

# 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

原文地址: <http://www.cnblogs.com/wosun/p/11505883.html>

版权

先查看源码。。。没东西，抓包

**Request**

Raw Params Headers Hex

```
GET /Challenges/test.php HTTP/1.1
Host: f80196ff0cb84376a43222a39b93fda66a627381d5cd450e.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/*,*;q=0.8
Referer: http://f80196ff0cb84376a43222a39b93fda66a627381d5cd450e.changame.ichunqiu.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f27eba
3; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000;
ci_session=7498c514alac16b42199add2c60aea03255c87e8;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1566238787,1567399102,1567415152,
1567533866; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1567533866;
_jsluid_h=bcde97b814dd77f9a22629afa3f11841
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

**Request**

Raw Params Headers Hex

```
GET /Challenges/test.php HTTP/1.1
Host: f80196ff0cb84376a43222a39b93fda66a627381d5cd450e.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/*,*;q=0.8
Referer: http://f80196ff0cb84376a43222a39b93fda66a627381d5cd450e.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-144000-16c5375f27eba
3; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000;
ci_session=7498c514alac16b42199add2c60aea03255c87e8;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1566238787,1567399102,1567415152,
1567533866; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1567533866;
_jsluid_h=bcde97b814dd77f9a22629afa3f11841
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

GET /Challenges/test.php HTTP/1.1
Host: ee967a51716244fe892ee136b52669c2f23a4b5048ba4852.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://ee967a51716244fe892ee136b52669c2f23a4b5048ba4852.changame.ichunqiu.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM\_distinctid=14b7d-144000-16c5375f27eba3; chk\_browse=CF1ZTxUYI; ci\_session=ea00; Hm\_lvt\_2d0601bd268102511,15680115680111
[Send to Spider](#)
[Do an active scan](#)
[Do a passive scan](#)
[Send to Repeater](#) **Ctrl+R**
[Send to Sequence](#)
[Send to Comparer](#)
[Send to Decoder](#)
[Show response in browser](#)
[Request in browser](#)
[Engagement tools](#)
[Change request method](#)
[Change body encoding](#)
[Copy URL](#)

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

更改GET url栏中的文件访问之

GET /Challenges/m4nage.php HTTP/1.1
Host: ee967a51716244fe892ee136b52669c2f23a4b5048ba4852.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://ee967a51716244fe892ee136b52669c2f23a4b5048ba4852.changame.ichunqiu.com/
Accept-Encoding: gzip, deflate
X-Forwarded-For: 10.0.0.0

```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 11:39:51
Content-Type: text/html
Content-Length: 16
Connection: close
X-Via-JSL: a84e2aa,-
X-Cache: bypass
show me your key
```

弹出show me your key

常规思路就是直接GET栏传入

**Request**

Raw Params Headers Hex

```
GET /Challenges/m4nager.php?key=1 HTTP/1.1
Host: ee967a51716244fe892ee136b52669c2f23a4b5048ba4852.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://ee967a51716244fe892ee136b52669c2f23a4b5048ba4852.changame.ichunqiu.com/
Accept-Encoding: gzip, deflate
X-Forwarded-For: 10.0.0.0
Accept-Language: zh-CN,zh;q=0.8
Cookie: UM_distinctid=16c5375f27d413; chkphone=acWxNpxhQpDiAcl; browse=CF12TxUYUOBfU1FGVQJ; ci_session=ea00cb4151689d05; Hm_lvt_2d0601bd28de7d4981821568115035; Hm_lpvt_2d0601b1jsluid_h=52ad81d1be56ce31; Connection: close
```

**Response**

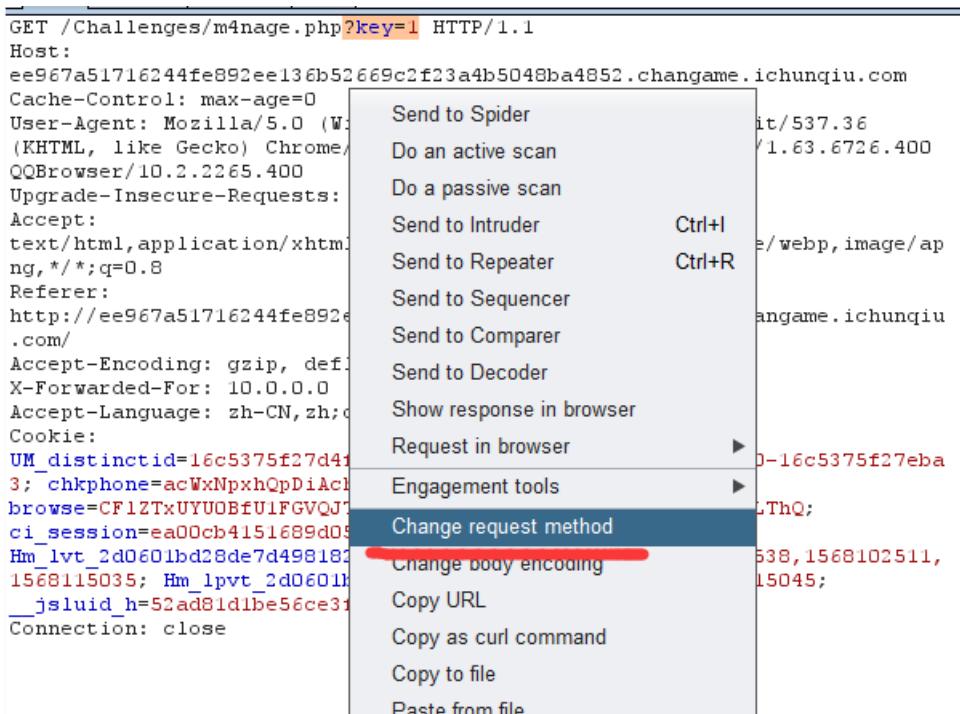
Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 11:41:02
Content-Type: text/html
Content-Length: 16
Connection: close
X-Via-JSL: a84e2aa,-
X-Cache: bypass
```

show me your key

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

**Request**

Raw Params Headers Hex

```
POST /Challenges/m4nager.php HTTP/1.1
Host: ee967a51716244fe892ee136b52669c2f23a4b5048ba4852.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://ee967a51716244fe892ee136b52669c2f23a4b5048ba4852.changame.ichunqiu.com/
Accept-Encoding: gzip, deflate
X-Forwarded-For: 10.0.0.0
Accept-Language: zh-CN,zh;q=0.8
Cookie: UM_distinctid=16c5375f27d413; chkphone=acWxNpxhQpDiAcl; browse=CF12TxUYUOBfU1FGVQJ; ci_session=ea00cb4151689d05; Hm_lvt_2d0601bd28de7d4981821568115035; Hm_lpvt_2d0601b1jsluid_h=52ad81d1be56ce31; Connection: close
```

**Response**

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 11:42:34 GMT
Content-Type: text/html
Content-Length: 110
Connection: close
Vary: Accept-Encoding
Vary: Accept-encoding
X-Via-JSL: a84e2aa,-
X-Cache: bypass
```

key is not right,md5(key)==="1b4167610ba3f2ac426a68488dbd89be", and the key is ichunqiu\*\*\*, the \* is in [a-z0-9]

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

**Request**

[Raw](#) [Params](#) [Headers](#) [Hex](#)

```
POST /Challenges/m4nage.php HTTP/1.1
Host: ee967a51716244fe892ee13eb52669c2f23a4b5048ba4852.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
QCBrowser/10.2.225.400
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/*,*;q=0.8
Referer: http://ee967a51716244fe892ee13eb52669c2f23a4b5048ba4852.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=16c5375f27d4fb-0df0d031400707-335a4b7d-144000-16c5375f27eba
3; chkphone=acWnNpxhQpD1AchhlNuSnEqyiQuD1CO000;
browser=CFIZTxUTU0EtUlFGVQNTRFZSKdeQFBTWpFPR9WURTU11PWONLTbQ;
ci_session=ea00cb415169d05c7e5cfec783930938309227d;
Hm_lvt_2d0601bd28de7d49818249ct35d95943=1567832865,1568012538,1568102511,
1568115035; Hm_lpvt_2d0601bd28de7d49818249ct35d95943=1568115045;
_Jsuid_h=52ad81d1be56ce3f1f8d84fc02b131dc
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 15
```

key=ichunqiu105

**Response**

[Raw](#) [Headers](#) [Hex](#)

```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2019 11:47:35 GMT
Content-Type: text/html
Content-Length: 27
Connection: close
X-Via-JSL: 294147f,-
X-Cache: bypass

the next step: xx00xx00.php
```

得到下一步提示

是个php文件，直接访问试试

Request

Raw Params Headers Hex

POST /Challenges/x00xx00.php HTTP/1.1  
Host: ee867a51716244fe082ee136b2d669cf23a4b5040ba4051.changeme.ichunqiu.com  
Cache-Control: max-age=0  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.36 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://ee867a51716244fe082ee136b2d669cf23a4b5040ba4051.changeme.ichunqiu.com  
Accept-Encoding: gzip, deflate  
X-Forwarded-For: 10.0.0.0  
Accept-Language: zh-CN, zh;q=0.9  
Cookie:  
...  
URL: dictinct=1fc5375ef27d425-0d7d0d03140707-335a4b7d-144000-16c5375ef27eba3; ckphone=aWdpoxhqphikchNbSuNxyq1Qn100000; browser=CF127aUYU008fLULFGwJTRFB23decf87VWVpFRF69WURTL1U1PWNLThQ; c1\_session=e00ccb4151609d05c7e9ff701910910591059176; Hs\_lvt\_2d0601bd7d495818245cf35d5543=1567832855,1568012538,1568102551,1568115013; Hs\_lvt\_2d0601bd2d8d7d49818249cf15d5943=1568115045; jslvid\_b=52ed0d1dib65ce3f1fb0d4fc05b131d; Connection: close  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 15  
key=ichunqiu105

Response

Raw Headers Hex

HTTP/1.1 200 OK  
Date: Tue, 10 Sep 2019 11:49:30 GMT  
Content-Type: text/html  
Content-Length: 168  
Connection: close  
Vary: Accept-Encoding  
Vary: Accept-Encoding  
X-Via: JSL: 294147f,-  
X-Cache: bypass

source code is in the x0.txt. Can you guess the key the puthedon(flag) is 5f04rJx7u0229mD4vUc0JB4Hx5nRyqzJbJRh6kH88H+T9R1pbwHIDCjWtqXjneJit26e0Uv61p0P265t/obCAEc

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

Burp Suite Professional v1.7.36 - Temporary Project - licensed to surferxyz

Burp Intruder Repeater Window Help

Target: http://ee967a51716244fe892ee136b52669c2f23a4b5048ba4852.changame.ichunqiu.com

Request

Raw Headers Hex

POST /Challenges/m0.txt HTTP/1.1  
Host: ee967a51716244fe892ee136b52669c2f23a4b5048ba4852.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/63.0.3239.36 Safari/537.36 Core/1.63.6716.400  
QCBrowser/10.2.225.400  
Upgrade-Insecure-Requests: 1  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap  
\*/,\*;q=0.8  
Referer:  
http://ee967a51716244fe892ee136b52669c2f23a4b5048ba4852.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=16c5375f27d4e5-0df0d031400707-335a4b7d-144000-16c5375f27eba  
3; cbkphone=ecWpfxhqDp1a1chNbhuNqyLQn1C000000;  
browse=CFl7TxUYU0BtUFQVQJTFB2zHdeQFBTVWvFfF5R8WURTb11Pw0HLtbQ  
ci\_session=ea0dcb145168d95c7e6fcfc67b393093303227d;  
Hs\_lvt\_2d0601bd28de7d480818248cf13d5843=1567812865,1568012538,15680102511,  
1568115035; Hs\_lvt\_52ad01d1be56ce3f1f0504toU2b1j1K  
Connection: close  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 15  
  
key=ichunqiu105

Response

Raw Headers Hex

HTTP/1.1 200 OK  
Date: Tue, 10 Sep 2018 11:53:02 GMT  
Content-Type: text/plain  
Content-Length: 1538  
Connection: close  
Vary: Accept-Encoding  
Last-Modified: Thu, 20 Oct 2016 08:14:07 GMT  
ETag: "602-53f4782cd91cd-qzip"  
Accept-Ranges: bytes  
Vary: Accept-Encoding  
X-Via: JSL; Ifc@010,-  
X-Cache: bypass

function authcode(\$string, \$operation = 'DECODE', \$key = '', \$expiry = 0) {  
 \$key\_length = 4;  
  
 if(\$key == md5(\$key ? \$key : UC\_KEY));  
 \$keya = md5(substr(\$key, 0, 16));  
 \$keyb = md5(substr(\$key, 16, 16));  
 \$keyc = \$keyb\_length ? (\$operation == 'DECODE' ?  
substr(\$string, 0, \$key\_length) : substr(md5(microtime()),  
-(\$key\_length)));  
  
 \$cryptkey = \$keya . md5(\$keya . \$keyc);  
 \$key\_length = strlen(\$cryptkey);  
  
 if(\$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 (\$i = \$i = 0; \$i < 256; \$i++) {  
 \$j = (\$i + \$box[\$i] + \$rndKey[\$i]) % 256;  
 \$tmp = \$box[\$i];  
 \$box[\$i] = \$box[\$j];  
 \$box[\$j] = \$tmp;  
 }  
  
 \$i = \$j = 0;  
 \$t = \$string\_length;  
 \$output = \$box[\$i];  
 \$i++;  
 \$j++;  
 while (\$t > 0) {  
 \$output .= \$box[\$i ^ \$j];  
 \$i++;  
 \$j++;  
 \$t--;  
 }  
 return \$output;  
}

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

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+T9RRipbwbHDlcRWtqXjemcJit26oE1Vu6lpdQPZ6St/obCAEc',
$operation = 'DECODE', $key = 'ichunqiu105');
?>

```

(string后面接密文)

本地运行得到flag



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