PIN

PIN

Can you crack my pin?

https://mega.nz/#!PXYjCKCY!F2gcs83XD6RxjOR-FNWGQZpyvUFvDbuT-PTnqRhBPGQ

Flag: CTFlearn{333333}

You can convert numbers (binary, octal, decimal and hexadecimal use a number converter

Writeup:

fired up ghidra

found login code in main.local_c function

noticed call ‘cek’ to authorize PIN, so I went to cek function

found pin ‘00051615h’ and converted to get decimal PIN ‘333333h’

removed ‘h’ and tested PIN on script and was successful

333333

files

rev1 file data:

----------------------------file-Supplied------------------------------

```
ELF 64-bit LSB executable
x86-64, version 1 (SYSV)
dynamically linked
interpreter /lib64/ld-linux-x86-64.so.2
for GNU/Linux 2.6.32
BuildID[sha1]=c5f9af621b132c2028d8e689cbb5b707f3f3cd28
not stripped
```

-------------------------Ghidra-Supplied----------------------------

```
Project File Name:      rev1
Last Modified:      Sat Jul 11 08:08:36 EDT 2020
Readonly:      false
Program Name:     rev1
Language ID:  x86:LE:64:default (2.8)
Compiler ID:   gcc
Processor:      x86
Endian:    Little
Address Size:        64
Minimum Address:       00400000
Maximum Address:       _elfSectionHeaders::0000077f
# of Bytes:     7052
# of Memory Blocks:     32
# of Instructions:  9
# of Defined Data:       102
# of Functions:      19
# of Symbols:       54
# of Data Types:    28
# of Data Type Categories:  2
Created With Ghidra Version:      9.1
Date Created:        Sat Jul 11 08:08:34 EDT 2020
```

```
ELF File Type:       executable
ELF Original Image Base:     0x400000
ELF Prelinked:       false
ELF Required Library [   0]:  libc.so.6
ELF Source File [   0]:   crtstuff.c
ELF Source File [   1]:   reverse1.c
ELF Source File [   2]:   crtstuff.c
Executable Format:      Executable and Linking Format (ELF)
Executable Location:    /home/taj702/Downloads/rev1
Executable MD5:   f1f17065b3243f5dc8d8fb5eca769762
Executable SHA256:     2e7241017ab1e831592f6116c641a2867fb7f687ddf991dc718750da3f66b169
FSRL:      file:///home/taj702/Downloads/rev1?MD5=f1f17065b3243f5dc8d8fb5eca769762
Relocatable:   false
```