**Sri Lanka Institute of Information Technology**



3rd Year 2st Semester 2016 **INFORMATION SECURITY PROJECT**

**Assignment 01**

From Sql Injection to shell

**Registration Number**: IT14026362

**Name**: S.H.M Lahiru Prabath.

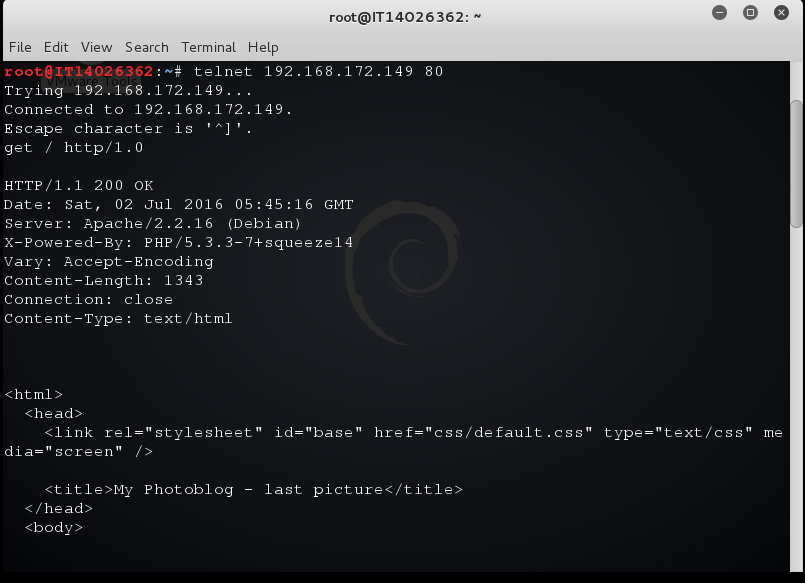
* This is about the exploitation of SQL injection in a PHP based website and how an attacker can use it to gain access to the administration pages.  
  Then, using this access, the attacker will be able to gain code execution on the server.

A lot of information can be retrieved by connecting to the web application using netcat or telnet

Where:

* vulnerable is the hostname or the IP address of the server;
* 80 is the TCP port used by the web application (80 is the default value for HTTP).

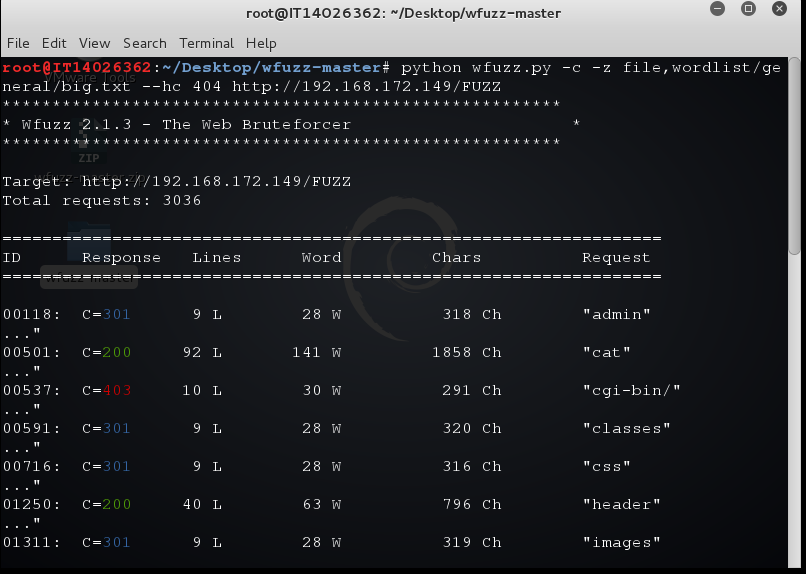
By sending the following HTTP request

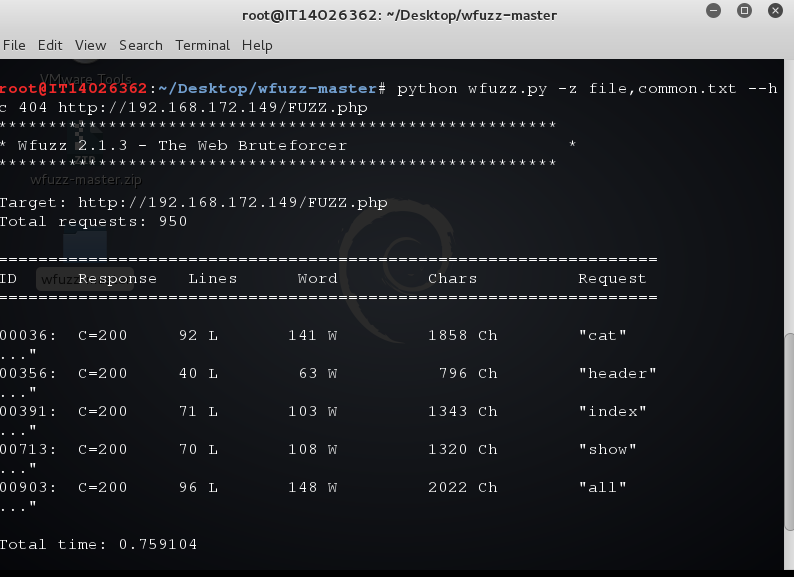


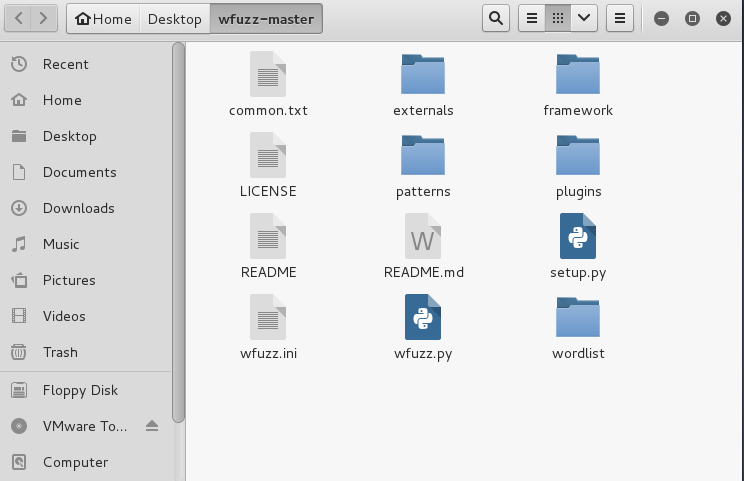
The following command can be run to detect remote files and directories

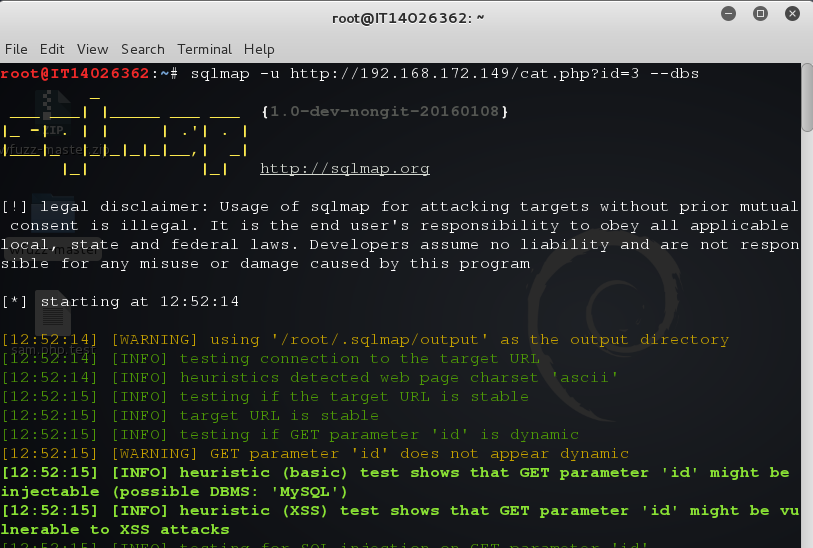
\*\* $ python wfuzz.py -c -z file,wordlist/general/big.txt --hc 404

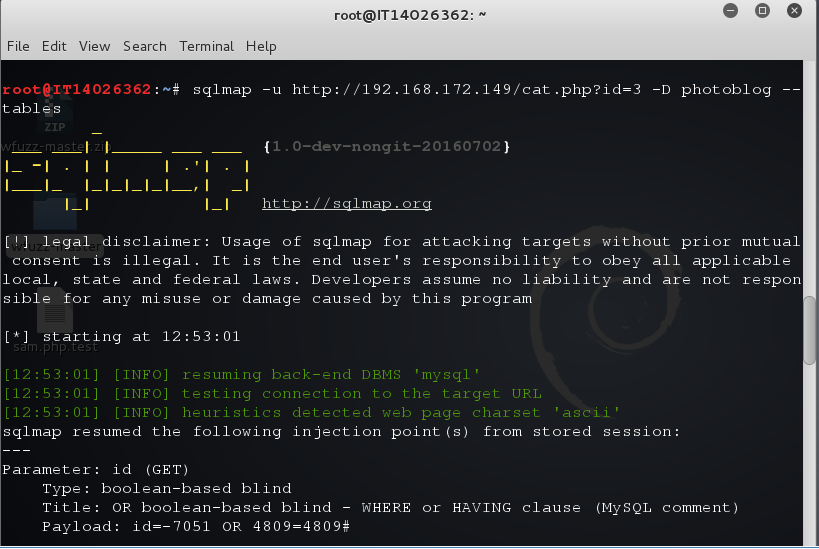
Wfuzz can also be used to detect PHP script on the server:

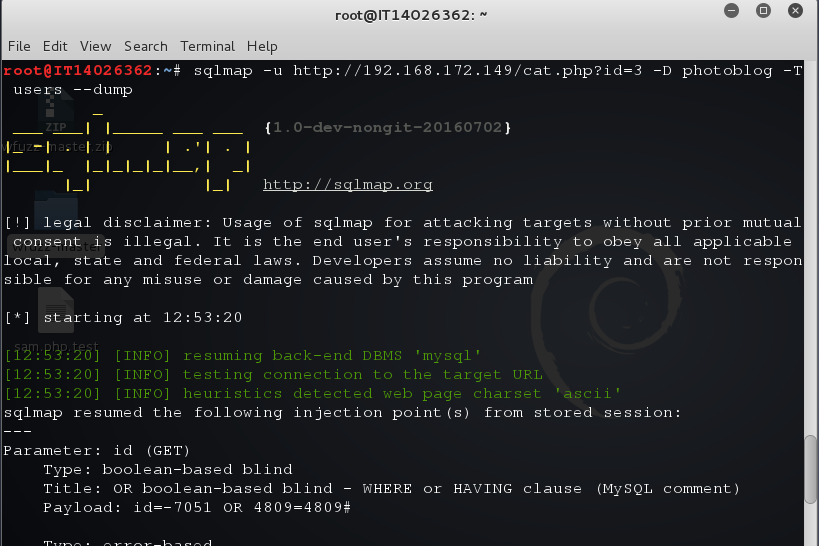


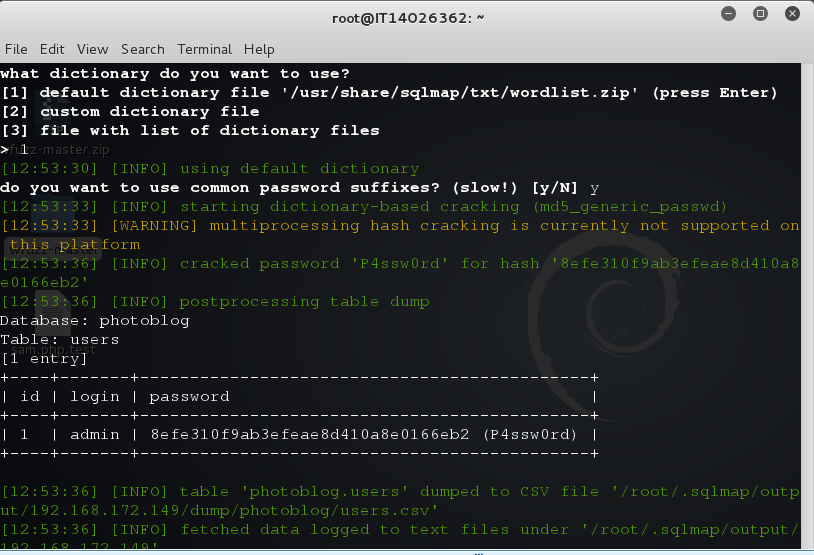


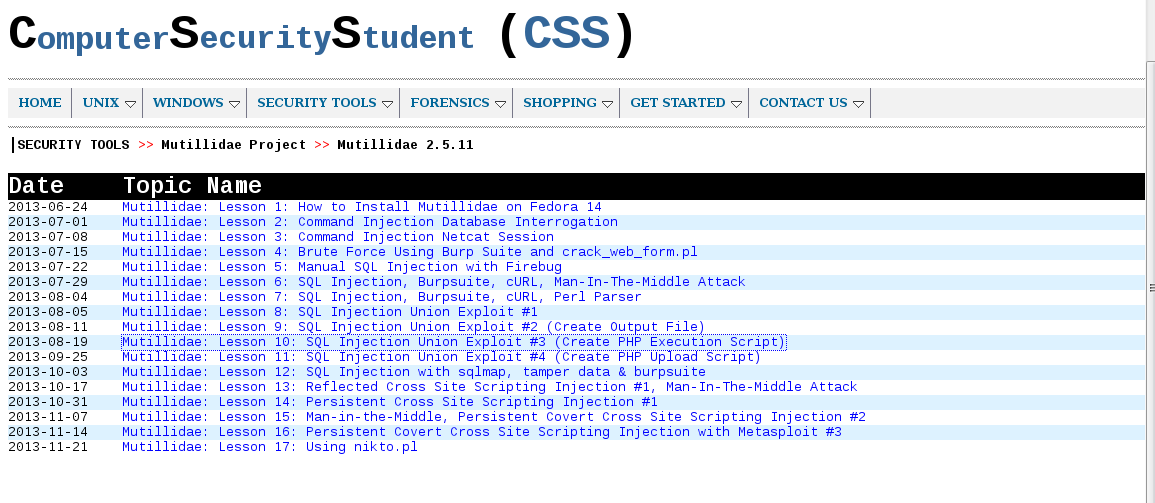


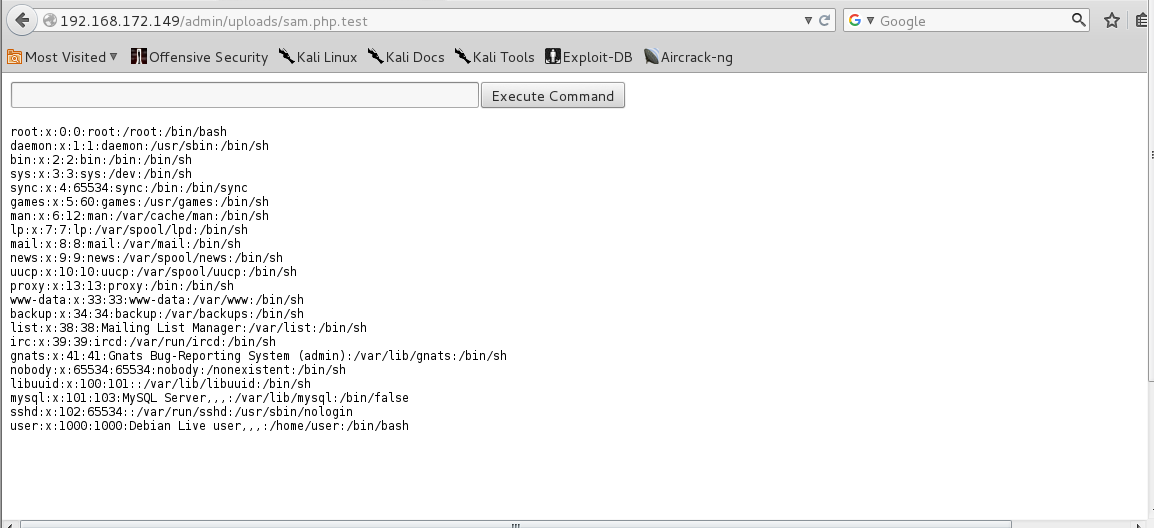












* This exercise showed you how to manually detect and exploit SQL injection to gain access to the administration pages. Once in the "Trusted zone", more functionality is often available which may lead to more vulnerabilities.