

LinkedIn: [Kelvin Kimotho](#)

Medium

Reverse Engineering

picoCTF 2022

Java

AUTHOR: LT 'SYREAL' JONES

Description

Can you get the flag?

Reverse engineer this [Java program](#).

Hints ?

1

Use a decompiler for Java!

Solution

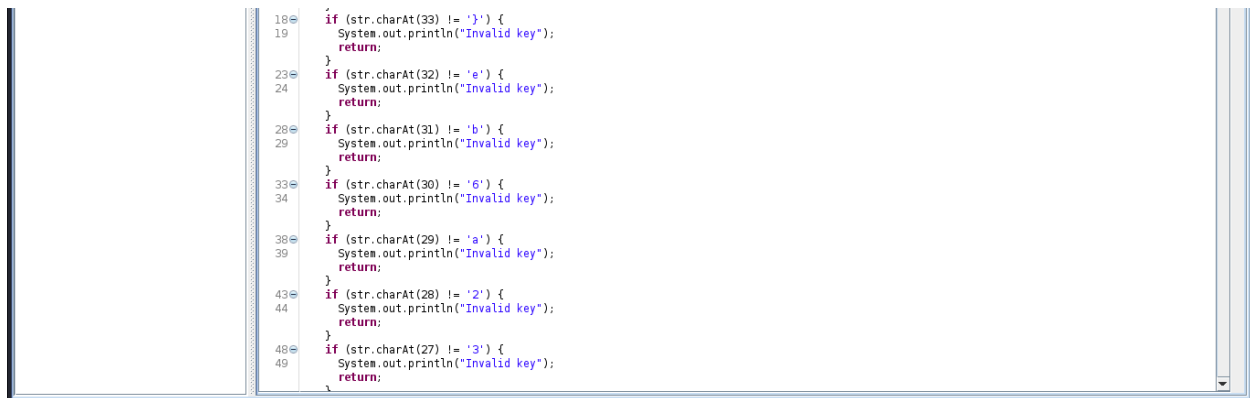
The hint suggested using a java decompiler since the file provided was a compiled java program. I went ahead and installed **jd-gui** decompiler on my kali.

```
(kali@kali)-[~/Downloads]
└─$ sudo apt install jd-gui
Installing:
jd-gui

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 2045
  Download size: 1,287 kB
  Space needed: 1,500 kB / 1,278 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 jd-gui all 1.6.6-0kali1 [1,287 kB]
Fetched 1,287 kB in 3s (370 kB/s)
Selecting previously unselected package jd-gui.
(Reading database ... 416728 files and directories currently installed.)
Preparing to unpack .../jd-gui_1.6.6-0kali1_all.deb ...
Unpacking jd-gui (1.6.6-0kali1) ...
Setting up jd-gui (1.6.6-0kali1) ...
Processing triggers for kali-menu (2024.3.1) ...
```

I then opened the compiler via the terminal and uploaded the java class i intended to decompile.



Each character in the key entered by the user is compared to another character which should match. I compiled all the characters and came up with a 34-character key which was indeed the flag **picoCTF{70011ng_r3qu1r3d_9332a6be}**.