**Phân tích bài**

Bài này là một bài CTF (Capture The Flag) với mục tiêu:

1. Hiểu và khai thác chương trình được cung cấp.
2. Tìm cách thay đổi giá trị của func\_table hoặc tận dụng lỗ hổng trong chương trình để gọi hàm win().

**Phân tích mã nguồn**

Chương trình có các thành phần chính:

1. **Bảng chức năng (func\_table)**:
   * Lưu danh sách các hàm được phép gọi. Ban đầu, nó bao gồm các hàm:

Sao chépChỉnh sửa

print\_table

read\_variable

write\_variable

getRandomNumber

* + Mỗi mục trong func\_table chiếm đúng **32 ký tự**, và tổng độ dài là 128 ký tự (với 4 mục).

1. **Hàm call\_func(n)**:
   * Cho phép gọi hàm trong func\_table dựa trên chỉ số n.
   * Nếu nội dung của func\_table bị thay đổi, bạn có thể "lừa" chương trình gọi hàm win().
2. **Hàm write\_variable()**:
   * Cho phép ghi giá trị mới cho biến toàn cục (global), bao gồm func\_table.
   * Đây là lỗ hổng chính vì bạn có thể ghi đè giá trị của func\_table.
3. **Hàm win()**:
   * Đọc nội dung file flag.txt và in kết quả theo định dạng mã ASCII hex.

**Chiến lược tấn công**

Mục tiêu là gọi được hàm win() bằng cách:

1. Ghi đè func\_table để thay thế tất cả các mục trong bảng bằng tên hàm win.
2. Sau đó, gọi hàm đầu tiên trong bảng (call\_func(0)).

**Các bước thực hiện**

**Bước 1: Ghi đè func\_table**

* Sử dụng hàm write\_variable để thay đổi nội dung của func\_table. Nhập các lệnh sau vào chương trình:

1. Gọi write\_variable:

plaintext

Sao chépChỉnh sửa

==> 3

Please enter variable name to write: func\_table

1. Ghi đè giá trị của func\_table:

plaintext

Sao chépChỉnh sửa

Please enter new value of variable: '''win win win win '''

* + Chuỗi này thay thế toàn bộ bảng chức năng bằng tên hàm win.
  + Đảm bảo mỗi mục (hàm win) có đúng **32 ký tự** để chương trình hoạt động bình thường.

**Bước 2: Gọi hàm win**

* Sau khi thay đổi func\_table, bạn có thể gọi hàm win bằng cách thực hiện:

plaintext

Sao chépChỉnh sửa

==> 1

* + Điều này sẽ gọi hàm đầu tiên trong bảng (là win) và in flag.

**Phân tích flag**

Khi hàm win() được gọi, chương trình đọc file flag.txt và in ra chuỗi mã ASCII hex. Sau đó, chuyển mã ASCII hex này thành flag:

**Flag:**

Sao chépChỉnh sửa

picoCTF{7h15\_15\_wh47\_w3\_g37\_w17h\_u53r5\_1n\_ch4rg3\_a186f9ac}

**Kết luận**

* **Lỗ hổng:** Hàm write\_variable cho phép người dùng thay đổi giá trị của func\_table, dẫn đến việc gọi được các hàm ngoài ý muốn.
* **Cách khai thác:** Ghi đè toàn bộ bảng chức năng bằng tên hàm win và gọi nó.
* **Flag:** picoCTF{7h15\_15\_wh47\_w3\_g37\_w17h\_u53r5\_1n\_ch4rg3\_a186f9ac}