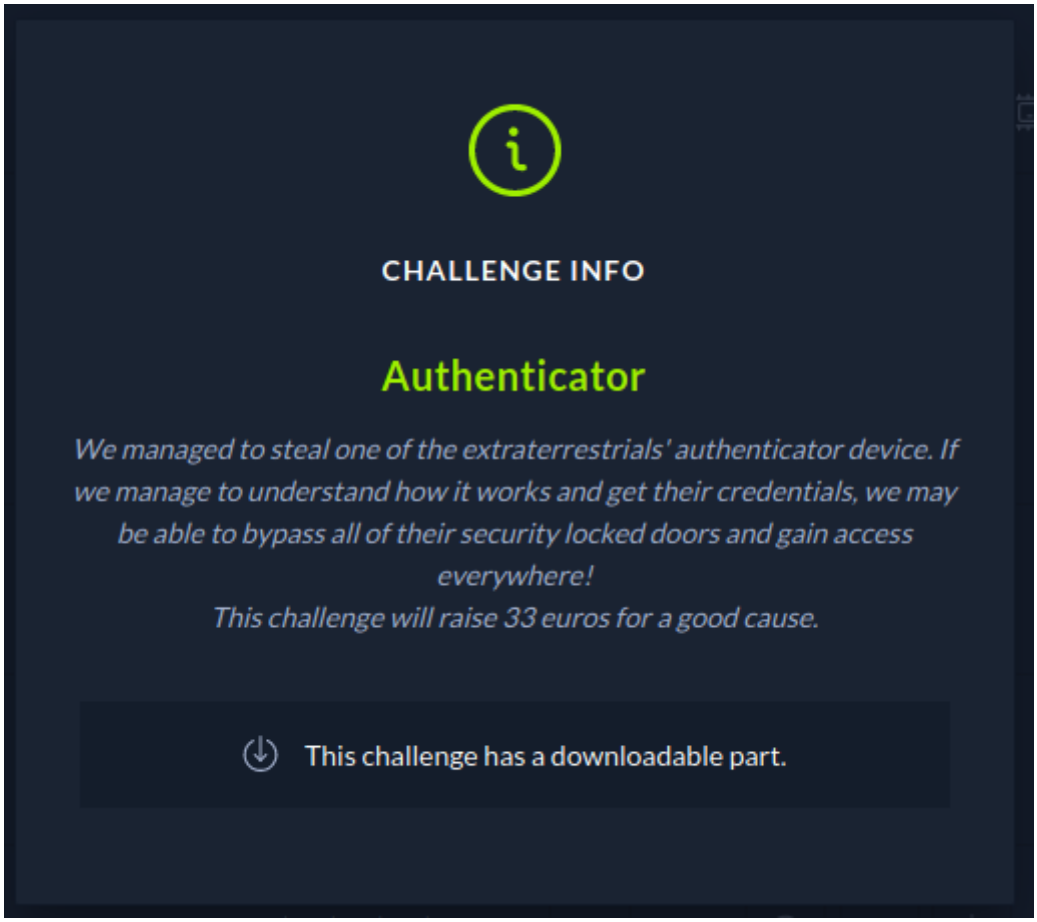
Authenticator



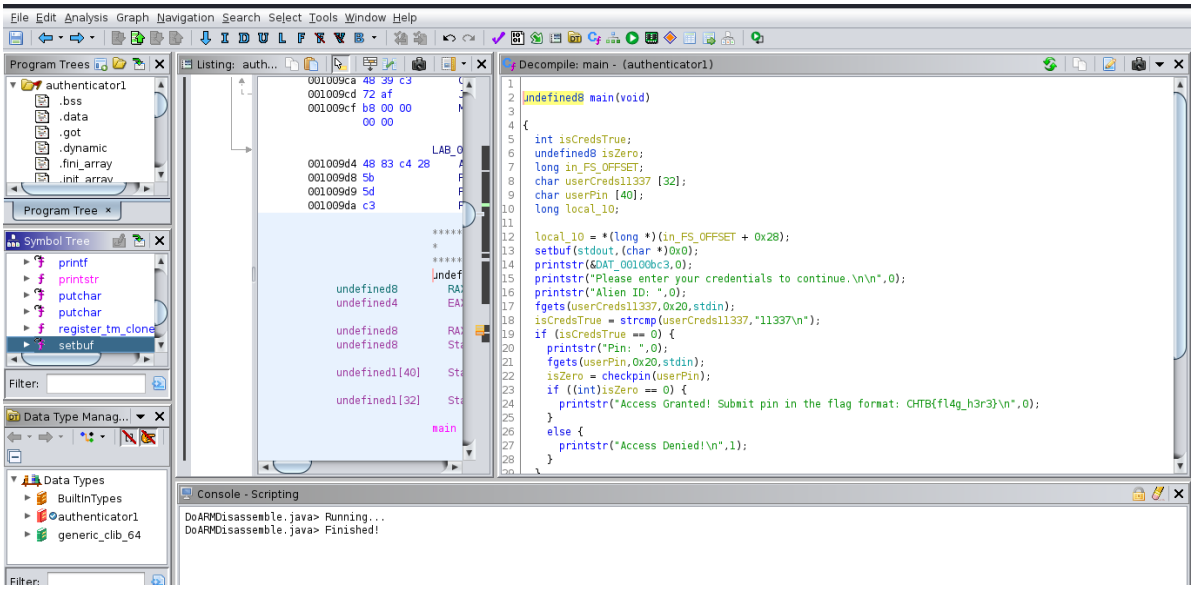
Solution

Download the binary and run it

```
┌──(kali㉿kali)-[~/Desktop/cyberApocalypse/rev]
└─$ ./authenticator

Authentication System 👽

Please enter your credentials to continue.

Alien ID:
```

First step is to crack alien IID

Fire up **authenticator** in **Ghidra**




```
undefined8 main(void)

{
  int isCredsTrue;
  undefined8 isZero;
  long in_FS_OFFSET;
  char userCreds11337 [32];
  char userPin [40];
  long local_10;

  local_10 = *(long *)(in_FS_OFFSET + 0x28);
  setbuf(stdout,(char *)0x0);
  printstr(&DAT_00100bc3,0);
  printstr("Please enter your credentials to continue.\n\n",0);
  printstr("Alien ID: ",0);
  fgets(userCreds11337,0x20,stdin);
  isCredsTrue = strcmp(userCreds11337,"11337\n");
  if (isCredsTrue == 0) {
    printstr("Pin: ",0);
    fgets(userPin,0x20,stdin);
    isZero = checkpin(userPin);
    if ((int)isZero == 0) {
      printstr("Access Granted! Submit pin in the flag format:
CHTB{fl4g_h3r3}\n",0);
    }
    else {
      printstr("Access Denied!\n",1);
    }
  }
  else {
    printstr("Access Denied!\n",1);
  }
  if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
  }
  return 0;
```

```
}
```

when user input key to credentials to this binary.

inputed string compare with

`isCredsTrue = strcmp(userCreds11337,"11337\n");`

> inputed string is compared using strcmp with 11337

```
└─$ ./authenticator


Authentication System 👽

Please enter your credentials to continue.

Alien ID: 11337
Pin:
```

First authentication bypassed using **11337**

Step 2 - For Pin

Pin was compared and validated using another function called **checkpin()**

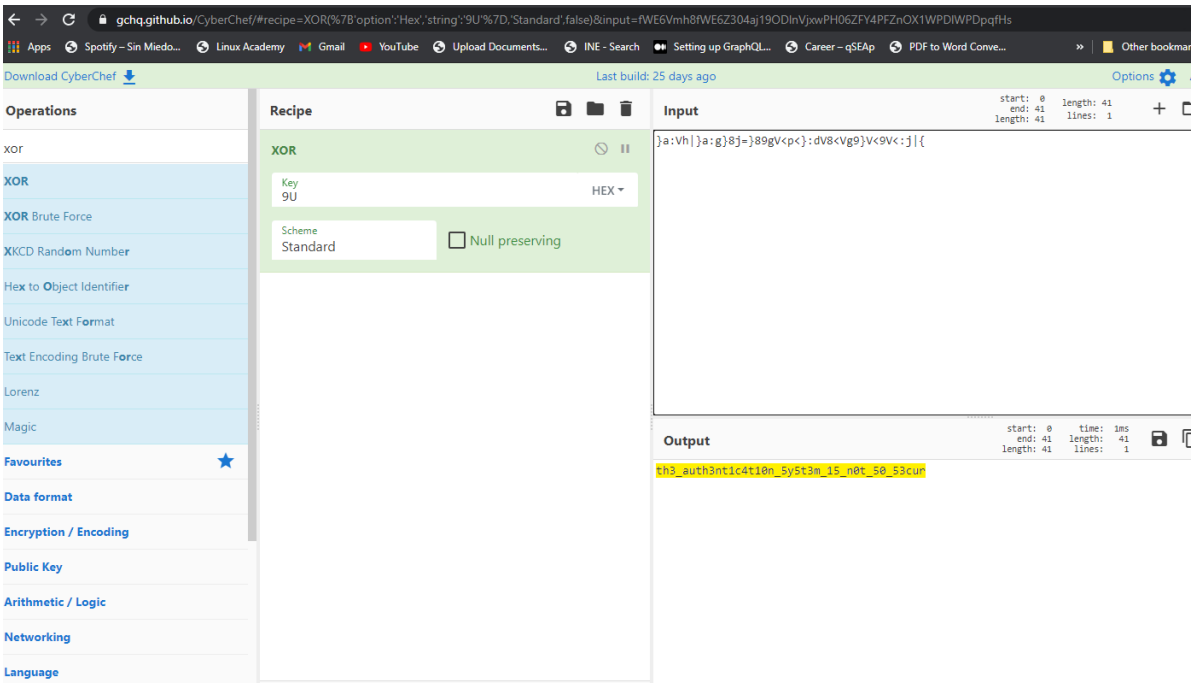
Lets decompile

```
undefined8 checkpin(char *userPin)

{
  size_t userPinLength;
  int index;

  index = 0;
  while( true ) {
    userPinLength = strlen(userPin);
    if (userPinLength - 1 <= (ulong)(long)index) {
      return 0;
    }
    if ((byte)("}a:Vh|}a:g}8j=}89gV<p<}:dV8<Vg9}V<9V<:j|{:"[index] ^ 9U) !=
userPin[index]) break;
    index = index + 1;
  }
  return 1;
}
```

User-input is looped and validating pin is correct.

- First if statement checks userinput length is < 0 then the loop return 0
- Second If statement is a XOR encryption checker with a random value with key 9U

> its not a random value its the encrypted pin
>
> lets decode with cyberchef



pin : **th3_auth3nt1c4t10n_5y5t3m_15_n0t_50_53cur3**

```
└─$ ./authenticator


Authentication System 👽

Please enter your credentials to continue.

Alien ID: 11337
Pin: th3_auth3nt1c4t10n_5y5t3m_15_n0t_50_53cur3
Access Granted! Submit pin in the flag format: CHTB{fl4g_h3r3}
```