PSP0201 Week 2 Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha Binti Muhd Firdaus	Member

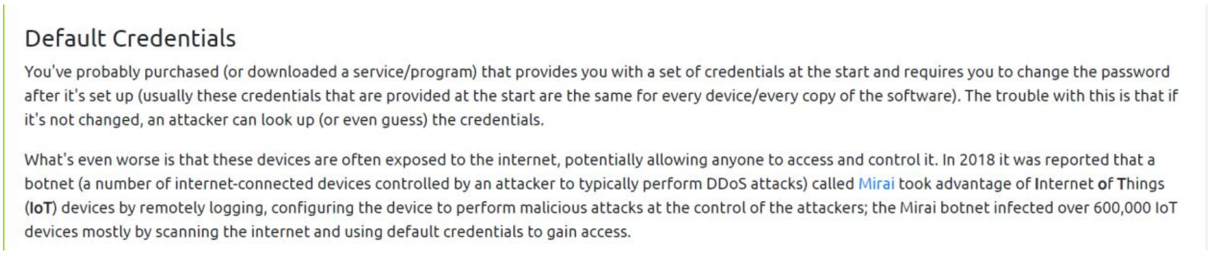
Day 3: Web Exploitation – Christmas Chaos

Tools used: AttackBox, Firefox, Burp Suite

Solution/walkthrough:

Question 1

Find the name under the Default Credentials and copy it.



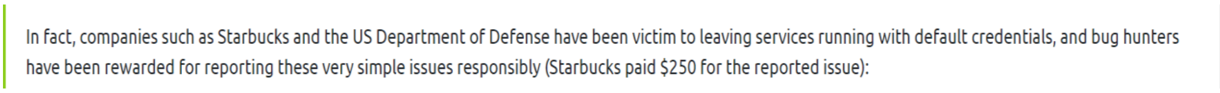
Default Credentials

You've probably purchased (or downloaded a service/program) that provides you with a set of credentials at the start and requires you to change the password after it's set up (usually these credentials that are provided at the start are the same for every device/every copy of the software). The trouble with this is that if it's not changed, an attacker can look up (or even guess) the credentials.

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.

Question 2

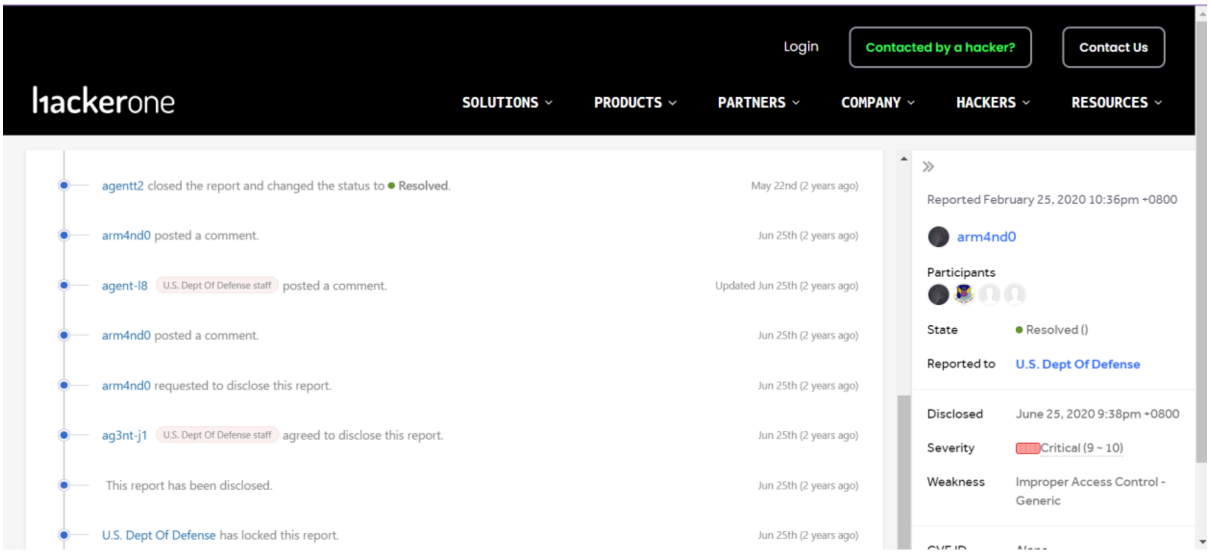
Find the amount ($) under the Default Credentials and copy it.



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):

Question 3

Find the agent from the given link(https://hackerone.com/reports/804548) under the Default Credentials and copy it.



agentt2 closed the report and changed the status to ● Resolved. May 22nd (2 years ago)

arm4nd0 posted a comment. Jun 25th (2 years ago)

agent-l8 U.S. Dept Of Defense staff posted a comment. Updated Jun 25th (2 years ago)

arm4nd0 posted a comment. Jun 25th (2 years ago)

arm4nd0 requested to disclose this report. Jun 25th (2 years ago)

ag3nt-j1 U.S. Dept Of Defense staff agreed to disclose this report. Jun 25th (2 years ago)

This report has been disclosed. Jun 25th (2 years ago)

U.S. Dept Of Defense has locked this report. Jun 25th (2 years ago)

Reported February 25, 2020 10:36pm +0800

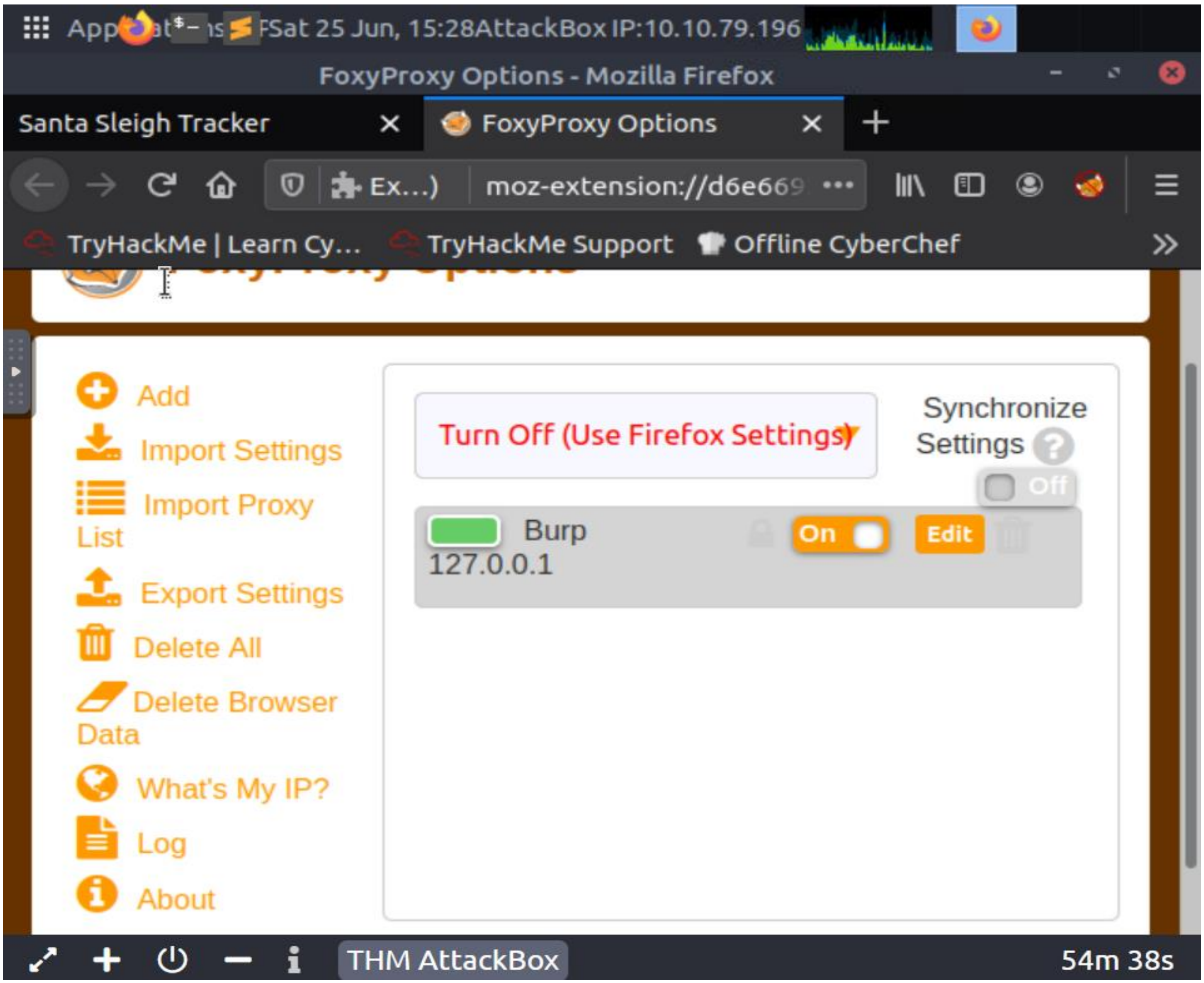
arm4nd0

Participants

State	● Resolved ()
Reported to	U.S. Dept Of Defense
Disclosed	June 25, 2020 9:38pm +0800
Severity	Critical (9 ~ 10)
Weakness	Improper Access Control - Generic

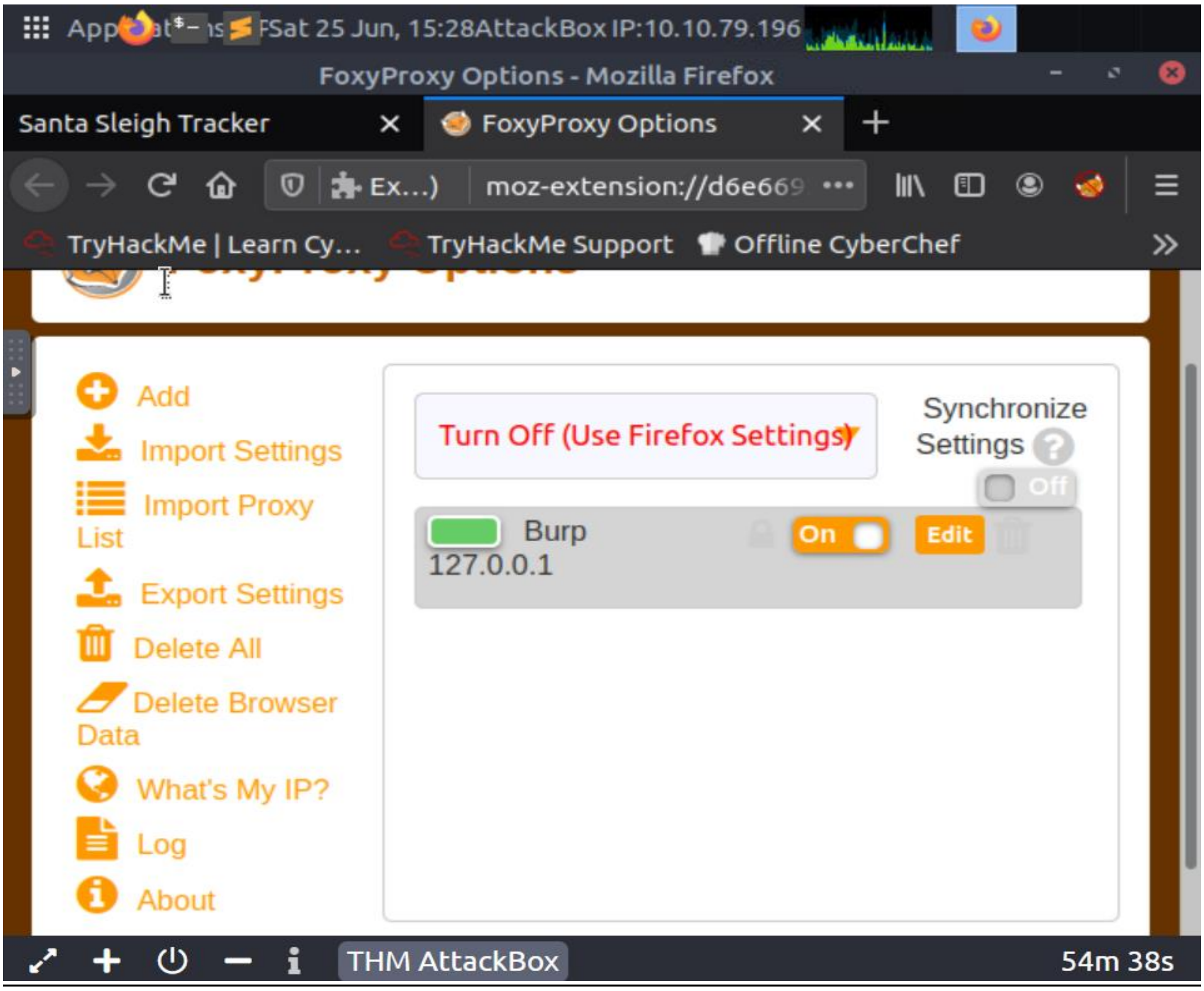
Question 4

Click the icon (FoxyProxy) at the top right corner and click on the options to find the port number for Burp. Then, copy it.

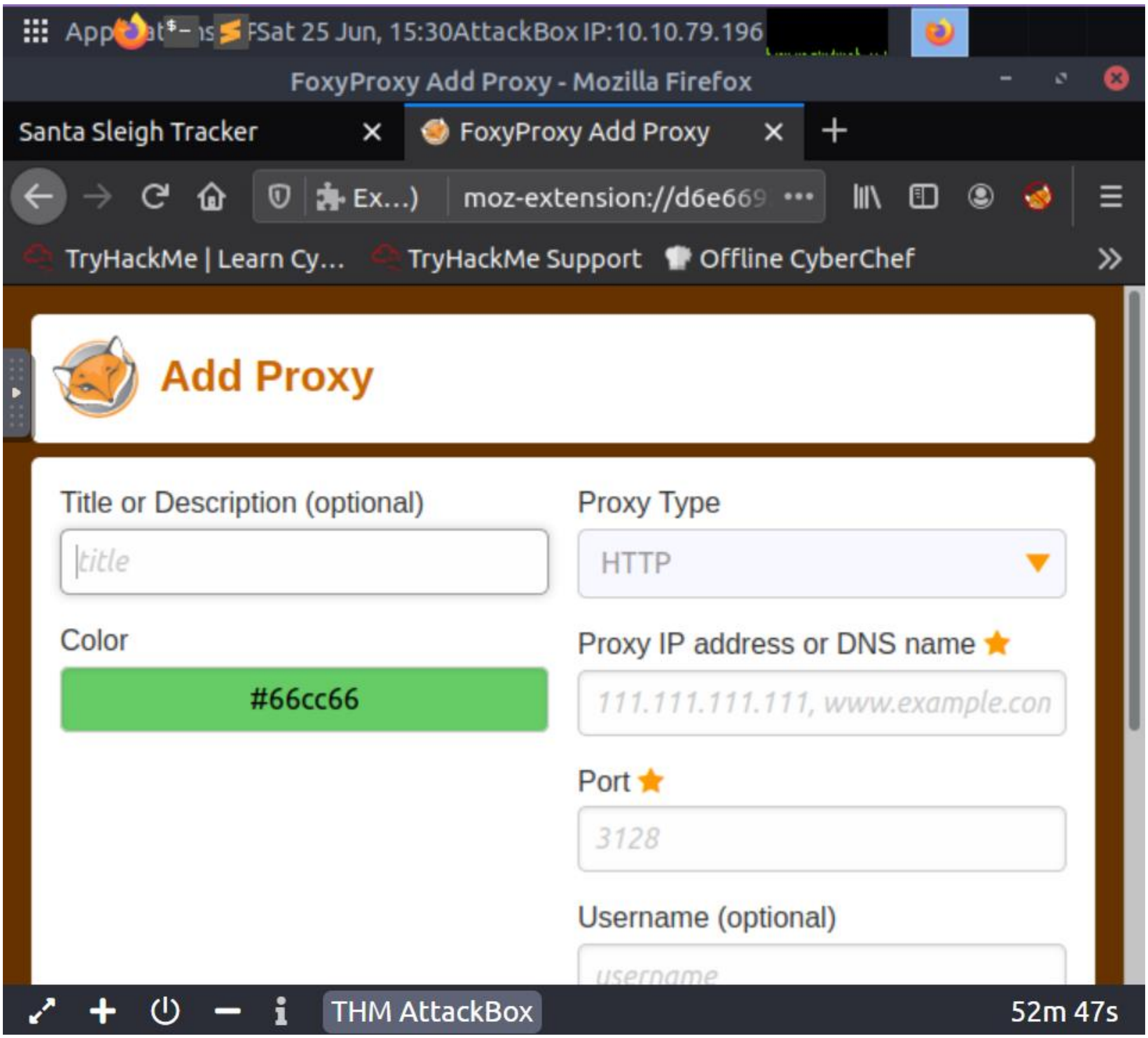


Question 5

Click the add option to access “Add Proxy”.



Find the Proxy Type and copy it.



Add Proxy

Title or Description (optional): title

Proxy Type: HTTP

Color: #66cc66

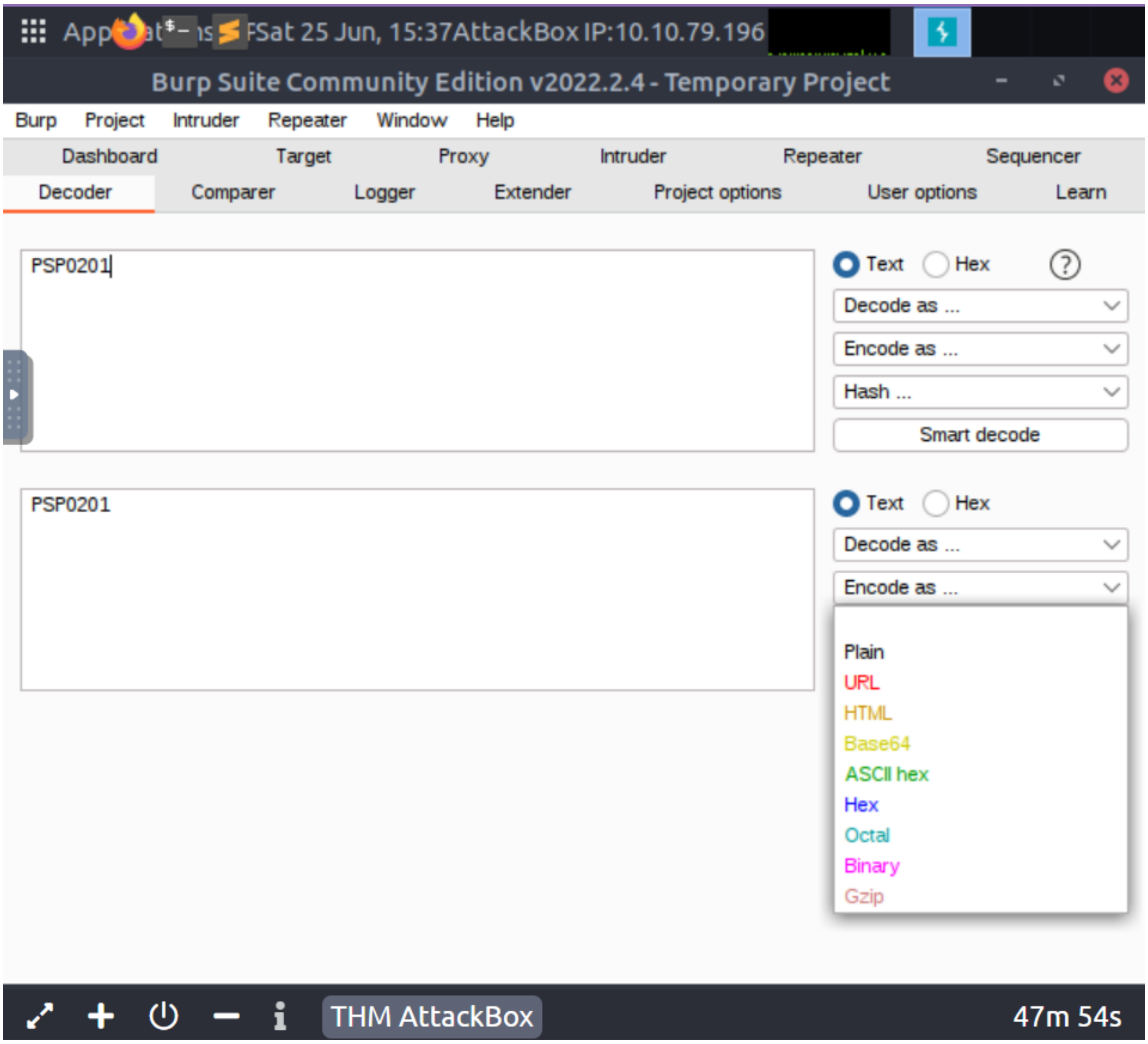
Proxy IP address or DNS name ★: 111.111.111.111, www.example.con

Port ★: 3128

Username (optional): username

Question 6

Open the BurpSuite Community Edition and click on decoder. Enter ‘PSP0201’ and choose to encode as URL.

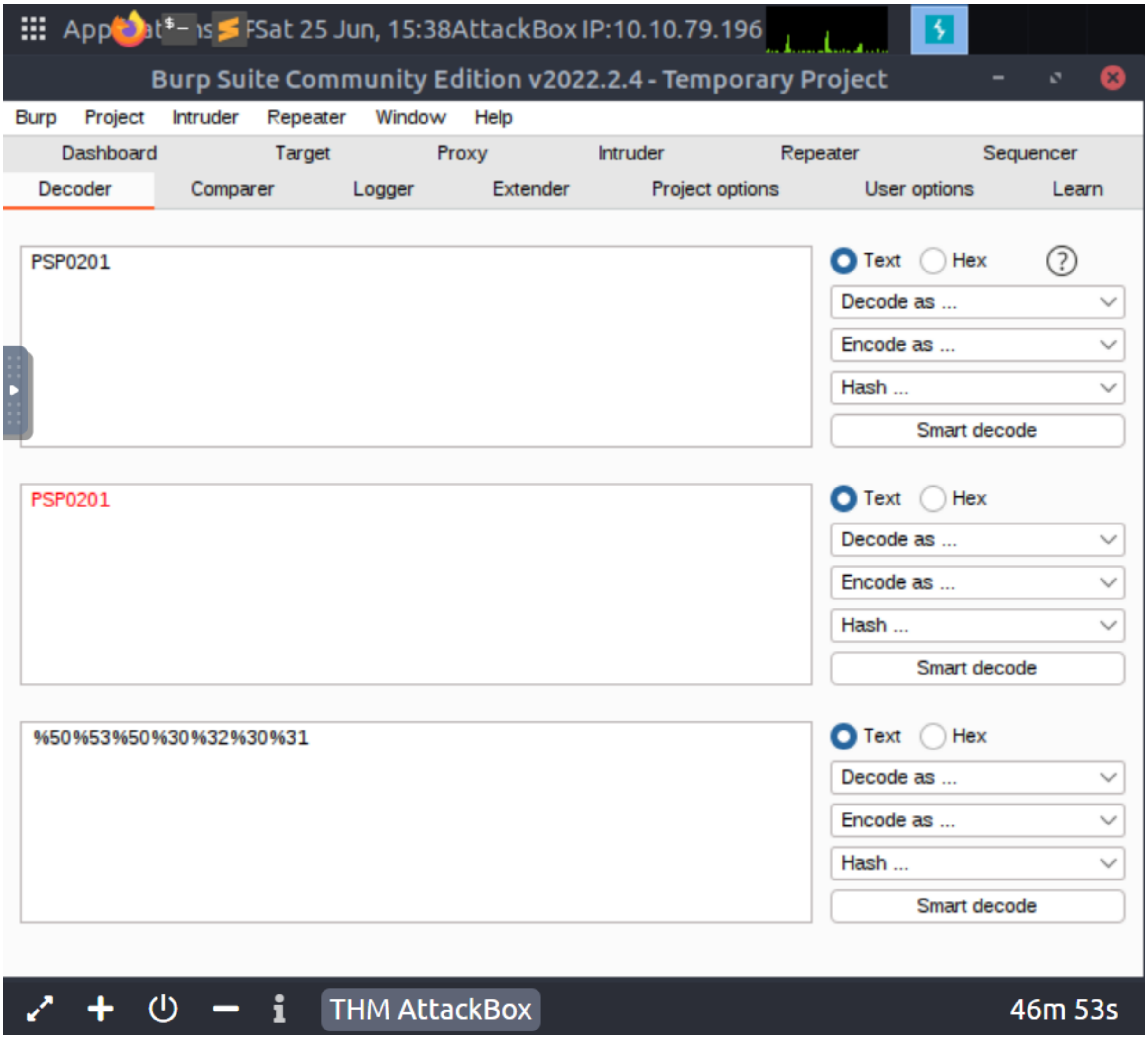


Apps
Sat 25 Jun, 15:37
AttackBox IP:10.10.79.196
Burp Suite Community Edition v2022.2.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer
Decoder Comparer Logger Extender Project options User options Learn
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
● Text ○ Hex
Decode as ...
Encode as ...
Plain
URL
HTML
Base64
ASCII hex
Hex
Octal
Binary
Gzip
THM AttackBox
47m 54s

PSP0201

PSP0201

Results would appear and copy it.



Applications Sat 25 Jun, 15:38 AttackBox IP:10.10.79.196
Burp Suite Community Edition v2022.2.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer
Decoder Comparer Logger Extender Project options User options Learn
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
THM AttackBox
46m 53s

```
PSP0201
```

```
PSP0201
```

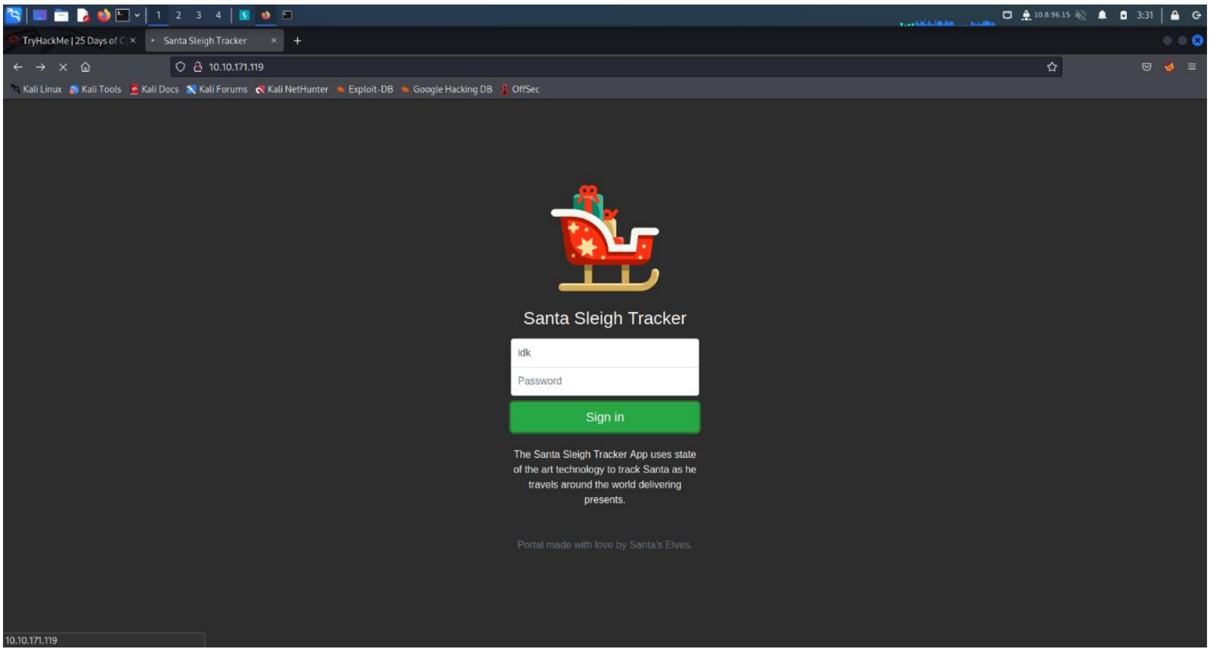
```
%50%53%50%30%32%30%31
```

Question 7

Click on the “Attack type” icon and search for the option that matches the one in the description (Cluster bomb).

Question 8

Open the website with the IP address provided. No access to content.



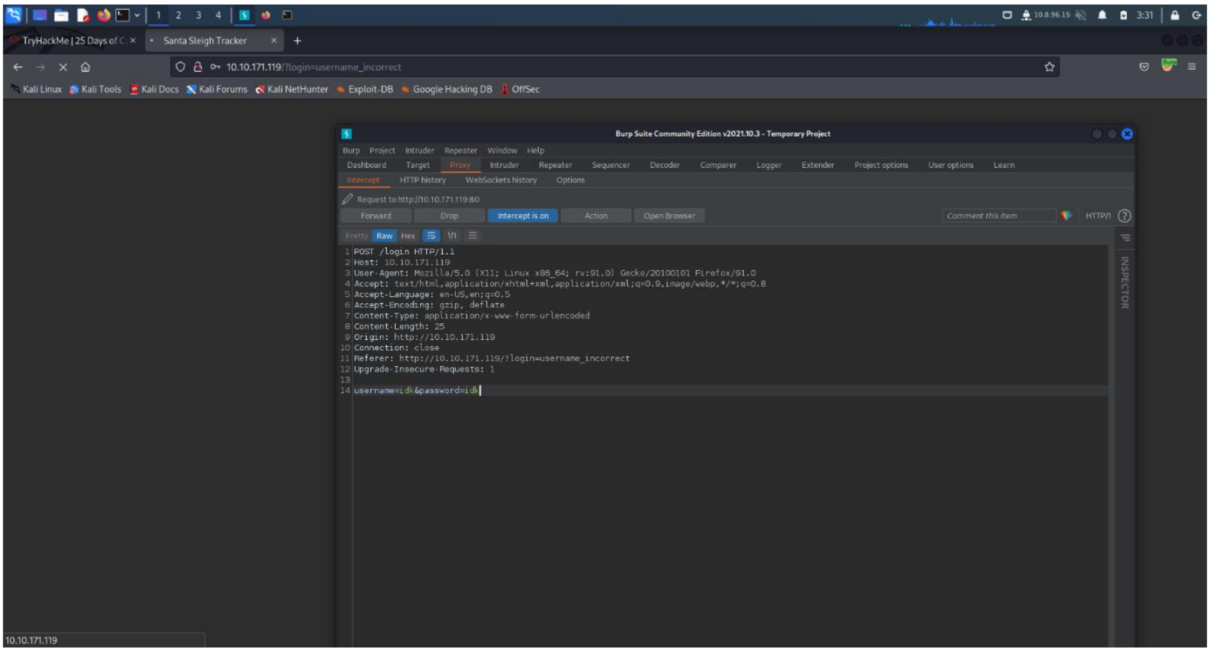
Santa Sleigh Tracker

idk

The Santa Sleigh Tracker App uses state of the art technology to track Santa as he travels around the world delivering presents.

Portal made with love by Santa's Elves.

Type in a random username and password. Then refresh the page and get back to BurpSuite to receive a captured request.

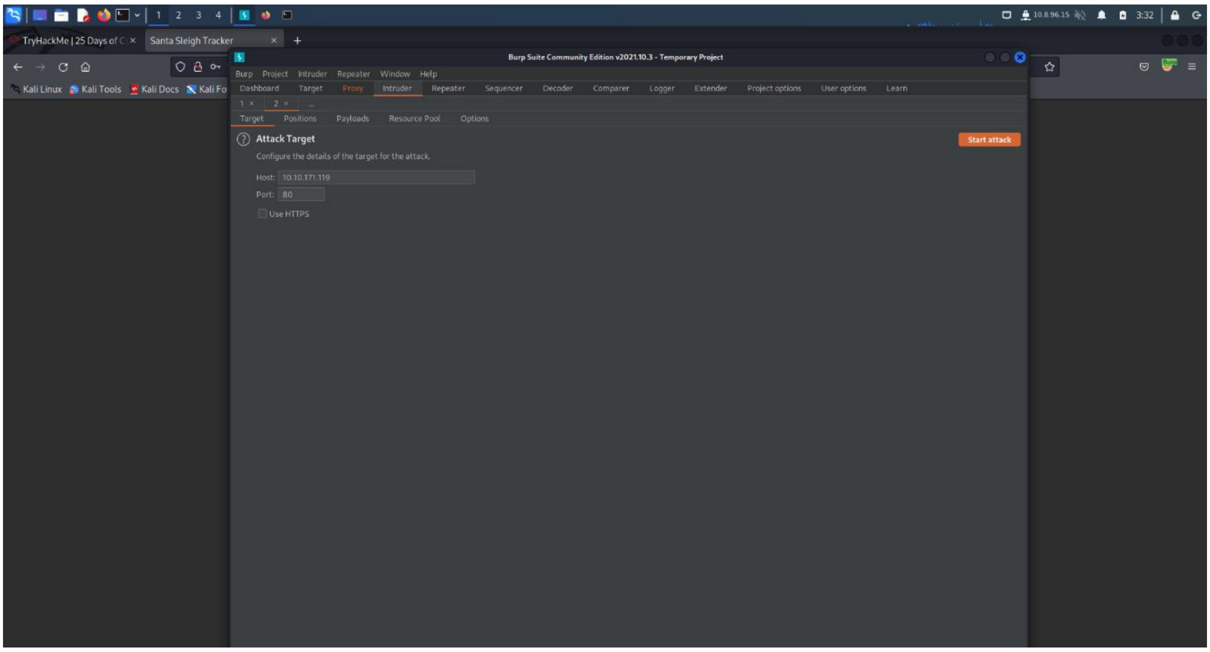


Request to http://10.10.171.119:80

```
POST /login HTTP/1.1
Host: 10.10.171.119
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: 25
Origin: http://10.10.171.119
Connection: close
Referer: http://10.10.171.119/?login=username_incorrect
Upgrade-Insecure-Requests: 1

username=idk&password=idk
```

Click "Ctrl+I" to send to the intruder.


TryHackMe | 25 Days of C
Santa Sleigh Tracker
Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Target Positions Payloads Resource Pool Options
Start attack

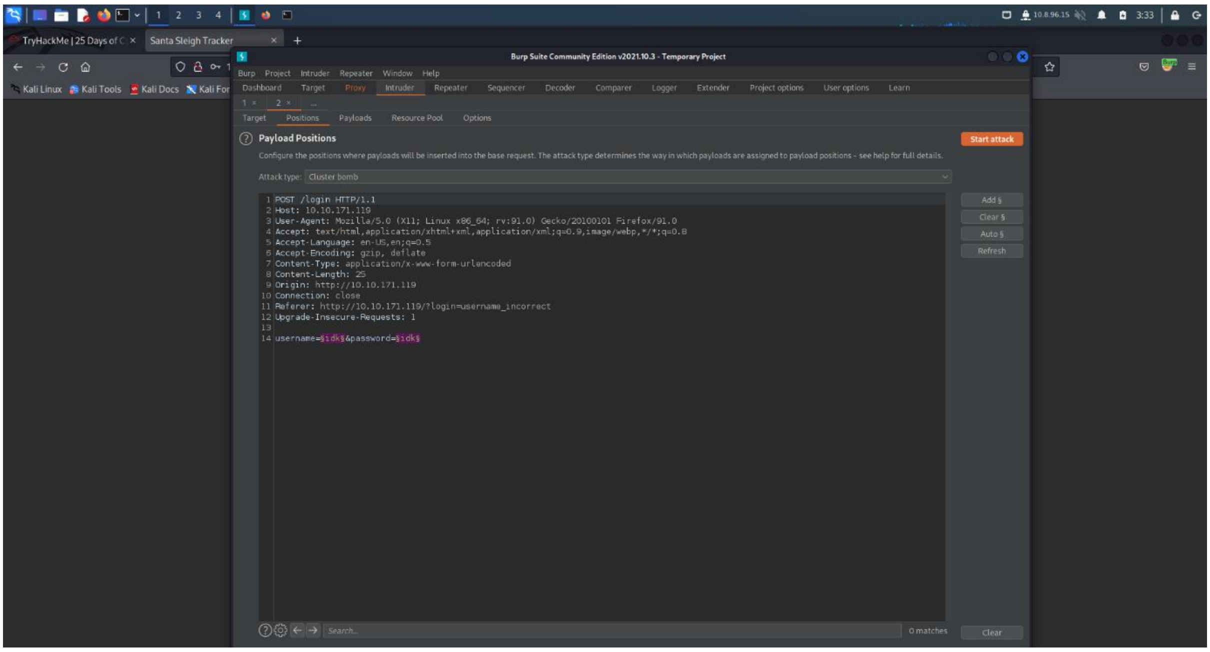
Attack Target

Configure the details of the target for the attack.

Host: 10.10.171.119

Port: 80

□ Use HTTPS


TryHackMe | 25 Days of C
Santa Sleigh Tracker
Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Target Positions Payloads Resource Pool Options
Start attack
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Clear

Payload Positions

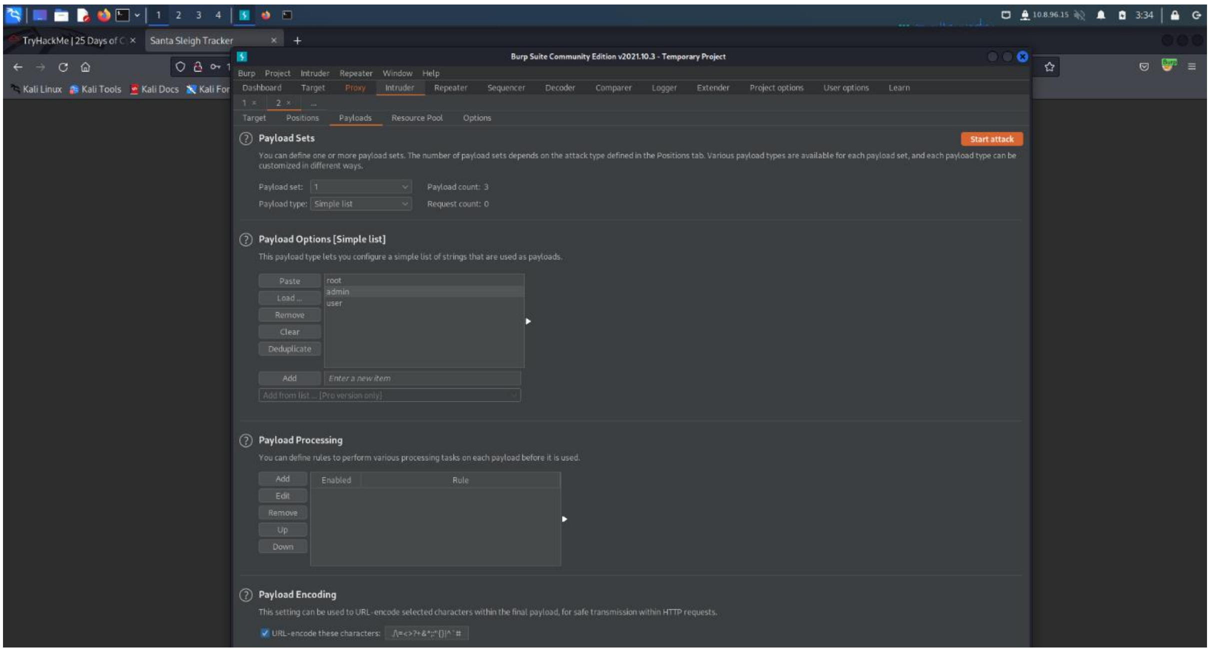
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

```
POST /login HTTP/1.1
Host: 10.10.171.119
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: 25
Origin: http://10.10.171.119
Connection: close
Referer: http://10.10.171.119/?login=username_incorrect
Upgrade-Insecure-Requests: 1

username=§idk§&password=§idk§
```

Click on the “payloads” tab and set to 1 for username. Then, add 3 common defaults which are admin, root and user.


Burp Suite Community Edition v2021.10.3 - Temporary Project

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 3
Payload type: Simple list Request count: 0

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
root
admin
user
```

Payload Processing

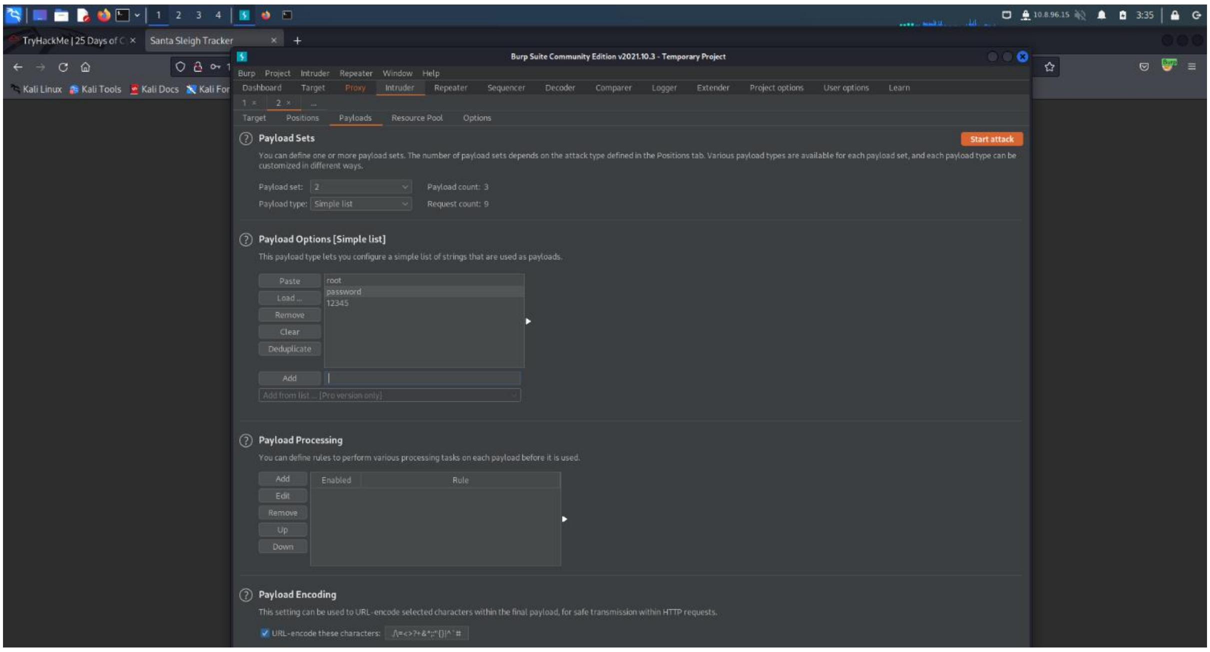
You can define rules to perform various processing tasks on each payload before it is used.

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

Set payload set to 2 for password and add another 3 common defaults which are password, admin and 12345.


Burp Suite Community Edition v2021.10.3 - Temporary Project

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 3
Payload type: Simple list Request count: 9

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
root
password
12345
```

Payload Processing

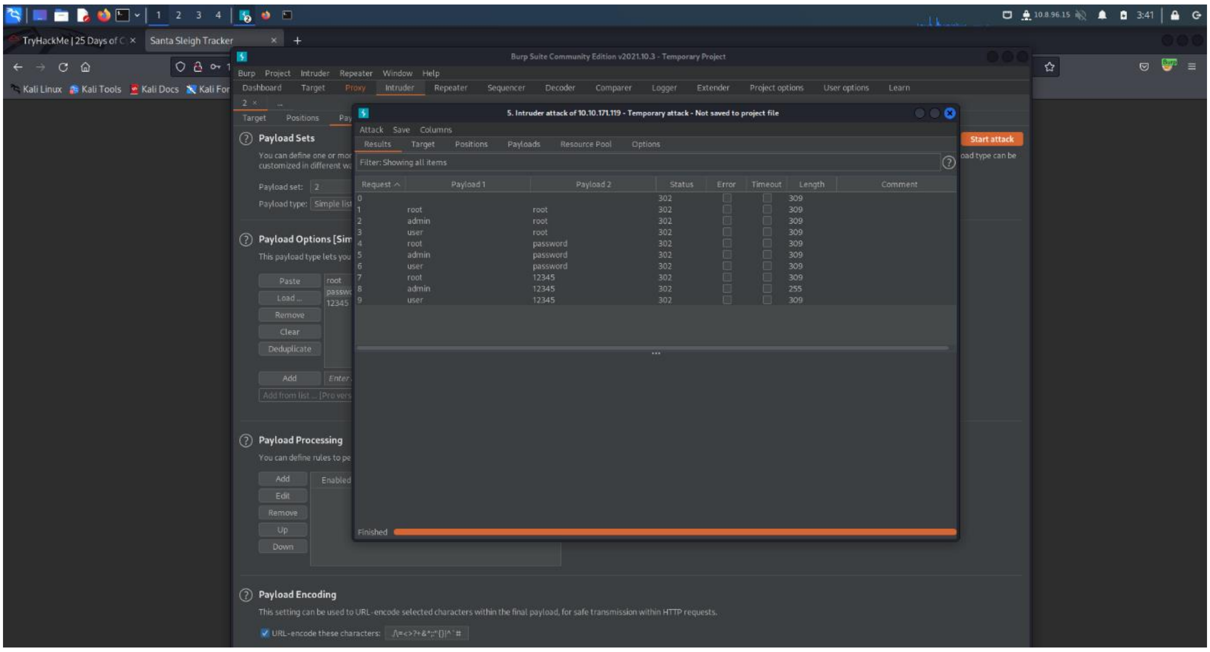
You can define rules to perform various processing tasks on each payload before it is used.

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

Click “Start attack” to receive results.



5. Intruder attack of 10.10.171.119 - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302	□	□	309	
1	root	root	302	□	□	309	
2	admin	root	302	□	□	309	
3	user	root	302	□	□	309	
4	root	password	302	□	□	309	
5	admin	password	302	□	□	309	
6	user	password	302	□	□	309	
7	root	12345	302	□	□	309	
8	admin	12345	302	□	□	255	
9	user	12345	302	□	□	309	

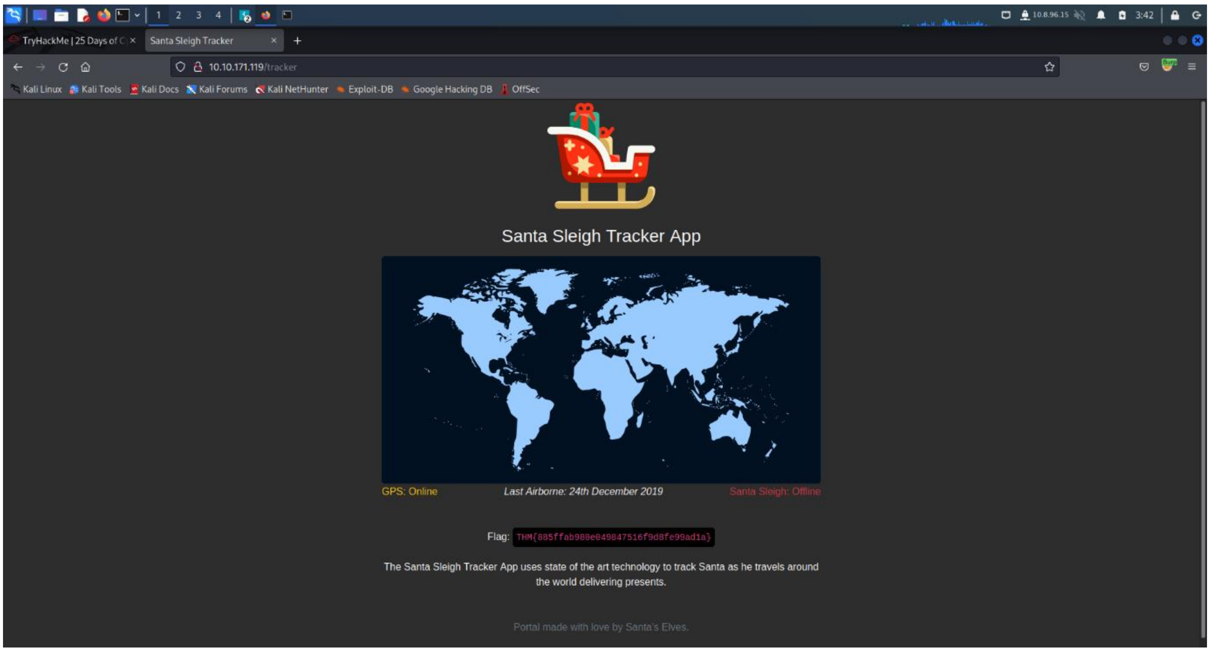
Finished

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

Based on the picture shown, the eight request receive different length compared to others so, we went back to the website and insert the username and password from the eight request. We manage to brute force into the website and receive our flag.



Santa Sleigh Tracker App

GPS: Online Last Airborne: 24th December 2019 Santa Sleigh: Offline

Flag: THM{885ffab980e049847516f9d8fe99ad1a}

The Santa Sleigh Tracker App uses state of the art technology to track Santa as he travels around the world delivering presents.

Portal made with love by Santa's Elves.

Thought Process/Methodology:

Firstly, we read the Default Credentials to receive answers for questions 1 till 3. Next, we needed to find the port number for Burp, thus we had to click on the icon (FoxyProxy) at the top right corner to choose options in which the results would be shown. Then, in order to find the proxy type, we had to click the add option to gain access to "Add Proxy". We clicked the decoder on the BurpSuite Community Edition to encode the URL for 'PSP0201' by typing it in the given space. We then proceeded on open the website by using the IP address provided. Next, we clicked on applications and chose BurpSuite Community under "others". When BurpSuite has loaded, we turned the intercept on. Once that has been done, we use random username(idk) and password(idk) to log in so it would show up in the proxy tab as a captured request. We then sent it to the intruder. We cleared the pre-selected positions under the intruder tab. Later, we highlighted the username and password values and clicked add. We then moved on to selecting “Cluster Bomb” for the attack type. Last but not least, we clicked on the “payloads” tab and set it to 1 for username. Then we added 3 common defaults which were admin, root and user. On the other hand, for password, we change payload set to 2 and added another 3 common defaults which were password, admin and 12345. After that, we clicked “Start attack” to receive results. With the results shown, we were able to identified username and password that will give us access into the page. With the credentials, we went back to the webpage and insert the details in order to get access and finally obtained the flag.