Friends

发表于 2021-01-09 分类于 Challenge， 2020， CSICTF， Misc
Challenge | 2020 | CSICTF | Misc | Friends

点击此处获得更好的阅读体验

WriteUp来源

https://dunsp4rce.github.io/csictf-2020/miscellaneous/2020/07/22/Friends.html

by `shreyas-sriram`

题目描述

> *I made a really complicated math function. Check it out.*

题目考点

解题思路

- *Go through the given source code to realize that the input entered goes through a set of manipulations*
- *And to get the flag, the result of manipulations should not be equal to the input number*
- *It can also be seen that the input should be between 3 and 100*
- *Running the code locally with different inputs tells us that there is no way to meet the necessary conditions to get the flag by entering a number*
- *One interesting thing to note is that the input lands inside* `float()`

```
x = round(float(input()), 0)
```

- *Reading up on float(), we realize that it takes* `nan` *as input*
- *Using* `nan` *as input, we meet the necessary conditions and* `namo.txt` *is obtained*
- `namo.txt` *is basically a* `conditional statement-expanded-code-snippet` *of the flag written in namo*
- *Flag can be obtained by parsing the file*

Response File

```
Mitrooon
bhaiyo aur behno "Enter a number"
mann ki baat nambar

agar nambar barabar 1 hai {
  bhaiyo aur behno "s"
}

nahi toh agar nambar barabar 13 hai {
  bhaiyo aur behno "_"
}


nahi toh agar nambar barabar 15 hai {
  bhaiyo aur behno "5"
}


nahi toh agar nambar barabar 22 hai {
  bhaiyo aur behno "4"
}

```

```
23
24 nahi toh agar nambar barabar 28 hai {
25   bhaiyo aur behno "k"
26 }
27
28
29 nahi toh agar nambar barabar 8 hai {
30   bhaiyo aur behno "y"
31 }
32
33
34 nahi toh agar nambar barabar 17 hai {
35   bhaiyo aur behno "4"
36 }
37
38
39 nahi toh agar nambar barabar 9 hai {
40   bhaiyo aur behno "_"
41 }
42
43
44 nahi toh agar nambar barabar 4 hai {
45   bhaiyo aur behno "t"
46 }
47
48
49 nahi toh agar nambar barabar 3 hai {
50   bhaiyo aur behno "c"
51 }
52
53
54 nahi toh agar nambar barabar 20 hai {
55   bhaiyo aur behno "r"
56 }
57
58
59 nahi toh agar nambar barabar 12 hai {
60   bhaiyo aur behno "n"
61 }
62
63
64 nahi toh agar nambar barabar 0 hai {
65   bhaiyo aur behno "c"
66 }
67
68
69 nahi toh agar nambar barabar 23 hai {
70   bhaiyo aur behno "t"
71 }
72
73
74 nahi toh agar nambar barabar 27 hai {
75   bhaiyo aur behno "0"
76 }
77
78
79 nahi toh agar nambar barabar 10 hai {
80   bhaiyo aur behno "n"
81 }
82
83
84 nahi toh agar nambar barabar 11 hai {
85   bhaiyo aur behno "4"
86 }
87
88
89 nahi toh agar nambar barabar 7 hai {
90   bhaiyo aur behno "m"
91 }
92
93
94 nahi toh agar nambar barabar 25 hai {
95   bhaiyo aur behno "c"
96 }
97
98
```

```
99  nahi toh agar nambar barabar 24 hai {
100   bhaiyo aur behno "_"
101 }
102
103
104 nahi toh agar nambar barabar 6 hai {
105   bhaiyo aur behno "{"
106 }
107
108
109 nahi toh agar nambar barabar 16 hai {
110   bhaiyo aur behno "_"
111 }
112
113
114 nahi toh agar nambar barabar 18 hai {
115   bhaiyo aur behno "_"
116 }
117
118
119 nahi toh agar nambar barabar 2 hai {
120   bhaiyo aur behno "i"
121 }
122
123
124 nahi toh agar nambar barabar 5 hai {
125   bhaiyo aur behno "f"
126 }
127
128
129 nahi toh agar nambar barabar 19 hai {
130   bhaiyo aur behno "g"
131 }
132
133
134 nahi toh agar nambar barabar 14 hai {
135   bhaiyo aur behno "1"
136 }
137
138
139 nahi toh agar nambar barabar 21 hai {
140   bhaiyo aur behno "3"
141 }
142
143
144 nahi toh agar nambar barabar 26 hai {
145   bhaiyo aur behno "0"
146 }
147
148
149 nahi toh agar nambar barabar 29 hai {
150   bhaiyo aur behno "}"
151 }
152
153 nahi toh {
154   bhaiyo aur behno ""
155 }
156
157 achhe din aa gaye
```

Solution File

```
#!/bin/bash

touch namo.txt
touch temp.txt

echo "nan" > payload.txt

# get nc response
cat payload.txt | nc chall.csivit.com 30425 > namo.txt

# get indexes
index=($(grep -o " [0-9]\{1,2\} " namo.txt))

# get bits of flag
bits=($(grep -o "\".\"" namo.txt))

# match the indexes with the flag and store in file
for(( j=0 ; j<${#index[@]} ; j++ ))
do
  printf -v s "%02d" ${index[$j]} # format index
  echo "$s:${bits[$j]}" >> temp.txt
done

# sort file and get flag
flag=($(sort temp.txt | cut -d '"' -f 2))

# remove files
rm namo.txt
rm temp.txt
rm payload.txt

printf %s "${flag[@]}" $'\n'
```

Flag

```
csictf{my_n4n_15_4_gr34t_c00k}
```


 # Challenge # 2020 # Misc # CSICTF
No-DIStractions
Escape Plan