**SQL Injection Attack exercise setup instructions**

This setup will create a system with a web server and a MySQL database server. The zip file contains the files needed to populate the web server and the files needed to initialize the MySQL database.

1. Make sure you have installed and working **apache2** web server
   1. issue "**systemctl enable apache2**" to enable it on boot
   2. issue "**systemctl start apache2**" to start apache2 now
   3. Download **SQL-Exercise.zip** file to /var/www/html and unzip. You should see a new index.html, and a sql-inj and blind directories. If you browse to your webserver you should see a descriptive web page about the exercise.
2. Make sure you have installed the **MySQL** database server.
   1. issue "**systemctl enable mysql**" to enable mysql at boot
   2. issue "**systemctl start mysql**" to start mysql now
   3. connect to the database with
      1. mysql
         1. create database directory;
         2. create database payload;
         3. exit
   4. initialize databases
      1. mysql directory < /var/www/html/sql-inj/directory.sql
      2. mysql payload < /var/www/html/blind/payload4.sql
3. turn on ssh server on Kali2 host
   1. issue "**systemctl enable ssh**" to enable ssh at boot
   2. edit /etc/ssh/sshd\_config
      1. change “PermitRootLogin without-password” line from “without-password” to “yes”
   3. issue "**systemctl start ssh**" to start ssh
4. clean up:
   1. cp /dev/null to /var/log/{messages,syslog,...} and /var/log/apache2/\*
   2. clear browser history
   3. clear shell history
   4. clear mysql history
   5. empty /tmp
   6. Change root password
   7. Remove \*.sql files

Deploy in RLES

1. Power down model vApp completely
2. Add vApp to catalog
3. Use deploy PowerShell script
4. Use start PowerShell script
5. Use harvest IPs PowerShell script to get front host IPs