Attacks depend on underlying SQL query

SQL Injection (Login page)

1. Trigger an error
2. Once verbose error is show you can derive info such as
   1. SQL column & table name 🡪 SELECT username FROM accounts WHERE usename = ‘ ’ ’
   2. SQL Server 🡪 MaraDB server
   3. Path of the website 🡪 C:\xampp\htdocs\mutillidae\classes\MySQLHandler.php
   4. Version of DB 🡪 mysqlnd 5.0.12-dev
3. Command (‘ or 1=1 -- ) to go into first account of the database
4. Use - - (sql comment syntax) to comment out the password so you do not need to input it (able to bypass the authentication)
5. Can use (username’ - - ) to bypass authentication, only need to know username

Graphical user interface, text, application, email

Description automatically generated

SQL Injection (User lookup page)

1. Trigger an error using ‘

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

' union Select null,null,null,null,null,null,null –

Used to enumerate number of columns in the table

Graphical user interface, text, application

Description automatically generated

'union select 1,2,3,4,5,6,7 –

Used to show which column number username, password and signature belong to.

Thus, only 3 columns are being showed to us of the 7 columns in the accounts table.

Graphical user interface, text, application, email

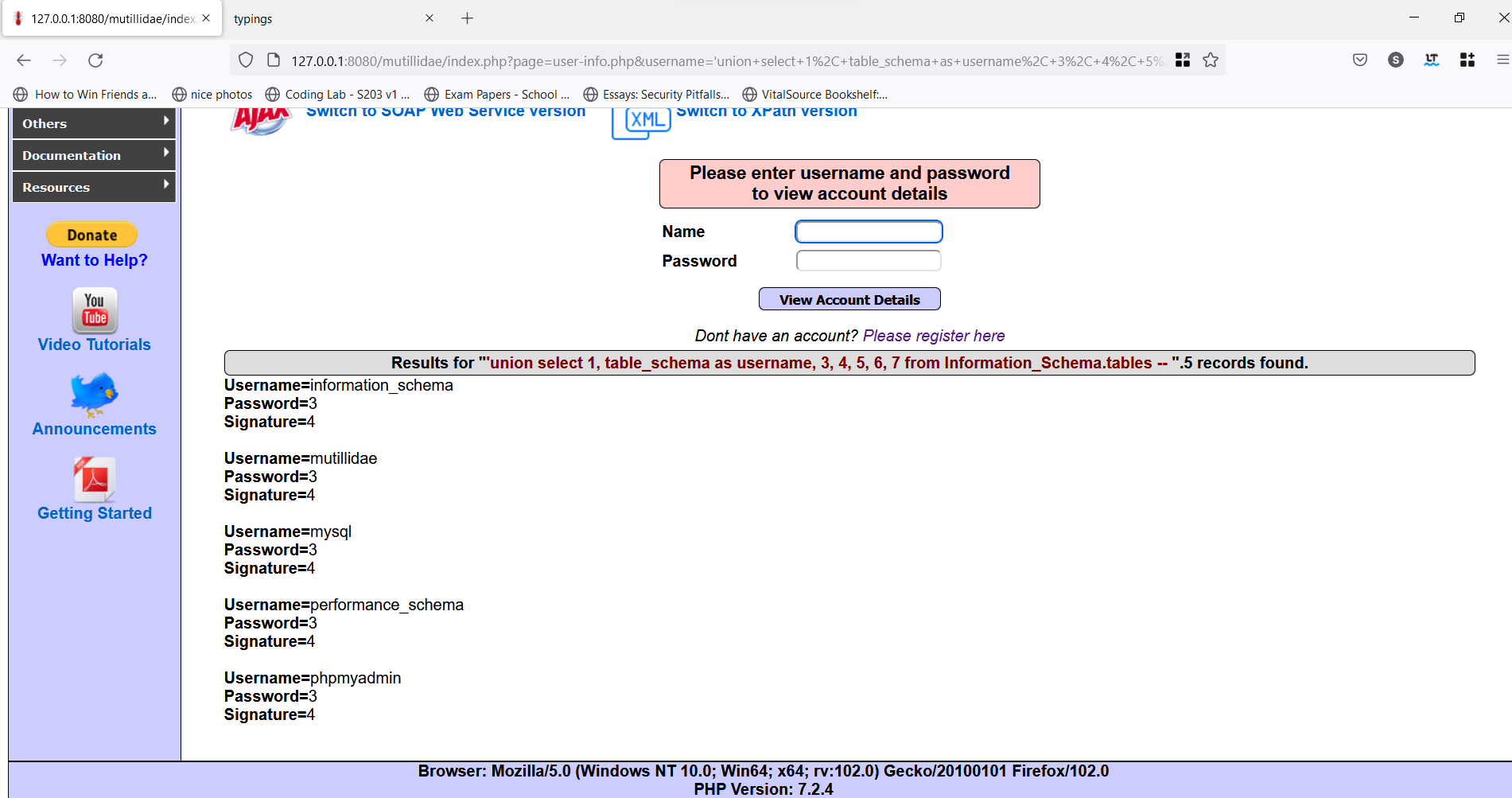
Description automatically generated

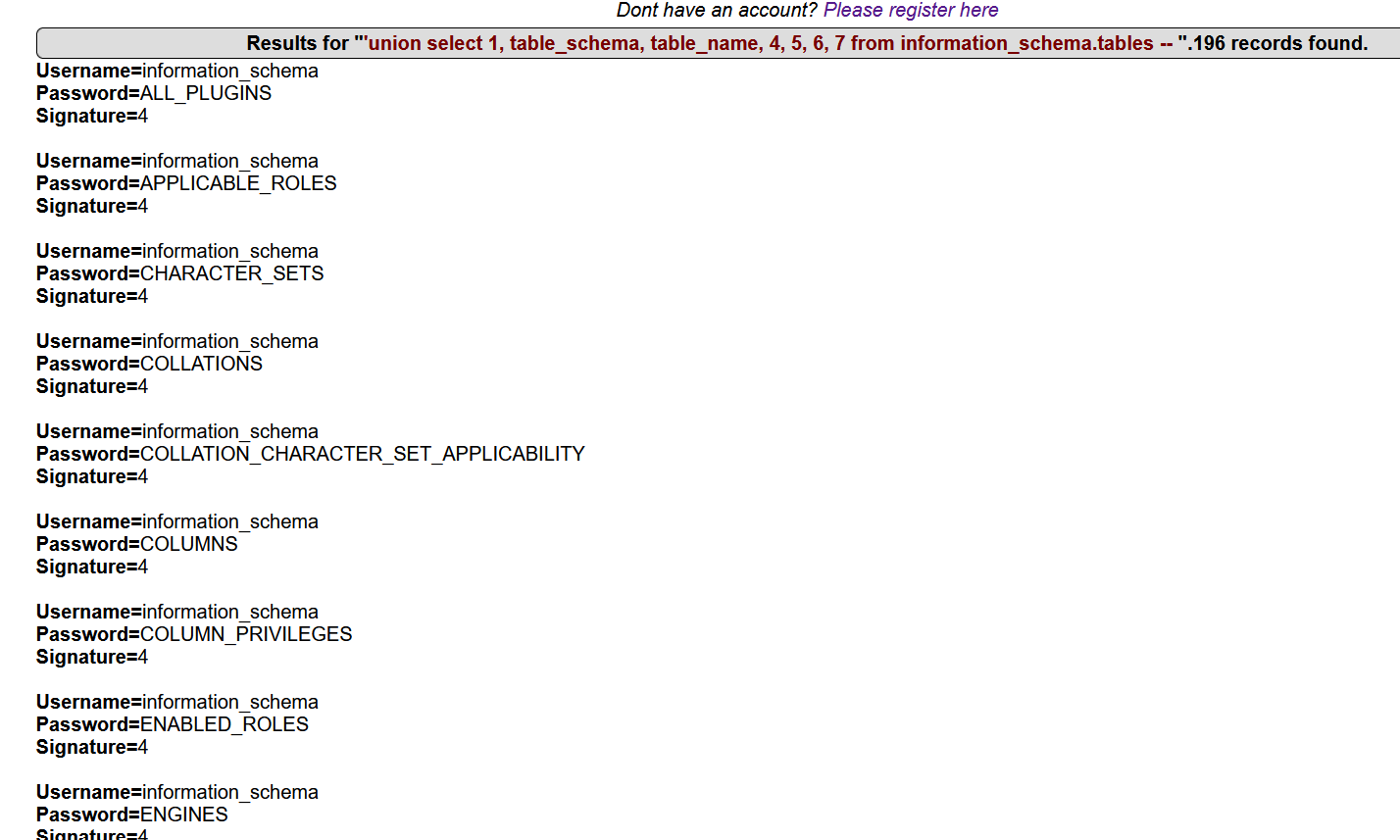
Replacing username (column 2) with version of the database.

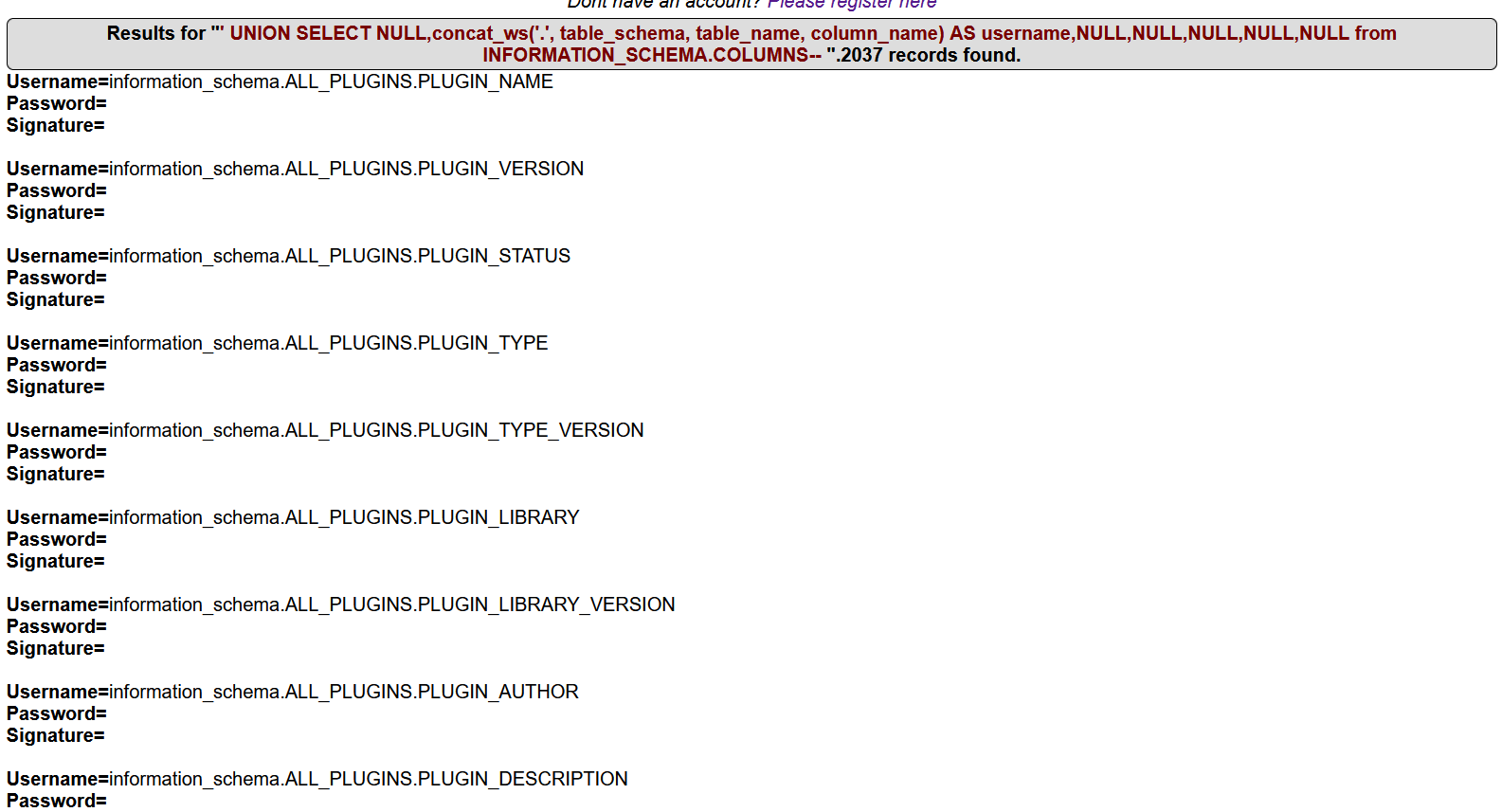
Graphical user interface, text, application, email

Description automatically generated

Replacing username (column 2) to find Database name.







Graphical user interface, text

Description automatically generated

