# Get a Head

# Overview

Points: 40

Category: Web Exploitation

**Appearance : picoCTF 2021**

## Challenge Description

Find the flag being held on this server to get ahead of the competition <http://mercury.picoctf.net:53554/>

# **Hints**

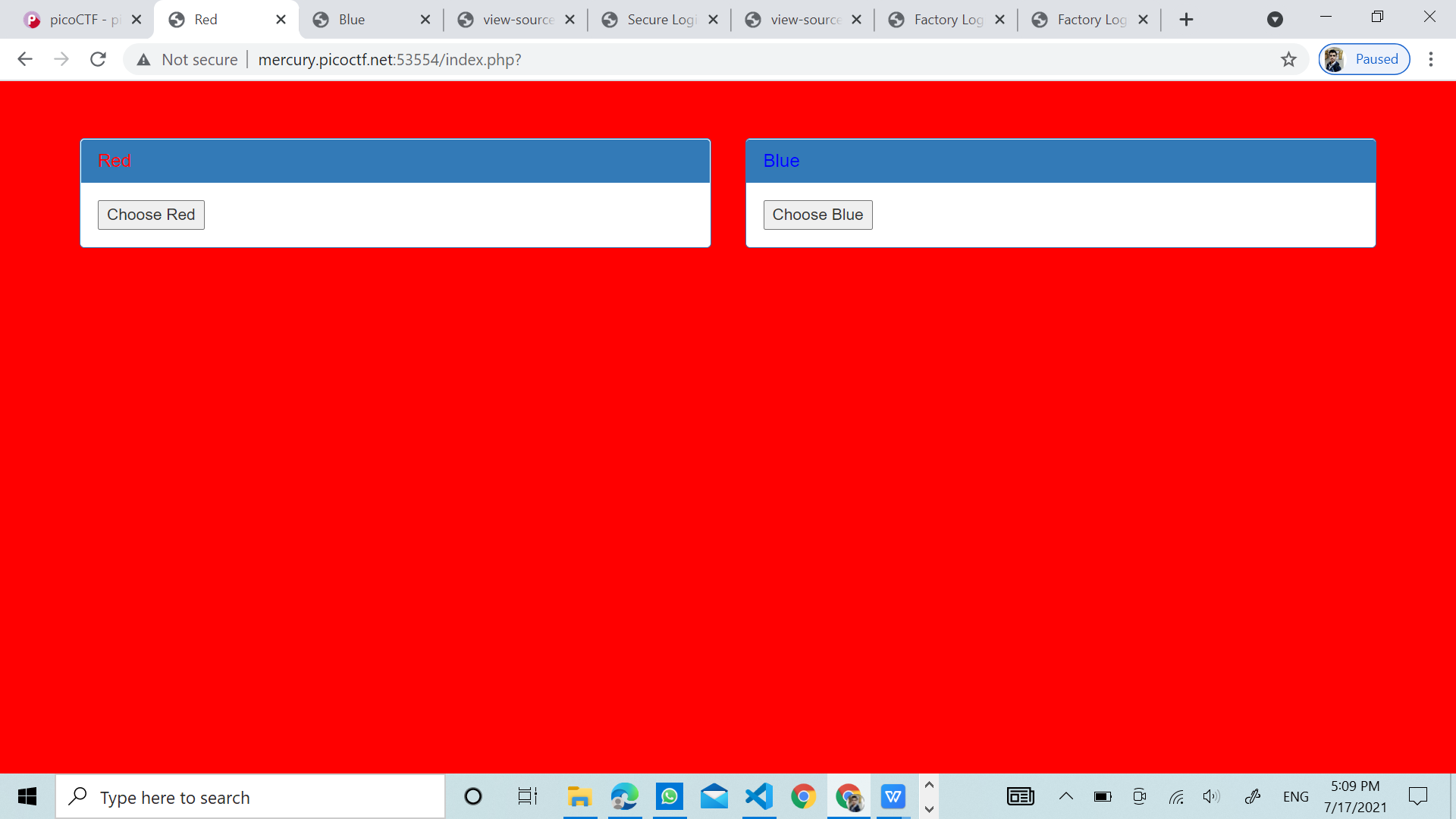
1. Maybe you have more than 2 choices

2. Check out tools like Burpsuite to modify your requests and look at the responses

**# Solution**

Checking out Burp Suite, one of it's main abilities it to intercept and modify requests. [Burp Suite](https://www.sciencedirect.com/topics/computer-science/burp-suite)

Now by inspecting the webpage, we get something that looks like



From here we see that the method that was used for Red was "GET" and for Blue was "POST". We can do more research on these, as they are different HTTP requests.

It makes sense, as we figured earlier that Burp Suite can intercept and change requests. Looking through the list, we see that the second request method is "HEAD" which seems quite familiar. If we look back at the challenge title "Get aHead", the word Head stands out, probably referring to the HTTP Request method "HEAD".

There's different ways to approach this section, but we found downloading "Postman" as a chrome extension the easiest.

After opening up the app (it download as an app), choose the "request" option and create a folder. Feel free to name it whatever you like. From there, insert the website link into the "Enter request url" bar, change the method to "HEAD" and then click send. Now, don't forget to click into the "Headers" tab below, to find the flag!

# Flag

picoCTF{r3j3ct\_th3\_du4l1ty\_6ef27873}

GAURAV JHA