

# Assignment 2: Reverse engineering

**Due** 8 May 2022 by 20:00    **Points** 12    **Submitting** a file upload  
**Available** until 8 May 2022 at 21:00

This assignment was locked 8 May 2022 at 21:00.

For this assignment you should reverse engineer the binary `bomb` (it is in the support files). Start by running `bomb` to get an idea of what the program does:

```
$ ./bomb
```

(If you dare.)

Your job is to defuse as many phases as you can. You should be able to solve at least the first 4 phases, and from phase 7 and onward are only for bonus points.


## What to hand in

You should hand in three things:

1. A text file, `solution.txt`, that defuses the phases you have solved when used as

```
./bomb < solution.txt
```

2. Commented assembly listing, `bomb-assembly.asm` of the phases you have defused, and possibly some psuedo code too. See `commented-assembly.asm` for an example of what we expect.
3. A report (`week2.txt`, `week2.md` or `week2.pdf`) that describe how you solved the phases you defused (what tools and techniques you have used).

You should hand in a `handin.zip` file that contains your (well commented) assembly code, `solution.txt`, other support files; and your report. Make sure to check your `handin.zip` file with **OnlineTA**  (<https://pcs.incorrectness.dk>) before handing in; otherwise you might risk to get your hand-in auto-failed.

## To keep your TA happy:

- Don't feel pressured to comment every single instruction. You probably don't want to comment every line.

See `badly-commented-assembly.asm` for an example of how *not* to comment assembly.

- Keep you reporting to one or two pages.

- Don't hand in a Word document, if you need fancy formatting and pictures then use PDF; otherwise hand in a text file perhaps with some separate graphics files.

## Hints

The following hints are not relevant for all phases. The first five should be relevant for all phases.

1. `$ objdump -M intel -d bomb`

2. `$ objdump -x bomb`

3. `$ readelf -x .data bomb`

4. `$ readelf -x .rodata bomb`

5. `$ gdb ./bomb`  
`(gdb) handle SIGALRM ignore`

6. `$ strace ./bomb`

7. If the bomb is too slow. Try patching the `sleep` call.

8. For those who does not get the [soldier crab reference](https://arxiv.org/abs/1204.1749) ➞ <https://arxiv.org/abs/1204.1749>