



Penetration Testing Report

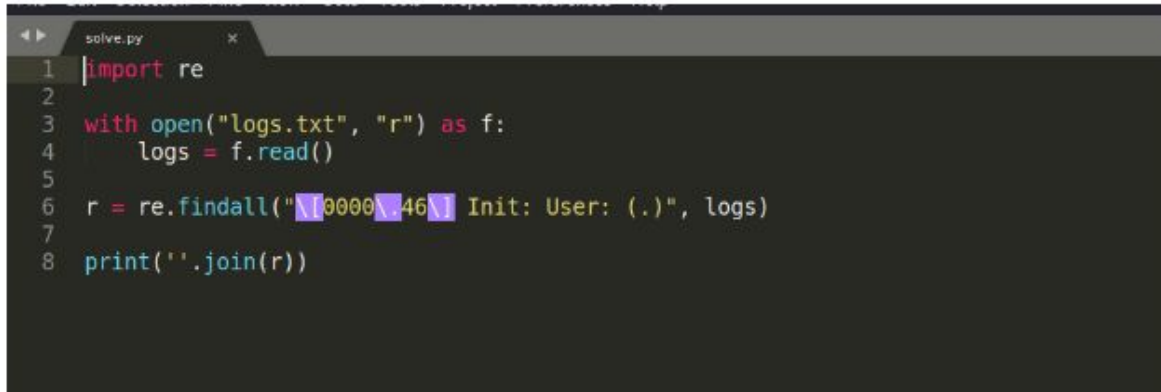
For

“Tiny Whiny Log Files”

S.NO.	Title	#
1.	Challenge Category	Network Security
2.	Challenge Related Files	N/A
3.	File Link / Target IP	N/A

PROCEDURE

1. Simple Log file is given
2. Go Through once and try to notice the pattern of flag
3. Use this given script to extract the flag.

A screenshot of a code editor window titled 'solve.py'. The editor contains a Python script with 8 lines of code. The code imports the 're' module, opens 'logs.txt' in read mode, reads its contents, and uses a regular expression to find all occurrences of a flag pattern. The flag pattern is '\x0000\x46' followed by 'Init: User: (.)'. The results are printed as a single string joined by dots.

```
1 import re
2
3 with open("logs.txt", "r") as f:
4     logs = f.read()
5
6 r = re.findall("\x0000\x46 Init: User: (.)", logs)
7
8 print(''.join(r))
```

Flags:

S.No.	Flag - No.	Flag
1.	Flag 1	HE{Im_way_to_lazy_to_solve}