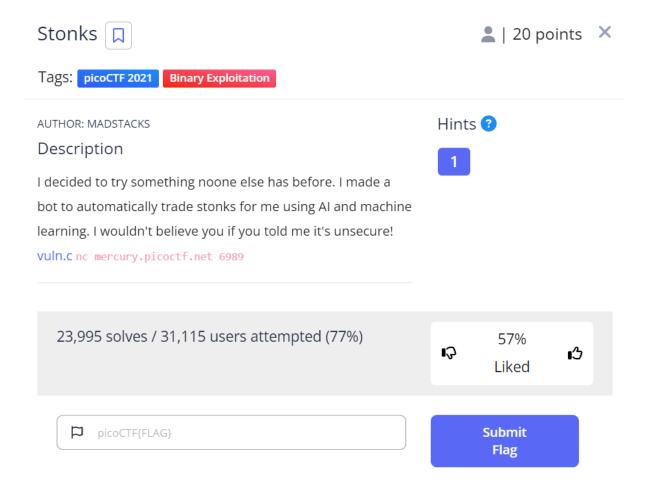
stonks (attempted but not accepting flag)



I ran the nc command in linux terminal:

```
tanay@ubuntu:~$ nc mercury.picoctf.net 6989
Welcome back to the trading app!
What would you like to do?
1) Buy some stonks!
2) View my portfolio
```

Since the vulnerability is in the API key,I picked option 1 (as per the code provided, API can only be accessed through this method)

```
tanay@ubuntu:~$ nc mercury.picoctf.net 6989
Welcome back to the trading app!
What would you like to do?
1) Buy some stonks!
2) View my portfolio
1
Using patented AI algorithms to buy stonks
Stonks chosen
What is your API token?
```

It is asking us for an API token.

In programs, local variables and other data are stored in stacks, buffers and other data structures, and passing a large input can cause them to overflow. We will exploit this by passing a large number format specifiers into the input, as this will cause the code to read out of bounds data, which might contain the flag.

I tried doing this using %c but there were too many non-printable characters, making reading the flag difficult. So I passed %X instead. This returned appropriate hex values. Also since the length is specified as less than 300, we have an estimate of how many to pass

I passed 120 such %X, following was the output:

Converting this hex to ascii text, we can clearly see a hidden flag:

```
Page 300 And 400 And 500 And 5
```

I converted this scrambled flag to a proper one manually:

```
ocip{FTC0l_I4_t5m_ll0m_y_y3n58a025e3��}
```

Here is an ss from notepad:

```
{01_I4_t5m_l10m_y_y3n58a025e3}

01_I
4_t5
m_l1
0m_y
_y3n
58a0
25e3
picoCTF{I_lo5t_4l1_my_m0n3y_0a853e52}
```

However this flag was not being accepted, even after I tried other combinations with the various pieces of characters. It is correct to my understanding.

[Sources: GeeksForGeeks, CodeWithHarry]