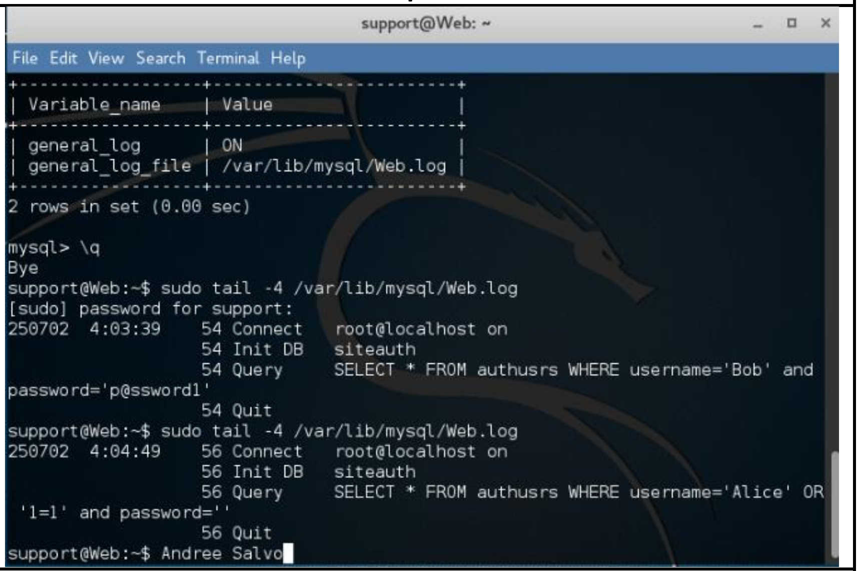
3-1 Lab Worksheet

Andree Salvo
Southern New Hampshire University
CYB 240-13711
Instructor: Brian Remson

Southern
New Hampshire
University

CYB 240 Module Three Lab Worksheet

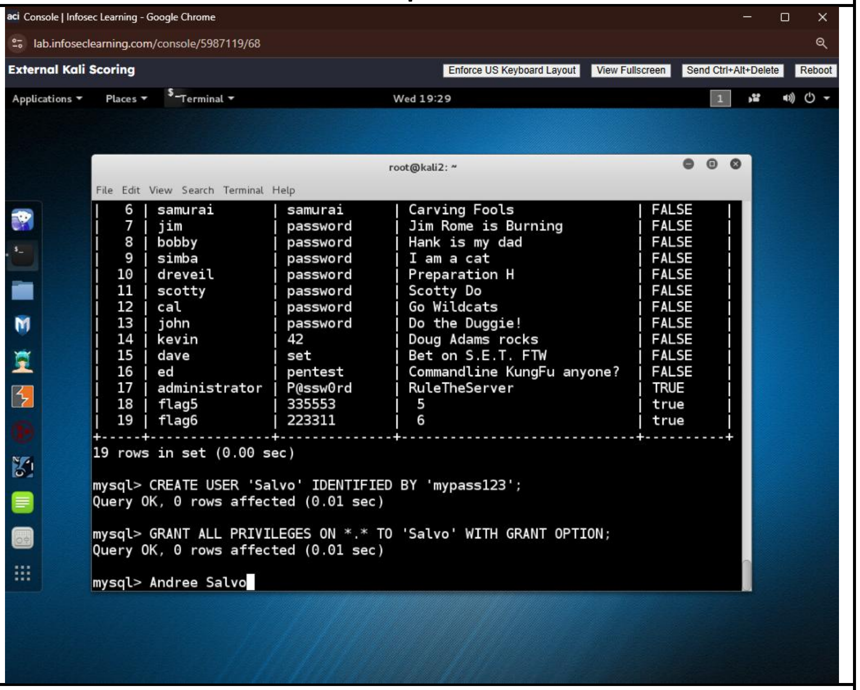
Lab: SQL Injections (SQLi)

Prompt	Response
In the lab section “Analysis of the Vulnerability,” **Step 20**, insert your name at the command line below the output and include it in your screenshot.	
In the lab, we demonstrated the dangers of unsecured input and how it can lead to SQLi. The lab also demonstrated how escaping can be used to mitigate an SQLi password bypass attack. Explain the steps of escaping and why it was successful in mitigating the SQL injection attack.	Escaping worked because it stopped the input from messing with the SQL query. It treated the special characters like normal text so that the injection couldn’t go through.

```
+-----------------+------------------------+
| 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:
250702  4:03:39     54 Connect   root@localhost on
                    54 Init DB   siteauth
                    54 Query     SELECT * FROM authusrs WHERE username='Bob' and
password='p@ssword1'
                    54 Quit
support@Web:~$ sudo tail -4 /var/lib/mysql/Web.log
250702  4:04:49     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:~$ Andree Salvo
```

Lab: Performing SQL Injection to Manipulate Tables in a Database

Prompt	Response
In the lab section “Stealing Data and Creating a Backdoor,” **Step 7**, insert your last name as the user that is created. Also use the name in Step 8. Take a screenshot after Step 8.	
Metasploit is an open source free tool that is shipped with Kali Linux. The tool can also be added to other distributions of Linux. How can this tool be used by security analysts to help secure computer systems that they are responsible for maintaining?	Metasploit is a pen-test tool security analysts use to simulate real-world attacks on the systems they manage. It helps them identify and address any weak spots before a real attacker can exploit them. It’s a go-to tool when they need to tighten up system security.

Console | Infosec Learning - Google Chrome
lab.infoseclearning.com/console/5987119/68
External Kali Scoring
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
Applications
Places
Terminal
Wed 19:29
root@kali2: ~
File Edit View Search Terminal Help

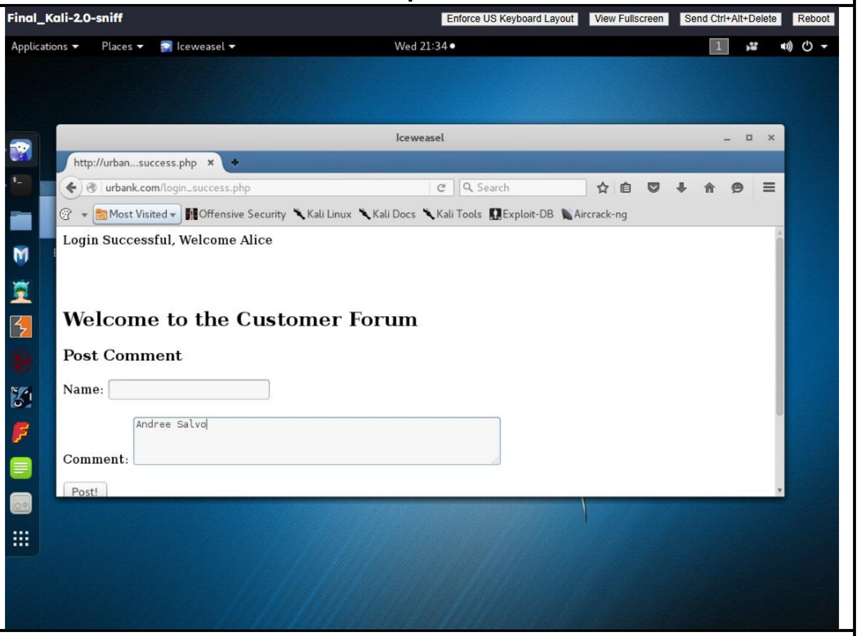
```
|  6 | samurai       | samurai      | Carving Fools              | FALSE    |
|  7 | jim           | password     | Jim Rome is Burning        | FALSE    |
|  8 | bobby         | password     | Hank is my dad             | FALSE    |
|  9 | simba         | password     | I am a cat                 | 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    |
| 17 | administrator | P@ssw0rd     | RuleTheServer              | TRUE     |
| 18 | flag5         | 335553       |  5                         | true     |
| 19 | flag6         | 223311       |  6                         | true     |
+----+---------------+--------------+----------------------------+----------+
19 rows in set (0.00 sec)

mysql> CREATE USER 'Salvo' IDENTIFIED BY 'mypass123';
Query OK, 0 rows affected (0.01 sec)

mysql> GRANT ALL PRIVILEGES ON *.* TO 'Salvo' WITH GRANT OPTION;
Query OK, 0 rows affected (0.01 sec)

mysql> Andree Salvo
```

Lab: Session Stealing (Stored XSS)

Prompt	Response
In the lab section “Alice Gets Owned,” **Step 12**, insert your name in the comment field and then take a screenshot of the dialog.	 Final_Kali-2.0-sniff Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete Reboot Applications Places Iceweasel Wed 21:34 Iceweasel http://urban...success.php urbank.com/login_success.php Search Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Login Successful, Welcome Alice Welcome to the Customer Forum Post Comment Name: Comment: Andree Salvo Post!
In the lab, you learn to exploit stored XSS. What steps can be taken on a form that would prevent the ability of a stored XSS to execute, and how should they be implemented?	To prevent stored XSS, validate and sanitize user input, escape output, and use a Content Security Policy (CSP).