DAY 3: Web Exploitation Christmas Chaos

Tool used: kali Linux, Firefox, burbsuite

Solution/Walkthrough:

Q1

What's even worse is that these devices are often exposed to the internet, potentially allowing anyone to access and control it. In 2018 it was reported that a botnet (a number of internet-connected devices controlled by an attacker to typically perform DDoS attacks) called Mirai took advantage of Internet of Things (IoT) devices by remotely logging, configuring the device to perform malicious attacks at the control of the attackers; the Mirai botnet infected over 600,000 IoT devices mostly by scanning the internet and using default credentials to gain access.

research and study from tryhackme.com

Q2

In fact, companies such as Starbucks and the US Department of Defense have been victim to leaving services running with default credentials, and bug hunters have been rewarded for reporting these very simple issues responsibly (Starbucks paid $250 for the reported issue):

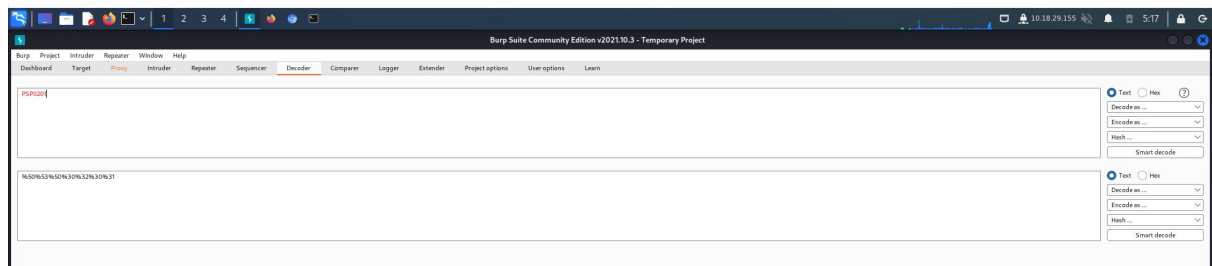research and study from tryhackme.com

Q3

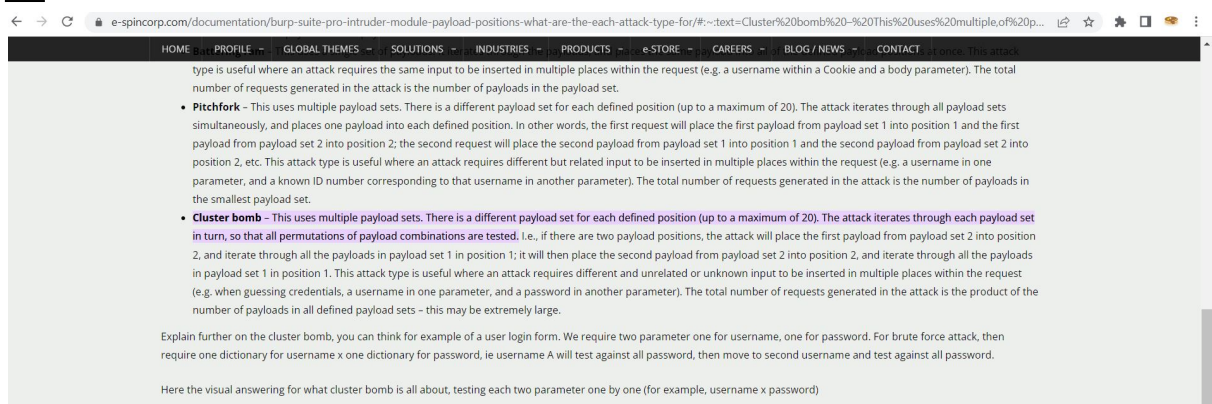Copy and paste from the Hackerone.com report

Q4 & Q5

Open foxyproxy's option, then select edit. The value of port and proxy type are shown.

Q6

Go to burpsuite, select the encoder. Type 'PSP0201' , choose [url] at the 'encode as' selection, copy the output.

Q7

Research and study from here.

Q8

Burp Project Intruder Repeater Window Help

Dashboard   Target   Proxy   Intruder   Repeater   Sequencer   Decoder   Comparer   Logger   Extender   Project options   User options   Learn

Intercept   HTTP history   WebSockets history   Options

Request to http://10.10.56.225:80

[Forward]   [Drop]   [Intercept is on]   [Action]   [Open Browser]   Comment this item   HTTP/1 (?)

Pretty Raw Hex

```
1  POST /login HTTP/1.1
2  Host: 10.10.56.225
3  Content-Length: 27
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://10.10.56.225
7  Content-Type: application/x-www-form-urlencoded
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
9  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://10.10.56.225/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15 username=test&password=test
```

Search...   0 matches

Open burp suite, turn on intercept option. After that, place a random input. BurpSuite held the request.

Send the request to intruder. Then select 'cluster bomb' in 'positon' selection.
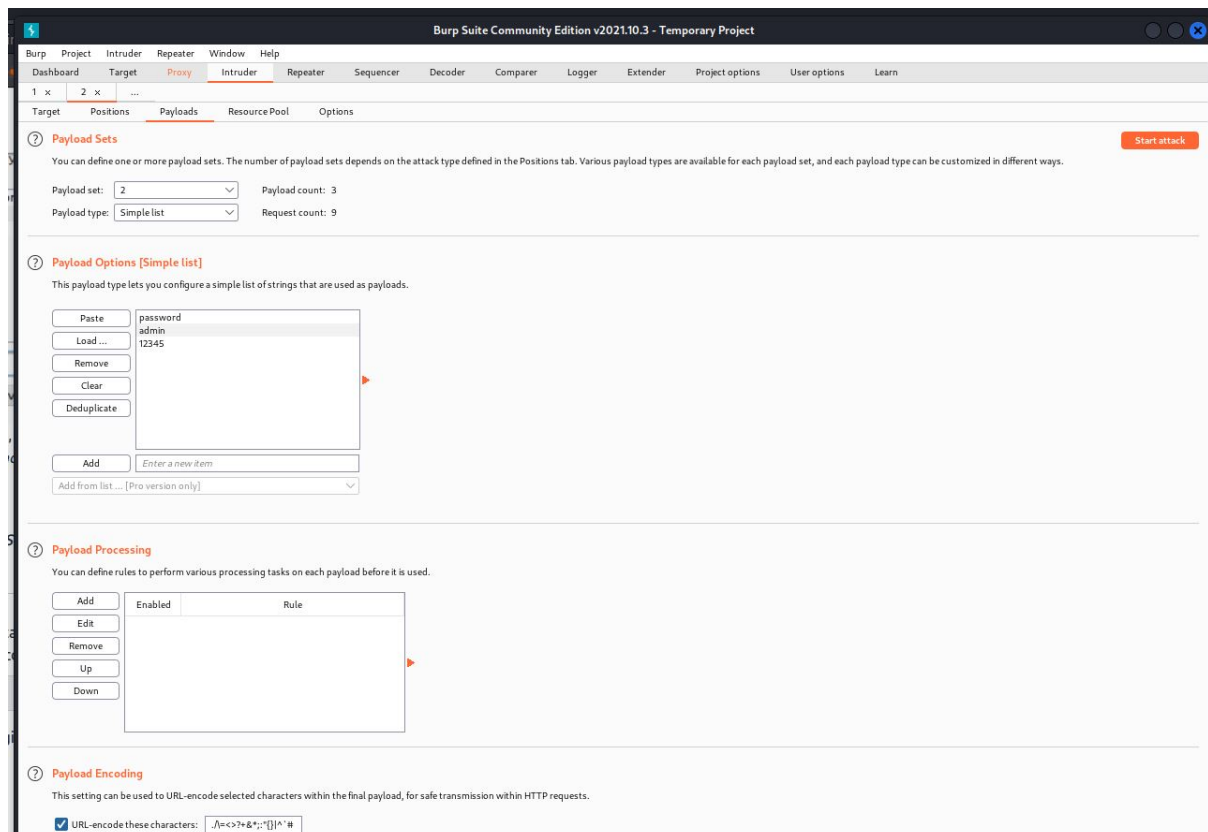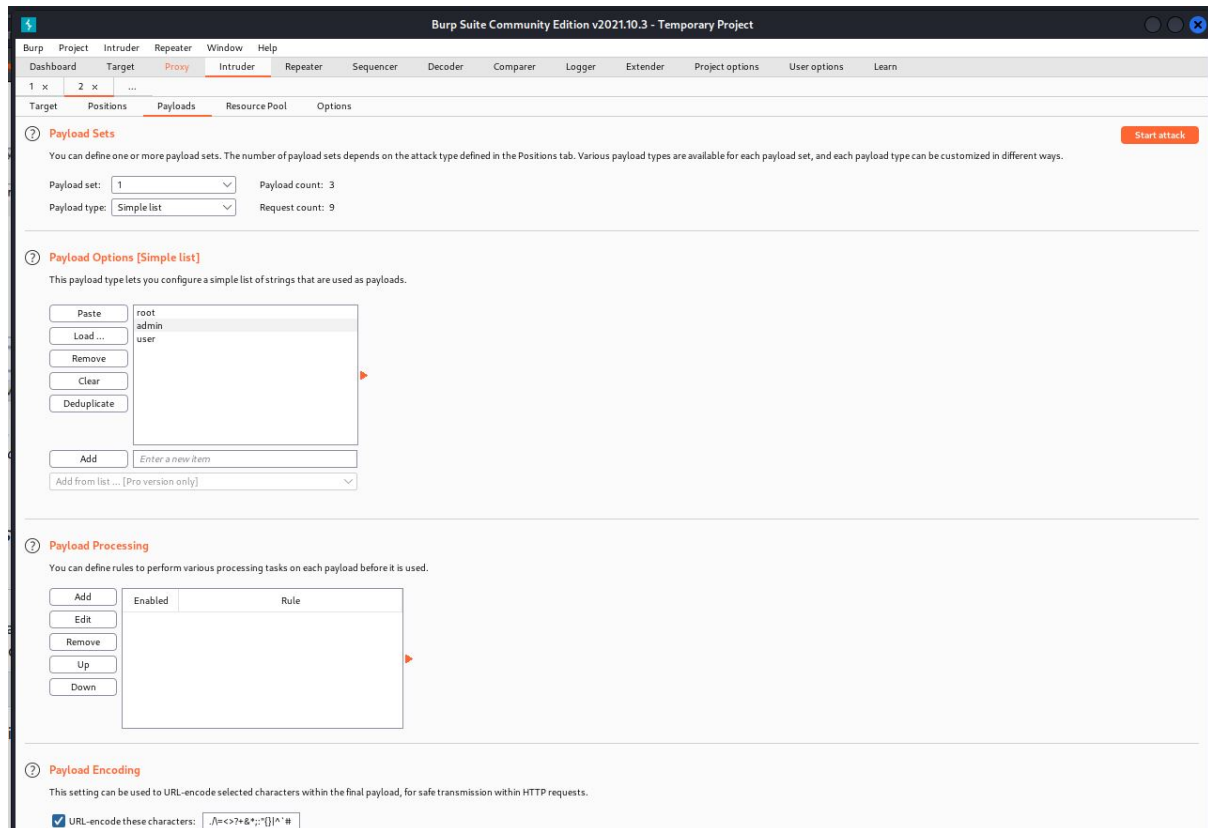
Go to 'payloads' selection. In set 1, add several common usernames such as root, admin, user. In set 2, add several common passwords such as password, admin, 12345.