# Walkthrough: Binary Gauntlet 3

## Step 1: Finding the Stages

Run the binary to observe inputs:

```shell  
./binary\_gauntlet3  
```

## Step 2: Bypassing Stage 1

The first stage asks for a password. Check the binary:

```shell  
strings binary\_gauntlet3 | grep 'hunter'  
```

## Step 3: Bypassing Stage 2

The second stage requires inputting `1337`.

## Step 4: Exploiting Stage 3

The `gets()` function is vulnerable. We can overwrite the return address to jump to `win()`.

## Step 5: Retrieving the Flag

After exploiting the overflow, `win()` prints the flag `G8KEY{JINW00\_RANK\_E\_HUNTER}`.