BINARY BOMB – PHASE 4

JOHN THOMAS
P2CSN17017

Phase 4 starts at address **08048AB8** ,

At address **08048ABB** there is a function call to **sub_80491FC** which gets the input for this phase. The input entered gets stored into eax register.

At address **08048AC4** there is another call to the function **sub_8048CE0**

Entering inside **sub_8048CE0,** there is a **sscanf** call.It is pointed by offset **unk_8049808.**

Now, there is a comparison taking place at address **08048D01** inside **sub_8048CE0**, the input is compared with 1 ie,**[cmp eax , 1].**
It will check and if failed it does jump if not zero to **loc_8048D09,** which calls the explode bomb function at **sub_80494FC** which prints that “bomb has exploded”.

Else it does a jump greater to short **loc_8048D0E.**In this location,the entered input value gets validated and pushed into eax and the **sub_8048CA0** function is called.

In function **sub_8048CA0**, a recursive function is done as it returns 1 if the value of input is less than or equal to 1.
If value greater than 1, the function **sub_8048CA0** gets called with arguments [ebx-1] and [ebx-2]. Then value is then pushed into eax.
Then at address **08048CCA** addition takes place. ie, **add eax , esi.**

Thus, we find that taking input, the fibonacci series is calculated by **sub_8048CA0.**

Then, again a comparison is taking place at address **08048D1D** with (37h) ie, 55, which is 9^{th} in fibonacci series.

If the calculated value is equal to 55 then comes at address **08048AD6** which calls printf and the output is printed as “So you got that one.Try this one ”

If the calculated value is not equal to 55,then it prints “Sorry Try again”

Thus, the input is 9.

SELF EVALUTION QUESTIONS

a. How many arguments does function at 0x8048CA0 accept? What is the return type?
1 value gets accepted . It is integer return type.

b. What does function at 0x8048ca0 do?
In this function ,a recursive function is done and called with arguments [ebx-1] and [ebx-2]
Thus a fibonacci series is generated.

c. 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 structures you claim them to be.

There were if condition at address of the function sub_8048CE0
There was for loop at the address of the function sub_8048CA0
These if and for loops are used for writing programs in language.

d. Are there multiple possible answers? If yes, find all possible answers. If no, explain why.
No multiple answers are possible because the entered input is checked against 55 which is the 9th value in fibonacci series.

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

Now, there is a comparison taking place at address 08048D01 inside sub_8048CE0, the input is compared with 1 ie,[cmp eax , 1].It will check and if failed it does jump if not zero to loc_8048D09, which calls the explode bomb function at sub_80494FC which prints that “bomb has exploded”.
Else it does a jump greater to short loc_8048D0E.In this location,the entered input value gets validated and pushed into eax and the sub_8048CA0 function is called.

Then, again a comparison is taking place at address 08048D1D with (37h) ie, 55, which is 9th in fibonacci series.
If the calculated value is equal to 55 then the output is printed as “So you got that one.Try this one”.
If the calculated value is not equal to 55,then it goes to explode bomb function sub_80494FC