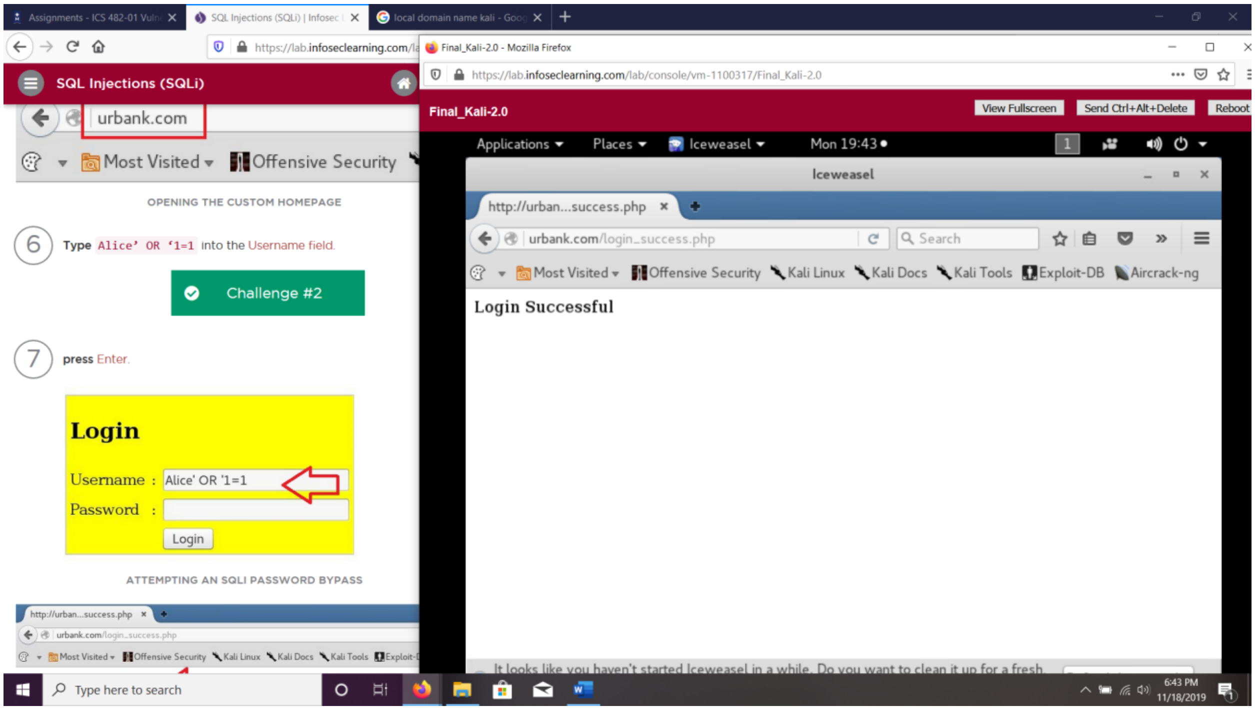
Ryan Brodsky

ICS482

11/18/19

InfoSec Lab: SQL Injection (SQLi)



OPENING THE CUSTOM HOMEPAGE

6 Type `Alice' OR '1=1` into the Username field.

Challenge #2

7 press Enter.

Login

Username : Alice' OR '1=1

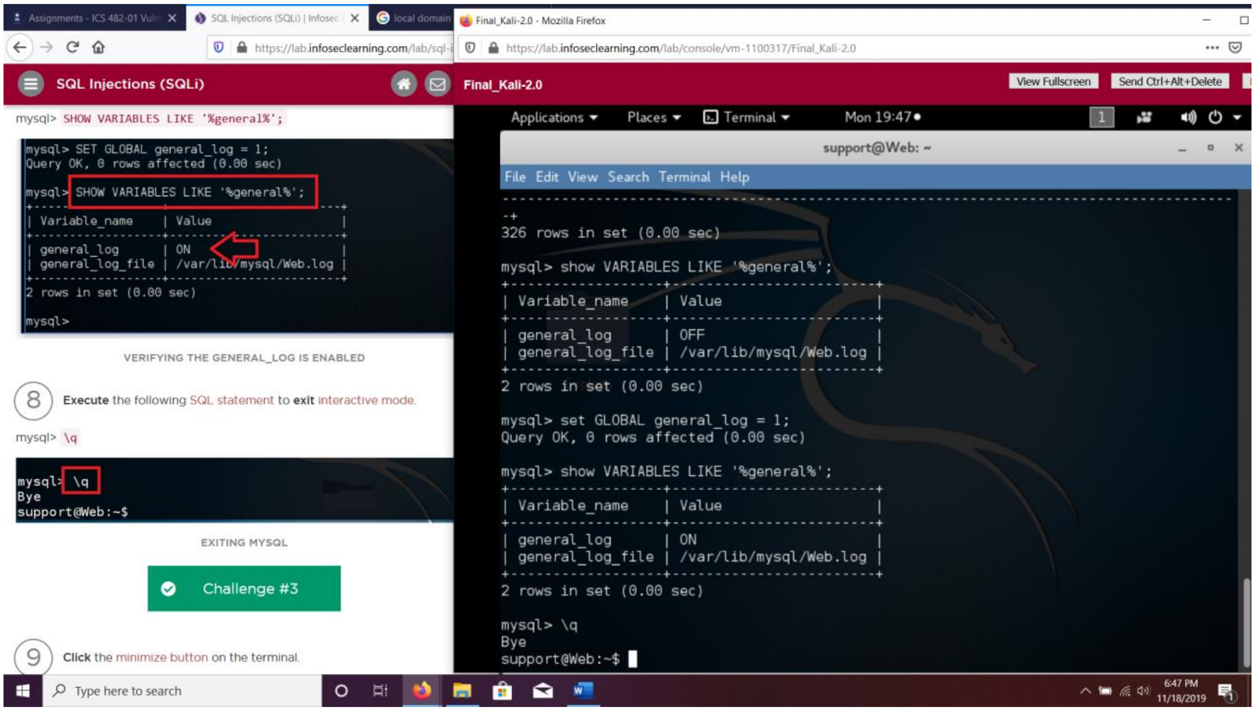
Password :

Login

ATTEMPTING AN SQLI PASSWORD BYPASS

Login Successful

It looks like you haven't started Iceweasel in a while. Do you want to clean it up for a fresh


Assignments - ICS 482-01 Vuln
SQL Injections (SQLi) | Infosec
local domain
https://lab.infoseclearning.com/lab/sql-i
SQL Injections (SQLi)
Final_Kali-2.0 - Mozilla Firefox
https://lab.infoseclearning.com/lab/console/vm-1100317/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Terminal
Mon 19:47
support@Web: ~
File Edit View Search Terminal Help
Type here to search
6:47 PM
11/18/2019

mysql> `SHOW VARIABLES LIKE '%general%';`

```
mysql> SET GLOBAL general_log = 1;
Query OK, 0 rows affected (0.00 sec)

mysql> SHOW VARIABLES LIKE '%general%';
+------------------+-----------------------+
| Variable_name    | Value                 |
+------------------+-----------------------+
| general_log      | ON                    |
| general_log_file | /var/lib/mysql/Web.log |
+------------------+-----------------------+
2 rows in set (0.00 sec)

mysql>
```

VERIFYING THE GENERAL_LOG IS ENABLED

8 Execute the following SQL statement to exit interactive mode.

mysql> `\q`

```
mysql> \q
Bye
support@Web:~$
```

EXITING MYSQL

Challenge #3

9 Click the minimize button on the terminal.

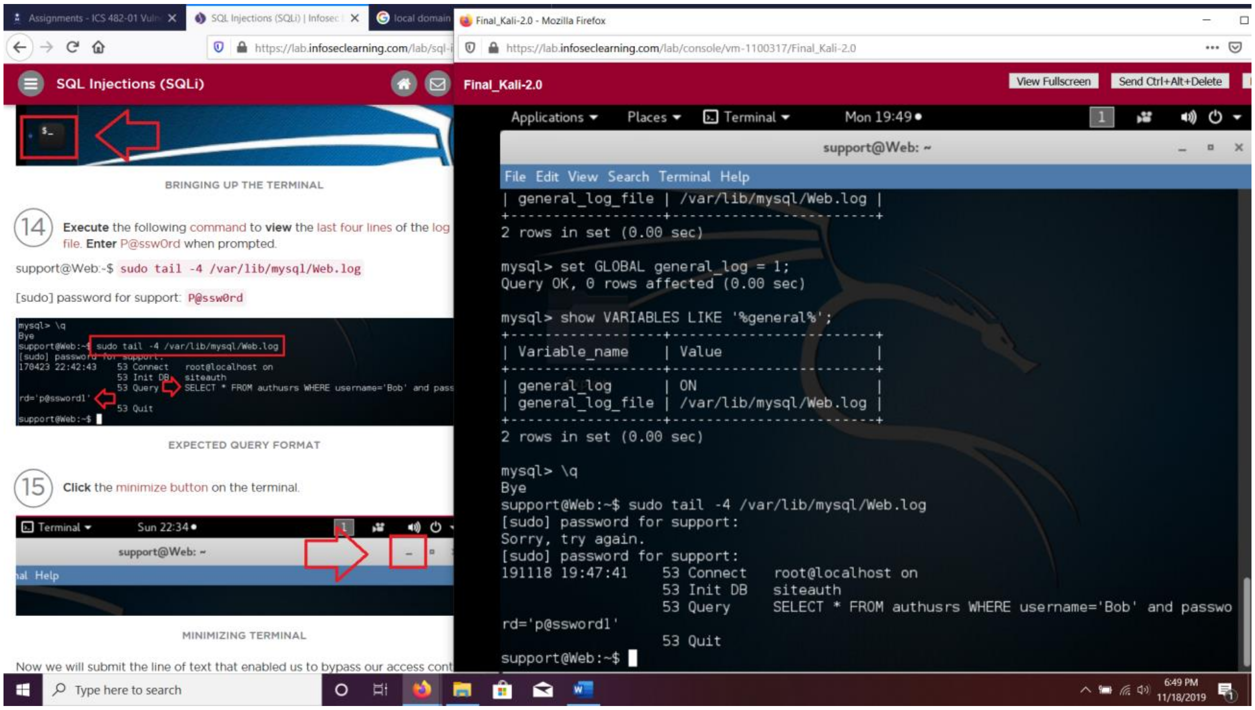
```
--+
326 rows in set (0.00 sec)

mysql> show VARIABLES LIKE '%general%';
+------------------+-----------------------+
| Variable_name    | Value                 |
+------------------+-----------------------+
| general_log      | OFF                   |
| general_log_file | /var/lib/mysql/Web.log |
+------------------+-----------------------+
2 rows in set (0.00 sec)

mysql> set GLOBAL general_log = 1;
Query OK, 0 rows affected (0.00 sec)

mysql> show VARIABLES LIKE '%general%';
+------------------+-----------------------+
| Variable_name    | Value                 |
+------------------+-----------------------+
| general_log      | ON                    |
| general_log_file | /var/lib/mysql/Web.log |
+------------------+-----------------------+
2 rows in set (0.00 sec)

mysql> \q
Bye
support@Web:~$
```


Assignments - ICS 482-01 Vuln
SQL Injections (SQLi) | Infosec
local domain
Final_Kali-2.0 - Mozilla Firefox
https://lab.infoseclearning.com/lab/sql-i
https://lab.infoseclearning.com/lab/console/vm-1100317/Final_Kali-2.0
SQL Injections (SQLi)
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Applications ▾
Places ▾
Terminal ▾
Mon 19:49 ●
support@Web: ~
File Edit View Search Terminal Help
Type here to search
6:49 PM
11/18/2019

BRINGING UP THE TERMINAL

(14) **Execute** the following command to **view** the last four lines of the log file. **Enter** P@ssw0rd when prompted.

support@Web:~$ `sudo tail -4 /var/lib/mysql/Web.log`

[sudo] password for support: `P@ssw0rd`

```
mysql> \q
Bye
support@Web:~$ sudo tail -4 /var/lib/mysql/Web.log
[sudo] password for support:
170423 22:42:43     53 Connect   root@localhost on
                    53 Init DB   siteauth
                    53 Query     SELECT * FROM authusrs WHERE username='Bob' and pass
rd='p@ssword1'
                    53 Quit
support@Web:~$
```

EXPECTED QUERY FORMAT

(15) **Click** the minimize button on the terminal.

MINIMIZING TERMINAL

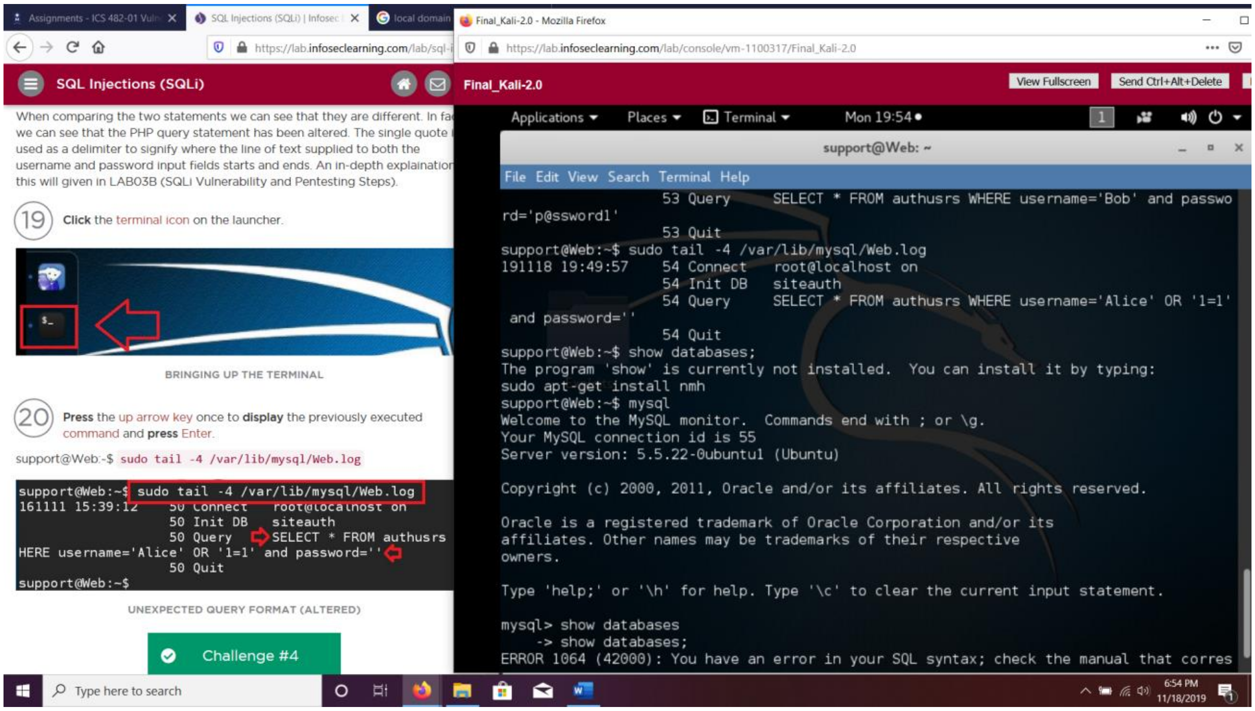
Now we will submit the line of text that enabled us to bypass our access cont

```
| general_log_file | /var/lib/mysql/Web.log |
+------------------+------------------------+
2 rows in set (0.00 sec)

mysql> set GLOBAL general_log = 1;
Query OK, 0 rows affected (0.00 sec)

mysql> show VARIABLES LIKE '%general%';
+------------------+------------------------+
| Variable_name    | Value                  |
+------------------+------------------------+
| general_log      | ON                     |
| general_log_file | /var/lib/mysql/Web.log |
+------------------+------------------------+
2 rows in set (0.00 sec)

mysql> \q
Bye
support@Web:~$ sudo tail -4 /var/lib/mysql/Web.log
[sudo] password for support:
Sorry, try again.
[sudo] password for support:
191118 19:47:41     53 Connect   root@localhost on
                    53 Init DB   siteauth
                    53 Query     SELECT * FROM authusrs WHERE username='Bob' and passwo
rd='p@ssword1'
                    53 Quit
support@Web:~$
```


Assignments - ICS 482-01 Vuln
SQL Injections (SQLi) | Infosec
local domain
Final_Kali-2.0 - Mozilla Firefox
https://lab.infoseclearning.com/lab/sql-i
https://lab.infoseclearning.com/lab/console/vm-1100317/Final_Kali-2.0
SQL Injections (SQLi)
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Applications ▾
Places ▾
Terminal ▾
Mon 19:54 ●
support@Web: ~
File Edit View Search Terminal Help
Type here to search
6:54 PM
11/18/2019

When comparing the two statements we can see that they are different. In fa we can see that the PHP query statement has been altered. The single quote used as a delimiter to signify where the line of text supplied to both the username and password input fields starts and ends. An in-depth explainatior this will given in LAB03B (SQLi Vulnerability and Pentesting Steps).

(19) **Click** the terminal icon on the launcher.

BRINGING UP THE TERMINAL

(20) **Press** the up arrow key once to **display** the previously executed command and **press** Enter.

support@Web:~$ `sudo tail -4 /var/lib/mysql/Web.log`

```
support@Web:~$ sudo tail -4 /var/lib/mysql/Web.log
161111 15:39:12      50 Connect   root@localhost on
                     50 Init DB   siteauth
                     50 Query     SELECT * FROM authusrs
HERE username='Alice' OR '1=1' and password=''
                     50 Quit
support@Web:~$
```

UNEXPECTED QUERY FORMAT (ALTERED)

Challenge #4

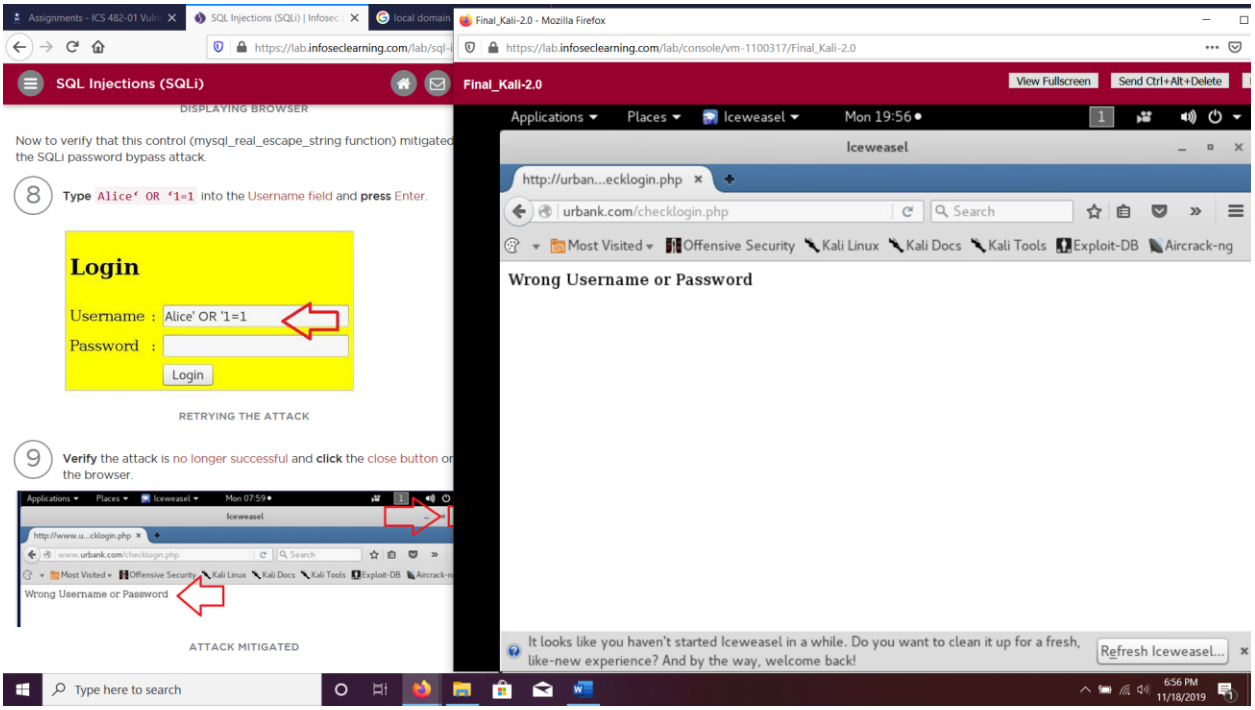
```
                    53 Query     SELECT * FROM authusrs WHERE username='Bob' and passwo
rd='p@ssword1'
                    53 Quit
support@Web:~$ sudo tail -4 /var/lib/mysql/Web.log
191118 19:49:57     54 Connect   root@localhost on
                    54 Init DB   siteauth
                    54 Query     SELECT * FROM authusrs WHERE username='Alice' OR '1=1'
 and password=''
                    54 Quit
support@Web:~$ show databases;
The program 'show' is currently not installed.  You can install it by typing:
sudo apt-get install nmh
support@Web:~$ mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 55
Server version: 5.5.22-0ubuntu1 (Ubuntu)

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases
    -> show databases;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corres
```


Assignments - ICS 482-01 Vuln
SQL Injections (SQLi) | Infosec
local domain
Final_Kali-2.0 - Mozilla Firefox
https://lab.infoseclearning.com/lab/sql-i
https://lab.infoseclearning.com/lab/console/vm-1100317/Final_Kali-2.0
SQL Injections (SQLi)
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Iceweasel
Mon 19:56
Iceweasel
http://urban...ecklogin.php
urbank.com/checklogin.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Type here to search
6:56 PM
11/18/2019

DISPLAYING BROWSER

Now to verify that this control (mysql_real_escape_string function) mitigated the SQLi password bypass attack.

8 **Type** `Alice' OR '1=1` into the Username field and **press** Enter.

Login

Username : Alice' OR '1=1

Password :

Login

RETRYING THE ATTACK

9 **Verify** the attack is no longer successful and **click** the close button o the browser.

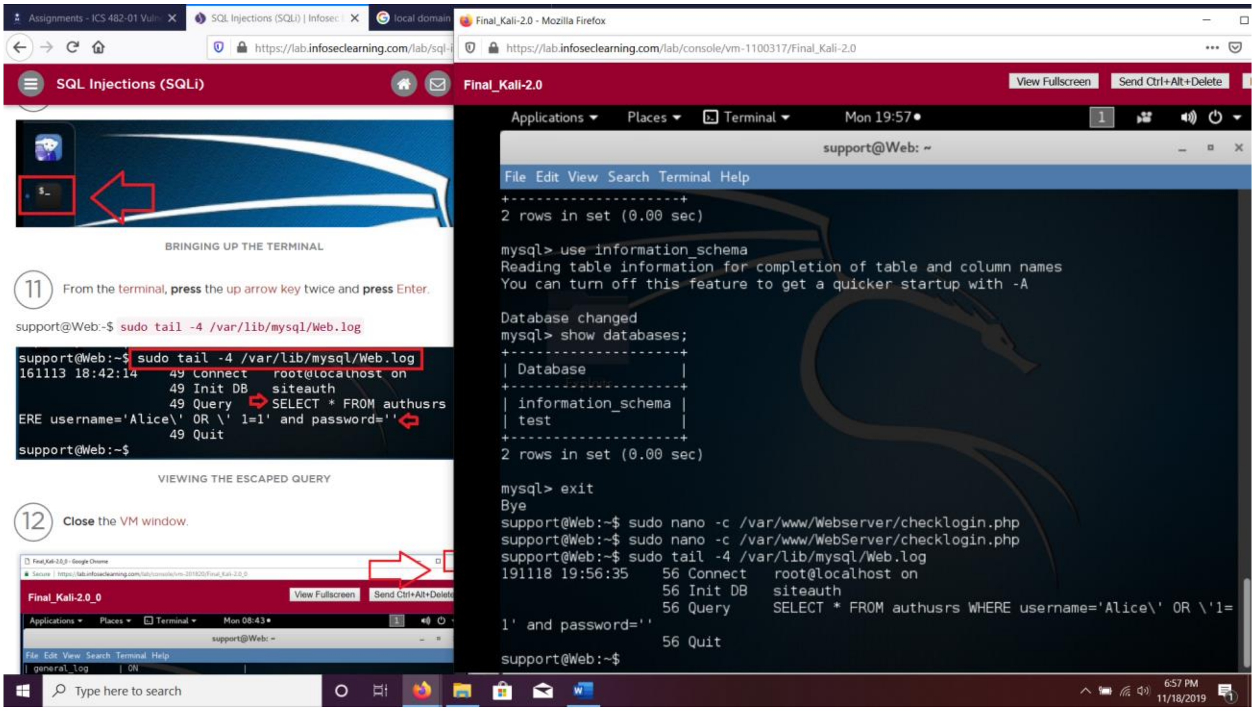
Wrong Username or Password

ATTACK MITIGATED

Wrong Username or Password

It looks like you haven't started Iceweasel in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Iceweasel...


Assignments - ICS 482-01 Vuln
SQL Injections (SQLi) | Infosec
local domain
Final_Kali-2.0 - Mozilla Firefox
https://lab.infoseclearning.com/lab/sql-i
https://lab.infoseclearning.com/lab/console/vm-1100317/Final_Kali-2.0
SQL Injections (SQLi)
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Terminal
Mon 19:57
support@Web: ~
File Edit View Search Terminal Help
Type here to search
6:57 PM
11/18/2019

BRINGING UP THE TERMINAL

11 From the terminal, **press** the up arrow key twice and **press** Enter.

support@Web:-$ `sudo tail -4 /var/lib/mysql/Web.log`

```
support@Web:~$ sudo tail -4 /var/lib/mysql/Web.log
161113 18:42:14     49 Connect   root@localhost on
                    49 Init DB   siteauth
                    49 Query     SELECT * FROM authusrs
ERE username='Alice\' OR \' 1=1' and password=''
                    49 Quit
support@Web:~$
```

VIEWING THE ESCAPED QUERY

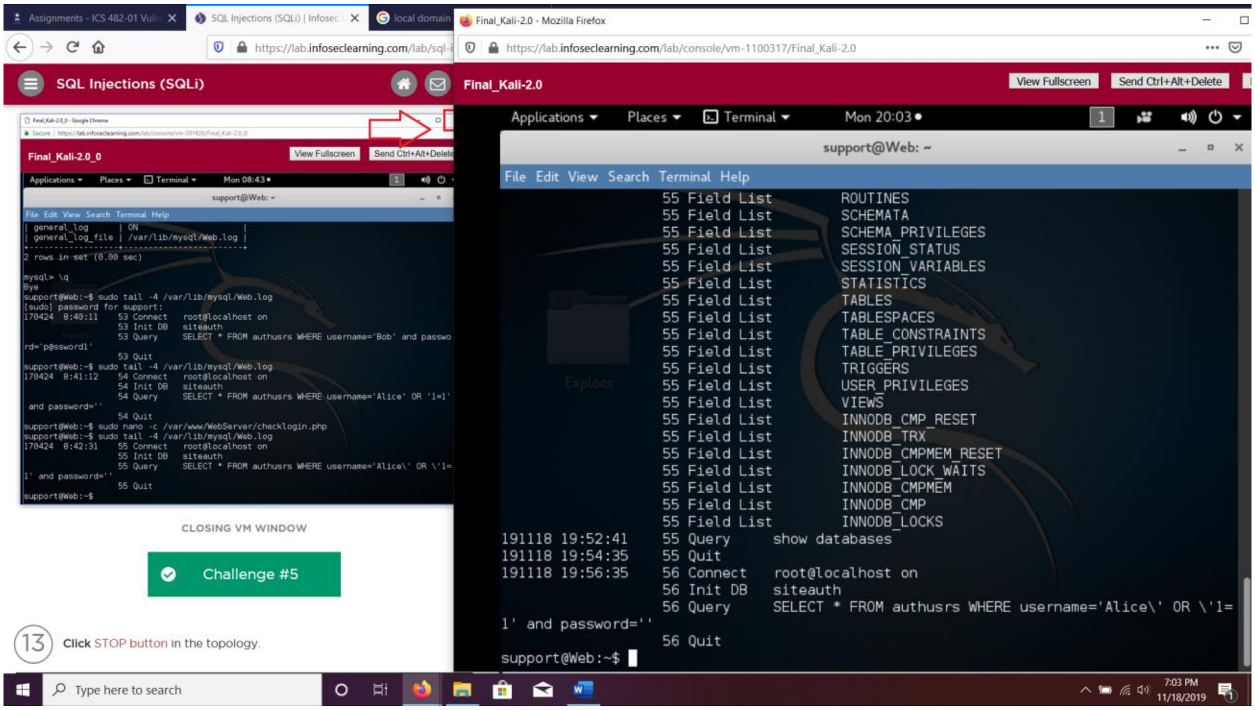
12 **Close** the VM window.

```
+--------------------+
2 rows in set (0.00 sec)

mysql> use information_schema
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| test               |
+--------------------+
2 rows in set (0.00 sec)

mysql> exit
Bye
support@Web:~$ sudo nano -c /var/www/Webserver/checklogin.php
support@Web:~$ sudo nano -c /var/www/WebServer/checklogin.php
support@Web:~$ sudo tail -4 /var/lib/mysql/Web.log
191118 19:56:35     56 Connect   root@localhost on
                    56 Init DB   siteauth
                    56 Query     SELECT * FROM authusrs WHERE username='Alice\' OR \'1=
1' and password=''
                    56 Quit
support@Web:~$
```


Assignments - ICS 482-01 Vuln
SQL Injections (SQLi) | Infosec
local domain
https://lab.infoseclearning.com/lab/sql-i
SQL Injections (SQLi)
Final_Kali-2.0_0 - Google Chrome
Secure | https://lab.infoseclearning.com/lab/console/vm-201820/Final_Kali-2.0_0
Final_Kali-2.0_0
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Terminal
Mon 08:43
support@Web: ~
File Edit View Search Terminal Help

```
| general_log      | ON                    |
| general_log_file | /var/lib/mysql/Web.log |
+------------------+-----------------------+
2 rows in set (0.00 sec)

mysql> \q
Bye
support@Web:~$ sudo tail -4 /var/lib/mysql/Web.log
[sudo] password for support:
170424  8:40:11     53 Connect   root@localhost on
                    53 Init DB   siteauth
                    53 Query     SELECT * FROM authusrs WHERE username='Bob' and passwo
rd='p@ssword1'
                    53 Quit
support@Web:~$ sudo tail -4 /var/lib/mysql/Web.log
170424  8:41:12     54 Connect   root@localhost on
                    54 Init DB   siteauth
                    54 Query     SELECT * FROM authusrs WHERE username='Alice' OR '1=1'
 and password=''
                    54 Quit
support@Web:~$ sudo nano -c /var/www/WebServer/checklogin.php
support@Web:~$ sudo tail -4 /var/lib/mysql/Web.log
170424  8:42:31     55 Connect   root@localhost on
                    55 Init DB   siteauth
                    55 Query     SELECT * FROM authusrs WHERE username='Alice\' OR \'1=
1' and password=''
                    55 Quit
support@Web:~$
```

CLOSING VM WINDOW

13 Click STOP button in the topology.

Final_Kali-2.0 - Mozilla Firefox
https://lab.infoseclearning.com/lab/console/vm-1100317/Final_Kali-2.0
Final_Kali-2.0
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Terminal
Mon 20:03
support@Web: ~
File Edit View Search Terminal Help

```
                         55 Field List       ROUTINES
                         55 Field List       SCHEMATA
                         55 Field List       SCHEMA_PRIVILEGES
                         55 Field List       SESSION_STATUS
                         55 Field List       SESSION_VARIABLES
                         55 Field List       STATISTICS
                         55 Field List       TABLES
                         55 Field List       TABLESPACES
                         55 Field List       TABLE_CONSTRAINTS
                         55 Field List       TABLE_PRIVILEGES
                         55 Field List       TRIGGERS
                         55 Field List       USER_PRIVILEGES
                         55 Field List       VIEWS
                         55 Field List       INNODB_CMP_RESET
                         55 Field List       INNODB_TRX
                         55 Field List       INNODB_CMPMEM_RESET
                         55 Field List       INNODB_LOCK_WAITS
                         55 Field List       INNODB_CMPMEM
                         55 Field List       INNODB_CMP
                         55 Field List       INNODB_LOCKS
191118 19:52:41          55 Query     show databases
191118 19:54:35          55 Quit
191118 19:56:35          56 Connect   root@localhost on
                         56 Init DB   siteauth
                         56 Query     SELECT * FROM authusrs WHERE username='Alice\' OR \'1=
1' and password=''
                         56 Quit
support@Web:~$
```