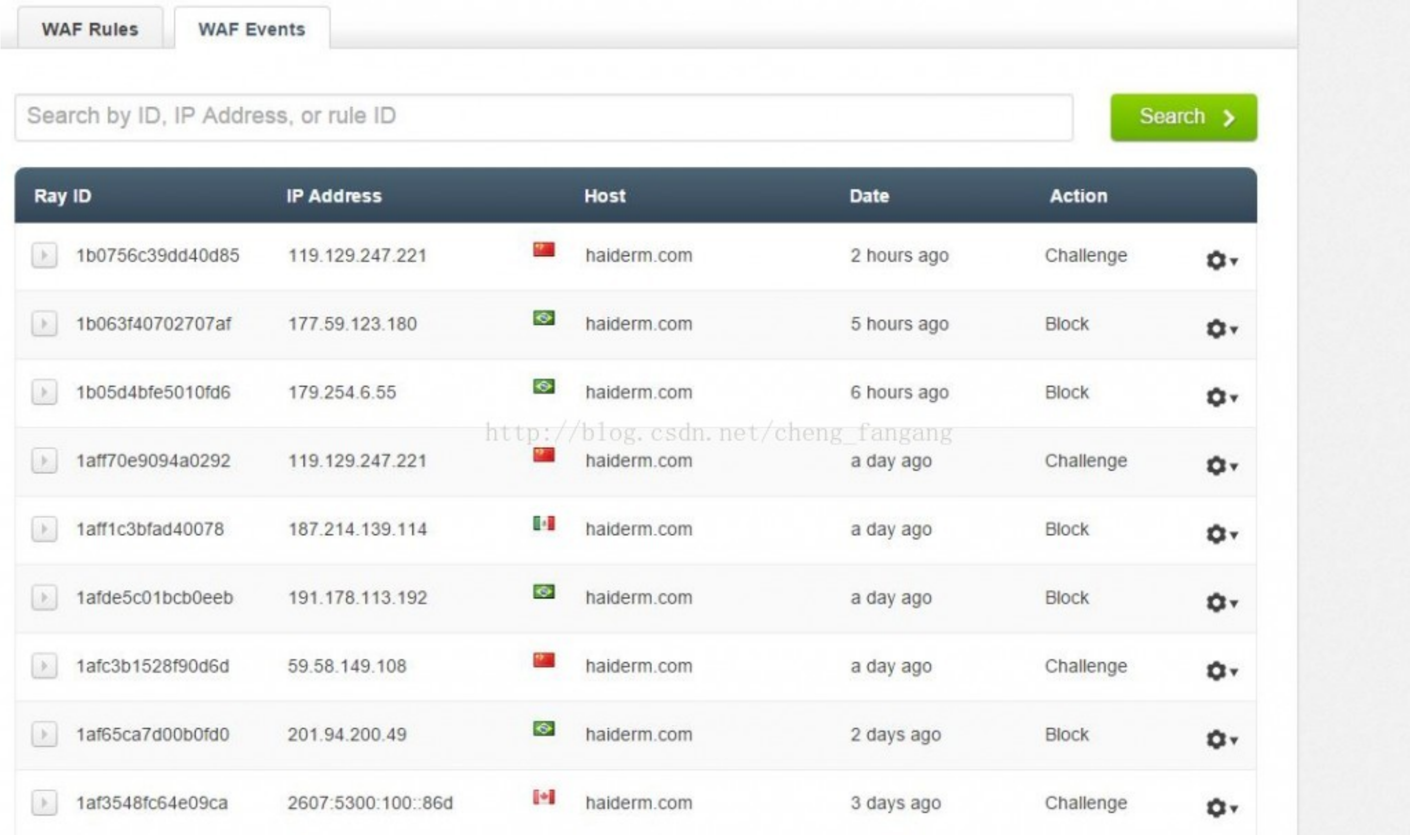
Inbound Anomaly Score Exceeded (Total Score: 66, SQLi=30, XSS=5): Last Matched Message: IE XSS Filters - Attack Detected.

Triggered Rules

ID ▲	Description	Status
981133	Prequalify PM	ON
981136	Check simple XSS patterns	ON
973335	IE XSS Filters - Attack Detected.	ON
981311	SQL limit	ON
981243	Detects classic SQL injection probings 2/2	ON

Cloudflare Web Application Firewall Review

This is an SQL injection attack on a specific application. Even if you are lucky you can also get Zero Day vulnerabilities. The screenshot below describes the overall look for WAF events. The features here are self explanatory in screenshot.



Ray ID	IP Address		Host	Date	Action
1b0756c39dd40d85	119.129.247.221	🇨🇳	haiderm.com	2 hours ago	Challenge
1b063f40702707af	177.59.123.180	🇧🇷	haiderm.com	5 hours ago	Block
1b05d4bfe5010fd6	179.254.6.55	🇧🇷	haiderm.com	6 hours ago	Block
1aff70e9094a0292	119.129.247.221	🇨🇳	haiderm.com	a day ago	Challenge
1aff1c3bfad40078	187.214.139.114	🇲🇽	haiderm.com	a day ago	Block
1afde5c01bcb0eeb	191.178.113.192	🇧🇷	haiderm.com	a day ago	Block
1afc3b1528f90d6d	59.58.149.108	🇨🇳	haiderm.com	a day ago	Challenge
1af65ca7d00b0fd0	201.94.200.49	🇧🇷	haiderm.com	2 days ago	Block
1af3548fc64e09ca	2607:5300:100::86d	🇨🇦	haiderm.com	3 days ago	Challenge

Cloudflare Web Application Firewall Review

Conclusion

Cloudflare Web Application Firewall is simply great, it offers easy interface , a lots of features. The most important thing is the level of customization and details it offers. I personally recommend it as compared to Open sources WAF solutions. The easy to use interface and description of every makes it easy for non info security person to adopt to their settings. You may ask about negatives, i really tried to find negatives, I dont seem to find any, if you have any negatives, feels free to post in comments, i will include them in this article. Thanks for reading Cloudflare Web Application Firewall Review.

source: https://haiderm.com/cloudflare-web-application-firewall-review/