# Walkthrough: Binary Gauntlet 1

## Step 1: Understanding the Binary

Run the binary and check its behavior:

```shell  
./binary\_gauntlet1  
```

## Step 2: Checking for Protections

Use checksec to see security features:

```shell  
checksec --file=binary\_gauntlet1  
```

## Step 3: Finding the Vulnerability

The program uses `gets()`, which is vulnerable to buffer overflow.

## Step 4: Crafting the Exploit

Use ROP techniques to call `stage1()`, `stage2()`, and finally `win()`.

## Step 5: Retrieving the Flag

Once exploited, `win()` will print `G8KEY{RED\_GATE\_TRAP}`.