

48730-32548, Cyber Security Lab 1 (Week-2)

- Lab Environment Setup- Information Gathering - SQL Injection -

Introduction to Lab Environment

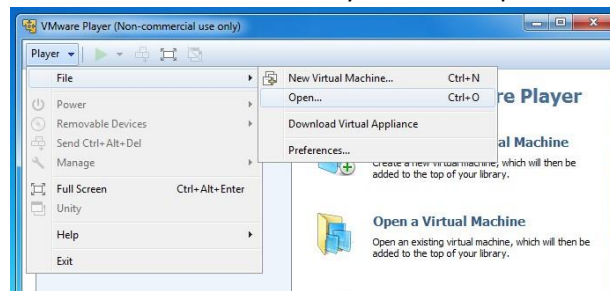
The Virtual Machine Images for the required lab will be available to download from cloud storage for which the link will be provided before the lab. We will be using VMware Player 14 to run our virtual lab environment, instructions for which follow.

If you wish to use your own laptop, you can get VMWare Workstation 15(WIN/LINUX) or Fusion 11(MAC) from the UTS repository <http://goo.gl/gx7H4g>.

Important: Due to multiple lab activities and use of multiple VM images, you are expected to bring your own USB/External Storage with a minimum capacity of 64GB (USB-3.0 Standard). To run the VM image,

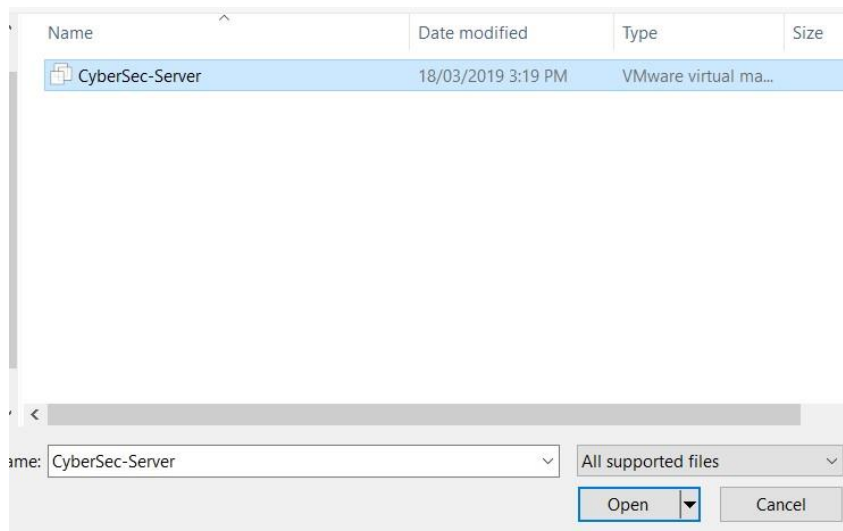
Step 1.

Open VMware Player from the Start Menu and Go to Player > File > Open...



Step 2

Browse to the folder where you have downloaded/copied your VM Image and Open the CyberSec-Server file



48730-32548, Cyber Security Lab 1 (Week-2)

- Lab Environment Setup- Information Gathering - SQL Injection -

Step 3

Run the VM Image. If during the boot you are asked about ownership – **select Take Ownership**. If during the boot you are asked if you moved/copied it – **select I Moved It**. If all goes well, you will get the login screen. Login with the following credentials.

Username: CyberSec

Password: cybersec



Ethical hacker

An ethical hacker is a computer and networking expert who systematically attempts to penetrate a computer system or network on behalf of its owners for the purpose of finding security vulnerabilities that a malicious hacker could potentially exploit.

Passive information gathering

A lot of important information can be passively gathered and subsequently used in a direct attack or to reinforce other attacks targeted at an organization. Some Web Hosting service providers provide Website analysis that may pose a risk to security of an organization. There are some tools as NetCraft, NSlookup, Shodan.io, Alexa Top Sites, Whois search, or Censys Search Engine.

48730-32548, Cyber Security Lab 1 (Week-2)

- Lab Environment Setup- Information Gathering - SQL Injection -

NetCraft

Netcraft is an internet services company providing internet security services, including anti-fraud and antiphishing services, application testing, code reviews, and automated penetration testing. It also provides research data and analysis on many aspects of the internet. Netcraft has explored the internet since 1995 and is a respected authority on the market share of web servers, operating systems, hosting providers, ISPs, encrypted transactions, electronic commerce, scripting languages and content technologies on the internet. Visit www.netcraft.com

Censys search engine

Censys search engine scans the Internet and returns public IP addresses of the target site and statistics about the Internet protocols used by the target system. Visit <https://censys.io/domain>

Alexa Top Sites

It is an Amazon Web service (AWS) providing lists of the highest-performing websites and network traffic statistics regarding the target site in accordance with Alexa Traffic Rank algorithm. Visit <https://www.alexa.com/topsites> or [alexa.com/siteinfo](https://www.alexa.com/siteinfo)

Shodan.io

It is a search engine for security. It provides specific types of computers connected to the Internet. Visit shodan.io

Active information gathering

Unlike passive information gathering, active information gathering collects the most updated and current data. The information collected in this manner can be influenced by various factors that include your current location, ISP, network constraints, etc. This information can be used to investigate the current state of the target. One of the most popular tools is Nmap/Zenmap.

Zenmap



Zenmap or Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. It is useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Read more at www.nmap.org

Task (1): Information Gathering

Using Zenmap and any of passive information gathering tools to scan www.uts.edu.au. Gather and compare the information collected.

48730-32548, Cyber Security Lab 1 (Week-2)

- Lab Environment Setup- Information Gathering - SQL Injection -

 Network			
Site	http://uts.edu.au	Domain	uts.edu.au
Netblock Owner	Amazon Corporate Services Pty Ltd	Nameserver	ns.uts.edu.au
Hosting company	Amazon - Asia Pacific (Sydney) datacenter	Domain registrar	audns.net.au
Hosting country	 au	Nameserver organisation	whois.audns.net.au
IPv4 address	54.79.20.73 (VirusTotal)	Organisation	unknown
IPv4 autonomous systems	AS16509	DNS admin	dnsadmin@uts.edu.au
IPv6 address	Not Present	Top Level Domain	Australia (.edu.au)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	ec2-54-79-20-73.ap-southeast-2.compute.amazonaws.com		

1. What is its Ip address?
54.79.20.73
2. Type the IP address in the browser to access the webpage, explain your observations.
The Website URL Cannot be found, instead it asked if I am a Customer of the hosting service and I have to add domain name
3. Who is the IP owner?
Amazon
4. What is the server's operating system?
Linux
5. What type of web server is being used?
Nginx
6. What is its server-side scripting technology?
XML and SSL

48730-32548, Cyber Security Lab 1 (Week-2)

- Lab Environment Setup- Information Gathering - SQL Injection -

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
XML	No description	www.xvideos.com , www.ecosia.org , www.virustotal.com
SSL ↗	A cryptographic protocol providing communication security over the Internet	yandex.ru

7. Can you find the email for the domain admin of this website for a possible phishing attack?

NO

8. What is the 'Reverse DNS' for the website?

ec2-54-79-20-73.ap-southeast-2.compute.amazonaws.com

9. Who is the domain registrar?

Audns.net.au

10. What is nameserver organization?

Whois.audns.net.au

11. What company is hosting the website?

Amazon - Asia Pacific (Sydney) datacenter

12. Where is the hosting company geologically located?

Australia

Information gathering can be achieved using various open source tools, a list of such possible tools can be found at: <https://securitytrails.com/blog/top-20-intel-tools>. As always, use the tools within a controlled safe environment.

SQL injection

SQL injection is one of the most common vulnerability in web applications today. It is one of the web hacking techniques that are very popular and dangerous because successful SQL injection could allow hackers to compromise your servers, networks, personal computers and confidential data. According to The Open Web Application Security Project Report released in 2017, SQL Injection is amongst the number 1 risks out of top 10 security risks.

What is SQL Injection? SQL injection is an attack injection technique that exploits vulnerability in SQL query via user's input data from client to the database layer of an application. This vulnerability exists in custom Web application that lacks proper input validation, fails to use parameterized SQL statements, and/or creates dynamic SQL with user-supplied data. It is occurred when user input is incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.

48730-32548, Cyber Security Lab 1 (Week-2)

- Lab Environment Setup- Information Gathering - SQL Injection -

Normally, attacker will test SQL injection by typing malformed SQL commands into front-end Web application input boxes that are tied to database accounts in order to trick the database into offering more access to information than the developer intended. A successful SQL injection exploit can read sensitive data from the database, modify database data, execute administration operations on the database, and recover the content of a given file present on the database file system and in some cases issue commands to the operating system. This attack allows attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, destroy the data and become administrators of the database server.

Task (2): SQL Injection tasks

You need to use the browser and open [localhost](#) to perform this lab.

Login bypass is without a doubt one of the most popular SQL injection techniques. This lab will give explanations and a little deep understanding with some new flavors of bypasses.

Note: Please work through the information in the following link to understand how SQL query works: <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>

Your aim is to perform the following tasks.

- I. Login when the Username is '123456789' but the Password is not known.



You have successfully logged in !!

Welcome to the other side !!

[Sign Out](#)

Username : 123456789

Password : 'or'1'='1

48730-32548, Cyber Security Lab 1 (Week-2)

- Lab Environment Setup- Information Gathering - SQL Injection -

- II. Login when both the Username and Password are not known.



Login

UserName :
'or'1'='1

Password :

Please enter your Username & Password

You have successfully logged in !!

Welcome to the other side !!

[Sign Out](#)

Username : 'or'1'='1

Password : 'or'1'='1

48730-32548, Cyber Security Lab 1 (Week-2)

- Lab Environment Setup- Information Gathering - SQL Injection -

III. Find table details containing all the Usernames and Passwords through SQL injection.

Login

UserName :

Password :

Please enter your Username & Password

Login

UserName :

Password :

Error : Please check the Username and Password : File '/tmp/sql.txt' already exists

```
cybersec-server@ubuntu: /tmp
cybersec-server@ubuntu:~$ cd /
cybersec-server@ubuntu:/$ ls
bin      dev      initrd.img  lib64      mnt      root     srv      usr      vmlinuz.old
boot     etc      initrd.img.old  lost+found  opt      run      sys      var
cdrom    home     lib         media      proc     sbin     tmp      vmlinux
cybersec-server@ubuntu:/$ cd tmp
cybersec-server@ubuntu:/tmp$ ls
config-err-YVx6L9  unity_support_test.0  VMwareDnD  vmware-root-3980165237
sql.txt           vmware-cybersec-server  vmware-root
cybersec-server@ubuntu:/tmp$ cat sql.txt
11046354      abcd1234
11550124      abcd1234
11851173      abcd1234
12624894      abcd1234
11698584      abcd1234
11391087      abcd1234
11914153      abcd1234
11725797      abcd1234
11993882      abcd1234
11981204      abcd1234
12021008      abcd1234
98104108      abcd1234
12594949      abcd1234
12600060      abcd1234
10460285      abcd1234
99128237      abcd1234
99160970      abcd1234
12611909      abcd1234
97114060      abcd1234
12588974      abcd1234
11981317      abcd1234
11656509      abcd1234
11804984      abcd1234
99047121      abcd1234
```

IV. Login into a specific user account by extracting the username and password from the table.

48730-32548, Cyber Security Lab 1 (Week-2)

- Lab Environment Setup- Information Gathering - SQL Injection -



Login

UserName :
11550124

Password :

Submit

Error : Please check the Username and Password : File '/tmp/sql.txt' already exists

You have successfully logged in !!

Welcome to the other side !!

[Sign Out](#)

Based on your Observations from the above task, suggest possible defense

Using Web Application Firewall and input Validation to increase security