暑期练习web16：fuzzing（i春秋）百度杯十月 md5解密脚本

原创

何家公子 于 2018-08-21 17:14:28 发布 803 收藏

分类专栏： ctf web 文章标签： web ctf

本文链接：https://blog.csdn.net/qq_41618162/article/details/81911116

版权

ctf 同时被 2 个专栏收录

32 篇文章 0 订阅

订阅专栏

web

32 篇文章 0 订阅

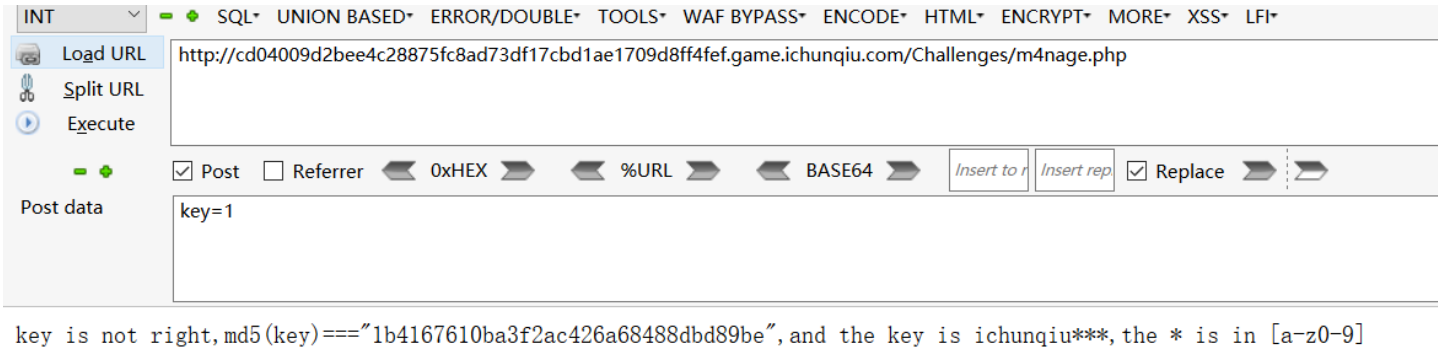
订阅专栏

这题嘛。虽然名字叫fuzzing，但和fuzz似乎没什么关系。。

题目首页面就是一句话：show me your key

源码也没什么东西，索性我就直接get和post传值一下试试

结果post随便传个值及就出来了



```
http://cd04009d2bee4c28875fc8ad73df17cbd1ae1709d8ff4fef.game.ichunqiu.com/Challenges/m4nage.php
```

☑ Post □ Referrer ☑ Replace

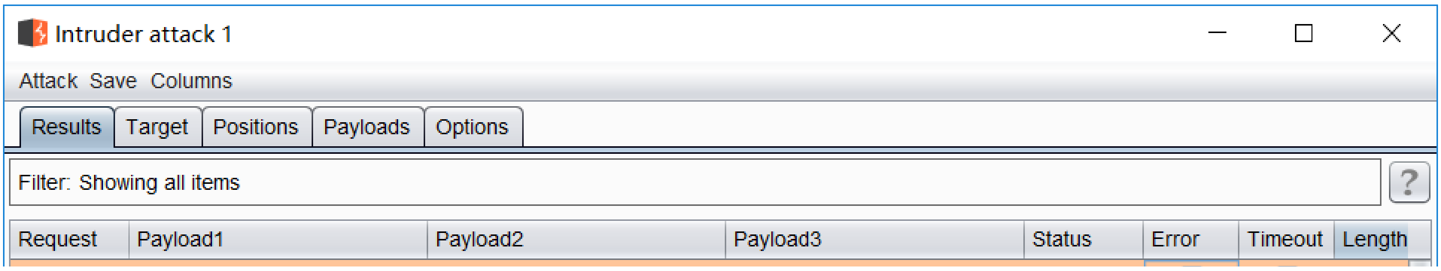
```
key=1
```

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

这里说md5加密后的key是那一段字符串，直接丢到一些md5解密网上，解不开，这下我就纳闷了，查了资料才知道：md5理论上是不能破解的，因为md5采用的是不可逆算法。

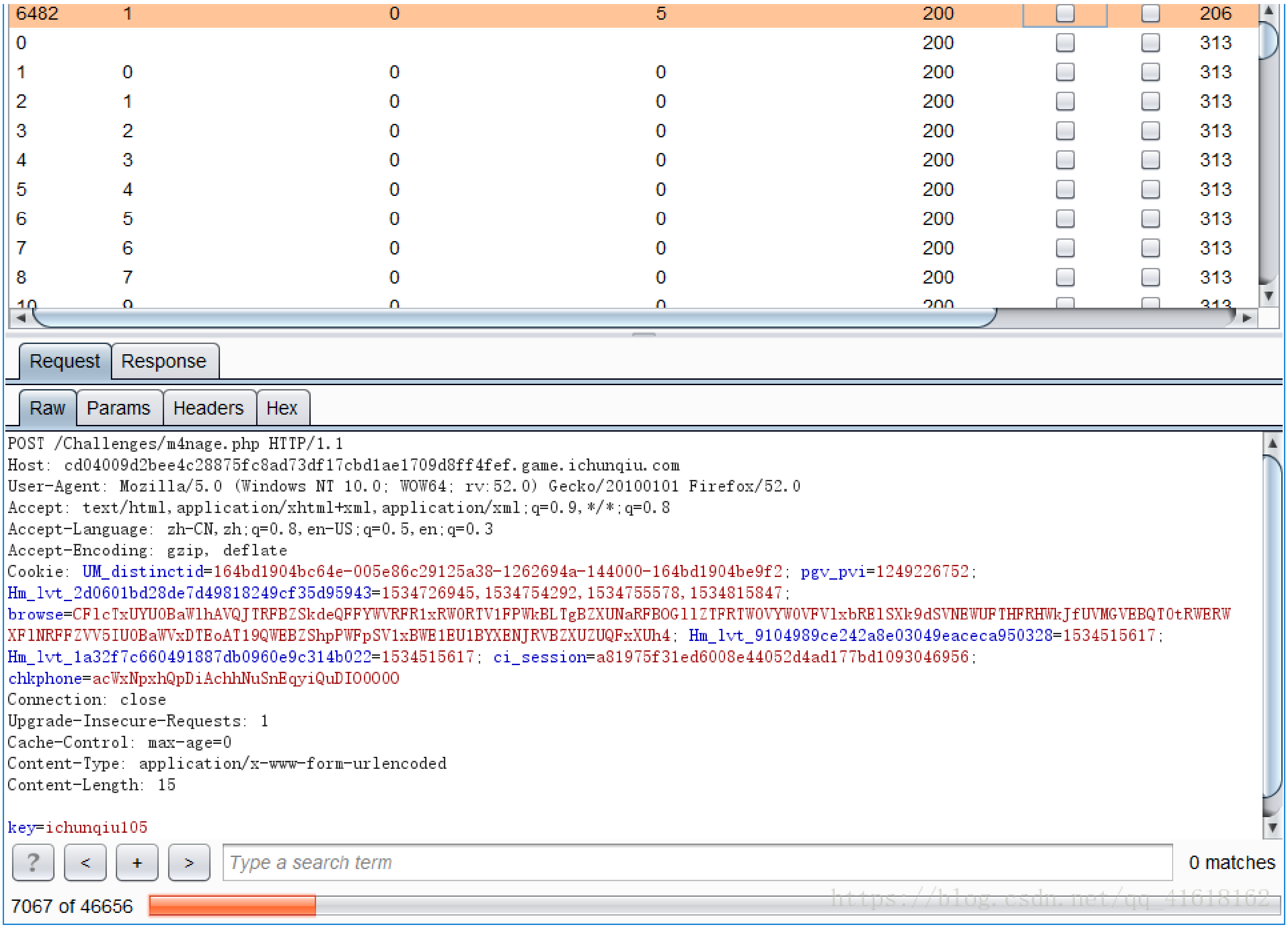
有的网站上提供MD5解密，是因为有大量的存储空间来保存源码和加密后的密码，当解密时就是一个查询的过程，稍微复杂点的查询就无法完成。

我也不会写解密的脚本，就直接拿bp爆破了（反正也就三位数。。。。）



Filter: Showing all items

Request	Payload1	Payload2	Payload3	Status	Error	Timeout	Length



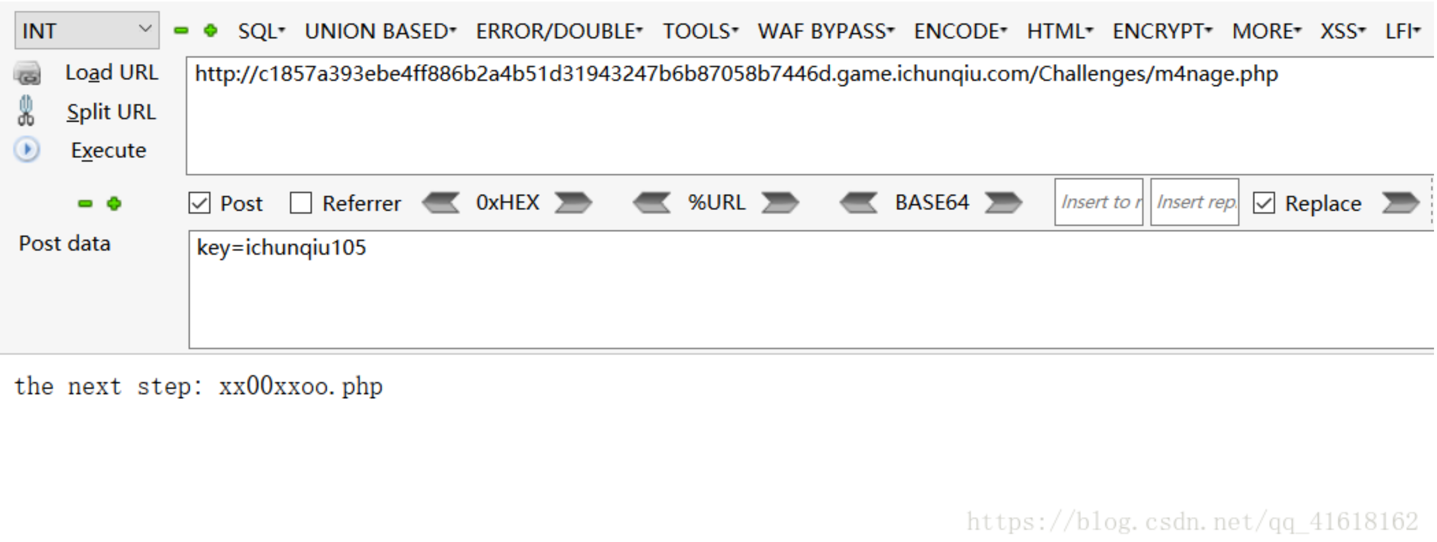
6482	1	0	5	200	☐	☐	206
0				200	☐	☐	313
1	0	0	0	200	☐	☐	313
2	1	0	0	200	☐	☐	313
3	2	0	0	200	☐	☐	313
4	3	0	0	200	☐	☐	313
5	4	0	0	200	☐	☐	313
6	5	0	0	200	☐	☐	313
7	6	0	0	200	☐	☐	313
8	7	0	0	200	☐	☐	313
10	9	0	0	200	☐	☐	313

```
POST /Challenges/m4nage.php HTTP/1.1
Host: cd04009d2bee4c28875fc8ad73df17cbd1ae1709d8ff4fef.game.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: UM_distinctid=164bd1904bc64e-005e86c29125a38-1262694a-144000-164bd1904be9f2; pgv_pvi=1249226752;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1534726945,1534754292,1534755578,1534815847;
browse=CFlcTxUYU0BaWlhAVQJTRFBZSkdeQFFYWVRFR1xRW0RTV1FPWkBLTgBZXUNaRFBOGllZTFRTW0VYW0VFV1xbRElSXk9dSVNEWUFTHFRHWkJfUVMGVEBQT0tRWERW
XFlNRFFZVV5IU0BaWVxDTEoAT19QWEBZShpPWFpSV1xBWE1EU1BYXENJRVBZXUZUQFxXUh4; Hm_lvt_9104989ce242a8e03049eaceca950328=1534515617;
Hm_lvt_1a32f7c660491887db0960e9c314b022=1534515617; ci_session=a81975f31ed6008e44052d4ad177bd1093046956;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 15

key=ichunqiu105
```

后面查了其他大佬的wp，这里贴一份python脚本把

```
#!/bin/bash
import hashlib
def md5(data):
    m = hashlib.md5()
    m.update(data)
    a = m.hexdigest()
    return a

a = 'ichunqiu'
b = 'abcdefghijklmnopqrstuvwxyz1234567890'
for i in b:
    for j in b:
        for k in b:
            if md5(a+i+j+k)=='1b4167610ba3f2ac426a68488dbd89be':
                print a+i+j+k
```

输入正确的key后，提示我们进入下一个文件

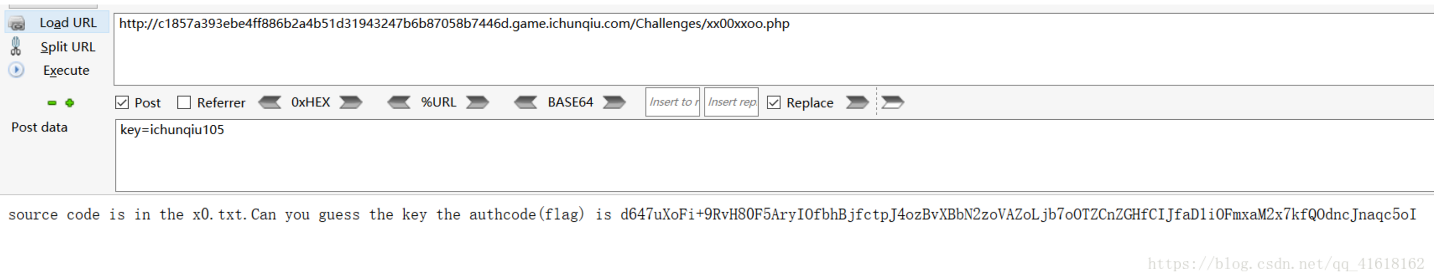


http://c1857a393ebe4ff886b2a4b51d31943247b6b87058b7446d.game.ichunqiu.com/Challenges/m4nage.php

key=ichunqiu105

```
the next step: xx00xxoo.php
```

打开后，给了我们一串密文，和一段代码



http://c1857a393ebe4ff886b2a4b51d31943247b6b87058b7446d.game.ichunqiu.com/Challenges/xx00xxoo.php

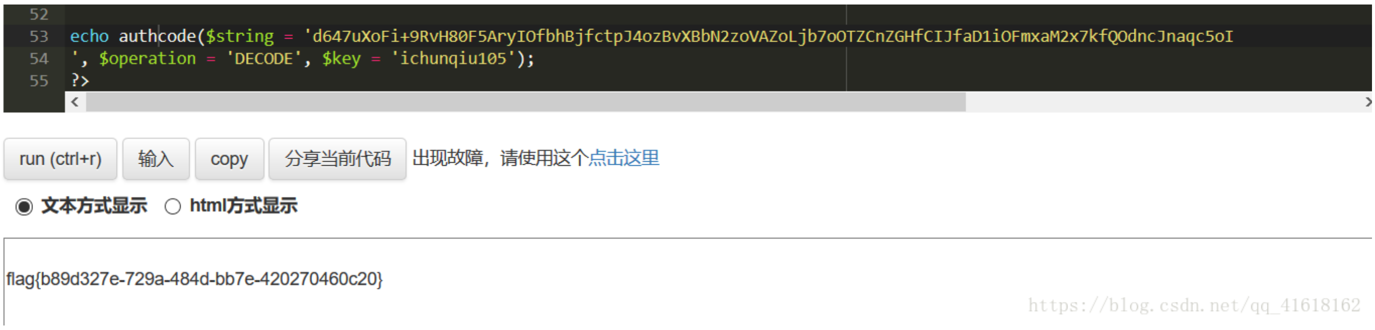
key=ichunqiu105

```
source code is in the x0.txt.Can you guess the key the authcode(flag) is d647uXoFi+9RvH80F5AryIOfbhBjfctpJ4ozBvXBbN2zoVAZoLjb7oOTZCnZGHfCIJfaD1iOFmxaM2x7kfQOdncJnaqc5oI
```

密文是：
d647uXoFi+9RvH80F5AryIOfbhBjfctpJ4ozBvXBbN2zoVAZoLjb7oOTZCnZGHfCIJfaD1iOFmxaM2x7kfQOdncJnaqc5oI（每个人的不太一样）
打开x0.txt,得到代码：

```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(micr

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

    $string = $operation == 'DECODE' ? base64_decode(substr($string, $ckey_length)) : sprintf('%010d',
    $string_length = strlen($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,
            return substr($result, 26);
        } else {
            return '';
        }
    } else {
        return $keyc . str_replace('=', '', base64_encode($result));
    }

}
```

许多同学这时候估计会较劲脑汁的代码审计，但实际上重头到尾仔细看一看，这是段代码里没有涉及到flag，再加上之前给了段密文，所以这一段代码不是加密就是解密过程。
我们把这段copy下来，开头加上`<?php`，末尾加`?>`,中间加一个输出函数，得到flag



```

echo authcode($string = 'd647uXoFi+9RvH80F5AryIOfbhBjfctpJ4ozBvXBbN2zoVAZoLjb7oOTZCnZGHfCIJfaD1iOFmxaM2x7kfQOdncJnaqc5oI
', $operation = 'DECODE', $key = 'ichunqiu105');
?>
```

```
flag{b89d327e-729a-484d-bb7e-420270460c20}
```

总结：这题比较绕，最后的代码也容易混淆判断，不过总的做下来还是比较流畅的