Summary:
I utilized CentOS and Kali Linux to perform SQL injections. On CentOS, I setup a LAMP server, created a database and prepared an index.php file to connect the database to. On Kali Linux, I utilized the GUI to access the index.php and perform SQL injections. Finally, I perform countermeasures to safeguard from the injections.

1. Use one of the VMs as the target and install any application or service such as a web site, a database, a FTP server, a DHCP server, etc. (take screenshots of your set up).
This is the installation of the LAMP server and connection of the database to the index.php

Before installing the LAMP server, I executed 'sudo yum update -y' in order to make sure CentOS is up to date.

```
  Verifying  : selinux-policy-targeted-3.13.1-229.el7.noarch                                    122/129
  Verifying  : 7:lvm2-2.02.180-8.el7.x86_64                                                     123/129
  Verifying  : glibc-common-2.17-260.el7.x86_64                                                 124/129
  Verifying  : tzdata-2018e-3.el7.noarch                                                        125/129
  Verifying  : 1:NetworkManager-libnm-1.12.0-6.el7.x86_64                                       126/129
  Verifying  : polkit-0.112-18.el7.x86_64                                                       127/129
  Verifying  : cronie-1.4.11-19.el7.x86_64                                                      128/129
  Verifying  : ipset-libs-6.38-2.el7.x86_64                                                     129/129

Installed:
  kernel.x86_64 0:3.10.0-957.12.1.el7

Updated:
  NetworkManager.x86_64 1:1.12.0-10.el7_6                    NetworkManager-libnm.x86_64 1:1.12.0-10.el7_6
  NetworkManager-team.x86_64 1:1.12.0-10.el7_6               NetworkManager-tui.x86_64 1:1.12.0-10.el7_6
  bind-libs-lite.x86_64 32:9.9.4-73.el7_6                    bind-license.noarch 32:9.9.4-73.el7_6
  cronie.x86_64 0:1.4.11-20.el7_6                            cronie-anacron.x86_64 0:1.4.11-20.el7_6
  dbus.x86_64 1:1.10.24-13.el7_6                             dbus-libs.x86_64 1:1.10.24-13.el7_6
  device-mapper.x86_64 7:1.02.149-10.el7_6.7                 device-mapper-event.x86_64 7:1.02.149-10.el7_6.7
  device-mapper-event-libs.x86_64 7:1.02.149-10.el7_6.7      device-mapper-libs.x86_64 7:1.02.149-10.el7_6.7
  freetype.x86_64 0:2.8-12.el7_6.1                           glibc.x86_64 0:2.17-260.el7_6.4
  glibc-common.x86_64 0:2.17-260.el7_6.4                     grub2.x86_64 1:2.02-0.76.el7.centos.1
  grub2-common.noarch 1:2.02-0.76.el7.centos.1               grub2-pc.x86_64 1:2.02-0.76.el7.centos.1
  grub2-pc-modules.noarch 1:2.02-0.76.el7.centos.1           grub2-tools.x86_64 1:2.02-0.76.el7.centos.1
  grub2-tools-extra.x86_64 1:2.02-0.76.el7.centos.1          grub2-tools-minimal.x86_64 1:2.02-0.76.el7.centos.1
  iproute.x86_64 0:4.11.0-14.el7_6.2                         ipset.x86_64 0:6.38-3.el7_6
  ipset-libs.x86_64 0:6.38-3.el7_6                           kernel-tools.x86_64 0:3.10.0-957.12.1.el7
  kernel-tools-libs.x86_64 0:3.10.0-957.12.1.el7             kexec-tools.x86_64 0:2.0.15-21.el7_6.3
  krb5-libs.x86_64 0:1.15.1-37.el7_6                         libblkid.x86_64 0:2.23.2-59.el7_6.1
  libgcc.x86_64 0:4.8.5-36.el7_6.2                           libgomp.x86_64 0:4.8.5-36.el7_6.2
  libmount.x86_64 0:2.23.2-59.el7_6.1                        libsmartcols.x86_64 0:2.23.2-59.el7_6.1
  libssh2.x86_64 0:1.4.3-12.el7_6.2                          libstdc++.x86_64 0:4.8.5-36.el7_6.2
  libuuid.x86_64 0:2.23.2-59.el7_6.1                         lvm2.x86_64 7:2.02.180-10.el7_6.7
  lvm2-libs.x86_64 7:2.02.180-10.el7_6.7                     nss.x86_64 0:3.36.0-7.1.el7_6
  nss-pem.x86_64 0:1.0.3-5.el7_6.1                           nss-sysinit.x86_64 0:3.36.0-7.1.el7_6
  nss-tools.x86_64 0:3.36.0-7.1.el7_6                        nss-util.x86_64 0:3.36.0-1.1.el7_6
  openldap.x86_64 0:2.4.44-21.el7_6                          openssl.x86_64 1:1.0.2k-16.el7_6.1
  openssl-libs.x86_64 1:1.0.2k-16.el7_6.1                    policycoreutils.x86_64 0:2.5-29.el7_6.1
  polkit.x86_64 0:0.112-18.el7_6.1                           python.x86_64 0:2.7.5-77.el7_6
  python-libs.x86_64 0:2.7.5-77.el7_6                        python-perf.x86_64 0:3.10.0-957.12.1.el7
  selinux-policy.noarch 0:3.13.1-229.el7_6.12                selinux-policy-targeted.noarch 0:3.13.1-229.el7_6.12
  shadow-utils.x86_64 2:4.1.5.1-25.el7_6.1                   systemd.x86_64 0:219-62.el7_6.6
  systemd-libs.x86_64 0:219-62.el7_6.6                       systemd-sysv.x86_64 0:219-62.el7_6.6
  tuned.noarch 0:2.10.0-6.el7_6.3                            tzdata.noarch 0:2019a-1.el7
  util-linux.x86_64 0:2.23.2-59.el7_6.1                      xfsprogs.x86_64 0:4.5.0-19.el7_6

Complete!
[sysadmin@server0 ~]$ _
```

Once everything is updated, I began by installing apache: ‘Sudo yum install httpd -y’.

```
================================================================================================================================================
 Package                          Arch                     Version                                    Repository                          Size
================================================================================================================================================
Installing:
 httpd                            x86_64                   2.4.6-89.el7.centos                        updates                            2.7 M
Installing for dependencies:
 apr                              x86_64                   1.4.8-3.el7_4.1                            base                               103 k
 apr-util                         x86_64                   1.5.2-6.el7                                base                                92 k
 httpd-tools                      x86_64                   2.4.6-89.el7.centos                        updates                            90 k
 mailcap                          noarch                   2.1.41-2.el7                               base                               31 k

Transaction Summary
================================================================================================================================================
Install  1 Package (+4 Dependent packages)

Total download size: 3.0 M
Installed size: 10 M
Downloading packages:
(1/5): mailcap-2.1.41-2.el7.noarch.rpm                                                                  |  31 kB  00:00:00
(2/5): apr-util-1.5.2-6.el7.x86_64.rpm                                                                  |  92 kB  00:00:00
(3/5): httpd-tools-2.4.6-89.el7.centos.x86_64.rpm                                                       |  90 kB  00:00:00
(4/5): apr-1.4.8-3.el7_4.1.x86_64.rpm                                                                   | 103 kB  00:00:00
(5/5): httpd-2.4.6-89.el7.centos.x86_64.rpm                                                             | 2.7 MB  00:00:00
------------------------------------------------------------------------------------------------------------------------------------------------
Total                                                                                        3.1 MB/s | 3.0 MB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : apr-1.4.8-3.el7_4.1.x86_64                                                                                                   1/5
  Installing : apr-util-1.5.2-6.el7.x86_64                                                                                                  2/5
  Installing : httpd-tools-2.4.6-89.el7.centos.x86_64                                                                                       3/5
  Installing : mailcap-2.1.41-2.el7.noarch                                                                                                  4/5
  Installing : httpd-2.4.6-89.el7.centos.x86_64                                                                                             5/5
  Verifying  : httpd-tools-2.4.6-89.el7.centos.x86_64                                                                                       1/5
  Verifying  : mailcap-2.1.41-2.el7.noarch                                                                                                  2/5
  Verifying  : httpd-2.4.6-89.el7.centos.x86_64                                                                                             3/5
  Verifying  : apr-1.4.8-3.el7_4.1.x86_64                                                                                                   4/5
  Verifying  : apr-util-1.5.2-6.el7.x86_64                                                                                                  5/5

Installed:
  httpd.x86_64 0:2.4.6-89.el7.centos

Dependency Installed:
  apr.x86_64 0:1.4.8-3.el7_4.1        apr-util.x86_64 0:1.5.2-6.el7        httpd-tools.x86_64 0:2.4.6-89.el7.centos        mailcap.noarch 0:2.1.41-2.el7

Complete!
[sysadmin@server0 ~]$
```

To check if apache was installed I needed to make sure the virtual machines were able to communicate with one another, so I added another network adapter to each and set them to vmnet2.
Then, on CentOS: ‘Sudo vi /etc/sysconfig/network-scripts/ifcfg-ens37’, to configure a static IP address. In this case I used 192.168.1.2.

```
DEVICE="ens37"
ONBOOT="yes"
BOOTPROTO="static"
IPADDR=192.168.1.2
NETMASK=255.255.255.0
~
~
```

On Kali Linux: ‘Sudo vi /etc/network/interfaces’, to configure a static IP address. For Kali I used 192.168.1.1.

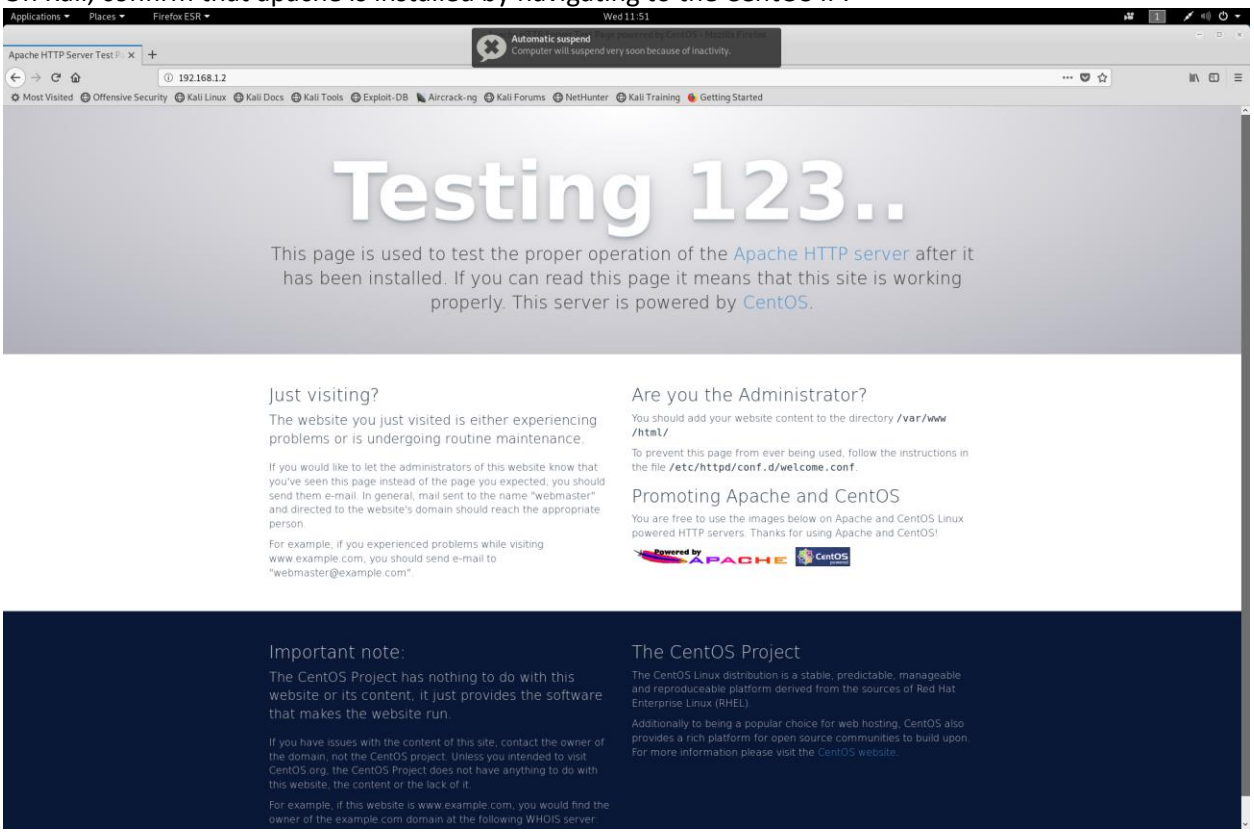
```
Applications ▾   Places ▾   Terminal ▾                    Wed 11:42
File  Edit  View  Search  Terminal  Help                  root@kali: ~
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth1
iface eth1 inet static
address 192.168.1.1/24
```

Automatic suspend
Computer will suspend very soon because of inactivity.

Once the networks are configured, restart each one to ensure the networks are updated. Then, on CentOS configure the firewall to allow apache through: ‘sudo firewall-cmd –permanent –add-service=http’. Then, restart the firewall.

```
[sysadmin@server0 ~]$ sudo firewall-cmd --permanent --add-service=http
success
[sysadmin@server0 ~]$ sudo firewall-cmd --reload
success
[sysadmin@server0 ~]$ _
```

On Kali, confirm that apache is installed by navigating to the CentOS IP.



To ensure apache is activated on system startup: 'Sudo systemctl enable httpd.service'

```
[sysadmin@server0 ~]$ sudo systemctl enable httpd.service
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[sysadmin@server0 ~]$ _
```

Now, time to install the database: ‘Sudo yum install maria-server mariadb –y’.

```
  Verifying  : 1:perl-parent-0.225-244.el7.noarch                                                    10/37
  Verifying  : 4:perl-5.16.3-294.el7_6.x86_64                                                        11/37
  Verifying  : perl-Net-Daemon-0.48-5.el7.noarch                                                     12/37
  Verifying  : 4:perl-libs-5.16.3-294.el7_6.x86_64                                                   13/37
  Verifying  : perl-File-Temp-0.23.01-3.el7.noarch                                                   14/37
  Verifying  : 1:perl-Pod-Simple-3.28-4.el7.noarch                                                   15/37
  Verifying  : perl-Time-Local-1.2300-2.el7.noarch                                                   16/37
  Verifying  : perl-DBI-1.627-4.el7.x86_64                                                           17/37
  Verifying  : 4:perl-macros-5.16.3-294.el7_6.x86_64                                                 18/37
  Verifying  : perl-Socket-2.010-4.el7.x86_64                                                        19/37
  Verifying  : perl-Encode-2.51-7.el7.x86_64                                                         20/37
  Verifying  : perl-Carp-1.26-244.el7.noarch                                                         21/37
  Verifying  : perl-Data-Dumper-2.145-3.el7.x86_64                                                   22/37
  Verifying  : 4:perl-Time-HiRes-1.9725-3.el7.x86_64                                                 23/37
  Verifying  : perl-Scalar-List-Utils-1.27-248.el7.x86_64                                            24/37
  Verifying  : 1:perl-Compress-Raw-Zlib-2.061-4.el7.x86_64                                           25/37
  Verifying  : perl-IO-Compress-2.061-2.el7.noarch                                                   26/37
  Verifying  : perl-Pod-Usage-1.63-3.el7.noarch                                                      27/37
  Verifying  : perl-PIRPC-0.2020-14.el7.noarch                                                       28/37
  Verifying  : 1:mariadb-server-5.5.60-1.el7_5.x86_64                                                29/37
  Verifying  : perl-Pod-Perldoc-3.20-4.el7.noarch                                                    30/37
  Verifying  : perl-podlators-2.5.1-3.el7.noarch                                                     31/37
  Verifying  : perl-File-Path-2.09-2.el7.noarch                                                      32/37
  Verifying  : perl-threads-1.87-4.el7.x86_64                                                        33/37
  Verifying  : perl-Filter-1.49-3.el7.x86_64                                                         34/37
  Verifying  : perl-Getopt-Long-2.40-3.el7.noarch                                                    35/37
  Verifying  : perl-Text-ParseWords-3.29-4.el7.noarch                                                36/37
  Verifying  : 1:mariadb-5.5.60-1.el7_5.x86_64                                                       37/37

Installed:
  mariadb.x86_64 1:5.5.60-1.el7_5                                       mariadb-server.x86_64 1:5.5.60-1.el7_5

Dependency Installed:
  perl.x86_64 4:5.16.3-294.el7_6                perl-Carp.noarch 0:1.26-244.el7                    perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7
  perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7   perl-DBD-MySQL.x86_64 0:4.023-6.el7                perl-DBI.x86_64 0:1.627-4.el7
  perl-Data-Dumper.x86_64 0:2.145-3.el7         perl-Encode.x86_64 0:2.51-7.el7                    perl-Exporter.noarch 0:5.68-3.el7
  perl-File-Path.noarch 0:2.09-2.el7            perl-File-Temp.noarch 0:0.23.01-3.el7              perl-Filter.x86_64 0:1.49-3.el7
  perl-Getopt-Long.noarch 0:2.40-3.el7          perl-HTTP-Tiny.noarch 0:0.033-3.el7                perl-IO-Compress.noarch 0:2.061-2.el7
  perl-Net-Daemon.noarch 0:0.48-5.el7           perl-PathTools.x86_64 0:3.40-5.el7                 perl-PIRPC.noarch 0:0.2020-14.el7
  perl-Pod-Escapes.noarch 1:1.04-294.el7_6      perl-Pod-Perldoc.noarch 0:3.20-4.el7               perl-Pod-Simple.noarch 1:3.28-4.el7
  perl-Pod-Usage.noarch 0:1.63-3.el7            perl-Scalar-List-Utils.x86_64 0:1.27-248.el7       perl-Socket.x86_64 0:2.010-4.el7
  perl-Storable.x86_64 0:2.45-3.el7             perl-Text-ParseWords.noarch 0:3.29-4.el7           perl-Time-HiRes.x86_64 4:1.9725-3.el7
  perl-Time-Local.noarch 0:1.2300-2.el7         perl-constant.noarch 0:1.27-2.el7                  perl-libs.x86_64 4:5.16.3-294.el7_6
  perl-macros.x86_64 4:5.16.3-294.el7_6         perl-parent.noarch 1:0.225-244.el7                 perl-podlators.noarch 0:2.5.1-3.el7
  perl-threads.x86_64 0:1.87-4.el7              perl-threads-shared.x86_64 0:1.43-6.el7

Complete!
[sysadmin@server0 ~]$ _
```

Once mariadb is installed: ‘sudo systemctl start mariadb’, to start the it.

Then, execute: ‘sudo mysql_secure_installation’, to configure the mariadb settings.

Finally, execute: ‘sudo systemctl enable mariadb.service’, to enable activation upon system start up.

```
Set root password? [Y/n] Y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] Y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] Y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] Y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] Y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
[sysadmin@server0 ~]$ sudo systemctl enable mariadb.service
Created symlink from /etc/systemd/system/multi-user.target.wants/mariadb.service to /usr/lib/systemd/system/mariadb.service.
[sysadmin@server0 ~]$
```

Once mariadb is installed we can now create the database.
So, to login: ‘mysql -u root -p’, and once logged in create a database: ‘CREATE DATABASE <NAME>’. For this assignment I simply named the database ‘FinalProject’.

```
[sysadmin@server0 ~]$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 11
Server version: 5.5.60-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> CREATE DATABASE FinalProject;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> USE FinalProject;
Database changed
MariaDB [FinalProject]> SHOW TABLES;
Empty set (0.00 sec)

MariaDB [FinalProject]>
```

To fill the database I created two files.
‘CreateTables.sql’ for the structure of the database

```
DROP TABLE IF EXISTS User;

CREATE TABLE User (
        UserID INT AUTO_INCREMENT,
        Name VARCHAR(50),
        Email VARCHAR(50),
        CONSTRAINT PKUser PRIMARY KEY (UserID)
);
```

‘TestData.sql’ to populate the database

```
INSERT INTO User (UserID, Name, Email) VALUES ("", "TestOne", "TestOne@TestOne.com");
INSERT INTO User (UserID, Name, Email) VALUES ("", "TestTwo", "TestTwo@TestTwo.com");
```

To import the files into the database:
‘mysql –u root –p FinalProject < CreateTables.sql’

```
[sysadmin@server0 ~]$ mysql -u root -p FinalProject < CreateTables.sql
Enter password:
[sysadmin@server0 ~]$ _
```

‘mysql –u root –p FinalProject < TestData.sql’

```
[sysadmin@server0 ~]$ mysql -u root -p FinalProject < TestData.sql
Enter password:
[sysadmin@server0 ~]$ _
```

Database confirmation

```
[sysadmin@server0 ~]$ mysql -u root -p FinalProject
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 15
Server version: 5.5.60-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [FinalProject]> SELECT * FROM User;
+--------+---------+---------------------+
| UserID | Name    | Email               |
+--------+---------+---------------------+
|      1 | TestOne | TestOne@TestOne.com |
|      2 | TestTwo | TestTwo@TestTwo.com |
+--------+---------+---------------------+
2 rows in set (0.00 sec)

MariaDB [FinalProject]>
```

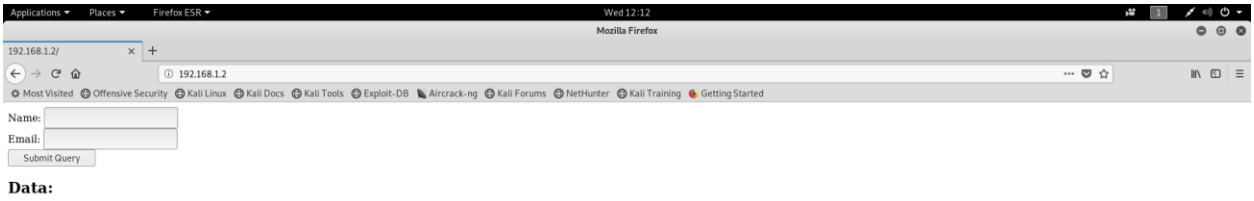
Continuing with the LAMP server, it is now time to install PHP: ‘Sudo yum install php php-mysql -y’

```
 php-mysql                          x86_64                          5.4.16-46.el7                          base                          101 k
Installing for dependencies:
 libzip                             x86_64                          0.10.1-8.el7                           base                           48 k
 php-cli                            x86_64                          5.4.16-46.el7                          base                          2.7 M
 php-common                         x86_64                          5.4.16-46.el7                          base                          565 k
 php-pdo                            x86_64                          5.4.16-46.el7                          base                           99 k

Transaction Summary
================================================================================================================================================
Install  2 Packages (+4 Dependent packages)

Total download size: 4.9 M
Installed size: 18 M
Is this ok [y/d/N]: y
Downloading packages:
(1/6): libzip-0.10.1-8.el7.x86_64.rpm                                                                                   |  48 kB  00:00:00
(2/6): php-mysql-5.4.16-46.el7.x86_64.rpm                                                                               | 101 kB  00:00:00
(3/6): php-pdo-5.4.16-46.el7.x86_64.rpm                                                                                 |  99 kB  00:00:00
(4/6): php-5.4.16-46.el7.x86_64.rpm                                                                                     | 1.4 MB  00:00:01
(5/6): php-cli-5.4.16-46.el7.x86_64.rpm                                                                                 | 2.7 MB  00:00:02
(6/6): php-common-5.4.16-46.el7.x86_64.rpm                                                                              | 565 kB  00:00:02
------------------------------------------------------------------------------------------------------------------------------------------------
Total                                                                                                          1.8 MB/s | 4.9 MB  00:00:02
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : libzip-0.10.1-8.el7.x86_64                                                                                                   1/6
  Installing : php-common-5.4.16-46.el7.x86_64                                                                                              2/6
  Installing : php-pdo-5.4.16-46.el7.x86_64                                                                                                 3/6
  Installing : php-cli-5.4.16-46.el7.x86_64                                                                                                 4/6
  Installing : php-5.4.16-46.el7.x86_64                                                                                                     5/6
  Installing : php-mysql-5.4.16-46.el7.x86_64                                                                                               6/6
  Verifying  : php-mysql-5.4.16-46.el7.x86_64                                                                                               1/6
  Verifying  : php-pdo-5.4.16-46.el7.x86_64                                                                                                 2/6
  Verifying  : php-cli-5.4.16-46.el7.x86_64                                                                                                 3/6
  Verifying  : libzip-0.10.1-8.el7.x86_64                                                                                                   4/6
  Verifying  : php-5.4.16-46.el7.x86_64                                                                                                     5/6
  Verifying  : php-common-5.4.16-46.el7.x86_64                                                                                              6/6

Installed:
  php.x86_64 0:5.4.16-46.el7                                            php-mysql.x86_64 0:5.4.16-46.el7

Dependency Installed:
  libzip.x86_64 0:0.10.1-8.el7        php-cli.x86_64 0:5.4.16-46.el7        php-common.x86_64 0:5.4.16-46.el7        php-pdo.x86_64 0:5.4.16-46.el7

Complete!
[sysadmin@server0 ~]$
```

Create a PHP file to test: ‘Sudo vi /var/www/html/index.php’

```
<!DOCTYP HTML>
<html>

<head>
</head>

<style>
</style>

<body>

<form method="post" action="">
Name: <input type="text" name="name">
<br>
Email: <input type="text" name="email">
<br>
<input type="submit">
</form>

<?php
echo "<h2>Data:</h2>";
?>

</body>
</html>
```

PHP confirmation

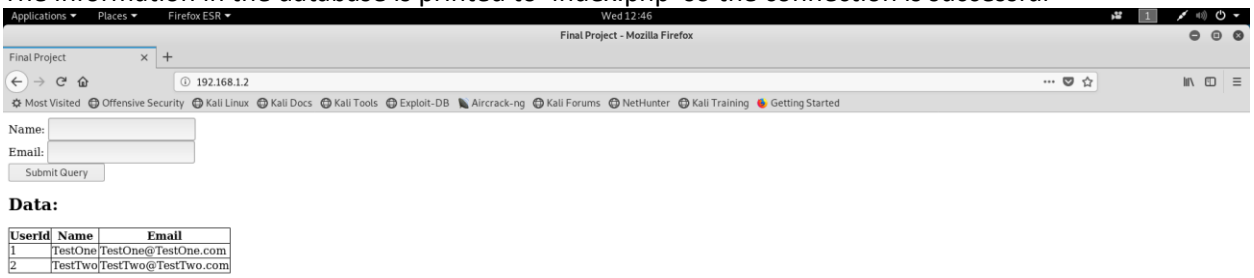


Now, I will link ‘index.php’ to the database

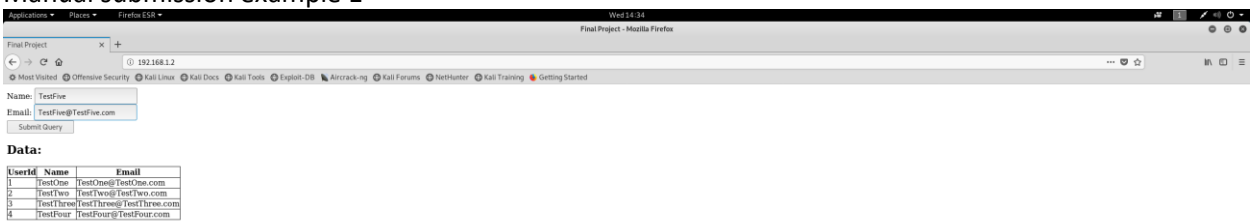
```
<!DOCTYPE HTML>
<html>

<title>
Final Project
</title>

<head>
</head>

<style>

table, th, td {
        border: 1px solid black;
}

table {
        border-collapse: collapse;
}

</style>

<body>

<form method="post" action="">
Name: <input type="text" name="name">
<br>
Email: <input type="text" name="email">
<br>
<input type="submit" name="submit">
</form>

<?php
// Database credentials
$dbhost = "localhost";
$dbusername = "root";
$dbpassword = "Asdfzxcv17";
$dbname = "FinalProject";
// Create connection
$conn = new mysqli($dbhost, $dbusername, $dbpassword, $dbname);

// Form to database
$name = $_POST['name'];
$email = $_POST['email'];

if (isset($_POST['submit'])) {
        $insert = "INSERT INTO User (UserID, Name, Email) VALUES ('', '$name', '$email')";
"/var/www/html/index.php" 69L, 1203C
<body>

<form method="post" action="">
Name: <input type="text" name="name">
<br>
Email: <input type="text" name="email">
<br>
<input type="submit" name="submit">
</form>

<?php
// Database credentials
$dbhost = "localhost";
$dbusername = "root";
$dbpassword = "Asdfzxcv17";
$dbname = "FinalProject";
// Create connection
$conn = new mysqli($dbhost, $dbusername, $dbpassword, $dbname);

// Form to database
$name = $_POST['name'];
$email = $_POST['email'];

if (isset($_POST['submit'])) {
        $insert = "INSERT INTO User (UserID, Name, Email) VALUES ('', '$name', '$email')";
        $conn->query($insert);
}

echo "<h2>Data:</h2>";
$sql = "SELECT * FROM User";
$result = mysqli_query($conn, $sql);

// Output
if($result->num_rows > 0) {
        echo "<table><tr><th>UserId</th><th>Name</th><th>Email</th></tr>";
        while($row = $result->fetch_assoc()) {
                echo "<tr><td>" .$row["UserID"]. "</td><td>" .$row["Name"]. "</td><td>" .$row["Email"]. "</td></tr>";
        }
        echo "</table>";
} else {
        echo "0 results";
}
$conn->close();
?>

</body>
</html>
```

Index.php connection to database confirmation

The information in the database is printed to ‘index.php’ so the connection is successful



Manual submission example 1



Manual submission example 2

Manual submission confirmation

The information that was manually inputted from Kali is stored in the database.

```
[sysadmin@server0 ~]$ mysql -u root -p FinalProject
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 110
Server version: 5.5.60-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [FinalProject]> SELECT * FROM User;
+--------+----------+-------------------------+
| UserID | Name     | Email                   |
+--------+----------+-------------------------+
|      1 | TestOne  | TestOne@TestOne.com     |
|      2 | TestTwo  | TestTwo@TestTwo.com     |
|      3 | TestThree | TestThree@TestThree.com |
|      4 | TestFour | TestFour@TestFour.com   |
|      5 | TestFive | TestFive@TestFive.com   |
+--------+----------+-------------------------+
5 rows in set (0.00 sec)

MariaDB [FinalProject]>
```

2. Use the second VM as the attacker and execute/extend any attack (that we did not cover in classes) such as Denial of Service Attack, SQL injection, Cross Site Scripting XSS, Form Tampering, etc. (take screenshots of your attacks).

Now that ‘index.php’ and the database are linked together it is time to perform SQL injections.

For the first injection I entered: “'); ALTER TABLE User ADD TestColumn VARCHAR(50);”

In the mariadb I include the previous table to ensure that SQL injection was performed on the Kali linux side and not within CentOS. So, as seen the table was altered and another column was added due to the SQL injection.

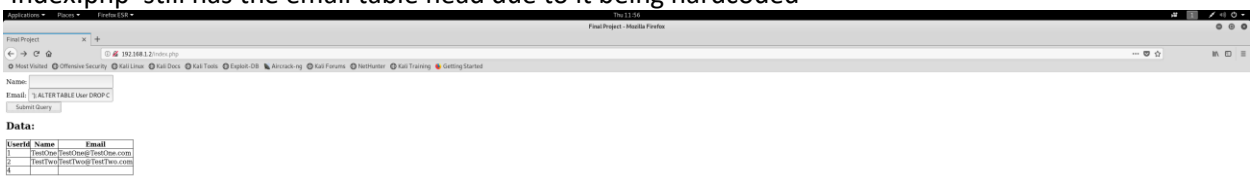
```
[sysadmin@server0 ~]$ mysql -u root -p FinalProject
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 20
Server version: 5.5.60-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [FinalProject]> SELECT * FROM User;
+--------+---------+---------------------+
| UserID | Name    | Email               |
+--------+---------+---------------------+
|      1 | TestOne | TestOne@TestOne.com |
|      2 | TestTwo | TestTwo@TestTwo.com |
+--------+---------+---------------------+
2 rows in set (0.00 sec)

MariaDB [FinalProject]> SELECT * FROM User;
+--------+---------+---------------------+------------+
| UserID | Name    | Email               | TestColumn |
+--------+---------+---------------------+------------+
|      1 | TestOne | TestOne@TestOne.com | NULL       |
|      2 | TestTwo | TestTwo@TestTwo.com | NULL       |
|      3 |         |                     | NULL       |
+--------+---------+---------------------+------------+
3 rows in set (0.00 sec)

MariaDB [FinalProject]>
```

The second injection: “'); DELETE FROM User WHERE UserID=3;”

Again, the previous table and the following table after the SQL injection showing the row with UserID=3 being deleted.

```
[sysadmin@server0 ~]$ mysql -u root -p FinalProject
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 5.5.60-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [FinalProject]> SELECT * FROM User;
+--------+---------+---------------------+------------+
| UserID | Name    | Email               | TestColumn |
+--------+---------+---------------------+------------+
|      1 | TestOne | TestOne@TestOne.com | NULL       |
|      2 | TestTwo | TestTwo@TestTwo.com | NULL       |
|      3 |         |                     | NULL       |
+--------+---------+---------------------+------------+
3 rows in set (0.00 sec)

MariaDB [FinalProject]> SELECT * FROM User;
+--------+---------+---------------------+------------+
| UserID | Name    | Email               | TestColumn |
+--------+---------+---------------------+------------+
|      1 | TestOne | TestOne@TestOne.com | NULL       |
|      2 | TestTwo | TestTwo@TestTwo.com | NULL       |
|      4 |         |                     | NULL       |
+--------+---------+---------------------+------------+
3 rows in set (0.00 sec)

MariaDB [FinalProject]>
```

The third injection: “'); ALTER TABLE User DROP COLUMN Email;”
‘Index.php’ still has the email table head due to it being hardcoded



However, in the database the column ‘Email’ is removed.

```
MariaDB [FinalProject]> SELECT * FROM User;
+--------+---------+---------------------+------------+
| UserID | Name    | Email               | TestColumn |
+--------+---------+---------------------+------------+
|      1 | TestOne | TestOne@TestOne.com | NULL       |
|      2 | TestTwo | TestTwo@TestTwo.com | NULL       |
|      4 |         |                     | NULL       |
+--------+---------+---------------------+------------+
3 rows in set (0.00 sec)

MariaDB [FinalProject]> SELECT * FROM User;
+--------+---------+------------+
| UserID | Name    | TestColumn |
+--------+---------+------------+
|      1 | TestOne | NULL       |
|      2 | TestTwo | NULL       |
|      4 |         | NULL       |
|      5 |         | NULL       |
+--------+---------+------------+
4 rows in set (0.00 sec)

MariaDB [FinalProject]> _
```

3. After that, implement countermeasures in the target system to prevent/stop the attack that you perform previously. (take screenshots of the implemented countermeasures, and of the new attempt of attack showing that it failed).

Now it is time to enable countermeasures to prevent the SQL injections that have just occurred.

Lines 26 and 28 I ensured that the Name and Email forms were required to prevent blank submissions.

Lines 43 and 44 I utilize mysqli_real_escape_string() to escape an special characters in the string.

It is always important to sanitize input. In addition to mysqli_real_escape_string() I could have also used trim() or htmlspecialchars() for the $name variable to remove white spaces or numbers for this variable as names typically do not have spaces or numbers.

Lines 47-50 is input validation for the email to ensure a valid email format is inputted.

It is also important to validate input as well. In addition to validating the email, I could have also validated overlapping usernames if the website were more than just for testing purposes as usernames should typically be unique.

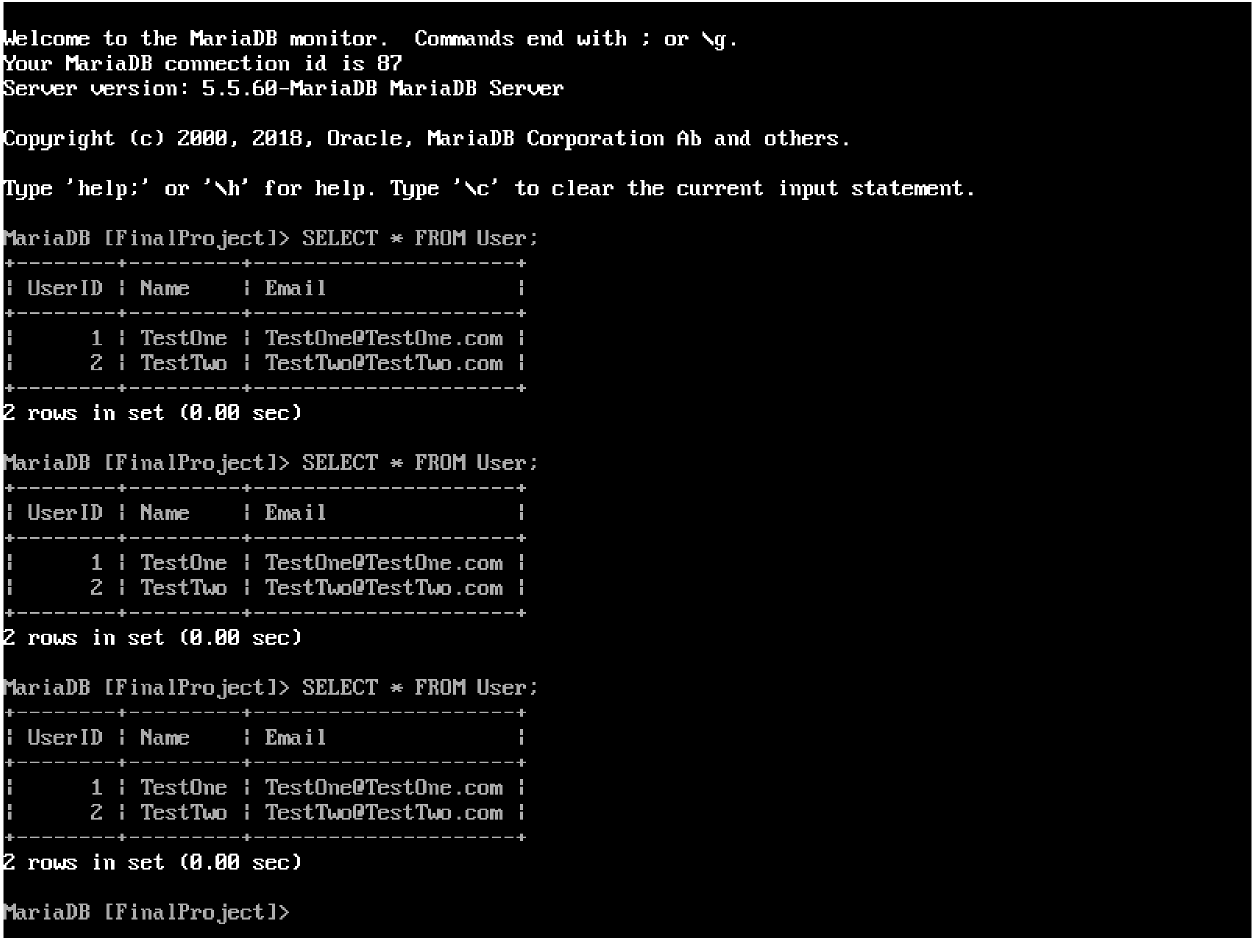
Lines 52-54 is the utilization of prepared statements rather than the previously used execution of SQL statements. Prepared statements transfer the variables using a different protocol than mysqli so the user input does not need to be escaped correctly as before.

```
 1 <!DOCTYPE HTML>
 2 <html>
 3
 4 <title>
 5 Final Project
 6 </title>
 7
 8 <head>
 9 </head>
10
11 <style>
12
13 table, th, td {
14         border: 1px solid black;
15 }
16
17 table {
18         border-collapse: collapse;
19 }
20
21 </style>
22
23 <body>
24
25 <form method="post" action="">
26 Name: <input type="text" name="name" required>
27 <br>
28 Email: <input type="text" name="email" required>
29 <br>
30 <input type="submit" name="submit">
31 </form>
32
33 <?php
34 // Database credentials
35 $dbhost = "localhost";
36 $dbusername = "root";
:set number
```

```php
$dbpassword = "Asdfzxcv17";
$dbname = "FinalProject";
// Create connection
$conn = new mysqli($dbhost, $dbusername, $dbpassword, $dbname);

// Form to database
$name = $conn->real_escape_string($_POST['name']);
$email = $conn->real_escape_string($_POST['email']);

if (isset($_POST['submit'])) {
        // Email validation
        if(!filter_var($email, FILTER_VALIDATE_EMAIL)) {
                exit;
        }

        $stmt = $conn->prepare("INSERT INTO User (UserID, Name, Email) VALUES (?, ?, ?)");
        $stmt->bind_param("iss", $userid, $name, $email);
        $stmt->execute();
}

echo "<h2>Data:</h2>";
$sql = "SELECT * FROM User";
$result = mysqli_query($conn, $sql);

// Output
if($result->num_rows > 0) {
        echo "<table><tr><th>UserId</th><th>Name</th><th>Email</th></tr>";
        while($row = $result->fetch_assoc()) {
                echo "<tr><td>" .$row["UserID"]. "</td><td>" .$row["Name"]. "</td><td>" .$row["Email"]. "</td></tr>";
        }
        echo "</table>";
} else {
        echo "0 results";
}

```

Execution of the same SQL injections from step 2.

The database for each time an attempt of SQL injection occurs and that it remains the same.



```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 87
Server version: 5.5.60-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [FinalProject]> SELECT * FROM User;
+--------+---------+---------------------+
¦ UserID ¦ Name    ¦ Email               ¦
+--------+---------+---------------------+
¦      1 ¦ TestOne ¦ TestOne@TestOne.com ¦
¦      2 ¦ TestTwo ¦ TestTwo@TestTwo.com ¦
+--------+---------+---------------------+
2 rows in set (0.00 sec)

MariaDB [FinalProject]> SELECT * FROM User;
+--------+---------+---------------------+
¦ UserID ¦ Name    ¦ Email               ¦
+--------+---------+---------------------+
¦      1 ¦ TestOne ¦ TestOne@TestOne.com ¦
¦      2 ¦ TestTwo ¦ TestTwo@TestTwo.com ¦
+--------+---------+---------------------+
2 rows in set (0.00 sec)

MariaDB [FinalProject]> SELECT * FROM User;
+--------+---------+---------------------+
¦ UserID ¦ Name    ¦ Email               ¦
+--------+---------+---------------------+
¦      1 ¦ TestOne ¦ TestOne@TestOne.com ¦
¦      2 ¦ TestTwo ¦ TestTwo@TestTwo.com ¦
+--------+---------+---------------------+
2 rows in set (0.00 sec)

MariaDB [FinalProject]>
```