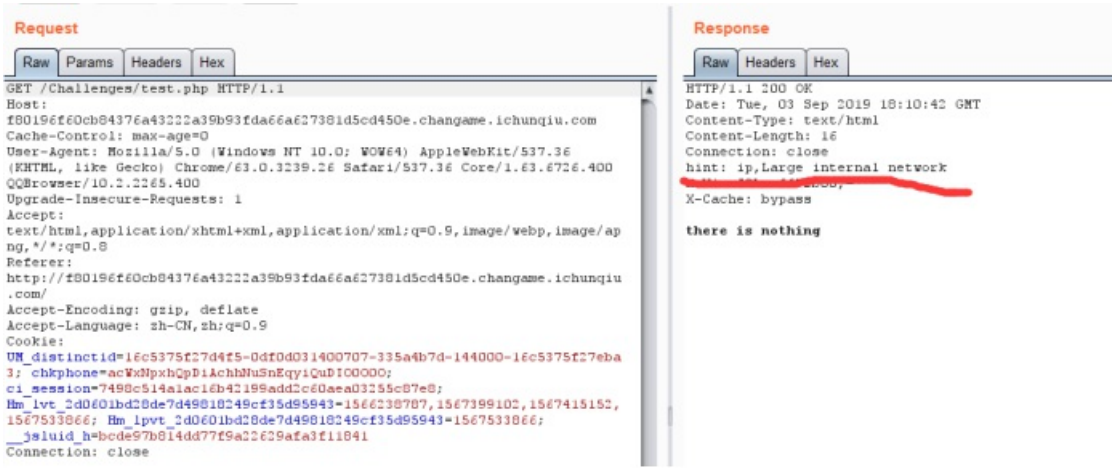
i春秋Fuzzing

转载

weixin_30701575 于 2019-09-11 13:58:00 发布 86 收藏
文章标签： php
原文链接：http://www.cnblogs.com/wosun/p/11505883.html

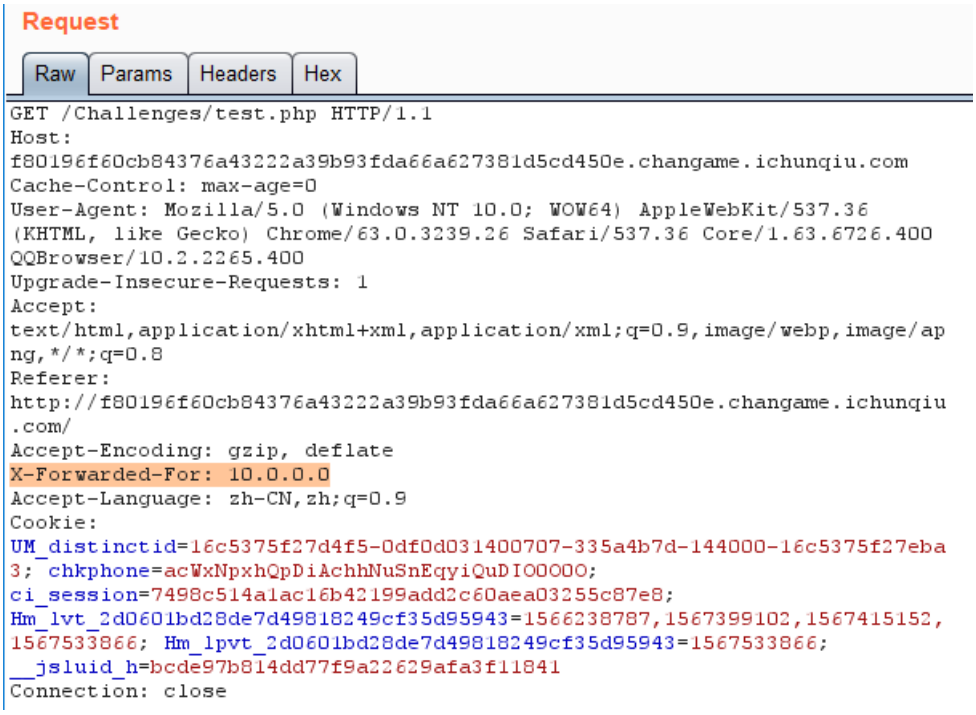
先查看源码。。。没东西，抓包



发现也没什么，但是右边有个提示hint: ip,Large internal network（**最大内网ip**）

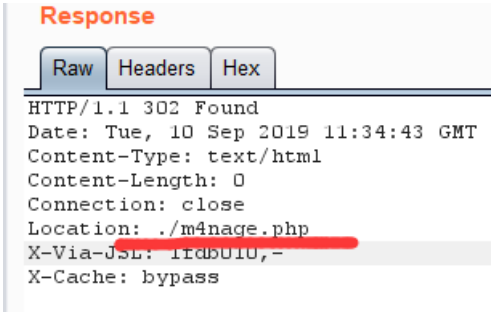
可能需要我们伪造代码进行访问，这还不简单，直接在request中加入

X-Forwarded-For: 10.0.0.0

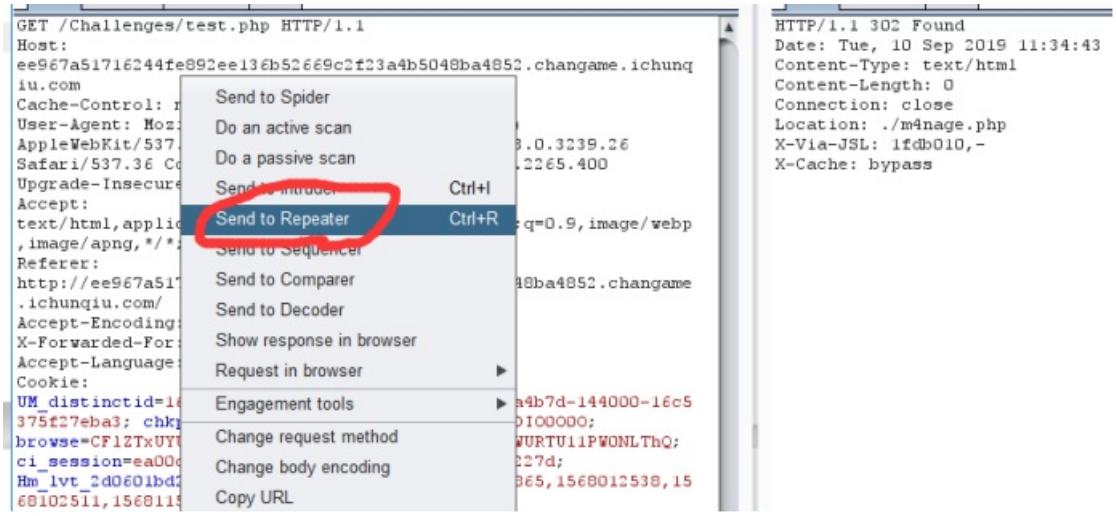


来进行伪造ip

Go一下发现request栏中出现了新文件



复制文件名，右键新建一个repeater访问试试



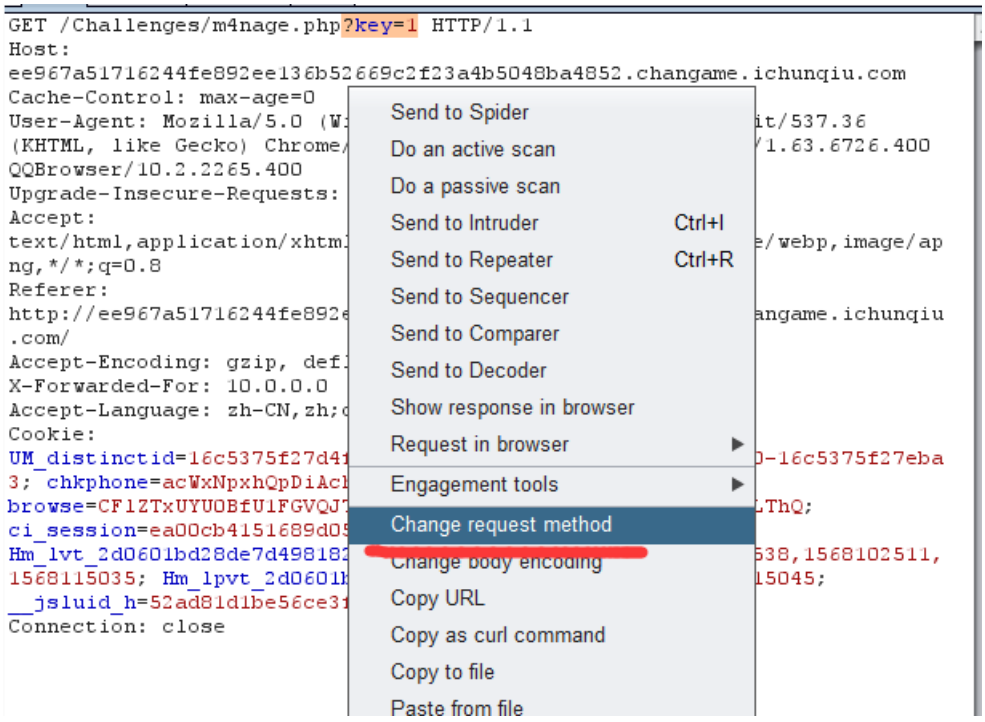
更改GET url栏中的文件访问之

弹出show me your key

常规思路就是直接GET栏传入

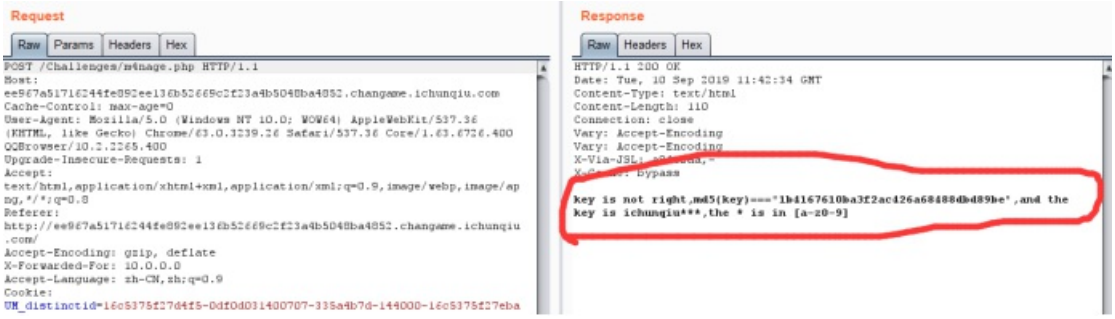
Go一下没反应。。。。试试POST传入

右键request栏选择改变请求方式



直接变成了POST传入，GO一下

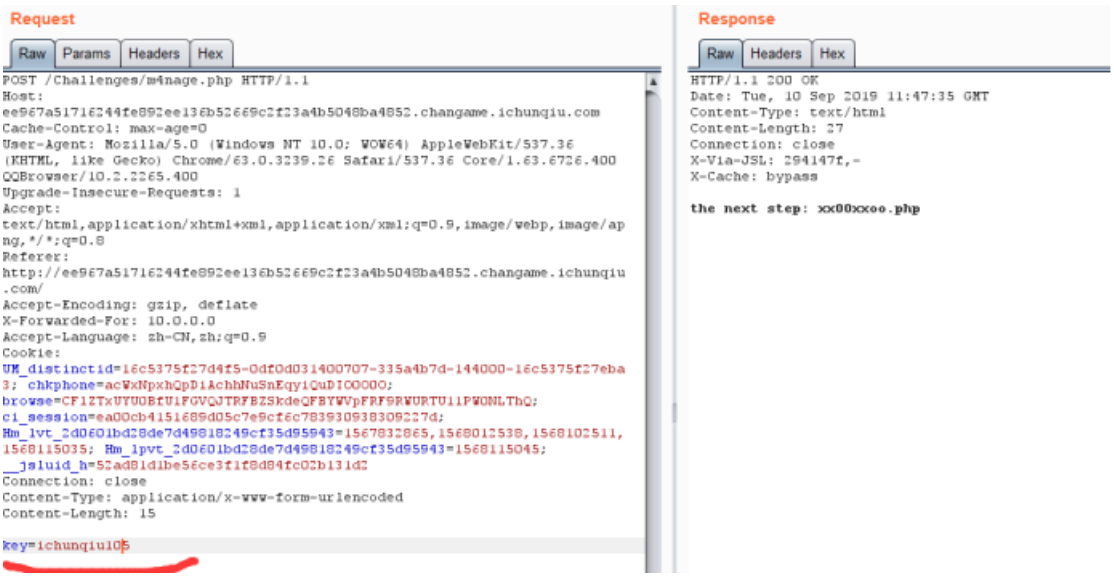
得到提示



我们的key不正确，正确的key的md5是。。。。。并且这key的形式是ichunqiu***（*的范围在。。。）

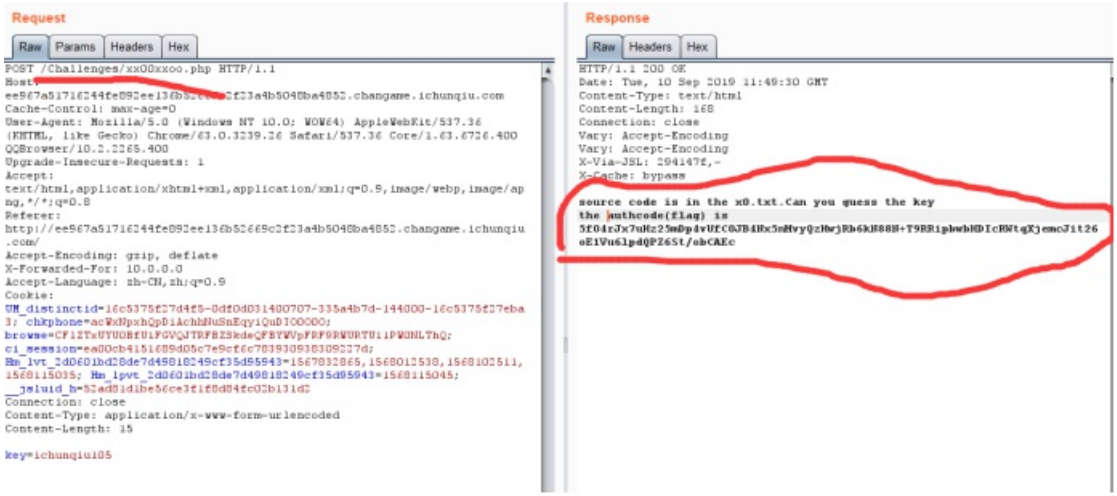
这里可以写脚本爆破（不断尝试***的组合）也可以直接去试试能不能翻译出来

将其拿回去传入



得到下一步提示

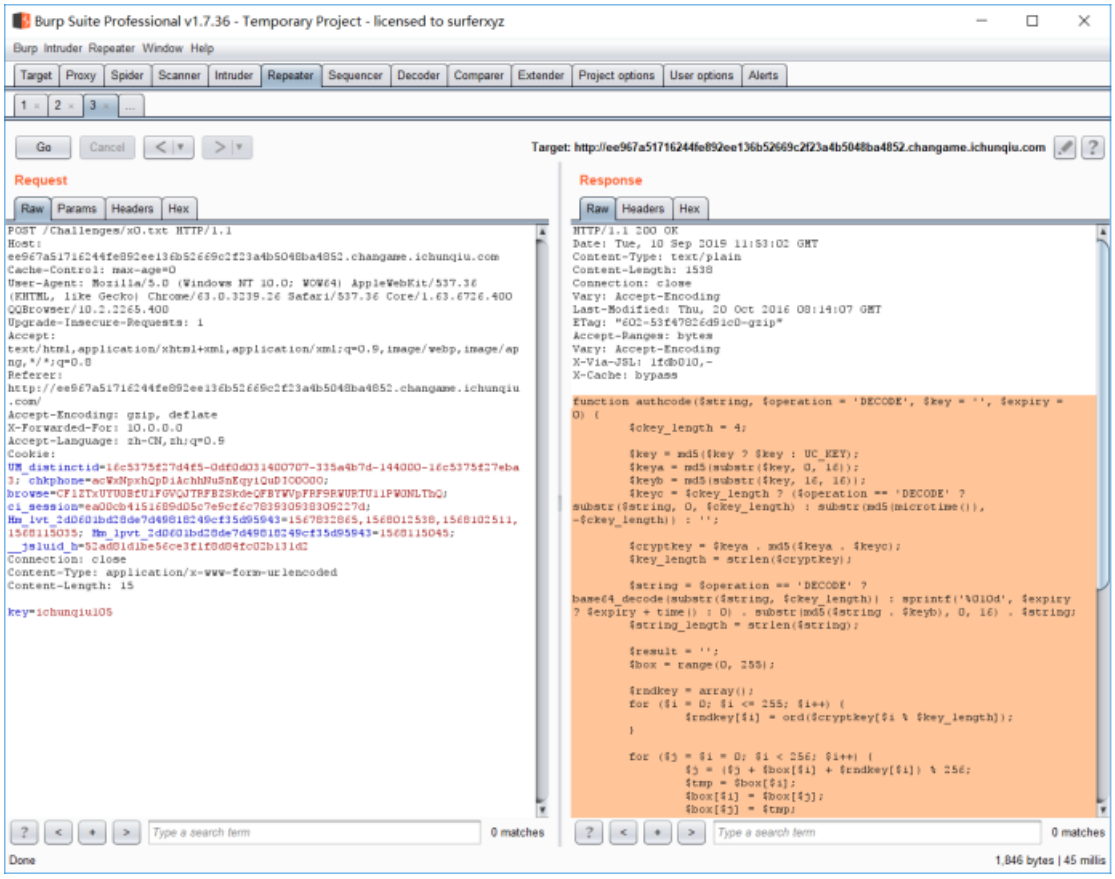
是个php文件，直接访问试试



给出下一步提示

这加密来源是x0.txt然后这加了密的flag是。。。。。

我们直接访问这个x0.txt



果真是个加密的流程

然后根据他这个加密流程反向写出解密的脚本

```php
<?php
function authcode($string, $operation = 'DECODE', $key = '', $expiry = 0) {
    $ckey_length = 4;

    $key = md5($key ? $key : UC_KEY);
    $keya = md5(substr($key, 0, 16));
    $keyb = md5(substr($key, 16, 16));
    $keyc = $ckey_length ? ($operation == 'DECODE' ? substr($string, 0, $ckey_length) :
substr(md5(microtime()), -$ckey_length)) : '';

    $cryptkey = $keya . md5($keya . $keyc);
    $key_length = strlen($cryptkey);

    $string = $operation == 'DECODE' ? base64_decode(substr($string, $ckey_length)) : sprintf('%010d',
$expiry ? $expiry + time() : 0) . substr(md5($string . $keyb), 0, 16) . $string;
    $string_length = strlen($string);

    $result = '';
    $box = range(0, 255);

    $rndkey = array();
    for ($i = 0; $i <= 255; $i++) {
        $rndkey[$i] = ord($cryptkey[$i % $key_length]);
    }

    for ($j = $i = 0; $i < 256; $i++) {
        $j = ($j + $box[$i] + $rndkey[$i]) % 256;
        $tmp = $box[$i];
        $box[$i] = $box[$j];
        $box[$j] = $tmp;
    }

    for ($a = $j = $i = 0; $i < $string_length; $i++) {
        $a = ($a + 1) % 256;
        $j = ($j + $box[$a]) % 256;
        $tmp = $box[$a];
        $box[$a] = $box[$j];
        $box[$j] = $tmp;
        $result .= chr(ord($string[$i]) ^ ($box[($box[$a] + $box[$j]) % 256]));
    }

    if ($operation == 'DECODE') {
        if ((substr($result, 0, 10) == 0 || substr($result, 0, 10) - time() > 0) && substr($result, 10, 16)
== substr(md5(substr($result, 26) . $keyb), 0, 16)) {
            return substr($result, 26);
        } else {
            return '';
        }
    } else {
        return $keyc . str_replace('=', '', base64_encode($result));
    }

}

echo authcode($string =
'5f04rJx7uHz25mDp4vUfC0JB4Nx5nMvyQzHwjRb6kN88N+T9RRipbwbHDIcRWtqXjemcJit26oE1Vu6lpdQPZ6St/obCAEc',
$operation = 'DECODE', $key = 'ichunqiu105');
?>
```

（string后面接密文）

本地运行得到flag

flag{e6240cc3-d3ea-41ec-9778-10f5ca5e308b}

转载于:https://www.cnblogs.com/wosun/p/11505883.html