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

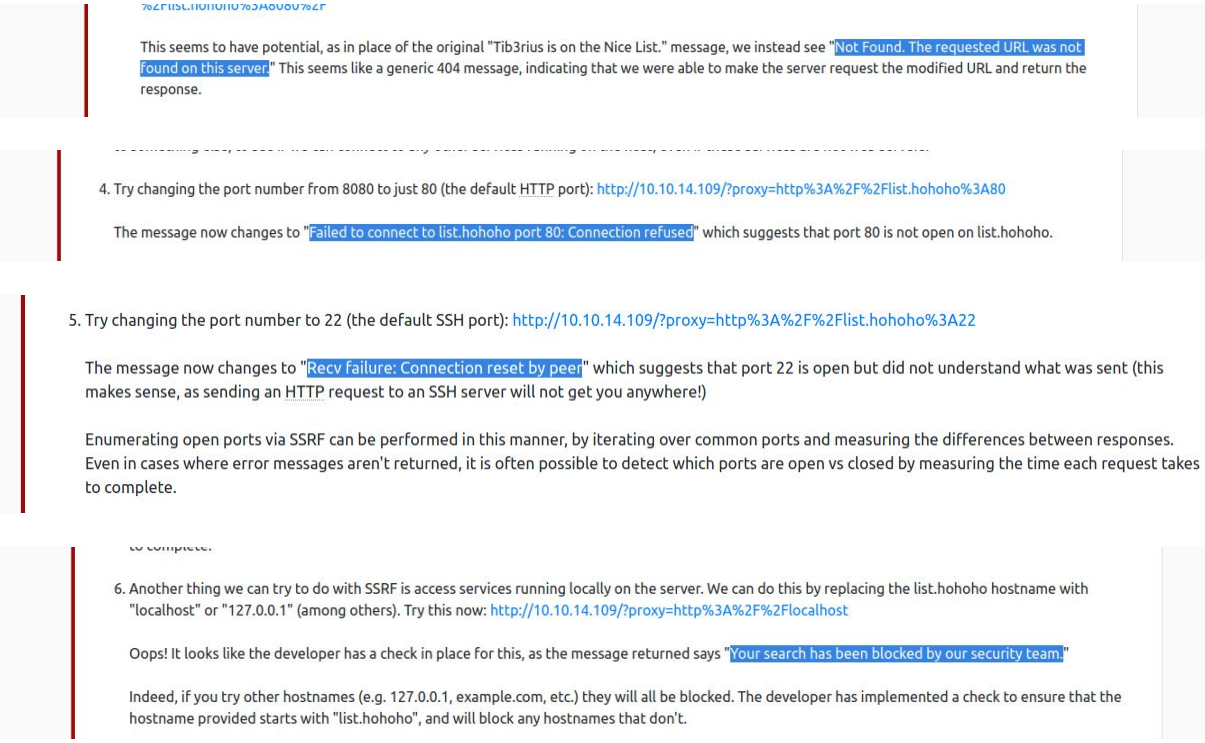
Tool Used: Kali Linux, firefox, Remmina, ILSpy

Solution/walkthrough:

Q1

key in the name one by one to find out if the person is on naughty or nice list.

Q2&Q3&Q4&Q5



%2Flist.hohoho%3A8080%2F

This seems to have potential, as in place of the original "Tib3rius is on the Nice List." message, we instead see "Not Found. The requested URL was not found on this server" This seems like a generic 404 message, indicating that we were able to make the server request the modified URL and return the response.

4. Try changing the port number from 8080 to just 80 (the default HTTP port): http://10.10.14.109/?proxy=http%3A%2F%2Flist.hohoho%3A80

The message now changes to "Failed to connect to list.hohoho port 80: Connection refused" which suggests that port 80 is not open on list.hohoho.

5. Try changing the port number to 22 (the default SSH port): http://10.10.14.109/?proxy=http%3A%2F%2Flist.hohoho%3A22

The message now changes to "Recv failure: Connection reset by peer" which suggests that port 22 is open but did not understand what was sent (this makes sense, as sending an HTTP request to an SSH server will not get you anywhere!)

Enumerating open ports via SSRF can be performed in this manner, by iterating over common ports and measuring the differences between responses. Even in cases where error messages aren't returned, it is often possible to detect which ports are open vs closed by measuring the time each request takes to complete.

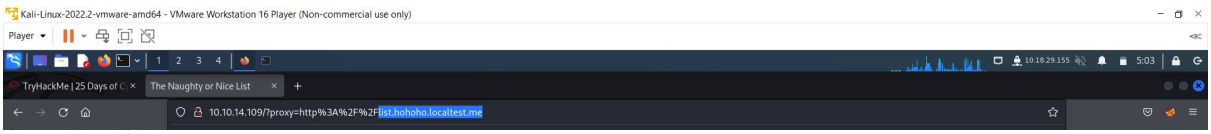
6. Another thing we can try to do with SSRF is access services running locally on the server. We can do this by replacing the list.hohoho hostname with "localhost" or "127.0.0.1" (among others). Try this now: http://10.10.14.109/?proxy=http%3A%2F%2Flocalhost

Oops! It looks like the developer has a check in place for this, as the message returned says "Your search has been blocked by our security team."

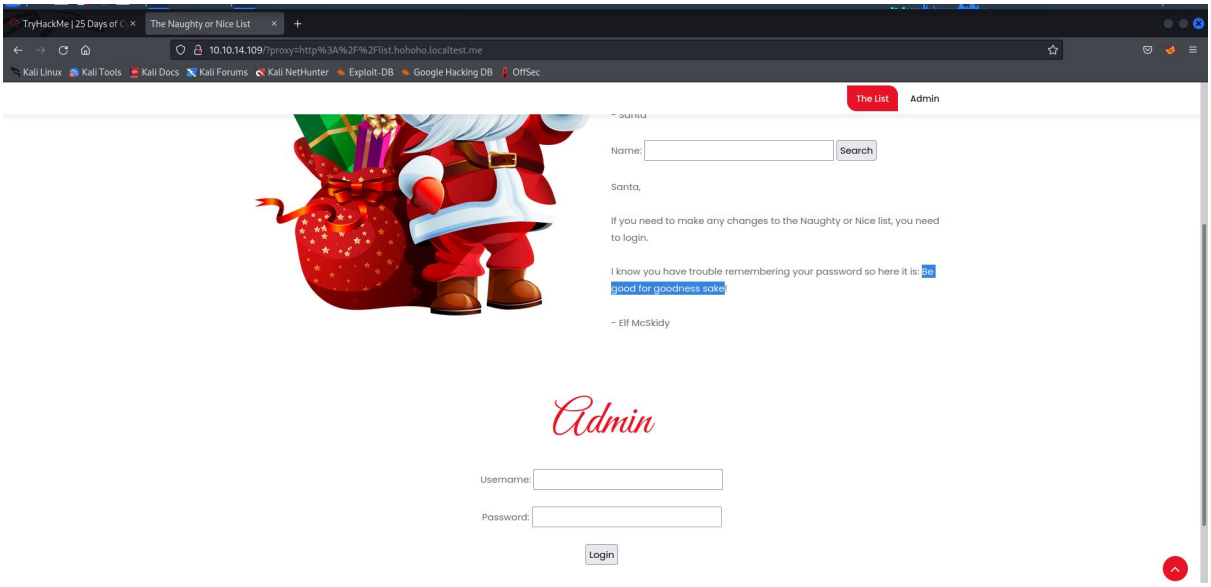
Indeed, if you try other hostnames (e.g. 127.0.0.1, example.com, etc.) they will all be blocked. The developer has implemented a check to ensure that the hostname provided starts with "list.hohoho", and will block any hostnames that don't.

study from Try Hack Me.

Q6

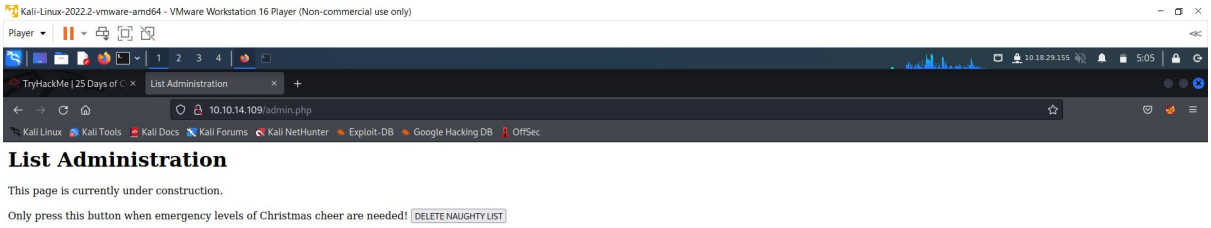


We know that the security team has made a check on 'list.hohoho'. this can can be bypassed with using list.hohoho.[subdomains]. Therefore, we use the domain provided in Try Hack Me to bypass it.

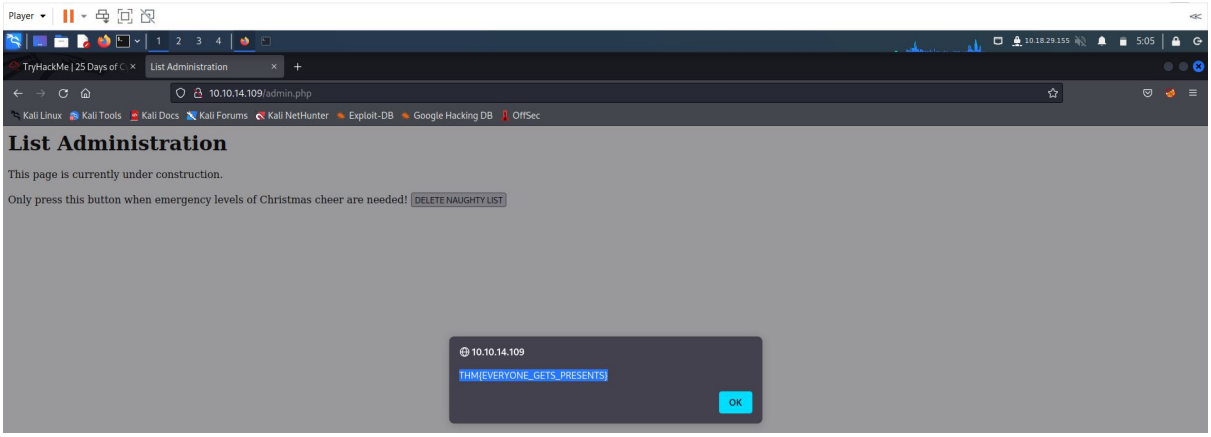


we bypass the check, and the message from Elf McSkidy has been revealed. In the message, we can see Santa's password.

Q7



we login using Santa's password and get into the list Administration. then we delete the naughty list we the button provided.



and click the button, the flag is revealed. capture the challenge flag.