BOMB LAB - PHASE 3

JOHN THOMAS
P2CSN17017

Phase 3 starts at address **08048A8B** which calls a printf function to print "**That's number 2. Keep going !** \n"

When we analyse it,we see that there are 3 functions called within, **sub_80491FC, sub_8048B98 and sub_804952C**

Now we analyse each functions seperately,

Now we enter into the function **sub_8048B98** at the address **08048AA1,** we see that there is a call for **sscanf** function at address **08048BB7** which is used to get input "**%d %c %d**"
%d stands for integer and %c stands for character.
So now we know that, we have to give the input 2 digits and a string.

Now coming to address **08048BBF**,there is a compare instruction, eax ,2.It will check whether more than 2 values are given as input.If the entered values are less than or equal to 2 ,it will call the explode function **sub_80494FC** to print that the bomb has exploded.

If the values are greater than 2, then it will perform a jump if greater operation to sub function **8048BC9 .**

Inside this function, the first entered value(first digit entered) is compared with the value 7 which consists of a switch case.
If the value is greater than 7 then it will come out of the loop and call the explode function **sub_80494FC**.
If the value entered is less than 7, it will jump inside the switch case for comparison.
There are a total of 8 switch cases.So the first entered value will from 0 to 7.

Inside the switch case, at each case ,the last input (%d) is compared with the value in that switch case.
So, in switch case 0 , the last input value **[ebp+var_4]** is compared with number stored in that switch case **309h ,**which has hex value **777.** If both the values are not equal then it will call the **sub_80494FC.**

Similarly, every switch statement contains a value stored in it and is it compared with the entered input.If both are same during comparison, then it performs a jump to the location **8048C8F.**

At location **8048C8F,** it checks the second value entered by the user , which is a character value.
It is compared with the value which is stored in the register **bl** which stores a character value .
In switch case 0, the value **71h,** which has **q** as the value.It is compared with entered value.

If both the values are not equal, it will call the function **sub_80494FC**
If both values are equal ,it will go back to function s**ub_804952C** which has a printf statement and prints "**Halfway there!**" .

Thus, the phase 3 of the bomb is defused.

SELF EVALUATION QUESTION

a. What programming structures(loops, conditional statements etc) were you able to identify in the binary? What addresses did you find them in the binary? Justify why you believe they are that programming construct you claim them to be.

There were **switch statements** in **loc_8048BC9**
These switch cases are also used inside the program inorder to do the check.

b. Are there multiple possible answers? If yes, find all possible answers. If no, explain why.

Yes because ,it depends upon the value entered and which switch case
Total there are switch cases, so 8 outputs will be there.
Outputs
switch 0: **0 q 777**
switch 1: **1 b 214**
switch 2: **2 b 755**
switch 3: **3 k 251**
switch 4: **4 o 160**
switch 5: **5 t 458**
switch 6: **6 v 780**
switch 7: **7 b 524**

c. Describe validation performed in phase three in your own words with evidence from the binary to support your reasoning.

Phase 3 gets 3 inputs and checks whether 3 inputs are entered.So it is a validation.
cmp (eax ,2) at address 08048BBF.

Again each inputs are compared
First input is compared with value 7 inside the function 8048BC9.
Then again comparison takes place inside the 8 switch statement,the last entered input is compared inside the switch statement.