Detecting SQL Injection using Snort IDS

Setting-up SQL Injection Lab in /var/www/html

Adding Document Root of SQL Lab in Sites-Available

```
root@kapil-wirtual-machine:/etc/apache2/sites-available × root@kapil-wirtual-machine:/etc/sno

*VirtualHost *:80>

# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
# ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html/sqli

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
# LogLevel info ssl:warn

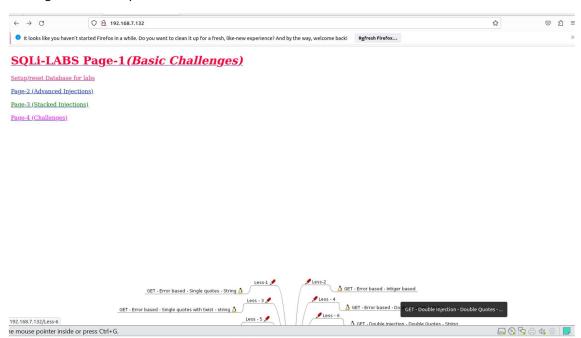
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".

*/VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Hosting Website on Apache2 Server



```
root@kapil-virtual-machine: ~
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# LOCAL RULES
# This file intentionally does not come with signatures. Put your local
# additions here.
alert tcp any any -> any 80 (msg: "Error Based SQL Injection Detected";
alert tcp any any -> any 80 (msg: "Error Based SQL Injection Detected";
```

Alerts are generated after performing SQL Injection