实验吧——WriteUp&&涨姿势（1）

原创

浅零半泣 于 2017-04-15 17:21:11 发布

分类专栏： CTF 文章标签： CTF wp web

WriteUp

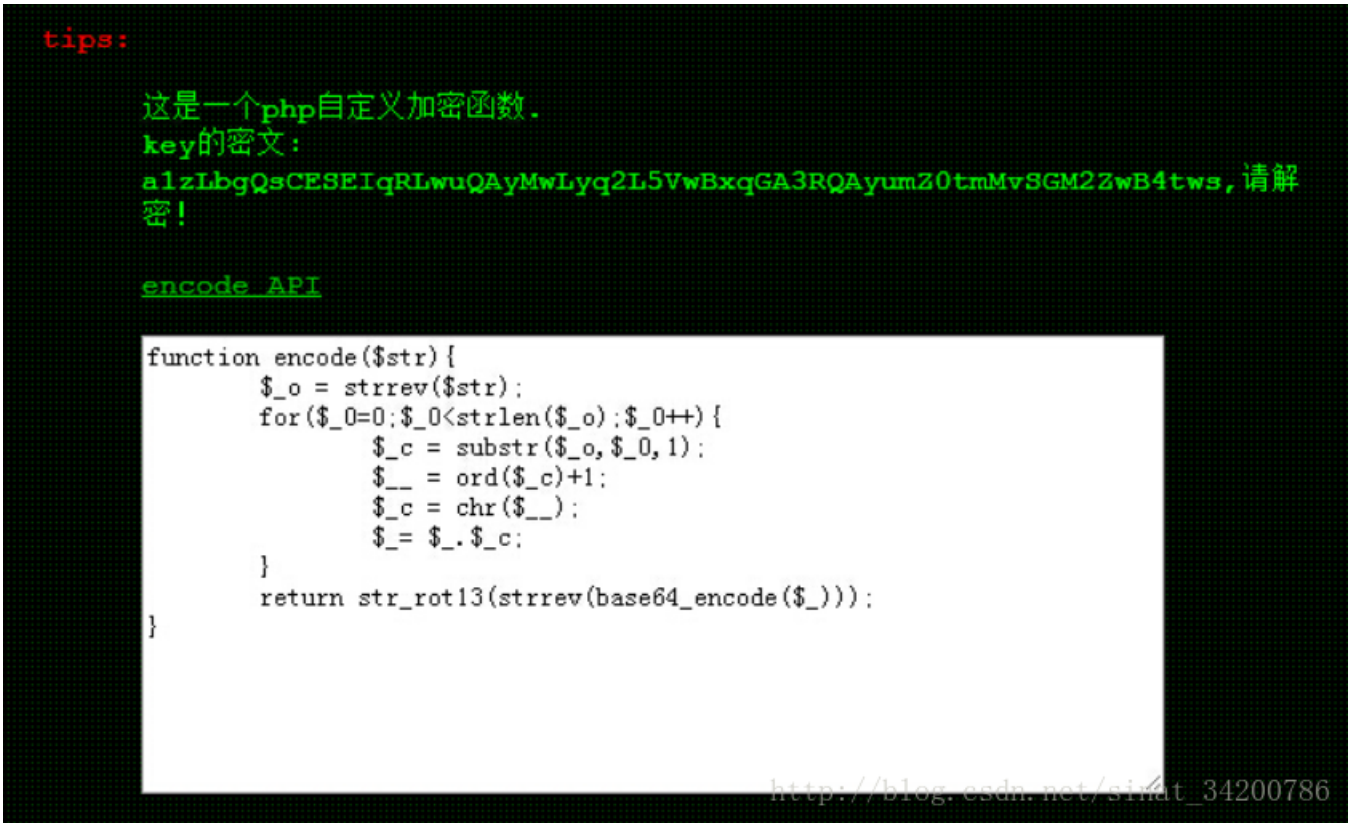
1.NSCTF web200
2.Forbidden
3.猫抓老鼠

涨姿势

1.上传绕过
2.Guess Next Session
3.天下武功唯快不破
4.what a fuck!这是什么鬼东西?
5.头有点大

NSCTF web200

原题



解题思路

```
就是一个很简单的逆向题，不多解释
```

WriteUp

```php
<?php
$str = "a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws";
$str = base64_decode(strrev(str_rot13($str)));
$vstr = "";
for($i = 0;$i<strlen($str);$i++)
{
    $c = substr($str,$i,1);
    $k = ord($c)-1;
    $c = chr($k);
    $vstr = $vstr.$c;
}
$str = strrev($vstr);
echo $str;
?>
```

Forbidden

原题

Forbidden

You don't have permission to access / on this server.

Make sure you are in HongKong

解题思路

```
抓包修改Accept-Language为zh-hk
```

WriteUp

猫抓老鼠

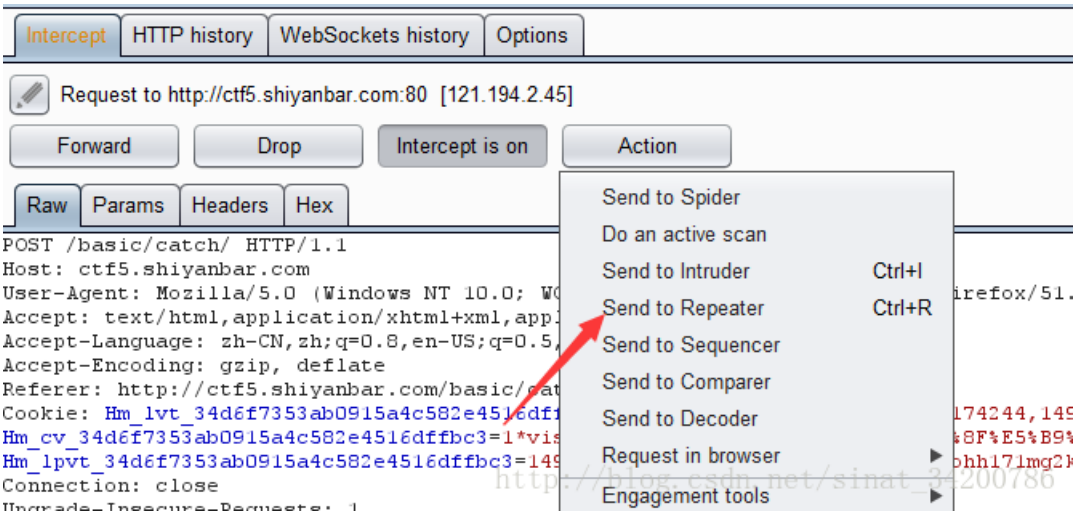
原题

解题思路

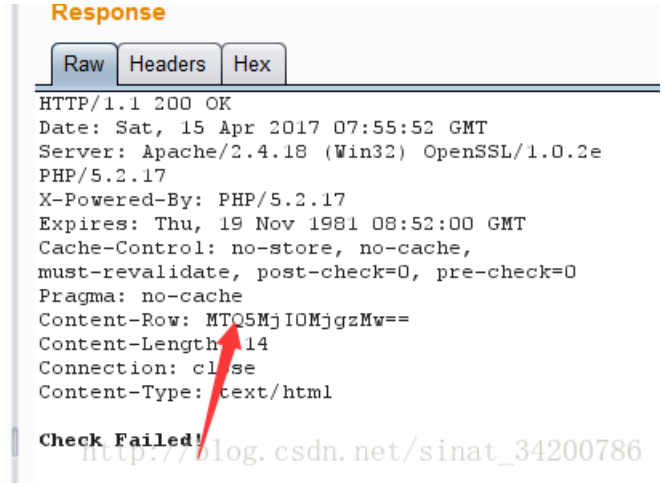
```
查看返回头可发现Content-Row是一个base64加密的密文，此题有个小小的脑洞，就是密文不解密
```

WriteUp

```
Burp Suide抓包后将包发到Repeader
```



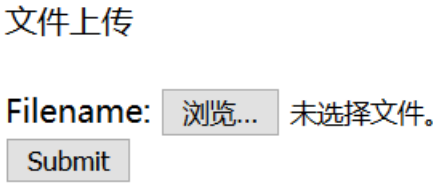
查看Respond可得密文



将密文直接输入即可

上传绕过

原题

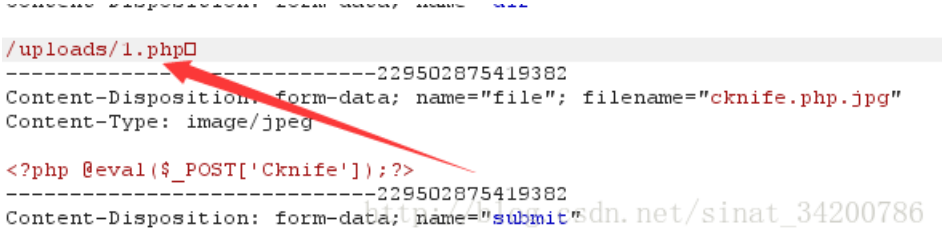


解题思路

经历了00截断，Content-Type修改，绕过前段检测，apache解析漏洞等各种方法无果后，通过查看wp知道了原来是路径截断

WriteUp

抓包后在路径后面添加/1.php%0，选中%0 shirt+ctrl+B(转换为Unicode字符)此处截断路径



涨姿势点

路径截断，又一个上传绕过的方法

Guess Next Session

原题

- 4929482
- 5206298
- 4968406

Next number

Guess

View the source code

```
<?php
session_start();
if (isset ($_GET['password'])) {
    if ($_GET['password'] ==
$_SESSION['password'])
        die 'Flag: '.$flag;
    else
        print '<p>Wrong guess.</p>';
}

mt_srand((microtime() ^ rand(1, 10000)) %
rand(1, 10000) + rand(1, 10000));
?>
```


解题思路

根据源码来看，如果想硬杠就得搞定那几个随机函数，这个可能性太低所以肯定另有妙计。仔细看可以发现只要$_GET['password']

WriteUp

抓包改数据如图

```
GET /web/Session.php?password=34553 HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
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
Referer: http://ctf5.shiyanbar.com/web/Session.php
Cookie: sample-hash=571580b26c65f306376d4f64e53cb5c7; source=0;
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1491999349,1492088891,1492174244,1492241613;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*87165%2CnickName%3A%E5%BA%8F%E5%B9%95%E4%B8%83%E7%AB%A0;
Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1492244003; PHPSESSID=14eq4pm4eupohh171mg2k6q764
Connection: close
Upgrade-Insecure-Requests: 1
```


直接将后面的参数删除即可

```
GET /web/Session.php?password= HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
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
Referer: http://ctf5.shiyanbar.com/web/Session.php?password=34553
Cookie: sample-hash=571580b26c65f306376d4f64e53cb5c7; source=0;
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1491999349,1492088891,1492174244,1492241613;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*87165%2CnickName%3A%E5%BA%8F%E5%B9%95%1
Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1492244003; PHPSESSID=
Connection: close
Upgrade-Insecure-Requests: 1
```


涨姿势点

抓包后将pass改为空则$_GET['pass']为""，不输入直接提交也是""
由自己控制上传的session
确定是哪个session

天下武功唯快不破

原题

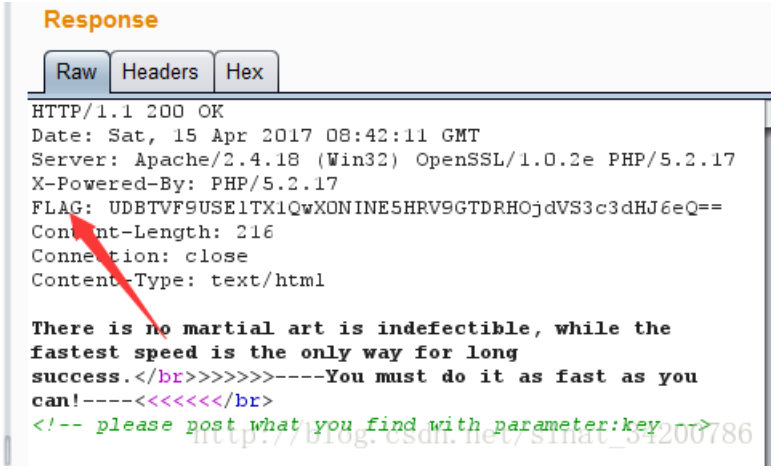
There is no martial art is indefectible, while the fastest speed is the only way for long success.
>>>>>>----You must do it as fast as you can!----<<<<<<

解题思路

很明显只有代码才够快

WriteUp

抓包查看Respond可以发现相应头有个FLAG




```
解密得到：P0ST_THIS_T0_CH4NGE_FL4G:7UKw7trzy
于是知道冒号后面的参数是解题关键，发送回去
```

Code(引用自实验吧@madman)

```
import urllib.request
import urllib.parse
import base64

opener = urllib.request.build_opener()
url = "http://ctf5.shiyanbar.com/web/10/10.php"

response = opener.open(url)
data = {"key": base64.b64decode(response.getheader("FLAG")).decode().split(":")[1]}
html = opener.open(url, urllib.parse.urlencode(data).encode()).read()

print(html)
```

涨姿势点

```
原来是发送回原来的网址，一开始就迷惑到底发送到哪里去
```

---

what a fuck!这是什么鬼东西？

原题

```
![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+
[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![
+[])[+[]]+(![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[]
+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]](([][(![]+[])[+[]]+([![]]+[][[]
[]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+
)[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+
+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]([][(![]+[])[+[]
[]]+(+[![]]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[
]+[])[!+[]+!+[]+!+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]
))[(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+
![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]
)[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(
+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+
)[+!+[]+[+[]]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]](!+[]+!+[]+!+[]
```


解题思路

这些符号在平时没什么意义，但在jsfuck中却可以用来写任意的js代码。所以这其实就是js代码，浏览器控制台执行一下就行了

WriteUp

涨姿势点

认识新事物—jsfuck

头有点大

原题

Tips　　http header

Forbidden

You don't have permission to access / on this server.

Please make sure you have installed .net framework 9.9!

Make sure you are in the region of England and browsing this site with Internet Explorer

解题思路

```
就按照题目的意思办，F12改请求头
```

WriteUp


```
编辑和重发，User-Agent中添加 .NET CLR 9.9，修改Accept-Language为en-gb
```


```
发送后查看预览
```

涨姿势点

```
    .net framework 9.9 在请求头中的表示—— .NET CLR 9.9
```