Exercise 1 (10 points)

Program `password` checks user's password and exhibits the following behaviour:

```
$ ./password
Password: AAAA
Wrong password: AAAA
$ ./password
Password: AAAA.%08x
Wrong password: AAAA.00000080
$ ./password
Password: AAAA.%08x.%08x.%08x.%08x.%08x.%08x.%08x
Wrong password: AAAA.00000080.b7fcc5a0.b7fd76b0.00000001.00000000.00000001.41414141
```

1. What kind of bug (just the bug, not the vulnerability) is present in the program? Illustrate through a simple source code example (3 points)
2. Explain in detail the last output (show the stack layout) (3 points)
3. What attack is possible if a sensitive value is stored on the stack before the buffer used to read the password? (2 points)
4. Discuss how it is possible to dump the content of arbitrary memory locations (it is not required to provide the exact attack payload) (2 points)

Exercise 2 (10 points)

Consider the following insecure PHP fragment:

```
if($input == $password) {
        // access to privilege area
    }
    else {
        // access forbidden
```

where `$input` contains a user-provided value of unknown type and `$password` is a secret unguessable password.

1. Discuss why the use of `==` is insecure in general (3 points)
2. Provide (different) realistic example values for `$input` and `$password` that bypass the check and discuss why this happens (3 points)
3. Propose a fix and discuss why the previous attack is prevented (2 points)
4. Discuss why using `strcmp($input,$password)==0` instead of `$input==$password` does not fix the problem (2 points)

Exercise 3 (10 points)

Cross-site request forgery (CSRF) is an attack that forces a user executing unwanted actions on a web application in which she is currently authenticated.

1. Describe a typical CSRF attack scenario (3 points)
2. Explain the role of session cookies in CSRF attacks (2 points)
3. Is it necessary for the attacker to intercept the communication between the victim browser and the victim web site? Motivate your answer (2 points)
4. Illustrate a security mechanism that prevents CSRF (3 points)