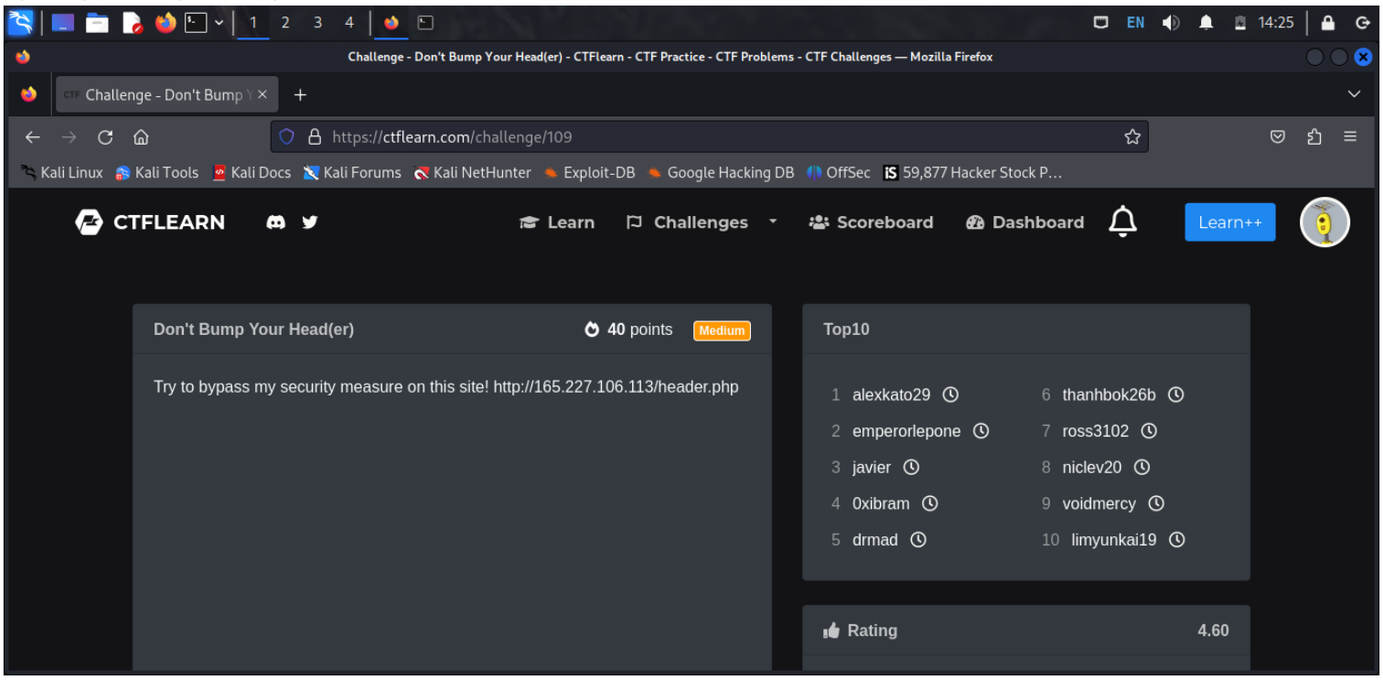
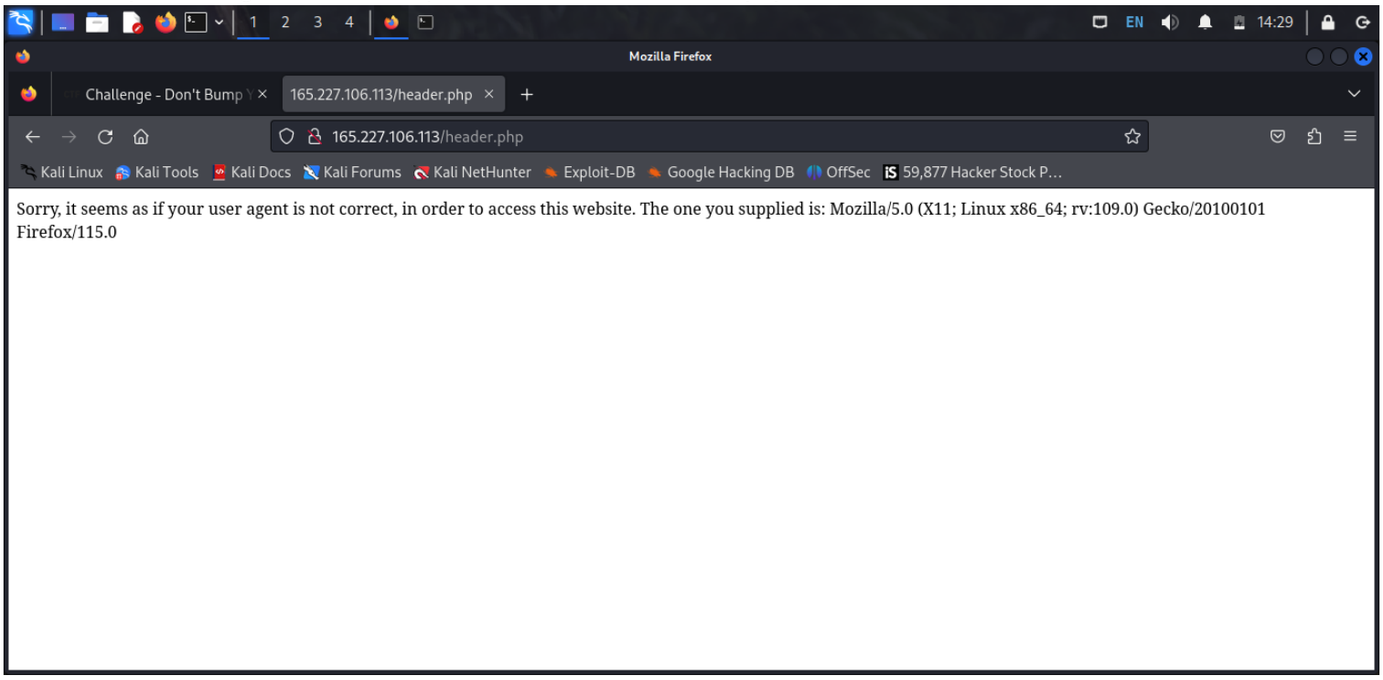
CTF Learn 109

link: https://ctflearn/challenges/109
title: don't bump the header
difficulty: medium

objective:
try to bypass my security measure on this site! http://165.227.106.113/header.php

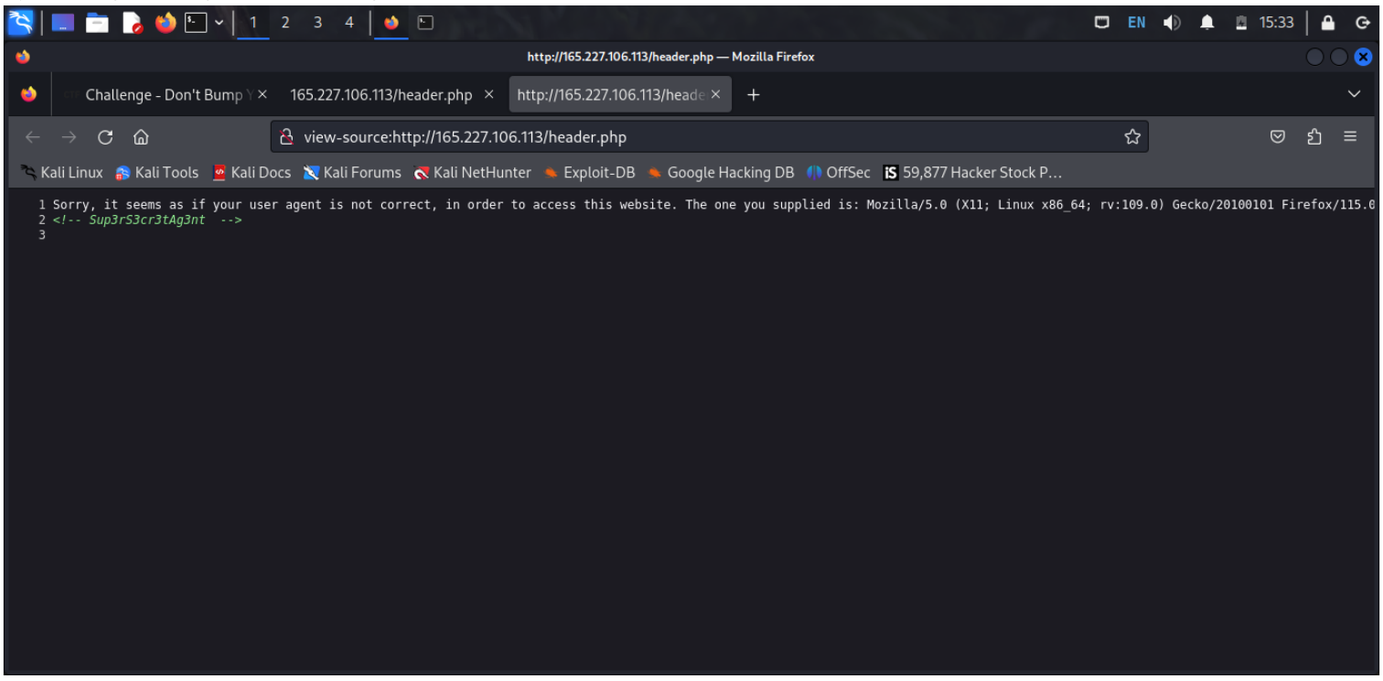


the first step is visiting the website http://165.227.106.113/header.php

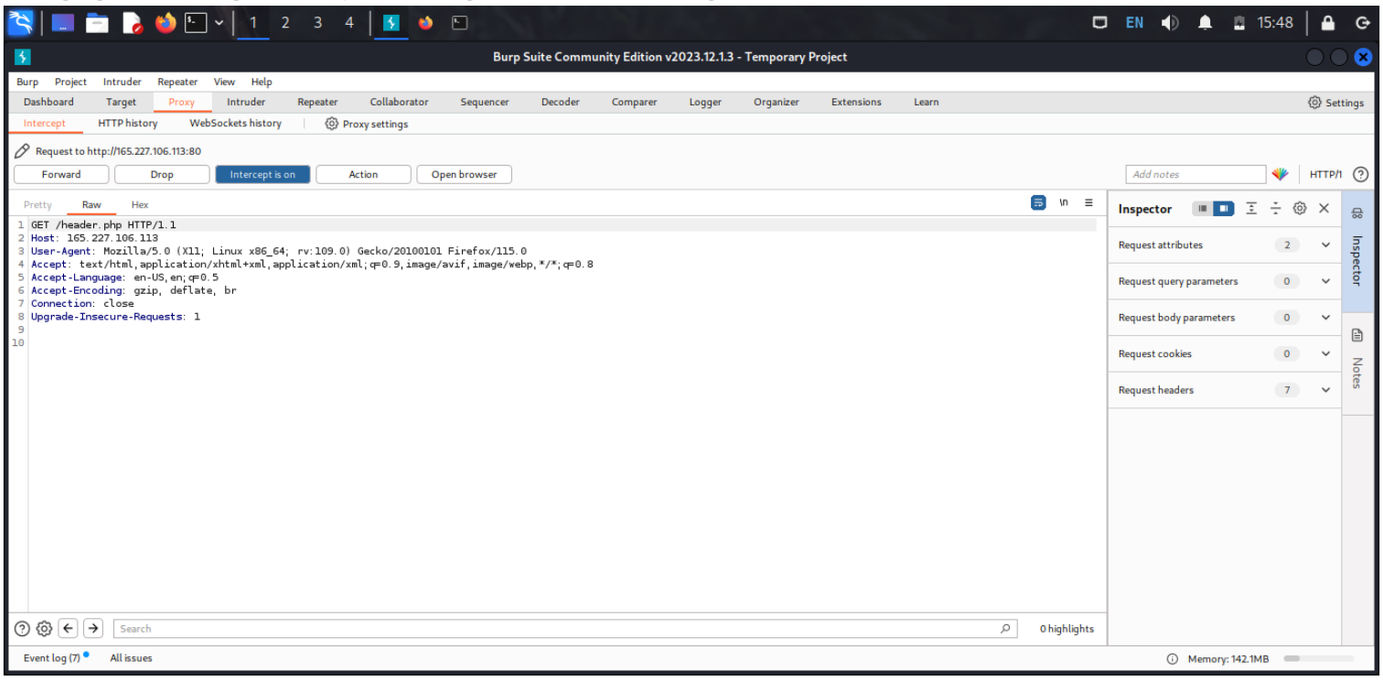


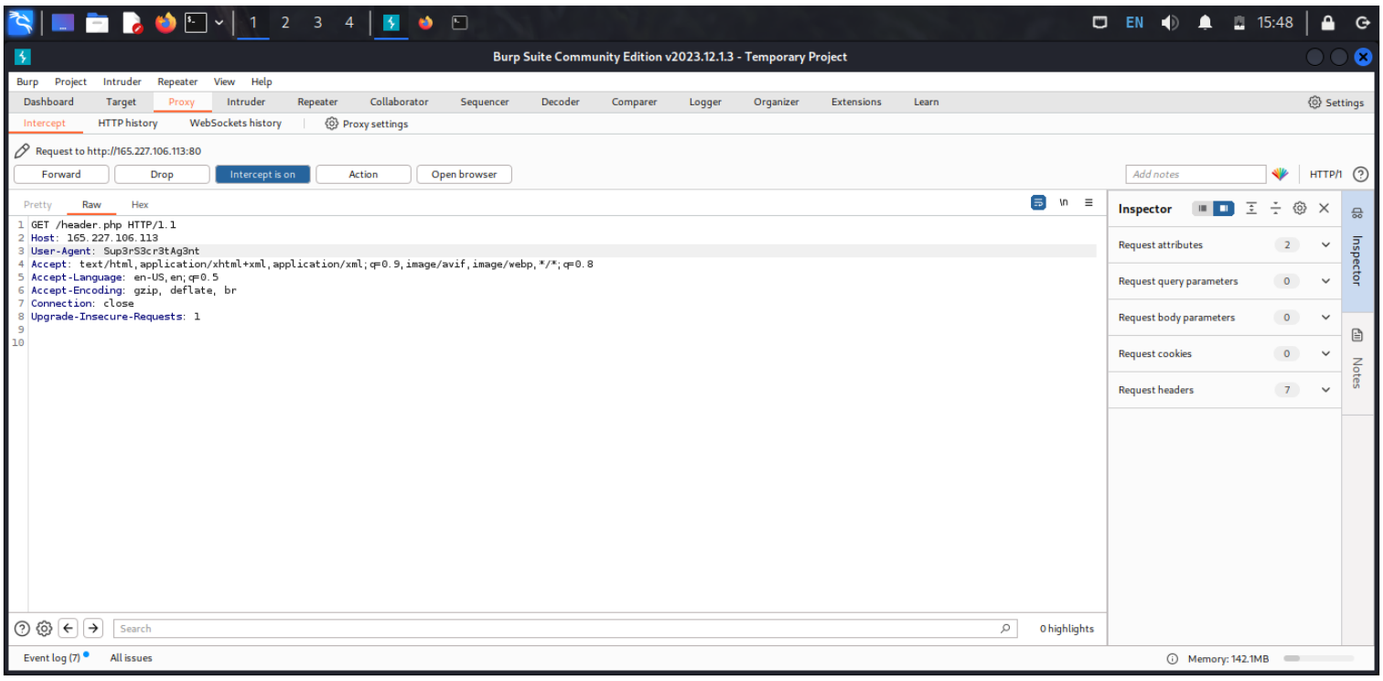
when we visited the url, we saw an error message displayed indicating that our user agent is not correct and we can't access the website, also telling us the version of the user-agent that is in use, which is mozilla 5.0 running on linux.

by viewing the page source, we get this:

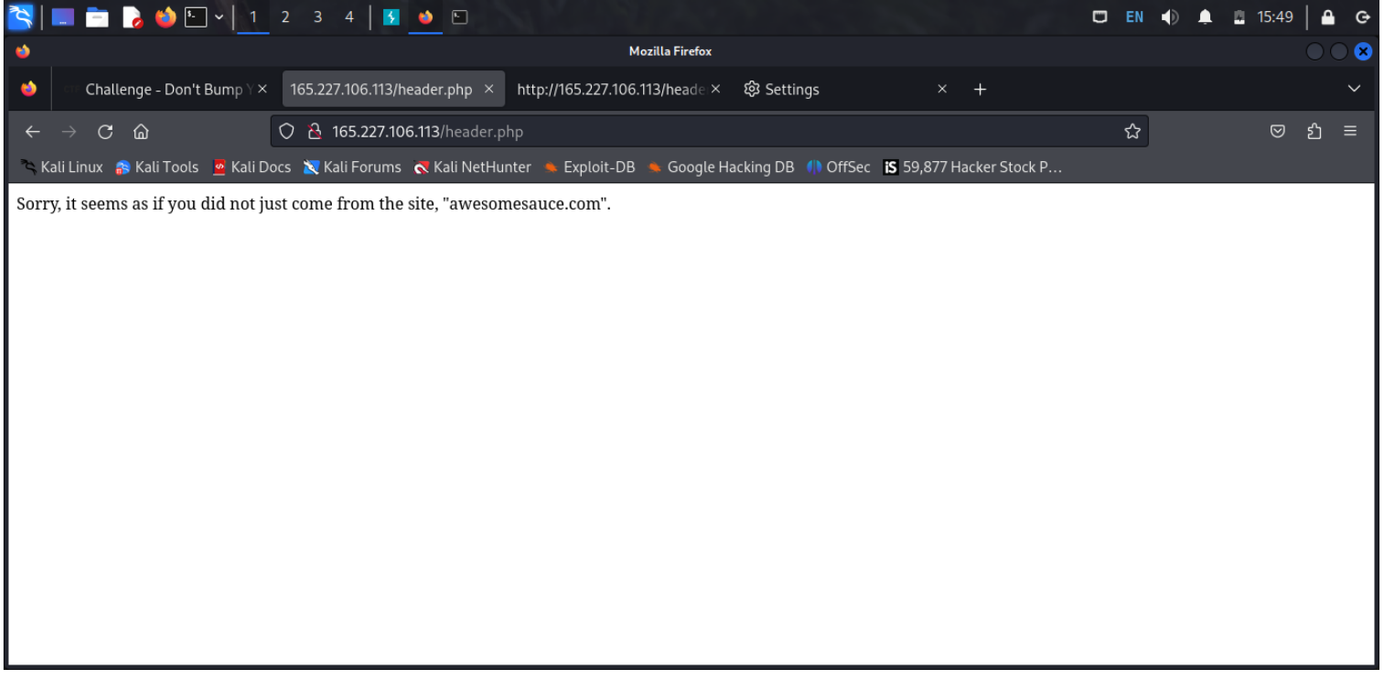


seems the website does'nt want us to have access because we are not using it's preffered user-agent "sup3rs3cr3tag3nt". what we can do now is try to intercept the http traffic and modify the http request with burpsuite and changing the user-agent to sup3rs3cr3tag3nt to see if we can gain access.

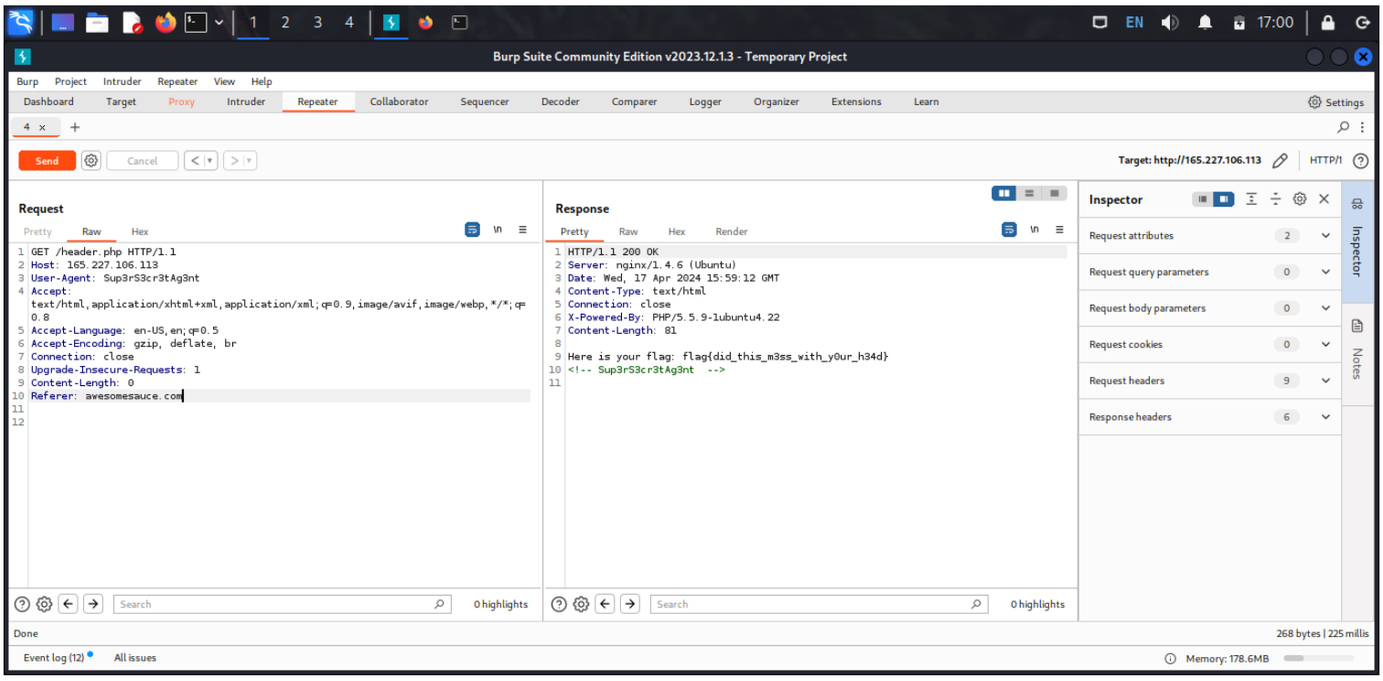




user-agent has been changed to sup3rs3cr3tag3nt, we can now forward the traffic to the target website.



we can see a message aboce saying we didn't come from the site "awesomesauce.com", which means our traffic isn't coming from "awesomesauce.com". we need to reload the page and forward the traffic to repeater to modify the request, then what we need to do is change our user-agent to " sup3rs3cr3tag3nt" again and act like the traffic is being forwarded from "awesomsauce.com" by adding a "referer" line in the header of the request pointing to that website. adding "referer: awesomesauce.com" to the http request header.



we can see we got a flag in the response header
flag: flag{did_this_m3ss_with_y0ur_h34d}