PSP0201 Week 5 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

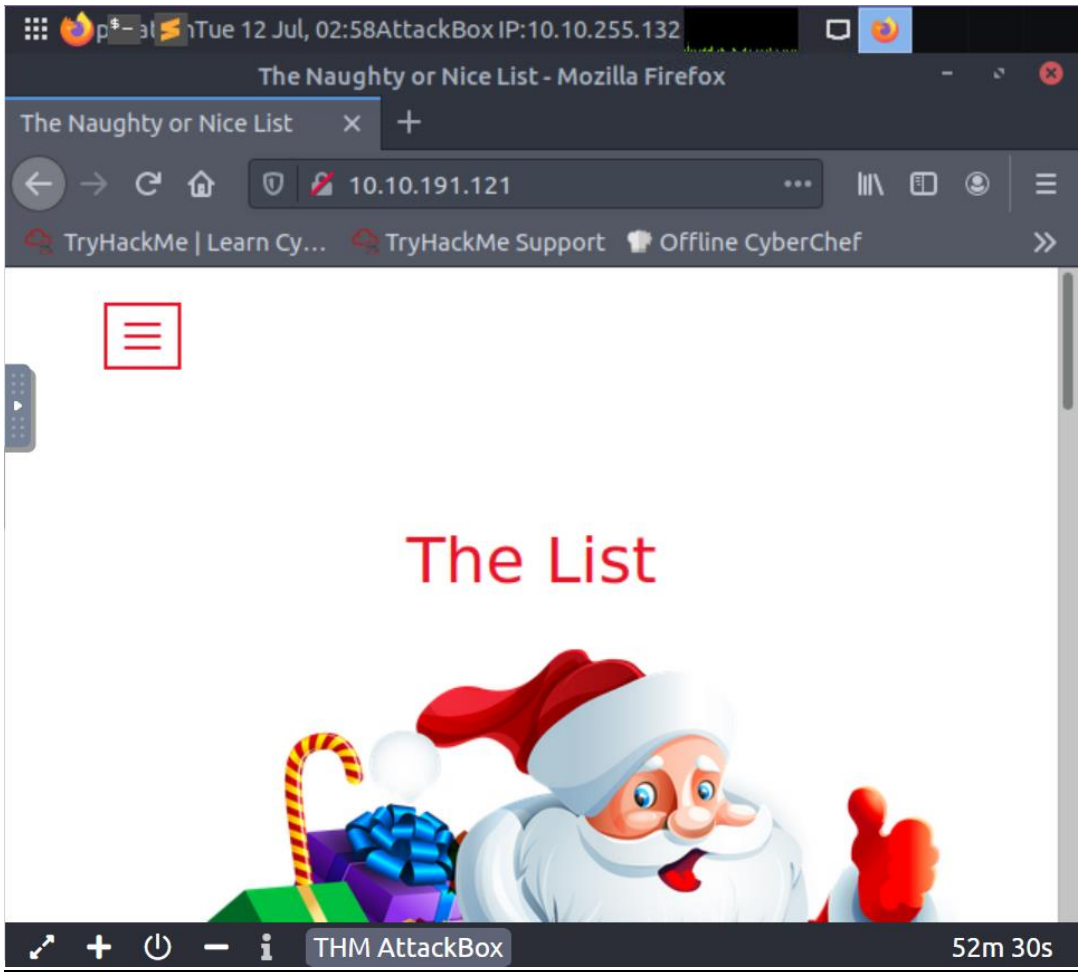
Day 19 : Web Exploitation – The Naughty or Nice List

Tools used: Attackbox, Firefox

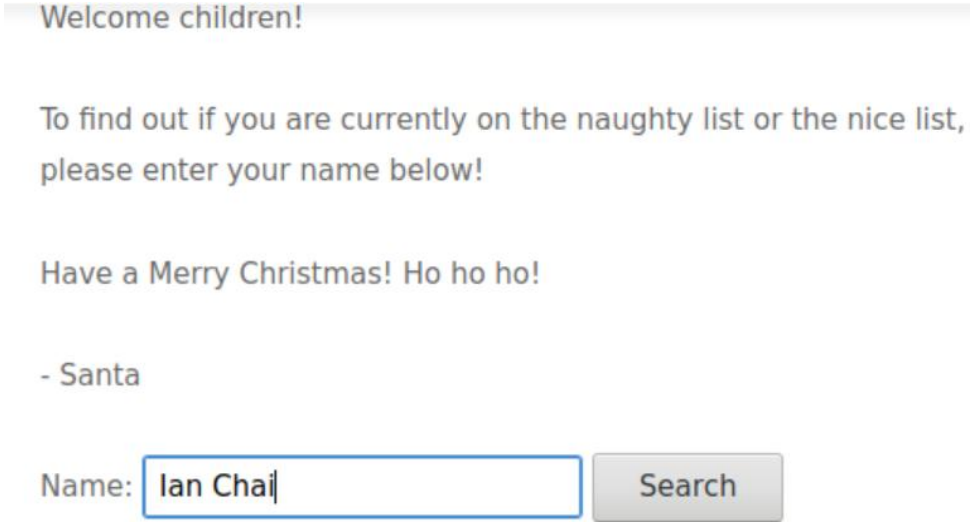
Solution/walkthrough:

Question 1

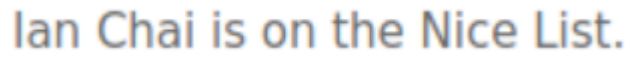
We started by typing in the IP address to get into "The Naughty or Nice List" webpage.



We then entered the name given, in the "Search" button to find out whether they are in the Nice List or the Naughty List.



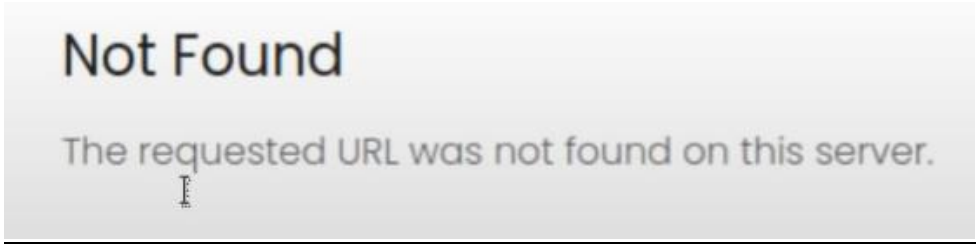
The result, to which list the names are on, would be shown below. Thus, repeat this step to each of the names given and answer the question.



Question 2

We typed in the url given, "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F".

We then scrolled down to find out what was displayed on the page.



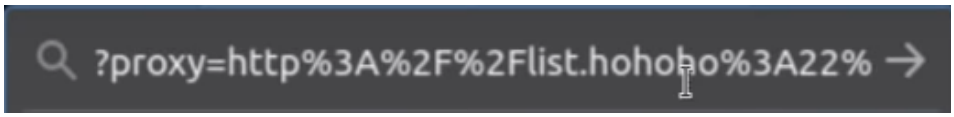
Question 3

We typed in the url given, "/?proxy=http%3A%2F%2Flist.hohoho%3A80".

We then scrolled down to find out what was displayed on the page.

Question 4

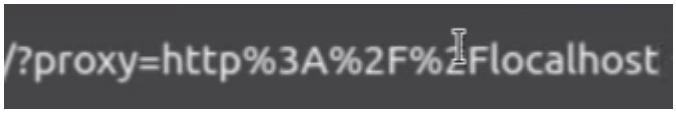
We typed in the url given, "/?proxy=http%3A%2F%2Flist.hohoho%3A22".



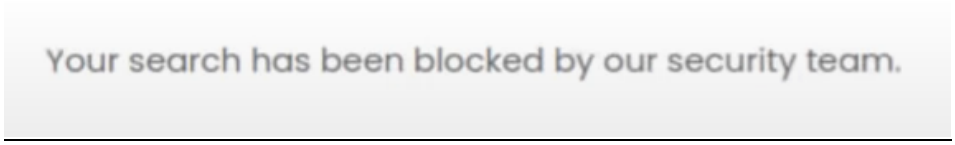
We then scrolled down to find out what was displayed on the page.

Question 5

We typed in the url given, "/?proxy=http%3A%2F%2Flocalhost".

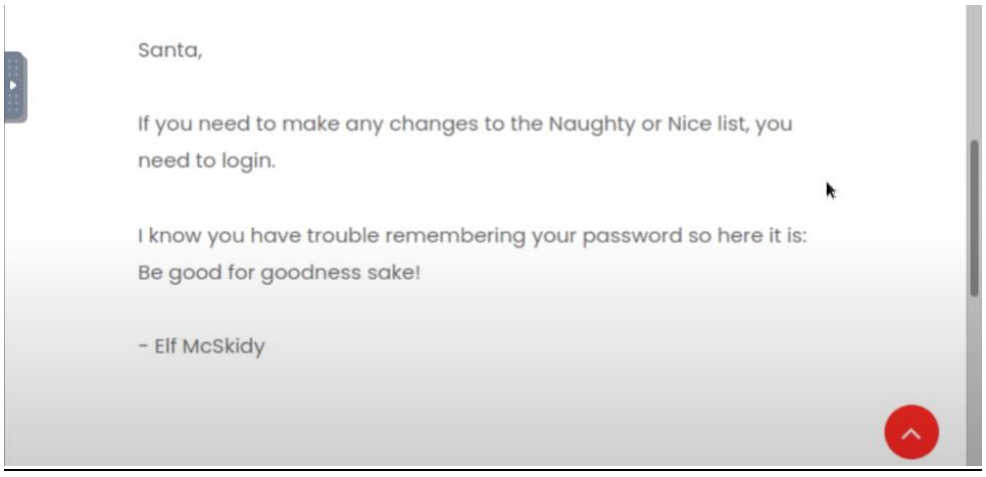


We then scrolled down to find out what was displayed on the page.



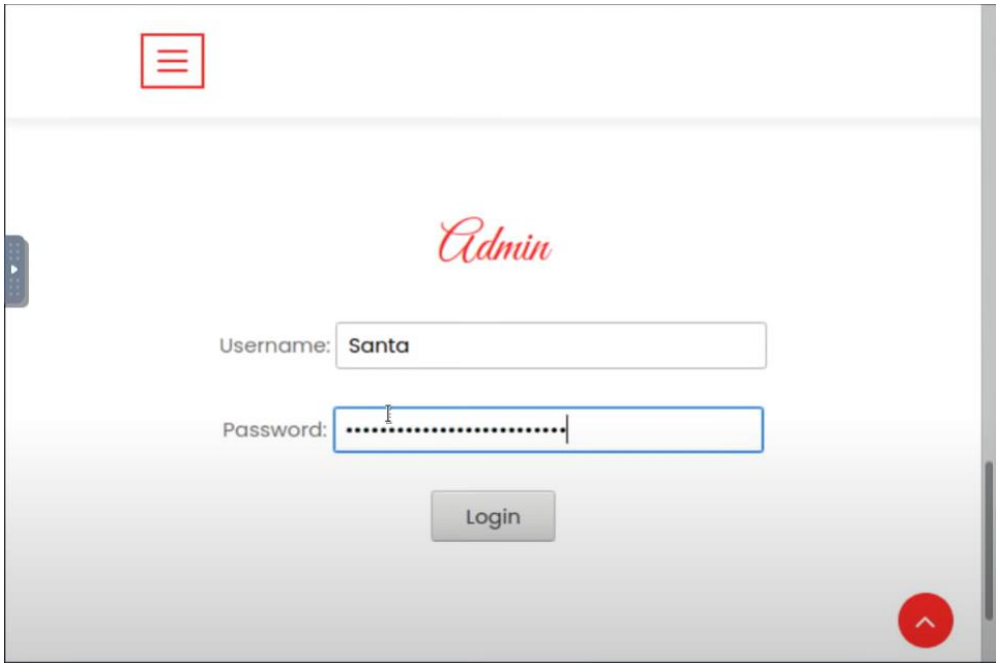
Question 6

We set the hostname in the URL to “list.hohoho.localtest.me” and clicked enter. The webpage showed a message from Elf McSkidy that contained a password. Thus, copy the password.



Question 7

At the admin login, we inserted the username (Santa) and password (Begoodforgoodnesssake!) that we received.



We then had access to the “List Administration” and clicked on the “delete naughty list” option in order to receive the challenge flag. Then, copy the flag.

Thought Process/Methodology:

Firstly, we began by starting our machine and then launched the AttackBox. We proceeded by typing in the IP address that we’ve received in order to get access to the webpage, “The Naughty or Nice List”. Next, we scrolled down to enter the names given one by one and clicked on the “Search” button. We then received a statement below it whether the name we had typed in belongs to the Naughty List or the Nice List. After that, we typed in the URL given, “/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F'' and clicked enter to scroll down and view what’s displayed on the webpage. We repeated this process for the rest of the URL’s, “/?proxy=http%3A%2F%2Flist.hohoho%3A80'', “/?proxy=http%3A%2F%2Flist.hohoho%3A22”, “/?proxy=http%3A%2F%2Flocalhost”. Next, we set the hostname in the URL to “list.hohoho.localtest.me” and clicked enter. Once the webpage was loaded, we scrolled down to find out that a message was shown from Elf McSkidy in which it contained a password. Thus, we

managed to copy it. The reason why we used localtest was because it resolves every subdomain to 127.0.0.1 and therefore, we were able to bypass the check and access local services with the hostname set as said before. Lastly, we clicked the “Admin” link at the top, then scrolled down to the login site and inserted the username (Santa) as well as the password(Begoodforgoodnesssake!) that we received. This enabled us to get through and reach the “List Administration''. We proceeded by clicking on the “delete naughty list” option in order to receive the challenge flag and copied it.