Practical Attack & Defence
Kimmo Saurén
Metropolia

Exercise 3. Information gathering & SQL-injections

The Internet is full of organisations and companies. All of them reveal information about themself intentionally and unintentionally. For criminals this information is valuable for gaining unauthorizated access to computer systems.

In this laboratory we will continue scanning activities.

For this laboratory we will need Burp Suite reconnaissance tool. You can download it from Internet.

Burp Suite is tool for intercepting HTTP traffic. So all communications between web-browser and web-server can be intercepted. HTTP messages can be modified or stored for later inspection.

To get Burb Suite working:

1. Launch the Burb Suite.
2. Change your web-browsers proxy settings to localhost and port should be 8080
3. Start browsing

In figure 1. you can see the Burp proxy.

Figure 1. Burp Poxy Suite

Intercept on/off is used when there is need to intercept and modify HTTP messages. It is not needed when logging responces from website.

Spider is automated website scanned, which tryes to follow every link in page. The usage of this feature is considered a dangerous operation since it will access every page. For example if admin interface is acceidently accessible, the spider could access pages like delete_user or delete_page. **Using spider against unknown website is really dangerous.** You could end up breaking the site.

Repeater is a nice tool for repeating messages to server. For example if you need to research a vulnerability in certain page, the repeater can be used to send a message or series of messages to get the vulnerable webpage break (or act in certain way). F.e. SQL-injections can be researched using repeater.

Decoder is for decoding encrypted messages in webpages.

Comparer is very important tool for comparing responces to certain HTTP requests. Minor differences in responces can reveal many things like: access-control vulnerabililties and blind SQL-injections.

SQL injections

SQL injection is very common vulnerability in Internet. In this laboratory you learn basics of SQL-injections.

Do following steps to start your laboatory:
1.Download a special xampp from http://users.metropolia.fi/~kimmosa/xampp-attack.zip
2.Extract and go to directory xampp
3.Run setup_xampp.bat (this will take care of right path for the software)
4.Run xampp_start.exe
5.Open Firefox and browse to http://localhost/lab-1-SQL
6.Open the first lab1

Read trought the exercise and get the information that you are supposed to.

Remember to use Burb proxy to investigate the exercises.