CSAW - LLM

Suriya Prakash Jambunathan - sj3828

rev/rebug 1

Observation:

The challenge provides us with a binary that accepts a string input from the user, and if the string matches a specific condition, prints the flag.

Approach:

1. Observe the decompiled version of the binary using Ghidra, and get the decompiled version of main.
2. Understand the conditions that the input string needs to satisfy.
3. Generate/design a string that satisfies the conditions.
4. Enter the generated string to the binary prompt, and get the flag.

Solution:

1. Open Ghidra and copy the decompiled main code.

```
undefined8 main(void)

{
  EVP_MD *type;
  char local_448 [44];
  uint local_41c;
  byte local_418 [16];
  char local_408 [1008];
  EVP_MD_CTX *local_18;
  int local_10;
  int local_c;

  printf("Enter the String: ");
  __isoc99_scanf(&DAT_00102017,local_408);
  for (local_c = 0; local_408[local_c] != '\0'; local_c = local_c + 1) {
  }
  if (local_c == 0xc) {
    puts("that\'s correct!");
    local_18 = (EVP_MD_CTX *)EVP_MD_CTX_new();
    type = EVP_md5();
    EVP_DigestInit_ex(local_18,type,(ENGINE *)0x0);
    EVP_DigestUpdate(local_18,&DAT_0010202a,2);
```

```
    local_41c = 0x10;
    EVP_DigestFinal_ex(local_18,local_418,&local_41c);
    EVP_MD_CTX_free(local_18);
    for (local_10 = 0; local_10 < 0x10; local_10 = local_10 + 1) {
      sprintf(local_448 + local_10 * 2,"%02x",(ulong)local_418[local_10]);
    }
    printf("csawctf{%s}\n",local_448);
  }
  else {
    printf("that isn\'t correct, im sorry!");
  }
  return 0;
}
```

2. Prompted ChatGPT to give a python code for steps 2-3 in the Approach.

```
Suggested String : "123456789012"
```

3. Enter the ChatGPT suggested string into the binary prompt, and get the flag.

Flag: *csawctf{c20ad4d76fe97759aa27a0c99bff6710}*
Chat: *CSAW LLM - Rebug 1 (openai.com)*