Introduction to InfoSec – SQLI and jQuery (R9)

Nir Krakowski (nirkrako at post.tau.ac.il)
Itamar Gilad (itamargi at post.tau.ac.il)

Covered material

- Useful SQL Tools
- SQL Injection over-view.
- More on SQL Injection
- Mass Code Reverse Engineering
- Javascript/Jquery primer.

Useful SQL Tools

- phpMyAdmin
- Mysql

SQLI

- What is SQL Injection ?
- Exploitation of string sanitation failure to make manipulated database queries by means of SQL (Structured Query Language).
- SQLI can be used for:
  - Information Leak
  - Modification of DB.
  - Bypassing of authentication checks
  - Hacking the underlaying OS.
- Not limited to HTTP(S) Requests, but most common there. Anything that uses SQL queries may be vulnerable.

SQL

- SQL is not a completely generic language.
- There are special modifications per DB manufacturer
- We will concentrate on mysql – open source very commonly in use DB.

Useful SQL Commands

- Mysql commands:
- Connect dbname
- Show tables
- Show columns from tablename;

SELECT

- Explanation by example:
- SELECT * FROM TABLENAME;
- SELECT FieldName1, FieldName2 FROM TABLENAME;
- SELECT 1;

CONCAT & AS

- SELECT CONCAT('1','2');
- SELECT CONCAT (username, '/', password) **as** username FROM some_user_table;
- SELECT GROUP_CONCAT(table_name) FROM information_schema.tables WHERE version=10;

UNION

- SELECT username, password FROM TABLENAME WHERE USER username UNION SELECT 1,2;
- Field count must match.
- Examples:
- SELECT * FROM USERS WHERE username = '1' UNION SELECT 1,2; -- Will not work, because number of fields doesn't match.
- SELECT * FROM USERS WHERE username = '1' UNION SELECT 1,2,3; -- will return one row with values 1,2,3, because no username named '1' exists.

Accessing Underlying OS

- SELECT **LOAD_FILE(**'/etc/passwd'**)**;
- SELECT * FROM TBL INTO OUTFILE '/tmp/asd';

Good Source for SQLI Info

- https://en.wikipedia.org/wiki/SQL_injection
- http://www.websec.ca/kb/sql_injection

Code Browsing with Source Insight

- Source based "RE".
- Target: Quickly come up with a location in the code that handles a specific function.
- http://www.sourceinsight.com
- Simple, yet fastest Editor out there for handling massive amounts of code.
- Need to manually fix it to work with PHP:
  - http://blog.sina.com.cn/s/blog_4e7453df010111v7.html
- Easy scroll through code.
- **Ctrl-/** - Search the database for pre-parsed words.
- **Ctrl+Left-Mouse-Click** on a word, follow link to definition.

Code browsing demo

- Let's browse elgg.
- .
- .
- **WAIT** Let's look at the interface first!! What is elgg?
- User: neo0 Password: neoqwerty
- Now let

Javascript and JQuery

- Javascript allows to make create callbacks from the DOM and modify settings in the DOM (Document Object Model).
- Furthermore AJAX allows creating dynamic web pages using HTTP Queries sent to the server from within the javascript (originally named DHTML)
  - This was created to alleviate the need for page refreshing (horrible).

Firebug/Chrome Developer Tools

- Firebug is a Web client-side developer tool.
- Can be used as a Javascript interpreter.
- Can be used to make on-the-fly modifications to the DOM.
- Can be used to understand outgoing/incoming HTTP headers/data of response and request.
- Browse and modify CSS Styling

Firebug

- Important functions:
  - Net View.
  - Console
  - Elements
- Using inspect element we can locate items from the screen on the DOM very easily.

jQuery

- jQuery is the most popular Javascript library used in the wild.
- $$$$$ - $ is used for quick access to the DOM.
- $(“body”)[0].ondrag = function () { alert("Hello, World!"); }
- $(“#itemid”).remove()
- $(“div”). css(‘color’, ‘red’).show()

- Quick Primer:
  - http://dotnetslackers.com/articles/ajax/JQuery-Primer-Part-1.aspx

Example

- [Remove commercial from screen using Element viewer and jQuery]

Appendix A

- Passwords for the DB:
- l/p: elgg/elggp4ss
- l/p: root/mysql_root_passwd