

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>

版权

先查看源码。。。没东西, 抓包

The screenshot shows a network request and response. The request is a GET to /Challenges/test.php. The response is a 200 OK with a hint: "ip, Large internal network".

```
Request
Raw Params Headers Hex
GET /Challenges/test.php HTTP/1.1
Host: f80196f60cb84376a43222a39b93fda66a627381d5cd450e.changame.ichunqiu.com
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400 QQBrowser/10.2.2265.400
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://f80196f60cb84376a43222a39b93fda66a627381d5cd450e.changame.ichunqiu.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f27eba3; chkphone=acWdJpxhQpDiAchhNuSnEqyiQuDIO0000; ci_session=7498c514a1ac16b42199add2c60aea03255c87e8; Hm_lvt_2d0601bd28de7d49818249cf35d95943=1566238787,1567399102,1567415152,1567533866; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1567533866; __jsluid_h=bcd97b814dd77f9a22629afa3f11841
Connection: close

Response
Raw Headers Hex
HTTP/1.1 200 OK
Date: Tue, 03 Sep 2019 18:10:42 GMT
Content-Type: text/html
Content-Length: 16
Connection: close
hint: ip, Large internal network
X-Cache: bypass

there is nothing
```

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

The screenshot shows a network request with the X-Forwarded-For header set to 10.0.0.0.

```
Request
Raw Params Headers Hex
GET /Challenges/test.php HTTP/1.1
Host: f80196f60cb84376a43222a39b93fda66a627381d5cd450e.changame.ichunqiu.com
Cache-Control: max-age=0
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400 QQBrowser/10.2.2265.400
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://f80196f60cb84376a43222a39b93fda66a627381d5cd450e.changame.ichunqiu.com/
Accept-Encoding: gzip, deflate
X-Forwarded-For: 10.0.0.0
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f27eba3; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000; ci_session=7498c514a1ac16b42199add2c60aea03255c87e8; Hm_lvt_2d0601bd28de7d49818249cf35d95943=1566238787,1567399102,1567415152,1567533866; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1567533866; __jsluid_h=bcd97b814dd77f9a22629afa3f11841
Connection: close
```

来进行伪造ip

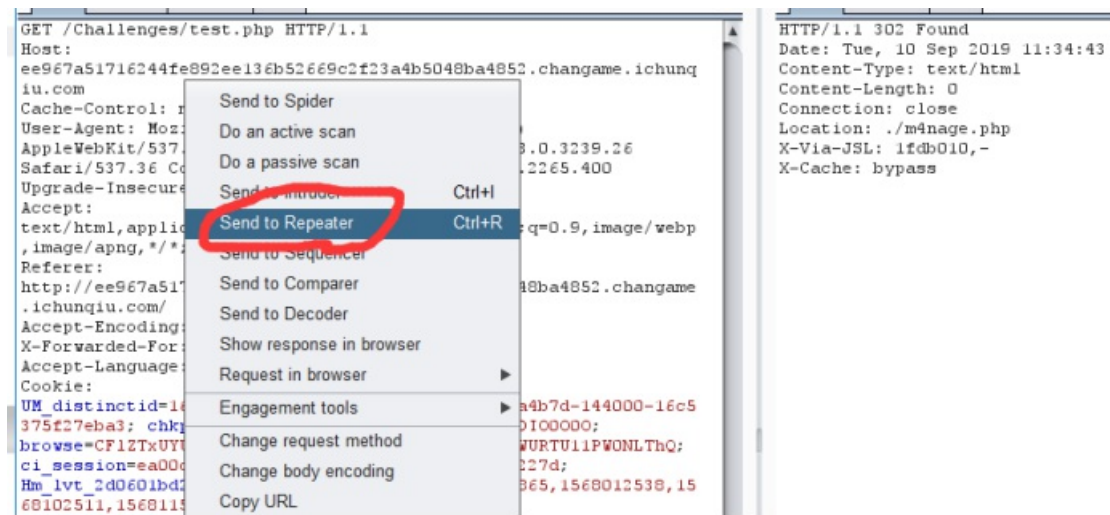
Go一下发现request栏中出现了新文件

```

Response
Raw Headers Hex
HTTP/1.1 302 Found
Date: Tue, 10 Sep 2019 11:34:43 GMT
Content-Type: text/html
Content-Length: 0
Connection: close
Location: ./m4nage.php
X-Via-JSL: 1fdb010,-
X-Cache: bypass

```

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



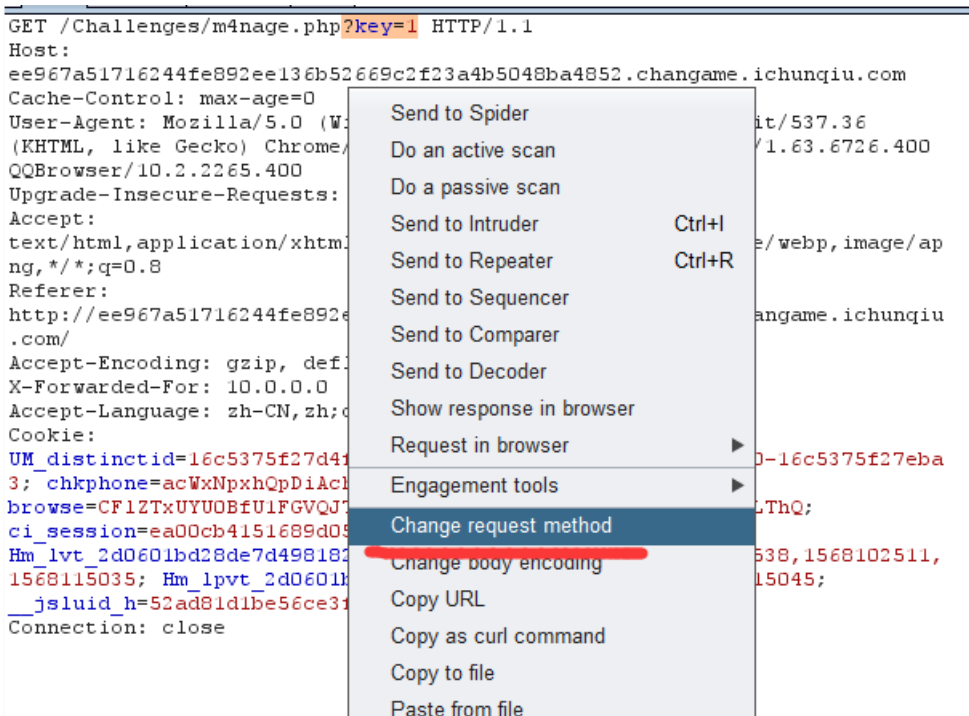
弹出show me your key

常规思路就是直接GET栏传入



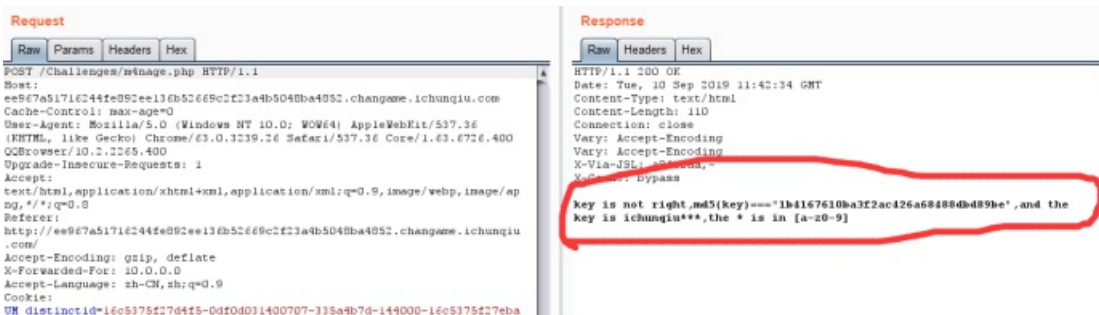
Go一下没反应。。。试试POST传入

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

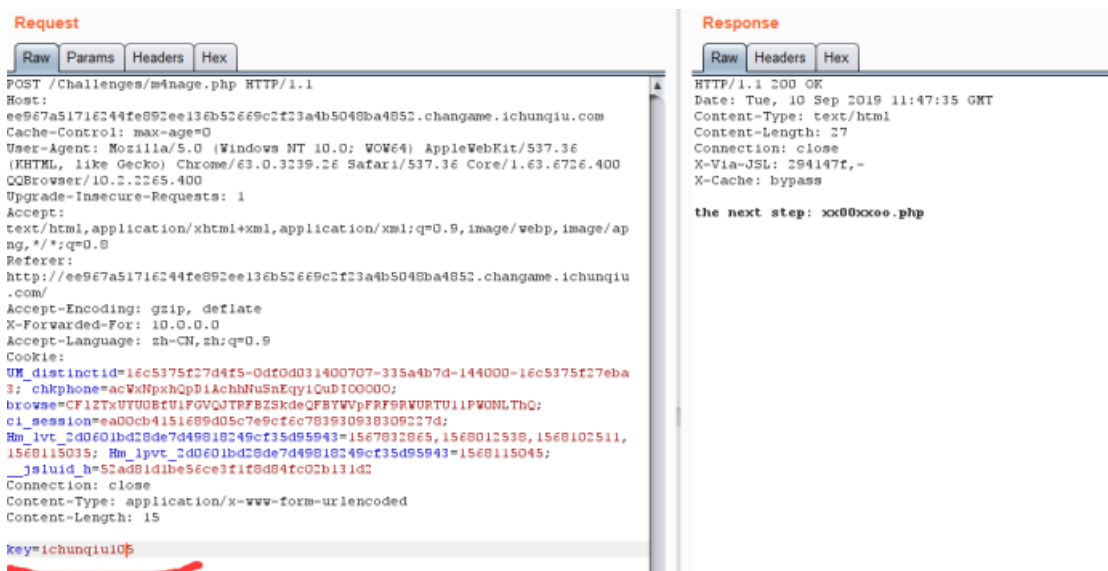


我们的key不正确，正确的key的md5是。。。。并且这key的形式是ichunqu*** (*的范围在。。。)

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

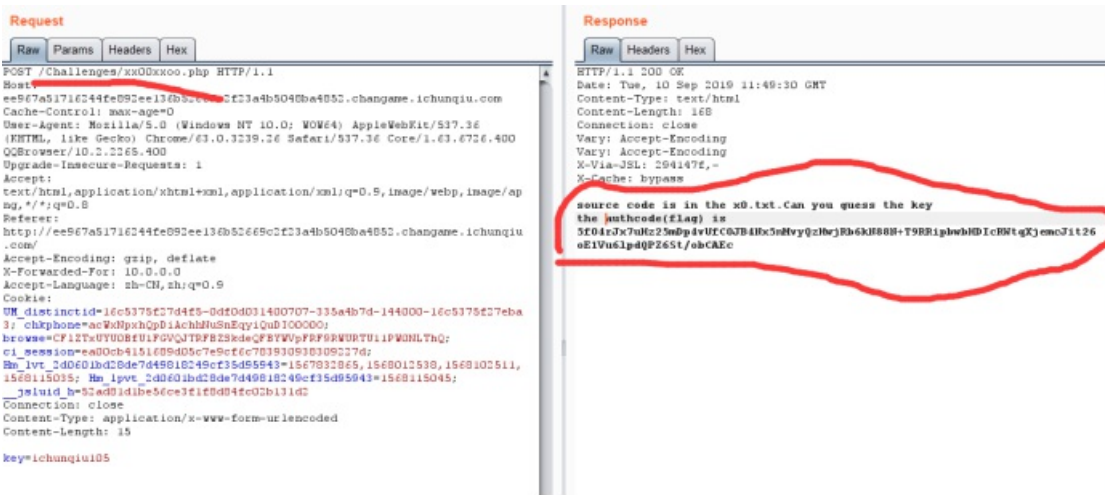


将其拿回去传入



得到下一步提示

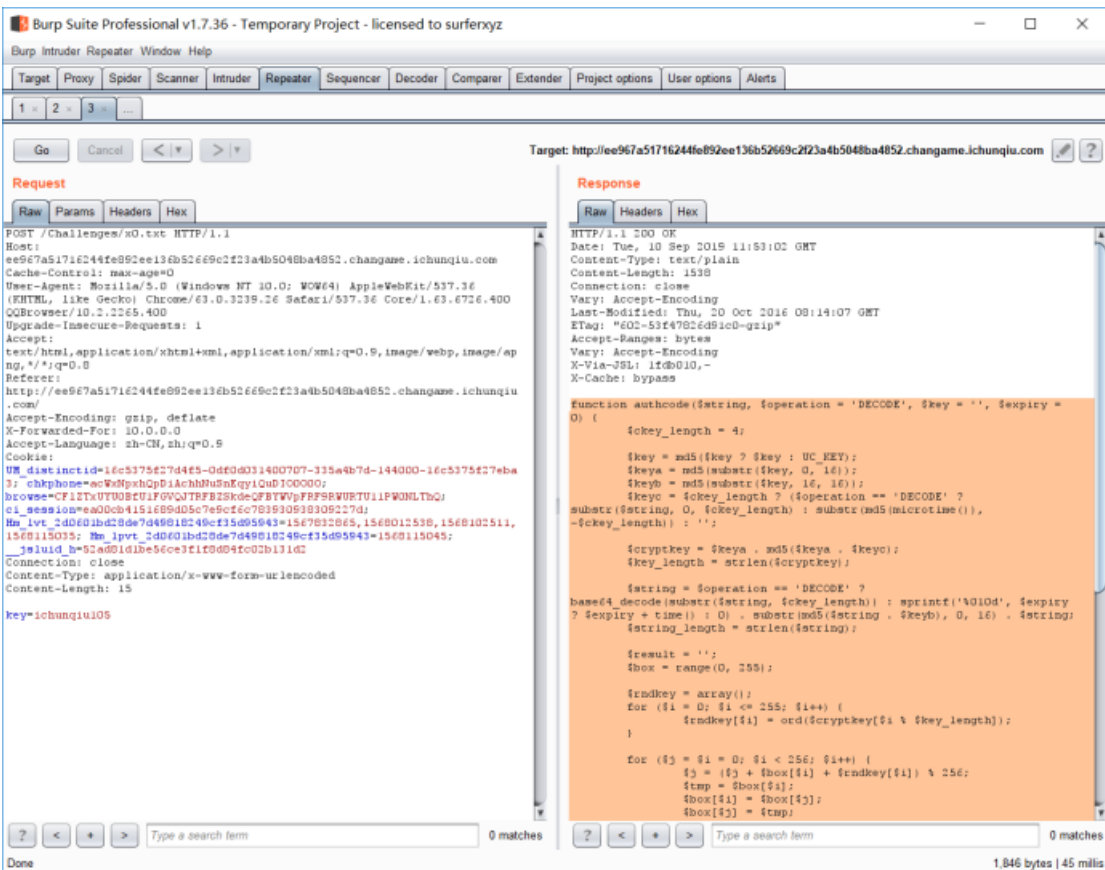
是个php文件，直接访问试试



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脚本

```

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

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

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

    $string = $operation == 'DECODE' ? base64_decode(substr($string, $key_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+T9RRipwbHDIcRWtqXjemcJit26oE1Vu6lpdQPZ6St/obCAEc',
$operation = 'DECODE', $key = 'ichunqiu105');
?>

```

(string后面接密文)

本地运行得到flag

< > ↻ 🏠 📖 | ☆ 127.0.0.1/13.php

★ 书签 | 📁 常用网址 🌐 京东商城 📖 中国大学MOOC(🌐) 🌐 C 语言

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

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