

Detecting SQL Injection using Snort IDS

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

```
root@kapil-virtual-machine:~# cd /sql
bash: cd: /sql: No such file or directory
root@kapil-virtual-machine:~# ls
go  perl  python  snmp  sql
root@kapil-virtual-machine:~# cd sql/sql_Edited_Version/
root@kapil-virtual-machine:~/sql/sql_Edited_Version# ls
root@kapil-virtual-machine:~/sql/sql_Edited_Version# mv sqllabs/ sqlt
root@kapil-virtual-machine:~/sql/sql_Edited_Version# ls
README.md  sqlt
root@kapil-virtual-machine:~/sql/sql_Edited_Version# mv sqlt /var/www/html
root@kapil-virtual-machine:~/sql/sql_Edited_Version# ls
README.md
root@kapil-virtual-machine:~/sql/sql_Edited_Version# cd
root@kapil-virtual-machine:~# cd /var/www/html
root@kapil-virtual-machine:~# ls
index.html  sqlt
root@kapil-virtual-machine:~# cd /var/www/html
root@kapil-virtual-machine:~# cd sqlt
root@kapil-virtual-machine:~/sqlt# ls
images  index.html  Less-14  Less-20  Less-26  Less-3  Less-36  Less-42  Less-49  Less-55  Less-61  Less-9  sql-lab.sql
index-1.html  index.html_files  Less-15  Less-21  Less-26a  Less-30  Less-37  Less-43  Less-5  Less-56  Less-62  sql-connections  toncat-Files.zip
index-1.html_files  Less-1  Less-16  Less-22  Less-27  Less-31  Less-38  Less-44  Less-50  Less-57  Less-63  'SQL Injections-1.rm'
index-2.html  Less-10  Less-17  Less-23  Less-27a  Less-32  Less-39  Less-45  Less-51  Less-58  Less-64  'SQL Injections-2.rm'
index-2.html_files  Less-11  Less-18  Less-24  Less-28  Less-33  Less-4  Less-46  Less-52  Less-59  Less-65  'SQL Injections-3.rm'
index-3.html  Less-12  Less-19  Less-25  Less-28a  Less-34  Less-40  Less-47  Less-53  Less-6  Less-7  'SQL Injections.rm'
index-3.html_files  Less-13  Less-2  Less-25a  Less-29  Less-35  Less-41  Less-48  Less-54  Less-60  Less-8  'SQL Injections.png'
root@kapil-virtual-machine:~/sqlt#
```

Adding Document Root of SQL Lab in Sites-Available

```
root@kapil-virtual-machine: /etc/apache2/sites-available  x  root@kapil-virtual-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/sqlt

# 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".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>

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

Hosting Website on Apache2 Server

192.168.7.132

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

Refresh Firefox...

SQLi-LABS Page-1 (Basic Challenges)

[Setup/reset Database for labs](#)
[Page-2 \(Advanced Injections\)](#)
[Page-3 \(Stacked Injections\)](#)
[Page-4 \(Challenges\)](#)

Less-1

GET - Error based - Single quotes - String

Less-2

GET - Error based - Integer based

Less-3

GET - Error based - Single quotes with twist - string

Less-4

GET - Error based - Double quotes - String

Less-5

GET - Double Injection - Double Quotes - String

Less-6

GET - Double Injection - Double Quotes - String

192.168.7.132/Less-6

the mouse pointer inside or press Ctrl+G.

A screenshot of a terminal window titled "root@kapil-virtual-machine: ~". The terminal displays the contents of a file named "local.rules". The first few lines are comments: "# \$Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp \$", "# -----", "# LOCAL RULES", and "# -----". A longer comment follows: "# This file intentionally does not come with signatures. Put your local additions here." Below the comments, two alert rules are defined: "alert tcp any any -> any 80 (msg: \"Error Based SQL Injection Detected\";" and "alert tcp any any -> any 80 (msg: \"Error Based SQL Injection Detected\";". The terminal has a dark background with light-colored text. On the left side, there is a vertical dock containing several application icons: a red circle, a blue Twitter bird, a folder icon, a yellow circular icon, a document icon, an orange shopping bag icon, a blue question mark icon, a grey monitor icon, and a CD/DVD icon. The top of the terminal window shows the title bar with the username and host name, and a close button (X) on the right.

```
root@kali:~# python3 exploit.py --url http://192.168.7.132:80 --ip 192.168.7.132 --port 80 --method GET --payload 'cmd=cat /etc/passwd' --output-dir ./
[+] [1:1917:6] SCAN UPnP service discover attempt [+] [Classification: Detection of a Network Scan] [Priority: 3] [UDP] 192.168.7.1:52770 -> 239.255.255.255:1900
root@kali-virtual-machine:/etc/snort/rules# cd ../
root@kali-virtual-machine:/etc/snort# sudo snort -q -l /var/log/snort -l enp2s1 -A console -C /etc/snort/snort.conf
ERROR: can't set DAQ BPF filter to '/etc/snort/snort.conf' (pcap_daq_set_filter: pcap_compile: can't parse filter expression: syntax error)
Fatal Error, Quitting..
root@kali-virtual-machine:/etc/snort# sudo snort -q -l /var/log/snort -l ens33 -A console -C /etc/snort/snort.conf
ERROR: can't set DAQ BPF filter to '/etc/snort/snort.conf' (pcap_daq_set_filter: pcap_compile: can't parse filter expression: syntax error)
Fatal Error, Quitting..
root@kali-virtual-machine:/etc/snort# sudo snort -q -c /etc/snort/snort.conf
[**] 2023-13-18:44.178675 [**] [1:100000012:0] Error Based SQL Injection Detected [**] [Priority: 0] [TCP] 34.167.221.82:80 -> 192.168.7.132:57214
[**] 2023-13-18:44.292234 [**] [1:100000012:0] Error Based SQL Injection Detected [**] [Priority: 0] [TCP] 34.167.221.82:80 -> 192.168.7.132:57222
```