UNIVERSITY OF WESTMINSTER

INFORMATICS INSTITUTE OF TECHNOLOGY

6COSC002W – Security and Forensics

Course: BEng (Hons) Software Engineering

Module Leader: Mr. Saman Hettiarachchi

Name: Mahanama Udajith

Student ID: 16737992/1

Submission Date: 29-04-2020

Contents

Table of figures

Question A

1)

By running the command nmap with the ip address gives the open ports in the server.

```
root@kali:~/w1673799# nmap 192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-27 23:39 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00018s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap
MAC Address: 08:00:27:B0:CB:BE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
root@kali:~/w1673799#
```

Figure 1 Open Ports

Opened ports are as follows,

Port	Protocol
22	tcp
80	tcp
139	tcp
143	tcp
443	tcp
445	tcp
5001	tcp
8080	tcp
8081	tcp

There are well known vulnerabilities in these tcp ports.
According to the Cars web application, by accessing the port 22, an attacker can tunnel random traffic towards different hosts. It can bypass security restrictions which has been implemented in this website as well. (Port 22 (tcp/udp), 2020)

There are some vulnerabilities such as SQL injections and cross-site scripting, over the port 80 (Geer, 2020)

There can be CSRF attacks because of the port 443 via malicious links.
NetBIOS attacks may occur over the port 139
CSRF attacks can occur over the ports 8080 and 8081\tcp as well.
(Beyond Security | Finding and Fixing Vulnerabilities in SMB Listens on Port, a Medium Risk Vulnerability, 2020)

2)
By running command nmap –sV –O with ip address will give running services on the server with their versions.

```
root@kali:~/w1673799# nmap -sV -O 192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-27 23:49 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00059s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; pro
tocol 2.0)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP
/5.3.2-1ubuntu4.5 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Pyth
on/2.6.5 mod_ssl/2.2.14 OpenSSL/ ... )
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
443/tcp  open  ssl/https?
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5001/tcp open  java-object Java Object Serialization
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8081/tcp open  http        Jetty 6.1.25
1 service unrecognized despite returning data. If you know the service/vers
ion, please submit the following fingerprint at https://nmap.org/cgi-bin/su
bmit.cgi?new-service :
SF-Port5001-TCP:V=7.80%I=7%D=4/27%Time=5EA7A7CA%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"\xac\xed\0\x05");
MAC Address: 08:00:27:B0:CB:BE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

Figure 2 Services and Versions

These are the running services in the server.

Port/Protocol	Service
22/tcp	ssh
80/tcp	http
139/tcp	netbios-ssn
143/tcp	imap
443/tcp	ssl/https
445/tcp	netbios-ssn
5001/tcp	Java-object
8080/tcp	http
8081/tcp	http

ssh, http services can be protected giving some priority. Because there can be so many threats over these services. For ssh also there can be Man in the middle attacks. Some common vulnerabilities and security threats which we can find in ssh and https as follows.
DoS attacks can be happened
Buffer overflow.
CSRF
SQL injection
Cross Site Scripting

3)

When these ports open, attackers can use these services and get the access to retrieve sensitive data.
When legitimate services are utilized by code vulnerabilities attackers can attack via them.
There can be vulnerabilities because of the ssh version. Here the version is 5.3.
There might be security issues if we don't update to the latest version.

Some internet vulnerabilities for those services are as follows.

Man In the Middle Attack
It prevents genuine communication between two parties.

Port scanning
That can exploit and access the system.

ARP Spoofing attack
Use to steal sensitive data. And also helps to other attacks as well.

Denial of Service Attack
By trying to access a server using multiple hosts. It will crash the server.

4)

ssh

SSH is a cryptographic network protocol.
It can be used inside the unsecured network to securely control network services. One vulnerability in ssh is it reuses private host keys. Buffer Overflow is also a vulnerability in ssh.

http

Hypertext Transfer Protocol is also not completely secure.
There are some vulnerabilities in HTTP as well.
CSRF
Cross Site Scripting
SQL injections

imap

To manage messages in mail servers, remote users can use imap.
It doesn't have strong authentication
Users can use plaintext login details and it accepts them.
It doesn't use multifactor authentication

netbios-ssn

PC which is running windows use NetBIOS to share or access file server.
It has vulnerabilities like Footprinting. And it can retrieve a lot of information about the computers, ip addresses.

Question B

1)

Normally when the user inputs the correct username password in the login form, it will successfully log in to the page.

When testing data tampering we can start tampering before the user inputs values to the login form and even user enters incorrect login details we can change the user entered values before the request leaves the browser and change it to correct details and send it and it will return a successful response.

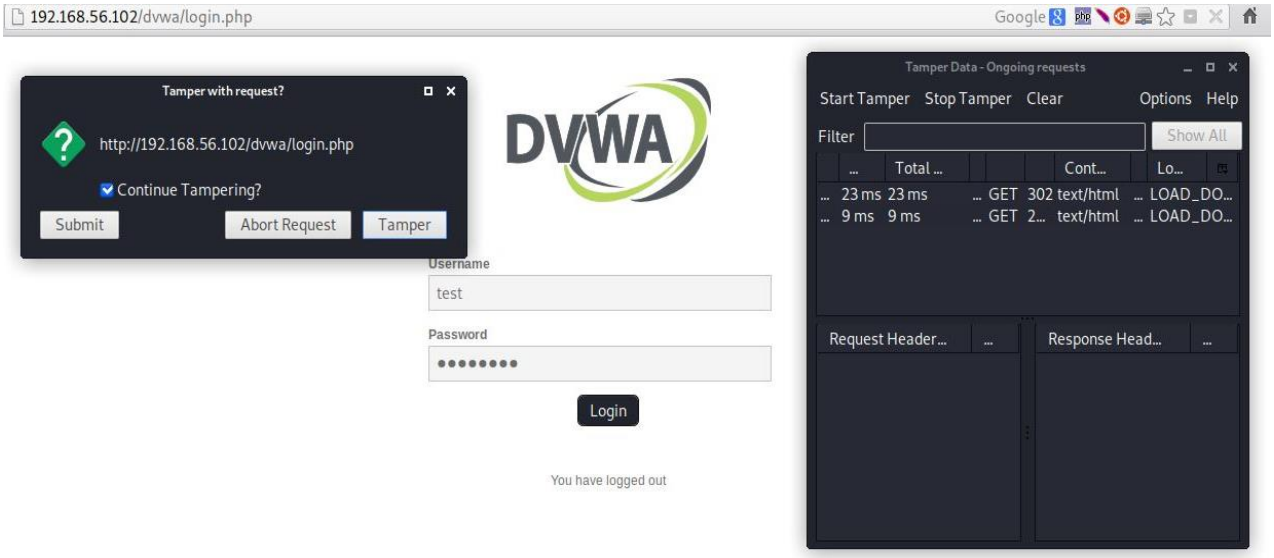

Figure 3 Data Tampering False Credentials

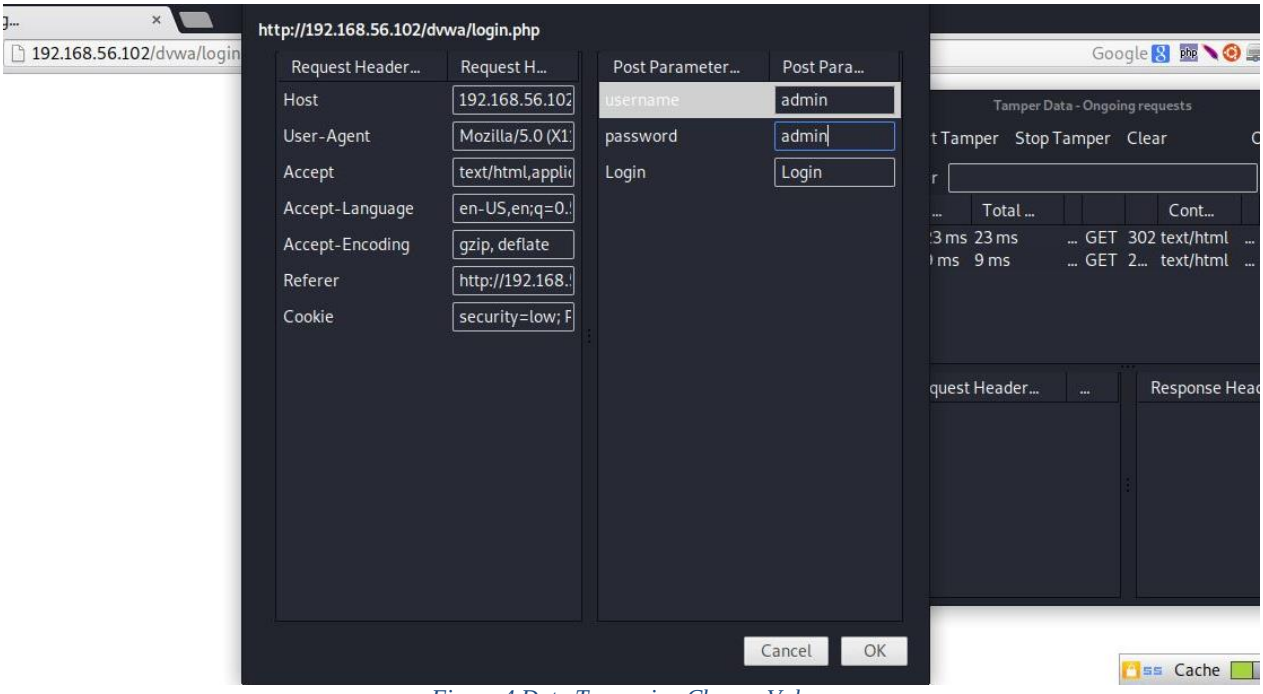

Figure 4 Data Tampering Change Values

2)

Assume that there's a form submit on our website. When the user inputs some value and if it queries to the database without any validation there can occur SQL injection.
If the user tries to send a malicious input then the PHP interpreter reads the code like this.

$query = "SELECT ∗ FROM u s e r s WHERE id =’" . " 1’" . " ’ " ;

After concatenated,

$query = "SELECT ∗ FROM u s e r s WHERE id = ’1 ’ " ;

Please check the figures to identify the successful and failed attempts.

Figure 5 SQL Injection Successful Submit

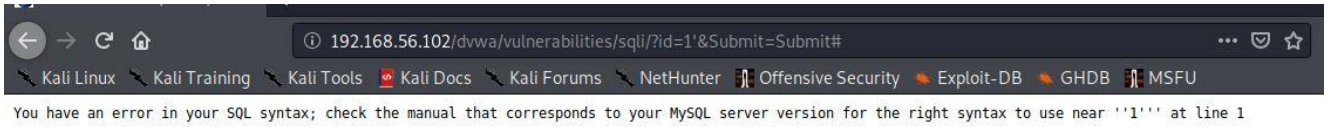

Figure 6 SQL Injection Incorrect Values

3)

When a user inputs some value and if it is not validated and if the output hasn't encoded accurately either in server or client-side there can be cross-site scripting vulnerabilities.
Then the user can input some values which have been already used in HTML code. Then it will interpret as source code and send to the page hence there is no encoding system.
EX: Bob<script >alert(’XSS’)</script>

Attackers can steal users' information by performing these types of vulnerabilities.

Please check the figures below.

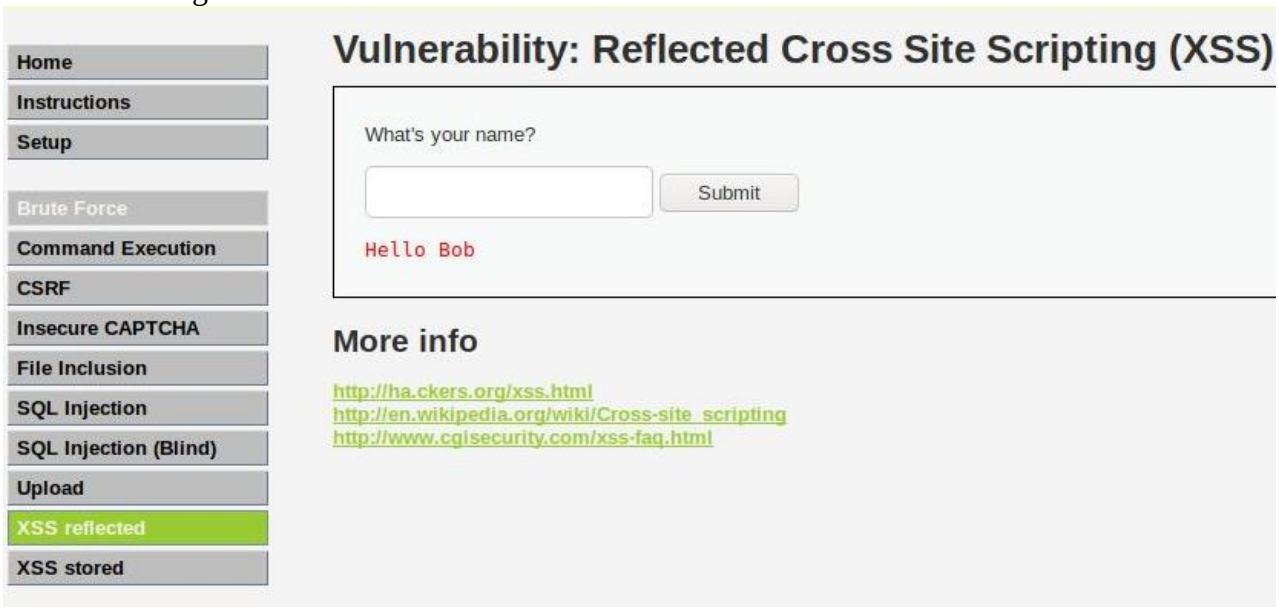

Figure 7 XSS Successful Submit 1.0

Figure 8 XSS Successful Submit 2.0

Figure 9 XSS Incorrect Value

4)

By performing SSLScan, we can retrieve SSL(Secure Sockets Layer) and TLS(Transport Layer Security) information.
It has been already identified that there are some vulnerabilities in implementing SSL protocol. Therefore it is mandatory to do secure connection testing.

Buffer overflow vulnerabilities

When char types of buffers have been operated by us, this can occur. This can happen in C and PHP languages. There are some other languages which don't allow buffer overflow errors.
When you give too much data also this can happen. With this mistake attacker can get the access to your system.

Question C

1)

User credential information.

While doing penetration testing we can use multiple tools to do packet capturing and analyzing. Wireshark, tshark etc. Using Wireshark testers can do investigations on hundreds of protocols and read live data and analyze.

Sometimes we can use another tool to capture packets and use Wireshark to analyze the traffic.

2)

By luring users to their machines attackers can get user credentials by performing Phishing attacks. Attack machine can be pretended as a real machine and user can't see whether it's real or not.

Then the user inputs the values and attacker can capture those details via credential harvester inside attacker's VM.

3)

We can use tools like Metasploit as well to do a penetration testing.
It's a kind of internal testing.
Client-side applications should be correctly patched.
Instruct employees not to open malicious links. And prevent employees from doing any suspicious activities by monitoring them.
Enable SSL(HTTPS) and restrain from using HTTP.
If iframes have been used they should be secured
(When is Client-Side Penetration Testing Appropriate?, 2020)

Question D

1)

It's a type of host-to-host communication.
In port knocking, we can open firewall ports externally.
When we use suitable connection attempts to change firewall rules dynamically, it will allow host to connect to those specific ports. Sometimes attackers try to scan the system to misuse the services by trying out port scans. We can use port knocking to prevent those kinds of things.
We can legitimate users by identifying them via port knocking and block them if we need.
Therefore it's better to implement port knocking on our server to prevent those kinds of attacks.

2)

Even though the Intrusion Detection System captured an attack we mentioned it as False positive state because the attack is tolerable. It's an alert that can be initiated because of nonmalicious traffic.

But the false-negative state is not tolerable. It is something like a critical state.
NIDS fails to detect some security issues in sometimes and there it is called False negative.

3)

Both of these read network packets and compare the contents to identify known threats.

IDS is not controlling the system but it monitors and detect.
Do not take action to their own.
To check the result there should be another system or a human.
It detects port scanners, policy violations and malwares.

IPS is handling or controlling the system.
According to a ruleset it can accept or reject a packet.
In IPS there should be an updated database with new threats regularly.

4)

IPTables is a Firewall.

To access outbound DNS connections,
Ip addresses can be blocked using Iptables,
To log dropped packets,
Accept the MYSQL connections which are coming from specific networks,
Accept any networks web traffic and it can help to prevent DoS attacks as well.

Snort is kind of IDS
Snort can alert you when there's an attack.
But IPTables are used to block the access or permit them using some ports and ips.
Using firewalls we can log events as well.
Snort is not a first line of defence.

5)

Insecure Direct Object References

When we expose an internal object to the user (customer who are looking for cars) this error will occur.
Ex: file or database key

Using session variables can prevent this issue
And using user authorization properly.

Security misconfiguration

Running the production application with debug mode can cause this issue.
Having a better and automated build and deploy process can prevent this issue.

Unvalidated redirects and forwards

Attackers can redirect to different url and User may think it's trusted and safe then the customer will click.
To prevent we can restrict from redirections
Also we can have static list of vlid loctions.

Sensitive data exposure

We need to encrypt sensitive data as always possible. Since we are not doing payments in our application this risk might be less but still, we have users' sensitive data.

References

SpeedGuide. 2020. Port 22 (Tcp/Udp). [online]
Available at: https://www.speedguide.net/port.php?port=22
[Accessed 2020].

Geer, D., 2020. Securing Risky Network Ports. [online] CSO Online.
Available at: https://www.csoonline.com/article/3191531/securing-risky-network-ports.html
[Accessed 2020].

Cvedetails.com. 2020. CVE-2018-11447 : A Vulnerability Has Been Identified In SCALANCE M875 (All Versions). The Web Interface On Port 443/Tcp Could Allow A Cro. [online]
Available at: https://www.cvedetails.com/cve/CVE-2018-11447/
[Accessed 2020].

Beyond Security. 2020. Beyond Security | Finding And Fixing Vulnerabilities In SMB Listens On Port , A Medium Risk Vulnerability. [online]
Available at: https://beyondsecurity.com/scan-pentest-network-vulnerabilities-smb-listens-on-port.html
[Accessed 2020].

Subscription.packtpub.com. 2020. {{Metadatacontroller.Pagetitle}}. [online]
Available at:
https://subscription.packtpub.com/book/networking_and_servers/9781784392918/4/ch04lvl1sec45/obtaining-ssl-and-tls-information-with-sslscan
[Accessed 2020].

Inside Out Security. 2020. IDS Vs. IPS: What Is The Difference?. [online]
Available at: https://www.varonis.com/blog/ids-vs-ips/
[Accessed 2020].

Inside Out Security. 2020. IDS Vs. IPS: What Is The Difference?. [online]
Available at: https://www.varonis.com/blog/ids-vs-ips/
[Accessed 2020].

Infosec Resources. 2020. When Is Client-Side Penetration Testing Appropriate?. [online]
Available at: https://resources.infosecinstitute.com/when-is-client-side-penetration-testing-appropriate
[Accessed 2020].

Beyond Security. 2020. Beyond Security | Finding And Fixing Vulnerabilities In SMB Listens On Port , A Medium Risk Vulnerability. [online]
Available at: https://beyondsecurity.com/scan-pentest-network-vulnerabilities-smb-listens-on-port.html
[Accessed 2020].