SarCTF

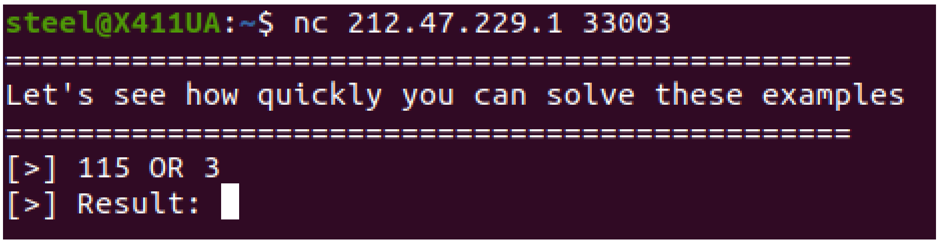
Crypto : Invitation

Description :   100% of brain CPU

nc 212.47.229.1 33003

Solution :

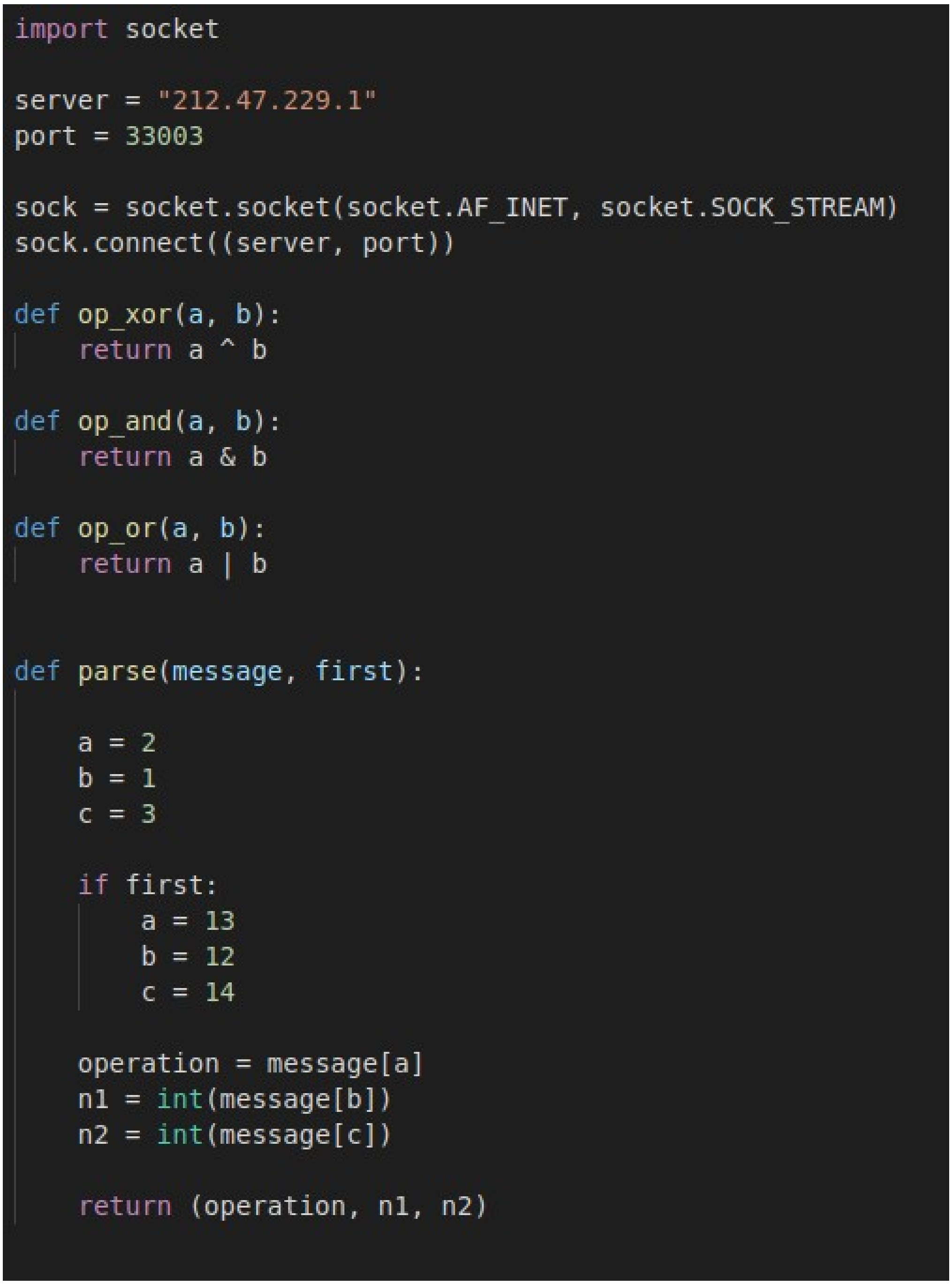
In this challenge, we had some binary operations to script to program.



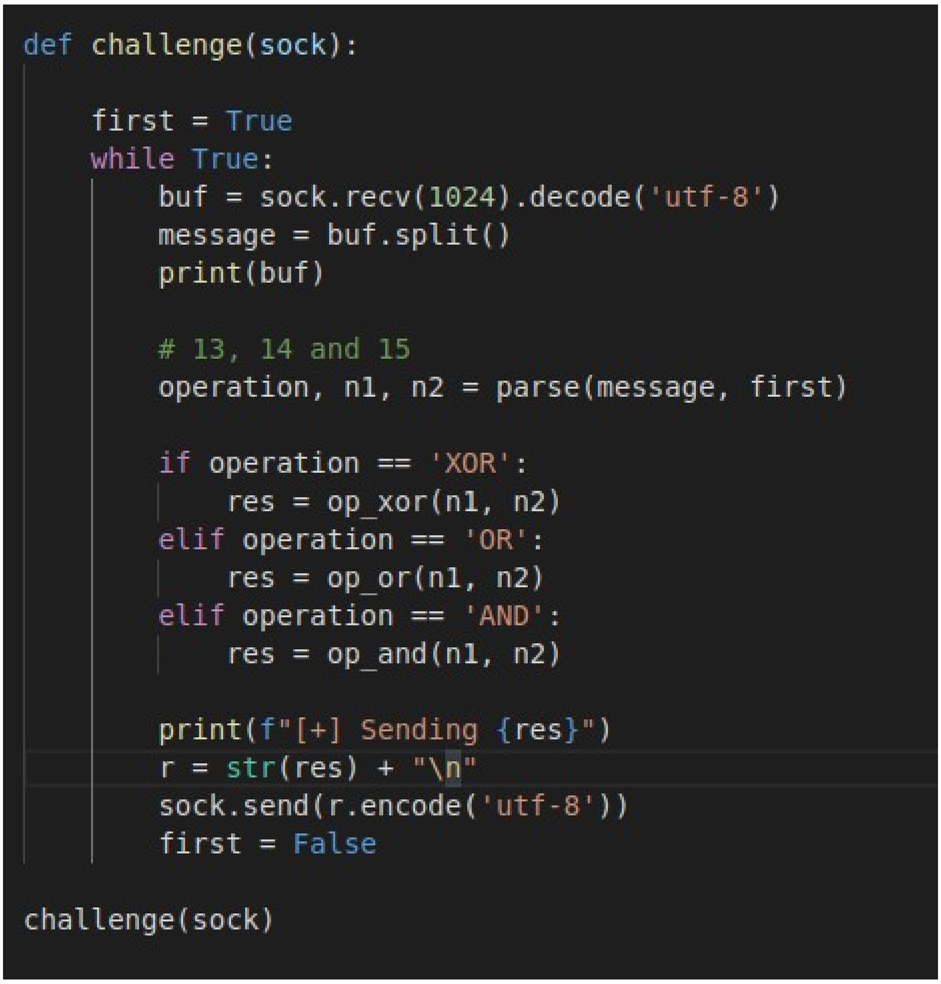
```
steel@X411UA:~$ nc 212.47.229.1 33003
===============================================
Let's see how quickly you can solve these examples
===============================================
[>] 115 OR 3
[>] Result: █
```

There are three operations that the server can ask for: AND, OR and XOR. Let’s program this script.

This programs loops to receive the questions from the server. It parses the numbers and the operator, then calculate the answer and send it to the server.

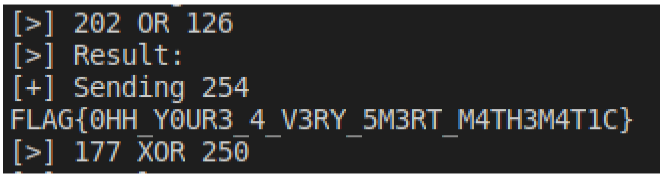


```python
import socket

server = "212.47.229.1"
port = 33003

sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect((server, port))

def op_xor(a, b):
    return a ^ b

def op_and(a, b):
    return a & b

def op_or(a, b):
    return a | b


def parse(message, first):

    a = 2
    b = 1
    c = 3

    if first:
        a = 13
        b = 12
        c = 14

    operation = message[a]
    n1 = int(message[b])
    n2 = int(message[c])

    return (operation, n1, n2)
```



```python
def challenge(sock):

    first = True
    while True:
        buf = sock.recv(1024).decode('utf-8')
        message = buf.split()
        print(buf)

        # 13, 14 and 15
        operation, n1, n2 = parse(message, first)

        if operation == 'XOR':
            res = op_xor(n1, n2)
        elif operation == 'OR':
            res = op_or(n1, n2)
        elif operation == 'AND':
            res = op_and(n1, n2)

        print(f"[+] Sending {res}")
        r = str(res) + "\n"
        sock.send(r.encode('utf-8'))
        first = False

challenge(sock)
```

In the end, we get the flag.



```
[>] 202 OR 126
[>] Result:
[+] Sending 254
FLAG{0HH_Y0UR3_4_V3RY_5M3RT_M4TH3M4T1C}
[>] 177 XOR 250
```

FLAG{0HH_Y0UR3_4_V3RY_5M3RT_M4TH3M4T1C}