PSP0201 Week 5 Writeup

Group Name: ikun no 1

Members

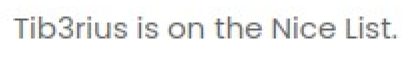
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 19 - [Web Exploitation] The Naughty or Nice List

Tool used: kali Linux, Firefox

Solution/Walkthrough:

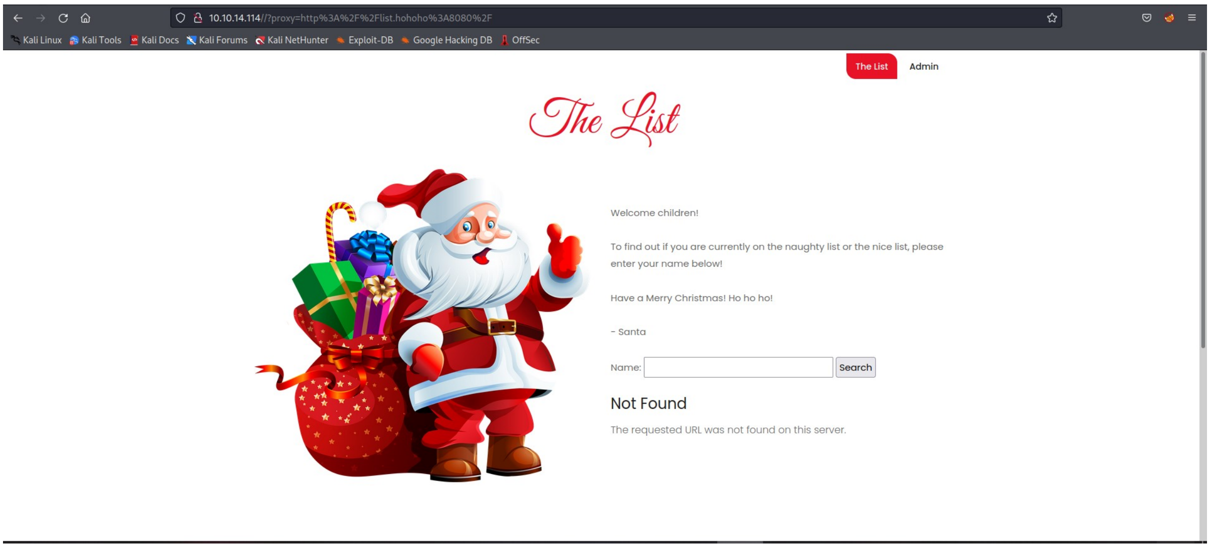
Q1



Tib3rius is on the Nice List.

Access to the site and type in the name into the query and the results will be shown.

Q2



10.10.14.114//?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F

Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

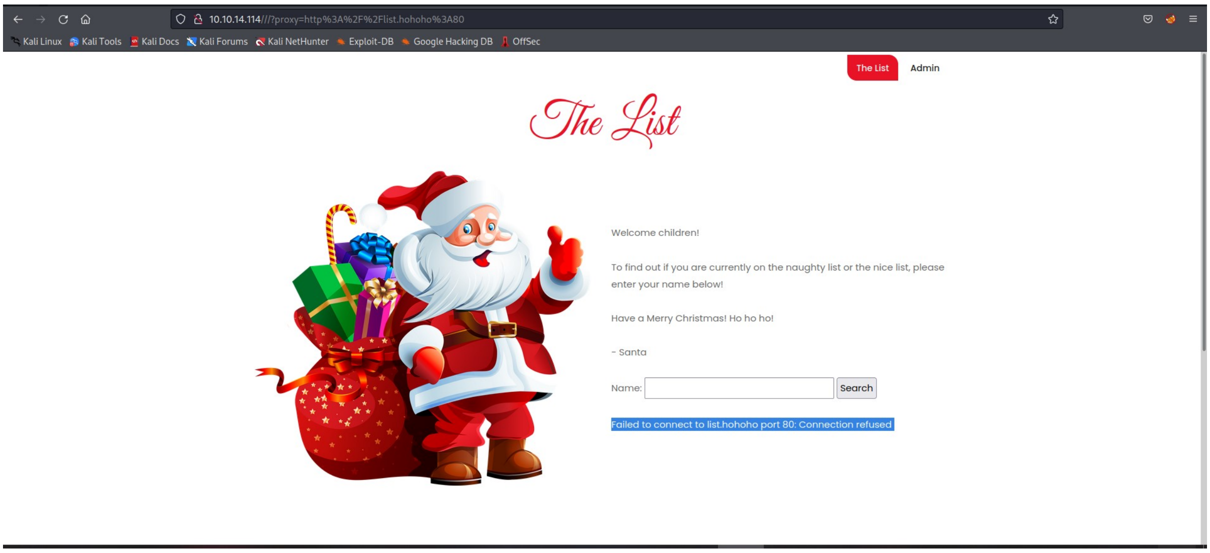
- Santa

Not Found

The requested URL was not found on this server.

It does not work because it shows “The requested URL was not found on this server.”

Q3.



10.10.14.114///?proxy=http%3A%2F%2Flist.hohoho%3A80

Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

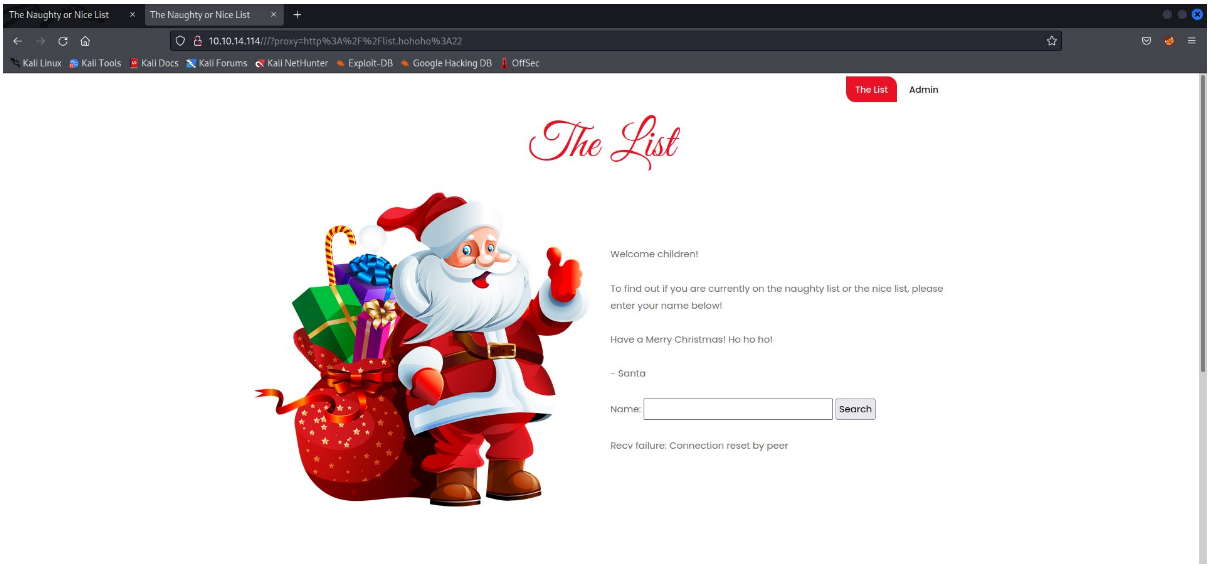
Have a Merry Christmas! Ho ho ho!

- Santa

Failed to connect to list.hohoho port 80: Connection refused

The results “Failed to connect to list.hohoho port 80: Connection refused” will be shown.This is because port 80 is not open.

Q4.



10.10.14.114///?proxy=http%3A%2F%2Flist.hohoho%3A22

Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

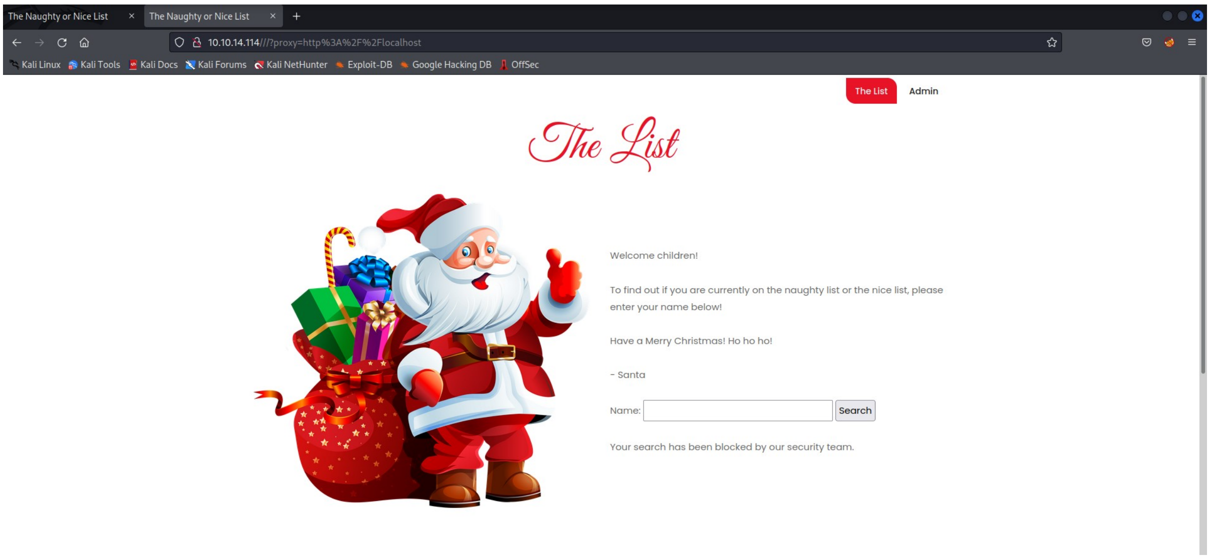
- Santa

Name: Search

Recv failure: Connection reset by peer

It shows “Recv failure: Connection reset by peer”. This means the port is open and can be accessed through ssh but since we are trying to access it through http so it does not work.

Q5.



10.10.14.114///?proxy=http%3A%2F%2Flocalhost

Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

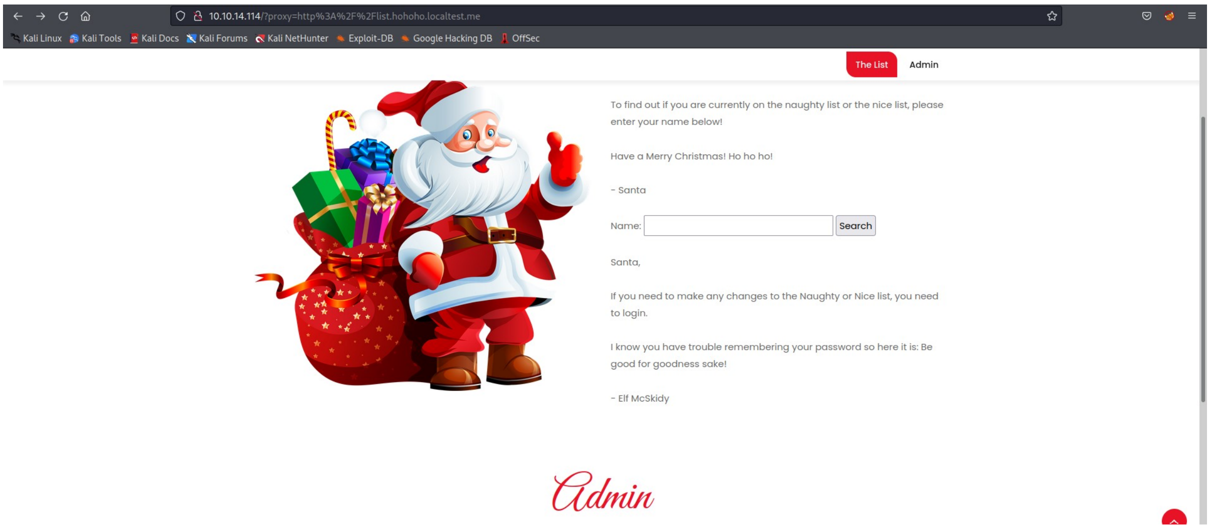
- Santa

Name: Search

Your search has been blocked by our security team.

It does not let us access because the security team only allows host names starting with “list.hohoho”.

Q6.



To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

Santa,

If you need to make any changes to the Naughty or Nice list, you need to login.

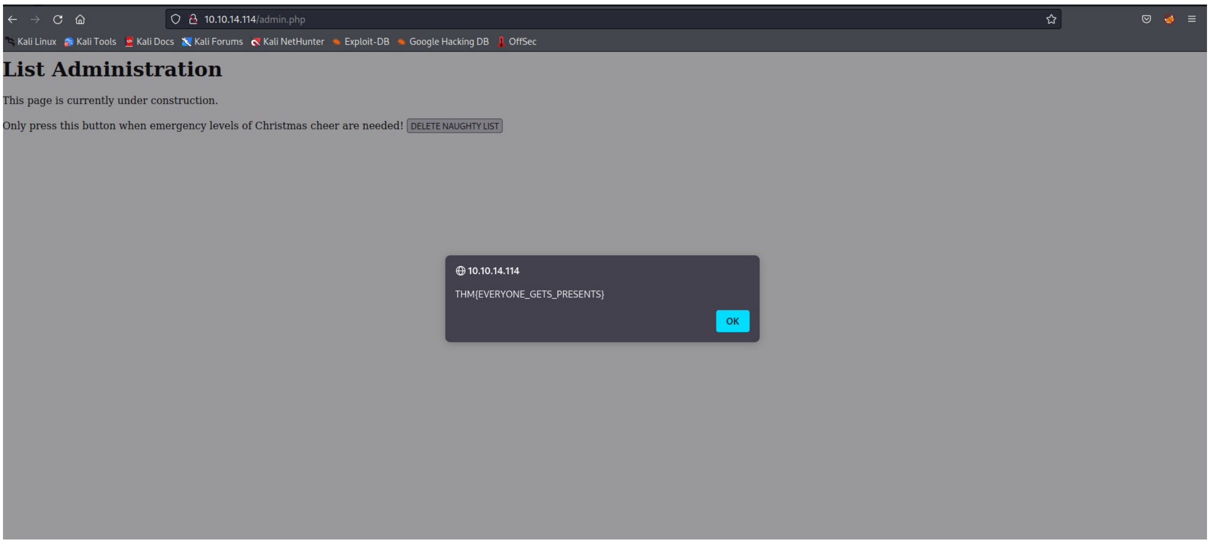
I know you have trouble remembering your password so here it is: Be good for goodness sake!

- Elf McSkidy

Admin

We can bypass this by using the other subdomain behind the hostname. In this case we are using “localtest.me” to set the hostname in the URL to "list.hohoho.localtest.me" and the local services can be accessed. The password now can be found.

Q7.



List Administration

This page is currently under construction.

Only press this button when emergency levels of Christmas cheer are needed! DELETE NAUGHTY LIST

10.10.14.114

THM{EVERYONE_GETS_PRESENTS}

OK

Login into the site with the credential info we can get from Q6. Delete the naughty list and the flag can be captured.