# Broken Access Control : Solution

## Missing Function Level Access Control

**Exercise 1.** For this exercise we use a new application for the management of marks Marks Manager. For this exercise, you will receive from the professor usernames and passwords of different users (admin, prof, student).
Normally a student can not change their own marks.
Visit the site using the different users. Note the URL's of the different resources.

Try to change the mark of a student (give them a 6.0 for instance).

### Solution

We visit the application and note which resources are available:

- Some pages are used by professors: `prof.php`, `prof2.php`,`viewMessages.php` ,`course.php?courseID=1` (can be used to set the marks)

We log as a student and access directly to the URL:
`https://www.benoist.ch/marksEsc/course.php?courseID=1`
We change the mark. Submit. The mark has been modified.
The process is much more difficult without the various accounts of different levels. You must "guess" the name of the resources.

## Attack your guestbook using insecure object references

**Exercise 2.**

- Login as a normal user.
- Get the ID of all users.
  For doing this, you do not have the right to look in the DataBase (too easy).
- Read some messages you do not have the right to read (changing the id in the URL)
- Send messages with a wrong author.
- Change the password of any user (other than the one your are).

### Solution

- ID can be found in the view source of the form (to send messages)
- Change the ID of the message in the URL.
- Change the Querry String inside the URL bar.
  `http://localhost/guestbook/index.php?userID=2&title=Essai&message=Ceci+est+un+message&dest=0`
  Write any number as a userID (not yours if you want).

Related Pages

Home

Slides

Exemples

Exercices

Resources

Contact

Prof. Dr. Emmanuel Benoist
Berner Fachhochschule - TI
Quellgasse 21
CH-2501 Biel/Bienne
Switzerland
Mail: emmanuel.benoist (at) bfh.ch

Social Networks

**Follow me on**
Linkedin, Scholar & Research gate

http://www.ti.bfh.ch/

BACK TO TOP