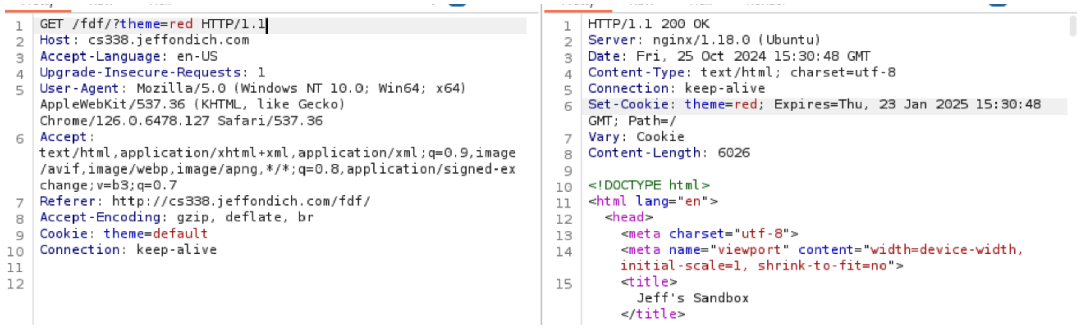
Part 1:

a) There is one, its name is Theme and its value is Default
b) The cookies name stayed the same, but the value changed to red
c) I do see the same cookie values as I did with inspector, it was originally set to default and then when I changed the theme to red it changed the cookies value to red
d) Yes the theme I selected is still there when I relaunch the browser
e) The current theme is transmitted through a header:
Set-Cookie: theme=default: Expires=Thu, 23, Jan 2025
f) The two highlighted sections are the user's request to change the theme and the servers response



```
GET /fdf/?theme=red HTTP/1.1
Host: cs338.jeffondich.com
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.7
Referer: http://cs338.jeffondich.com/fdf/
Accept-Encoding: gzip, deflate, br
Cookie: theme=default
Connection: keep-alive
```

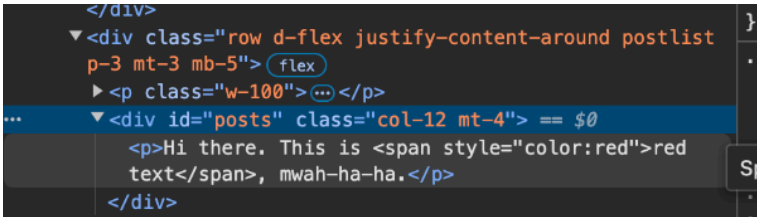
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 25 Oct 2024 15:30:48 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Set-Cookie: theme=red; Expires=Thu, 23 Jan 2025 15:30:48
GMT; Path=/
Vary: Cookie
Content-Length: 6026

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width,
    initial-scale=1, shrink-to-fit=no">
    <title>
      Jeff's Sandbox
    </title>
```

g) You just change the value of the cookie to the theme color you want
h) Use proxy intercept and then change the color on the website and then you get the cookie value for that color and you just simply need to change the color to the one you want and press forward
i) They are stored in my user profile folder

Part 2:

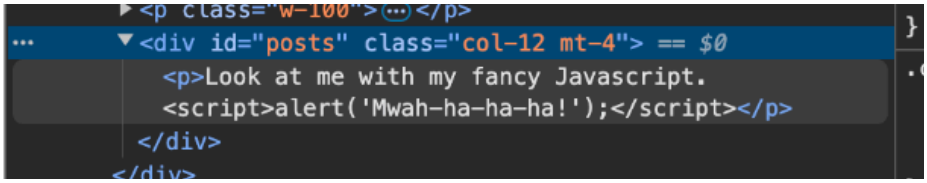
a) Moriarty's first attack is inserting code into the source code through his post and thus the website builder reads it as part of the website's code. thus he is able to change his text color to red



```
</div>
▼<div class="row d-flex justify-content-around postlist
p-3 mt-3 mb-5"> flex
  ▶<p class="w-100">…</p>
  ▼<div id="posts" class="col-12 mt-4"> == $0
    <p>Hi there. This is <span style="color:red">red
    text</span>, mwah-ha-ha.</p>
  </div>
```

Moriarty's second attack does the same thing and he puts javascript into his post and thus is able to get the website to read it as part of its source code and thus pulls up the

pop up



P.S. I don’t know any javascript and someone currently broke the website as I am trying to do this.

b) You can set up a paywall that doesn’t allow you to see the post until the person pays, you just simply include the javascript for that in your post and then your post will be locked behind a paywall

c) I don’t know how to do it, but you can get the entire website to shut down by putting something in your comment

d) To prevent these attacks you could add code to the website that checks a post before it is posted if it has javascript in it or not and not allow it to be posted if it does.