WAPH-Web Application Programming and Hacking

Instructor: Dr. Phu Phung

Student

Name: Ian Cannon

Email: mailto:cannoni1@udayton.edu

Short-bio: Ian Cannon interests in Reinforcement Learning for Autonomous Control.

Ian's headshot

Repository Information

Respository's URL: https://github.com/Spiph/WebAppDev

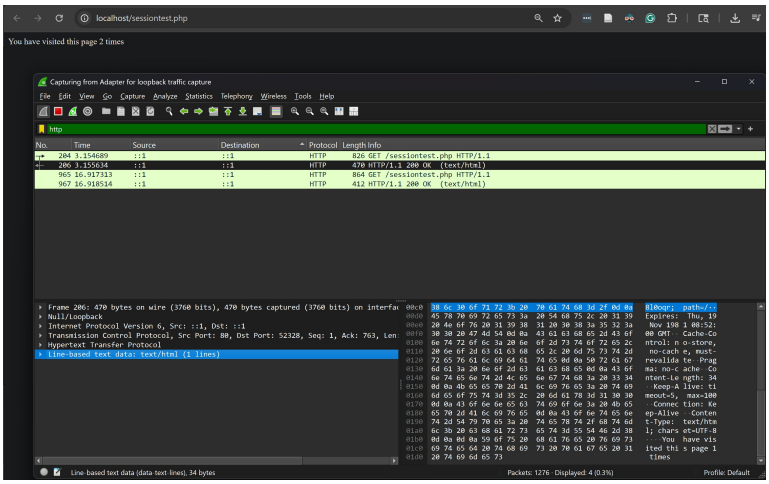
This is a public repository for Ian Cannon to store all code from the course. The organization of this repository is as follows.

Lab 4

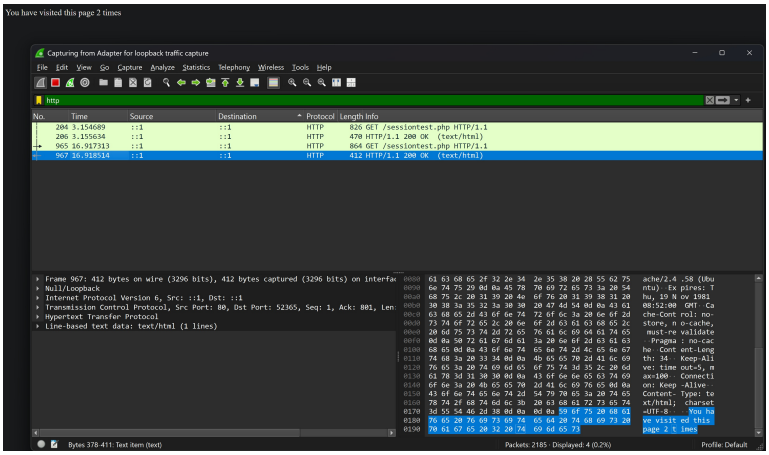
Task 1: Understanding Session Management in a PHP Web Application

1.a. Deploy and test sessiontest.php

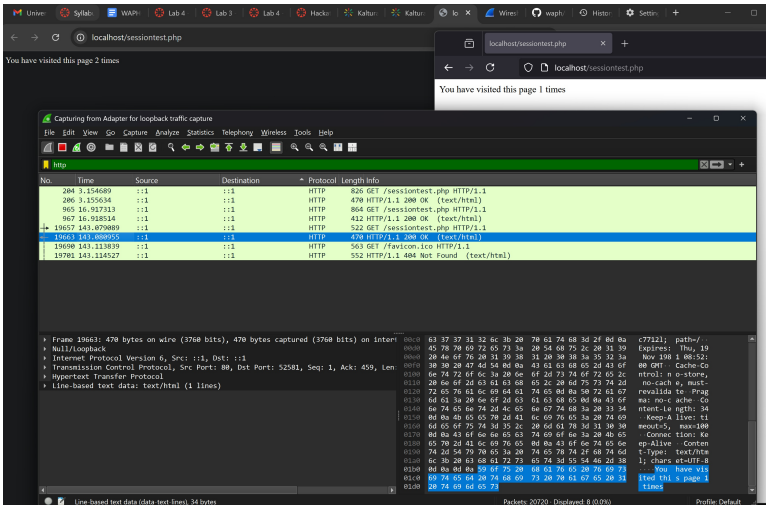
This shows my session is working



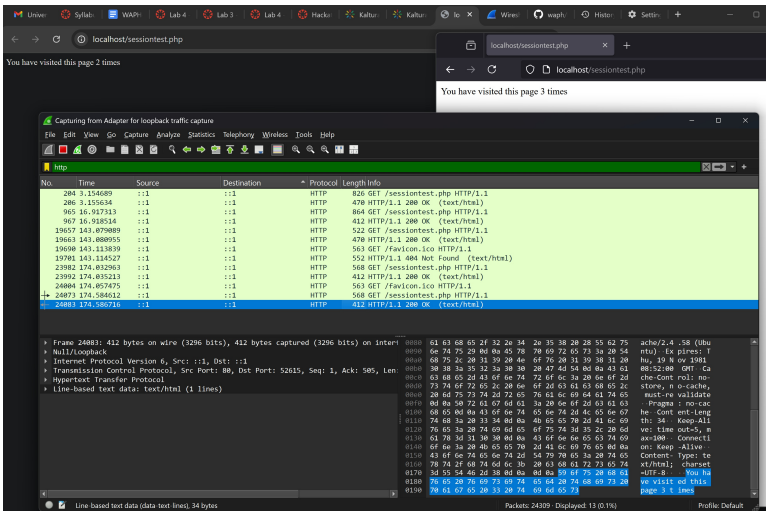
First Visit



Visited Twice



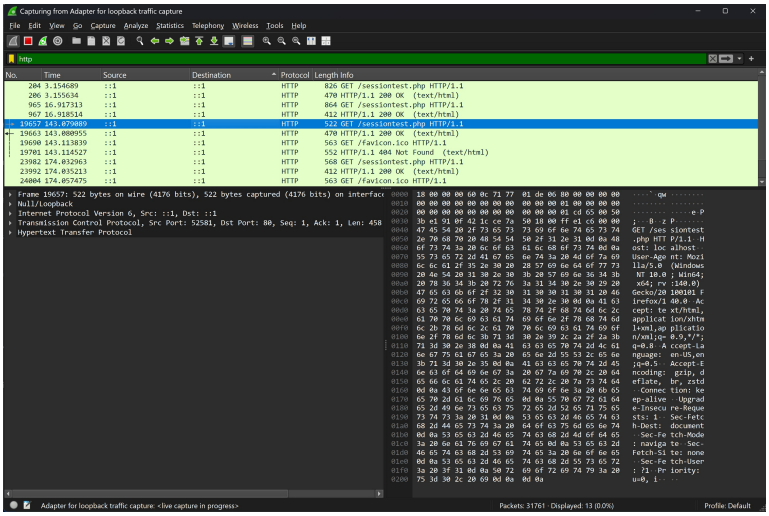
First Time on Firefox



Up to 3 on Firefox

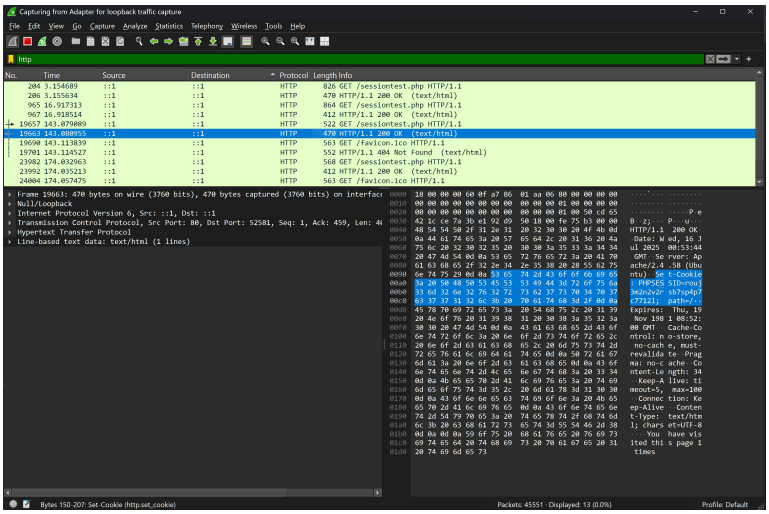
1.b. Observe the Session-Handshaking using Wireshark (6 pts)

Here is the first session on Firefox:



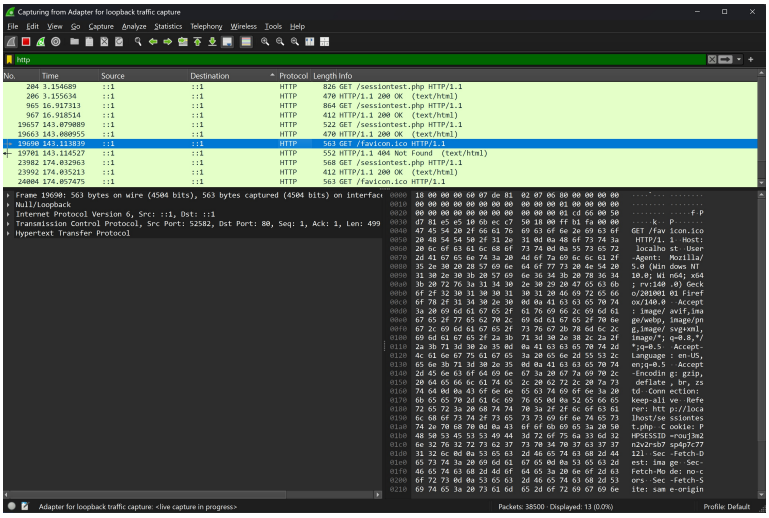
firefox first session

The response assigns an id for the cookie, PHPSESSID:



Mmmmm Cookies

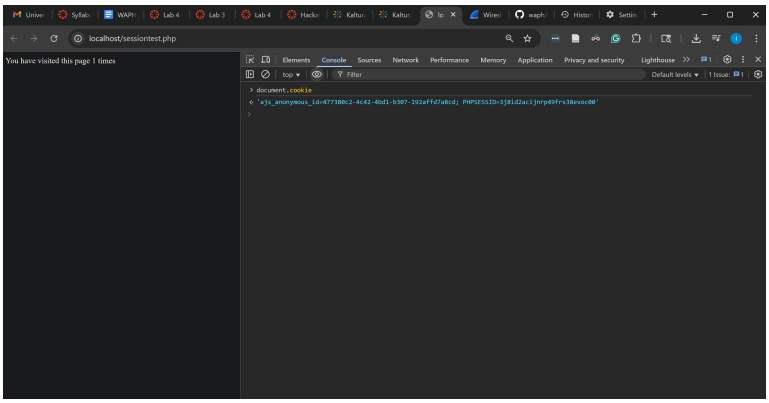
You can see the second GET request now has a cookie:



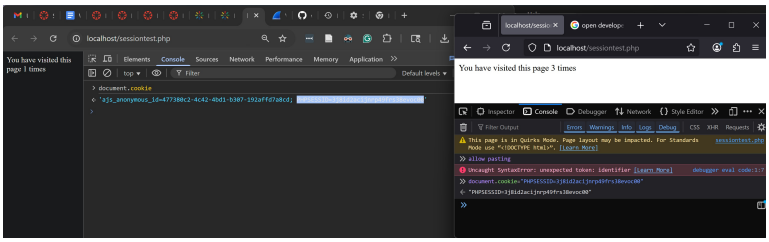
Cookie Use

You can see the server recognizes the session and replies without setting a new cookie

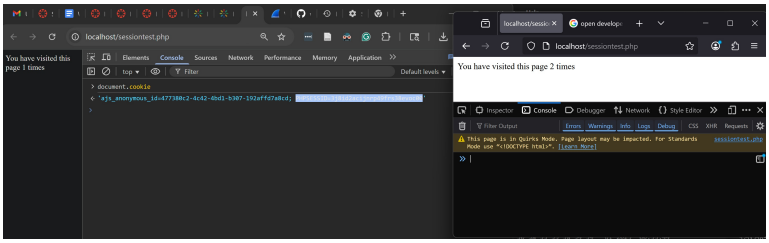
1.c. Understanding Session Hijacking (2 pts)



Chrome Cookie



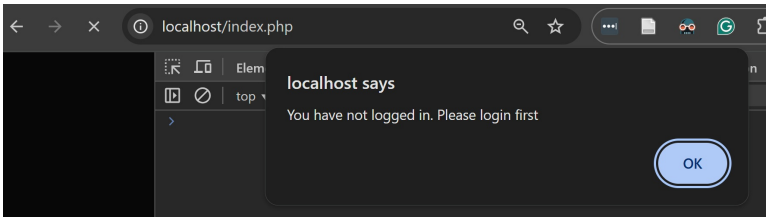
before refresh



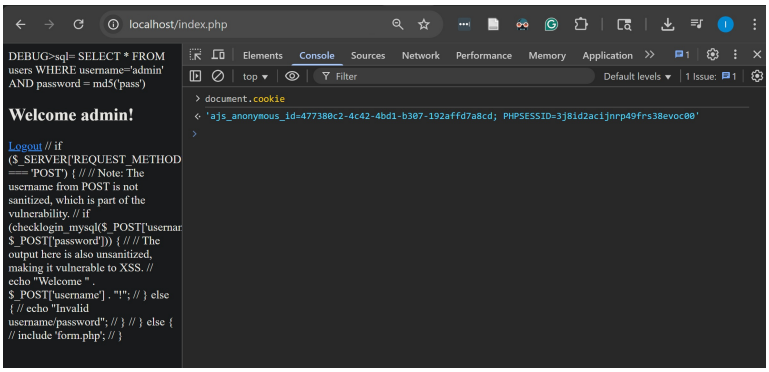
after refresh (it decremented to the chrome cookie)

Task 2: Insecure Session Authentication

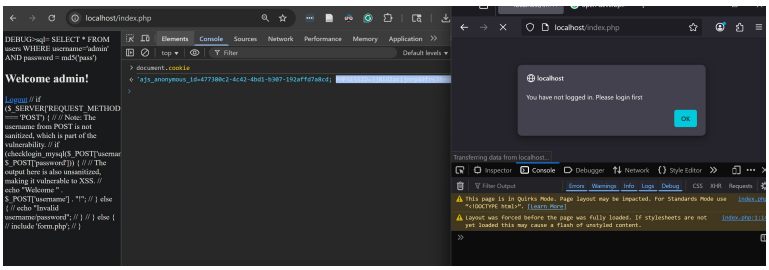
2.a. Revised Login System with Session Management (10 pts)



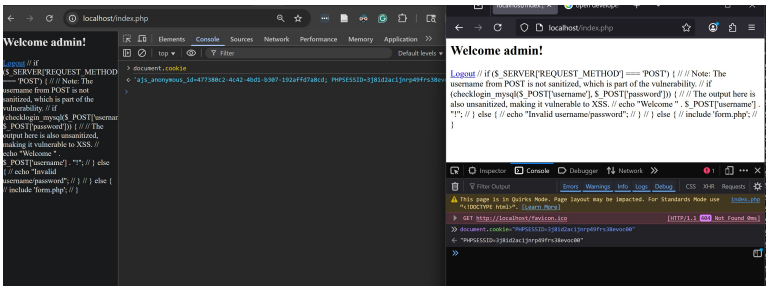
login required (chrome)



grab the cookie



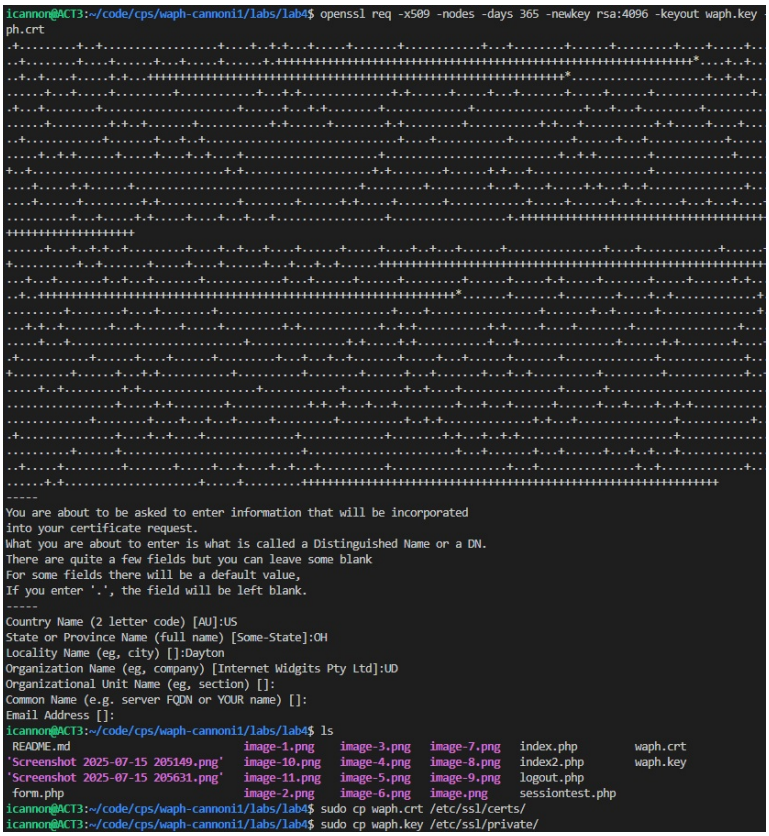
login required (firefox)



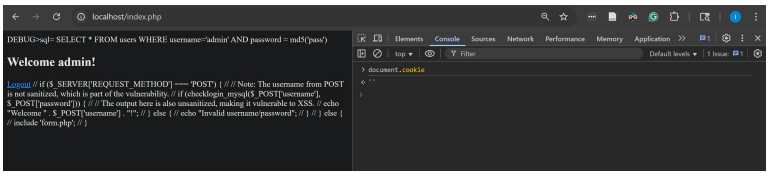
Access granted (firefox without signin)

Task 3

3.a. Data Protection and HTTPS Setup (10 pts)

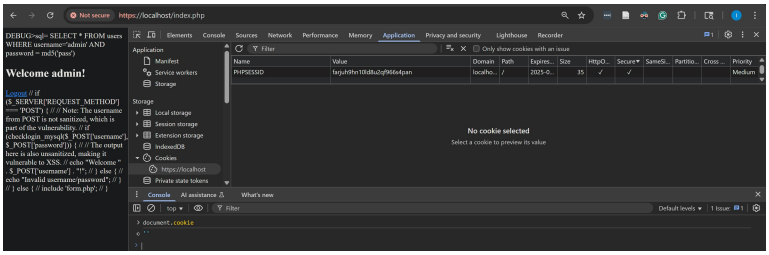


make some certs



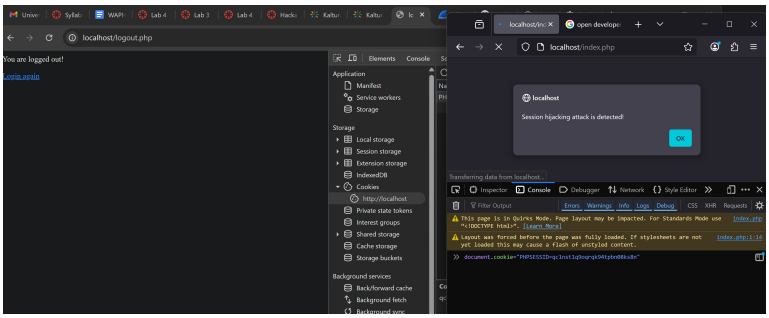
No cookies :(

3.b.



so secure

3.c.


localhost/logout.php
You are logged out!
Login again
localhost/index.php
localhost
Session hijacking attack is detected!
OK

caught ya!