

**Name: Pranav Patki**

**Roll No: 1911038**

**Batch: A3**

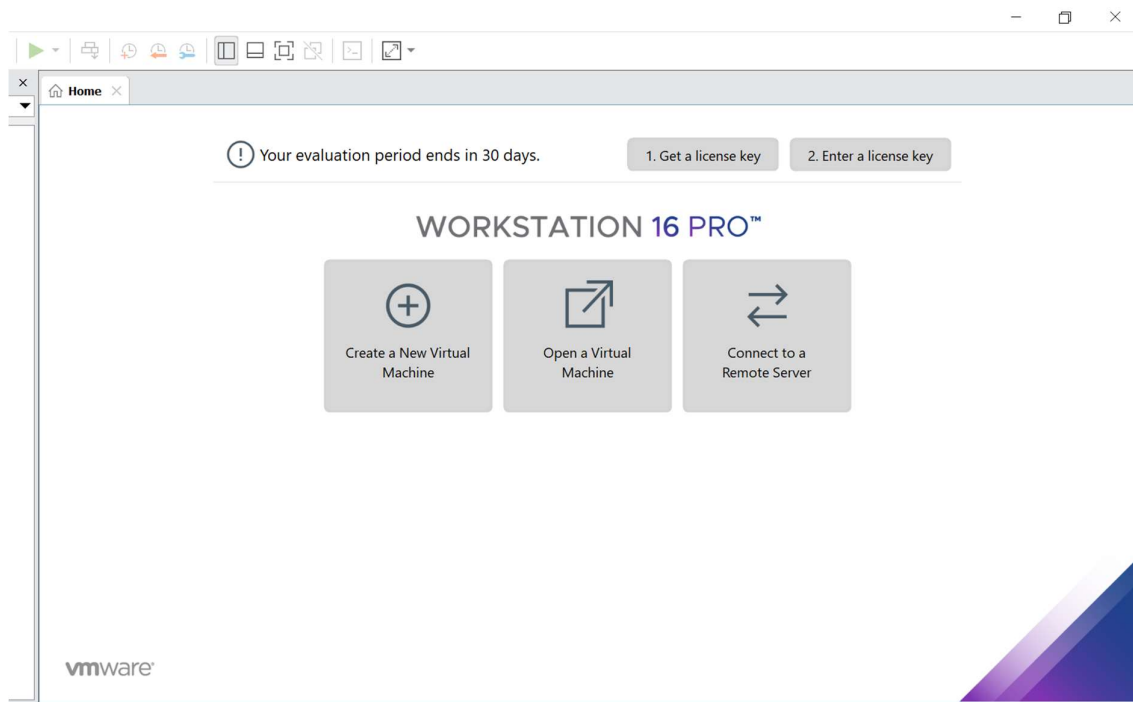
## **RDBMS IA2: Implementation of NoSQL injection**

### **Procedure**

Step 1: Go to <https://www.vmware.com/in/products/workstation-pro/workstation-pro-evaluation.html> and download the windows version of VMWare Workstation Pro.

Step 2: Now we need a web penetration testing framework. For that, go to [https://www.pentesterlab.com/exercises/web\\_for\\_pentester\\_II/attachments](https://www.pentesterlab.com/exercises/web_for_pentester_II/attachments) and download the ISO file.

Step 3: Open VMWare Workstation pro and click on “Create a virtual Machine”.



Step 4: Add the installer disc image which we downloaded:


New Virtual Machine Wizard

✕

**Guest Operating System Installation**  
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

☐ Installer disc:


 DVD Drive (E:) Debian squeeze 2

▼

☒ Installer disc image file (iso):

C:\Users\prana\Downloads\web\_for\_pentester\_II\_i386. ▼

Browse...

 Debian 6 detected.

☐ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

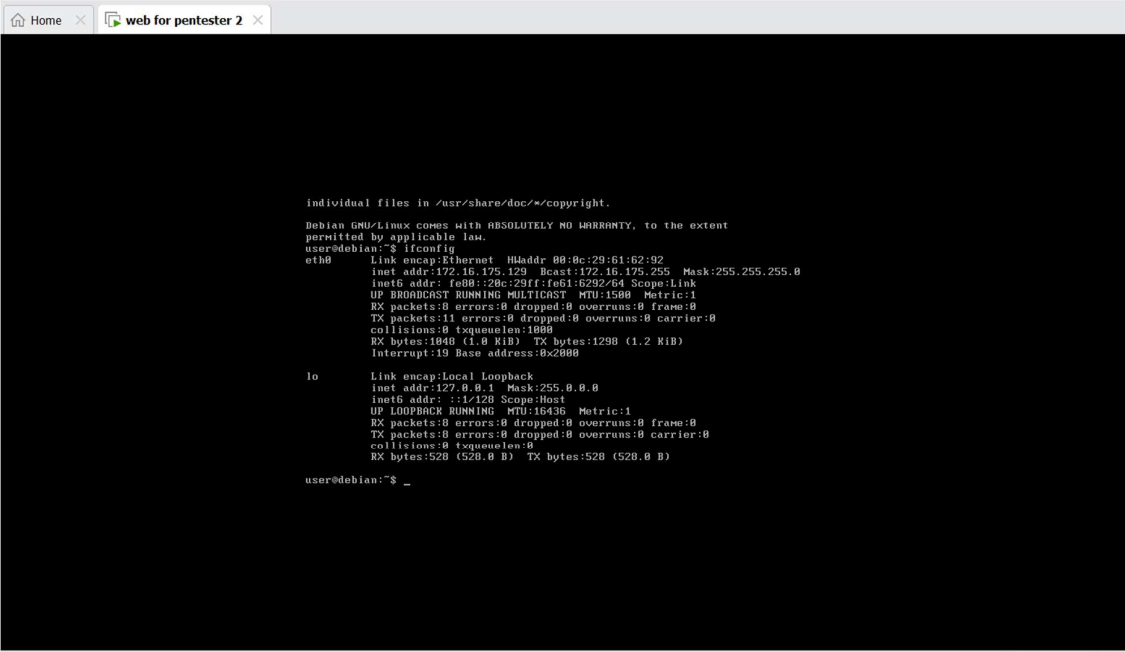
Help

< Back

Next >

Cancel

Step 5: Now power on the virtual machine and you will get the inet address

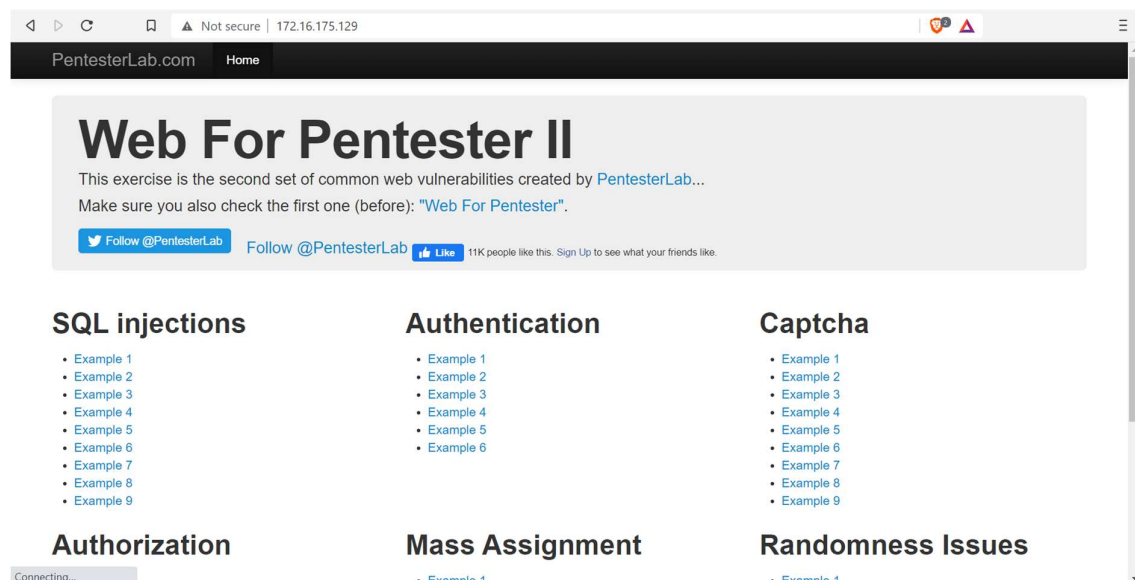


```
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debian:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:61:62:92
          inet addr:172.16.175.129  Bcast:172.16.175.255  Mask:255.255.255.0
          inet6 addr: fe80::29c:23ff:fe61:6292/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1040 (1.0 KiB)  TX bytes:1290 (1.2 KiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:520 (520.0 B)  TX bytes:520 (520.0 B)

user@debian:~$ _
```

Step 6: Copy the inet address and paste into your browser



# Authorization

- [Example 1](#)
- [Example 2](#)
- [Example 3](#)

# N

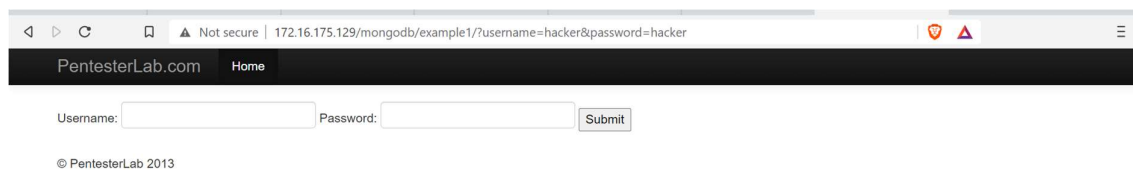
- 
- 
- 

# MongoDB injection

- [Example 1](#)
- [Example 2](#)

© PentesterLab 2013

Step 7: Go to example 1 under MongoDB injection



Browser address bar: 172.16.175.129/mongodb/example1/?username=hacker&password=hacker

Page header: PentesterLab.com Home

Form fields: Username:  Password:  Submit

Page footer: © PentesterLab 2013

Step 8: Now enter the following MongoDB query in username and password: `admin' || '1' == '1`

You will now be allowed access into the admin dashboard:



Step 9: Go to VMWare workstation pro and power off the virtual machine

