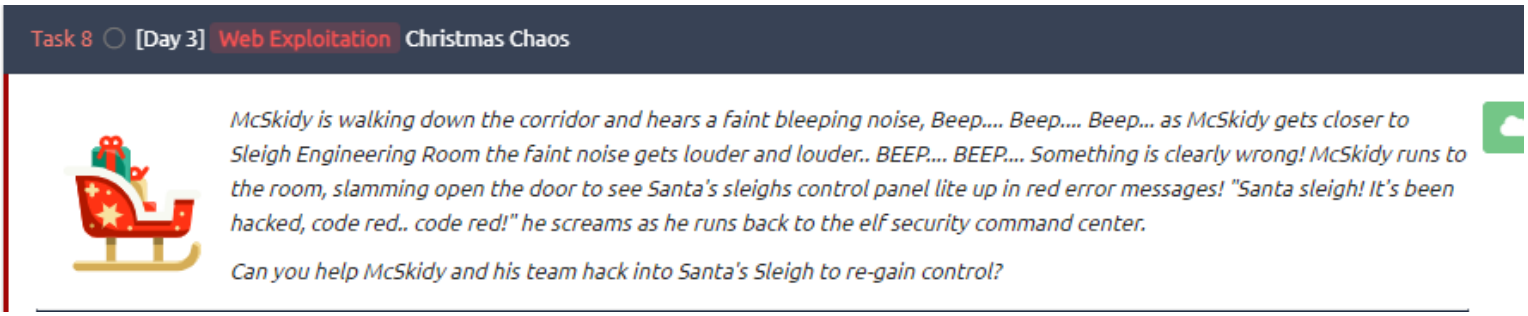
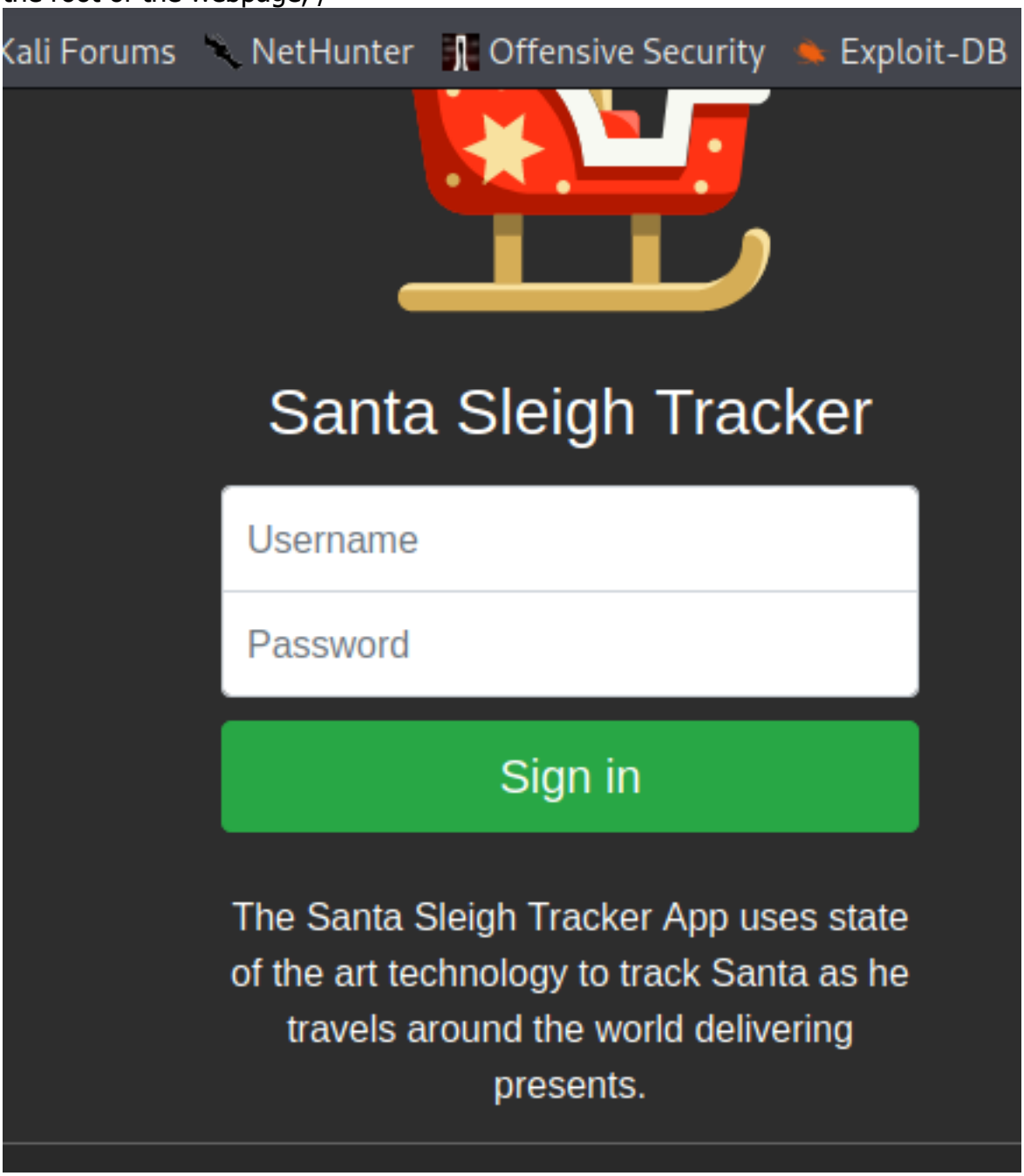
Day 3 - Christmas Chaos

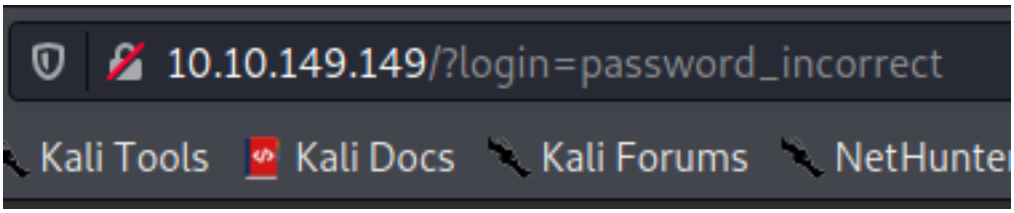
Scenario



the root of the webpage, /



try logging in as admin:admin & the url shows password incorrect



now let's use burpsuite to intercept the packet & perform some default credentials testing on the login page

send to intruder & use cluster bomb attack type as we need to inject 2 different payload on the username & password

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type

Attack type: Cluster bomb

```
1  POST /login HTTP/1.1
2  Host: 10.10.149.149
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Fir
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 29
9  Origin: http://10.10.149.149
10 Connection: close
11 Referer: http://10.10.149.149/?login=password_incorrect
12 Upgrade-Insecure-Requests: 1
13
14 username=§admin§&password=§admin§
```

add 3 user to payload 1

Payload Sets

You can define one or more payload sets. The r
be customized in different ways.

Payload set: 1

Payload type: Simple list

Payload Options [Simple list]

This payload type lets you configure a simple lis

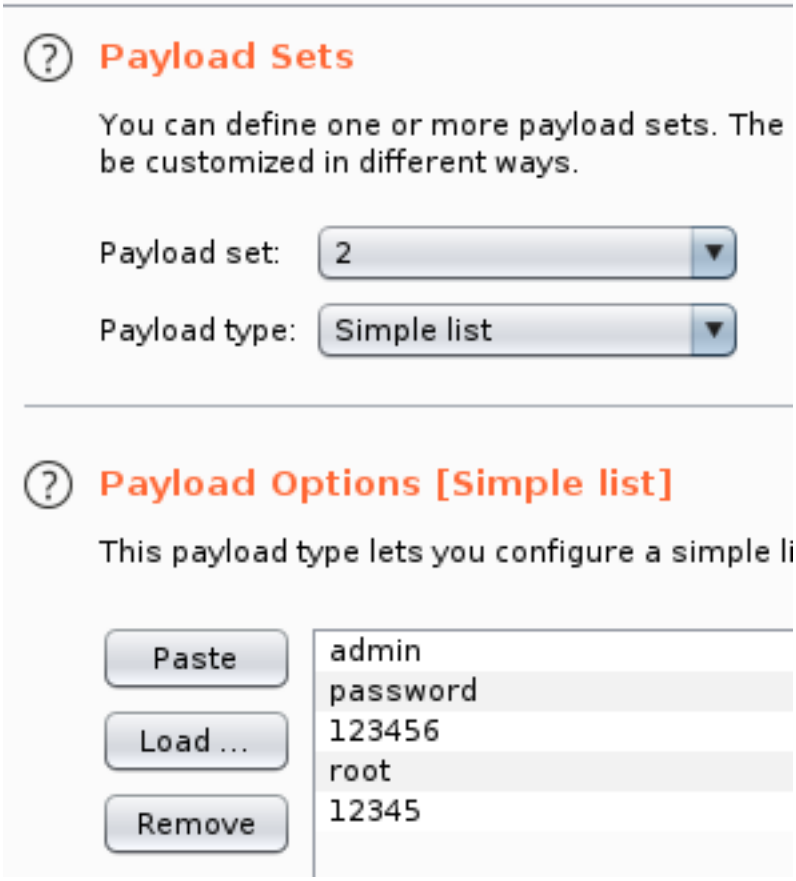
Paste

Load ...

Remove

admin
root
user

add several passwords for payload 2

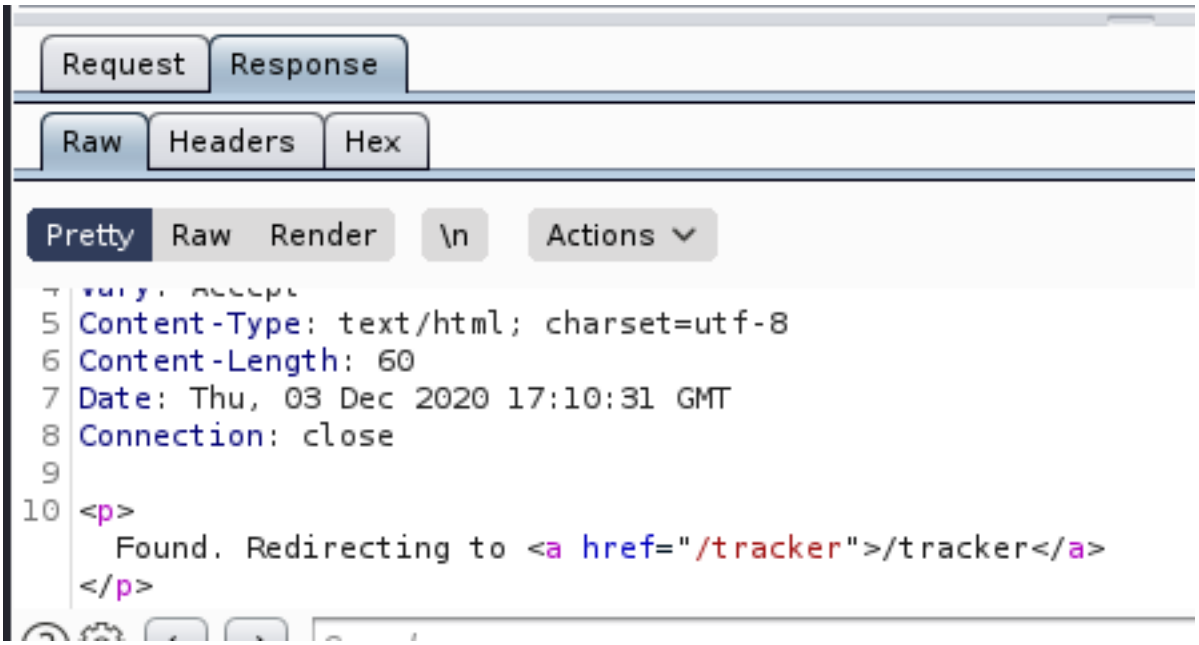


start the intruder attack

if we notice that the length of credential admin:12345 was different from the others

Request	Payload1	Payload2	Status	Error	Timeout	Length
13	admin	12345	302	☐	☐	255
0			302	☐	☐	309
1	admin	admin	302	☐	☐	309
2	root	admin	302	☐	☐	309
3	user	admin	302	☐	☐	309
4	admin	password	302	☐	☐	309

& the response shows that it'll be redirecting to the /tracker directory, so it seems that this was the correct credential



let's login using credential admin:12345 & voila we're in!

the flag are placed below the page