SQL Injection Continued

In this exercise we are going to be working on the ELGG platform. ELGG is an open-source platform for creating private/community-specific social networks (the ELGG platform you will use has been modified to be weaker than it originally is for the sake of the exercise).

Follow the steps before rushing off with the exercise:

1. If you haven't previously installed exercise 07's ex_pack – do it first. This is important.
   ex_unpack ex08.bin ex08
   Wait for it to end successfully!
2. Now, unpack exercise 09 –
   ex_unpack ex09.bin ex09
3. **During the exercise setup, follow these instructions –**
   a. An interactive (ncurses) console UI will open
   b. In the "Configuring phpmyadmin" window – choose
   c. After a little while, another prompt screen will show
   d. After a little while, another prompt screen will show
   e. Choose 'Yes'
   f. Enter the mysql root password: mysql_root_passwd
   g. Enter the phpmyadmin password: phpmyadmin_passwd
   h. Repeat the phpmyadmin password: phpmyadmin_passwd
4. Open Mozilla Firefox and check that elgg is up and running by opening the page at http://localhost/elgg/
5. Make sure you are able to connect to the elgg DB from the shell:
   a. mysql –u elgg –p
   b. use the password: elggp4ss
   c. connect elgg
   d. SHOW TABLES;
6. Set up Source Insight 3.5 on Windows:
   a. Download source insight: http://www.sourceinsight.com/downeval.htm l
   b. Get the extension for PHP:
      http://www.sourceinsight.com/public/languages/PHP%20Script.CLF
   c. Use these instruction to add PHP support:
      http://blog.sina.com.cn/s/blog_4e7453df010111v7.html
7. Download elgg.7z from the course site and open it under some library where you will find it later in your computer
8. Create a new Source Insight project and add all the elgg directory tree (recursively!).
9. Synchronize all the files
10. Open Mozilla Firefox and install FireBug:
    a. Go to the Menu: Tools->Add ons
    b. Add the FireBug extension and/or enable it.
    c. Check that its working by pressing F12 when inside a web page.

Now that we have all our tools working let 's get to it –

1. **Warm-up questions (MUST) –**
   a. Within the Source Insight Project:
      i. Click Ctrl-/ and enter elgg_view. How many results do you receive ? (hint: results < 100 = error).
      ii. Use Ctrl+Left-Mouse-Button to click on **elgg_view**. In which php file is it implemented?
   b. Surf to http://localhost/elgg/
   c. Operate the elgg platform to get a sense of how it is working.
      i. Use the credentials:
         1. User: neo0
         2. Password: neoqwerty
   d. You will have to confirm a security exception to let the login pass. Store this exception for the future.
   e. Use firebug (under 'view '->Firebug / hit the F12 key, refer to the "Net" tab to see HTTP request and responses) –
      i. What does the HTTP query to send a message to the adm in look like ?
      ii. What do the different fields of the HTTP query mean?
      iii. What do the different elgg code fields of the POST/GET query mean?
   f. Surf to http://localhost/phpmyadmin
   g. Login with the elgg credentials –
      i. User: elgg
      ii. Password: elggp4ss
   h. Select the 'elgg' DB
   i. Browse the various tables, and find the table that holds basic user info – name, username, password, etc.
   j. Take a screenshot (hit the PRNTSCR key on your keyboard), showing this information in the phpmyadmin interface. Include the image in your solution.

PLEASE PROVIDE THE FOLLOWING FILES WITH THE FOLLOWING NAMES IN THE ROOT DIRECTORY:

1. ex09.q1.txt – details of the work you did and answers.
2. ex09.q1.png – the PRINTSCR result.

2. **Mis-sanitized cookie –**
   a. Check the cookie handling code in ELGG (make sure to mark the "remember me" tick-box at login – or you won't have a stored cookie to work with!)
   b. How will you send an SQL injection via a cookie? Implement an SQL injection so that you are logged in as administrator (elgg administrator) (Do not use %00 and you can not rely on the default order or amount of the entries in the table).

PLEASE PROVIDE THE FOLLOWING FILES WITH THE FOLLOWING NAMES IN THE ROOT DIRECTORY:

1. ex09.q2.txt – details of the work you did and answers.

3. AJAX –

a. Surf to http://www.tau.ac.il
b. Go into FireBug console menu.
c. Use $.ajax to read /past-present-future
d. Use javascript alert() to print the returning html content of the page that you got as a result from ajax.
e. Write it as a one-line script.

PLEASE PROVIDE THE FOLLOWING FILES WITH THE FOLLOWING NAMES IN THE ROOT DIRECTORY:

1. ex09.q3.txt – details of the work you did and answers.