Don't bump your header

ctflearn.com

Jakub Kazimierski February 2023

1 Introduction

This sheet meant to be a walkthrough of CTF challenge from ctf [4]. Here I try to explain step by step what metodology for solving this problem was taken along with actions which were needed. Some of steps will be showed on screenshots and some just explained along with commands used.

OS which was used for this presentation is Kali Linux in version 2022.4

2 Problem overview

Description of this task is short, we should exploit site: [5]. When we open link we get home page:

Figure 1: Site home page

It looks that user agent from Firefox browser is not accepted by this site. Let's inspect this page so maybe we will find some more informations.

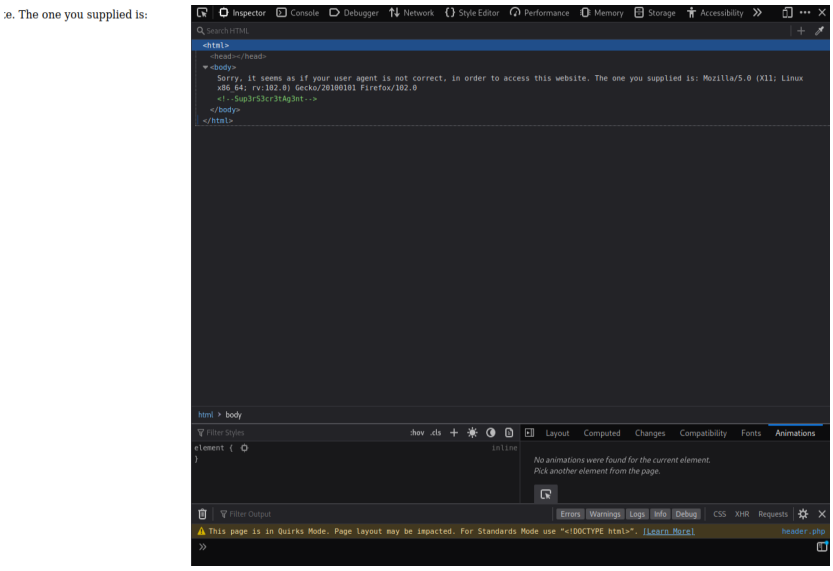

Figure 2: Inspecting page

Well it looks like some kind of clue what should user agent be named like. Lets try to edit name of our user agent while using BurpSuite [1] (also i reccomend to use FoxyProxy [2] to configure browser proxy while working with burp). Ok let's see at intercepted GET request:

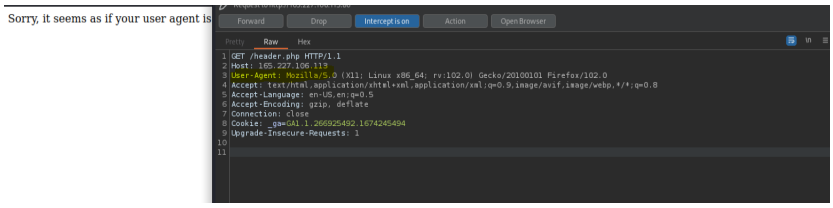

Figure 3: Base get request

User agent field has assigned firefox agent which is not accepted by this site, let's try and replace it with name given in the clue:

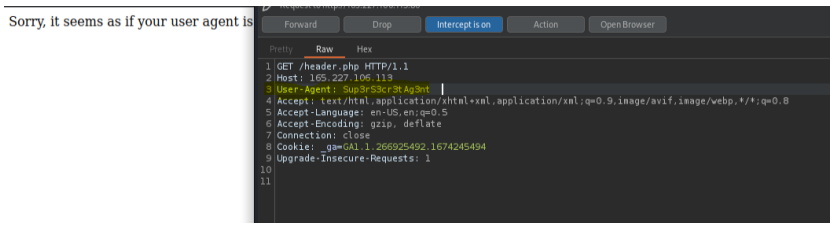

Figure 4: Edited get request

And after we send edited request, returned page is different than before:

Figure 5: Returned page changed

Inspecting this one does not bring any new clues:

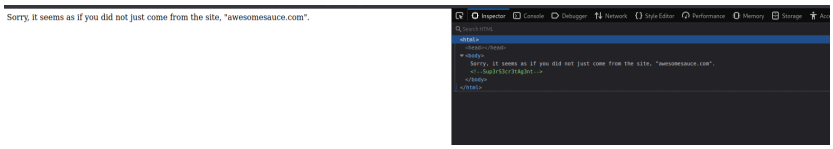

Figure 6: Inspecting returned one

So we have to base on returned message: Sorry, it seems as if you did not just come from the site, "awesomesauce.com".

It looks like the site expecting us to be transferred here from other site, as if we click hyperlink on "awesomesauce.com". Ok it seems to be fair enough to check this address out. But unfortunantely:

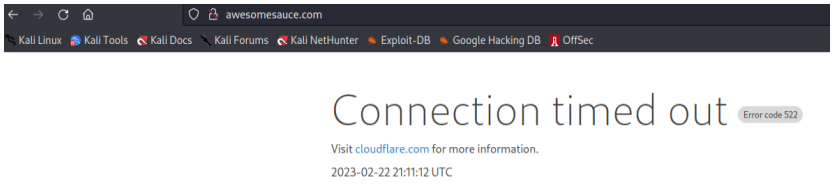

Figure 7: Trying to connect unsucessfull

Is there other way for our connection to look like coming from "awesome-sauce.com"? Yes, let's read about HTTP request heade named Referer [3]. We can find that: The Referer header allows a server to identify referring pages that people are visiting from or where requested resources are being used. This data can be used for analytics, logging, optimized caching, and more.

So let's again intercept our request, and change user agent name, but this time also we will add a header referring to sitw "awesomesauce.com":

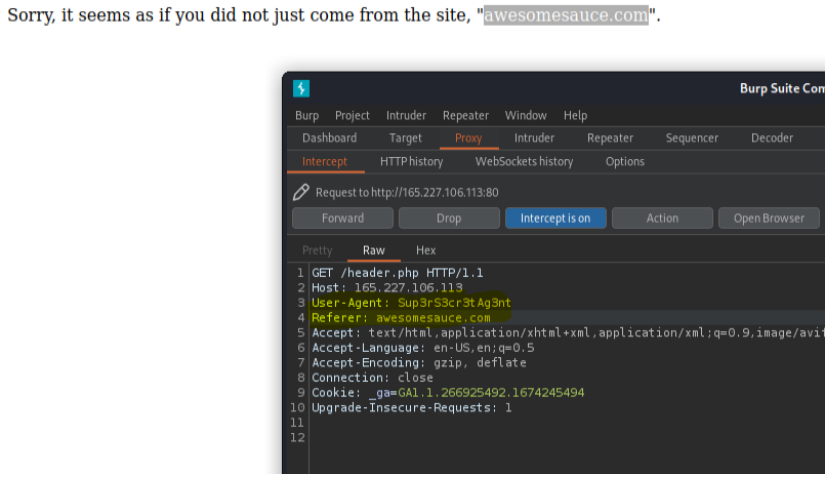

Figure 8: Request with Referer header

And after forwarding we are redirected to flag:

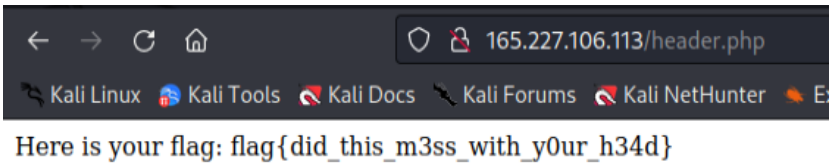

Figure 9: Request with Referer header

Flag: **flag{did_this_m3ss_with_y0ur_h34d}**

References

[1] Burp suite. https://portswigger.net/burp/communitydownload.

[2] Foxyproxy configuration. https://null-byte.wonderhowto.com/how-to/use-burp-foxyproxy-easily-switch-between-proxy-settings-0196630/.

[3] Http request header referer. https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referer.

[4] Reference to site with this challenge. https://ctflearn.com/.

[5] Site to exploit. http://165.227.106.113/header.php.