WAPH-Web Application Programming and Hacking

Instructor: Dr. Phu Phung

Bridget May

Name: Bridget May

Email: mailto:mayb05@udayton.edu

Short-bio: Hi! My name is Bridget May! I am a senior at the University of Dayton studying computer science and graphic design.

Figure 1: My headshot

Repository Information

Respository's URL: https://github.com/mayb05/waph-mayb05.git

This is a private repository for Bridget May to store all code from the course. The organization of this repository is as follows.

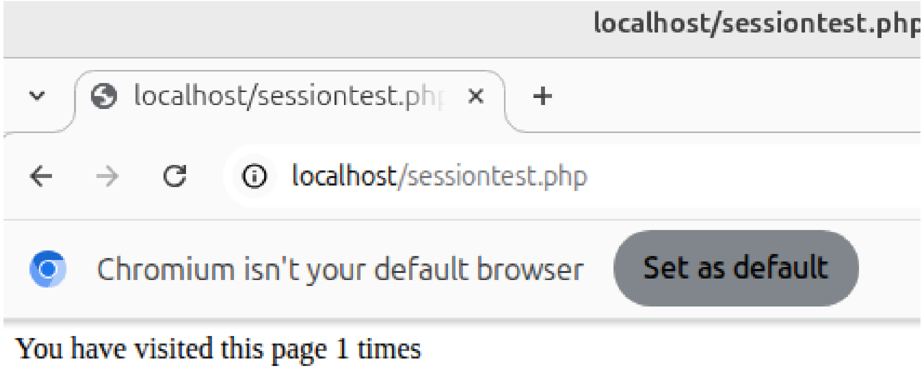
Lab 4 Overview

Lab link: https://github.com/mayb05/waph-mayb05/tree/main/labs/lab4

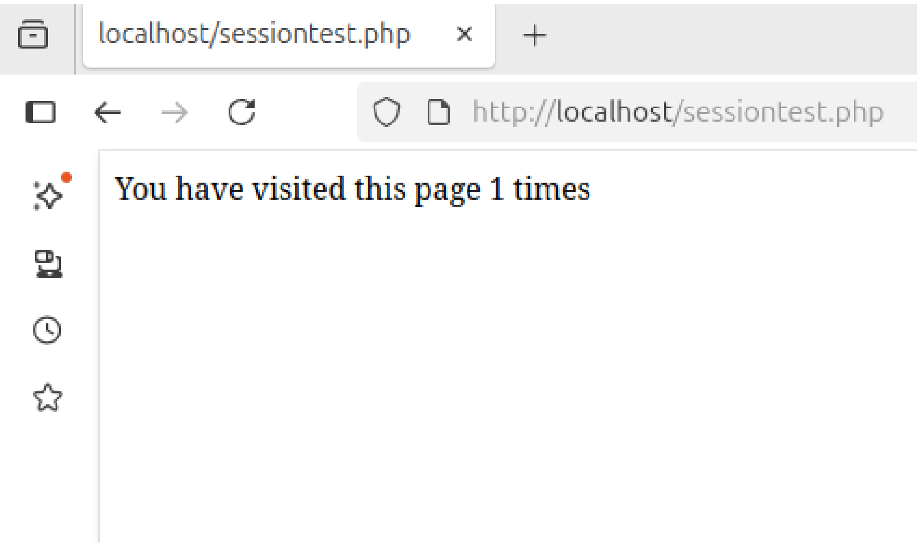
In this lab, I focused on session management in PHP applications. I learned how to mitigate a session hijacking attempt and secured my application. I also used wireshark to help understand the web traffic when using sessions.

Task 1: Session Management in PHP 101

1a: Sessiontest.php Here are the two different browser screenshots for the results of the code.


localhost/sessiontest.php
localhost/sessiontest.ph
localhost/sessiontest.php
Chromium isn't your default browser
Set as default

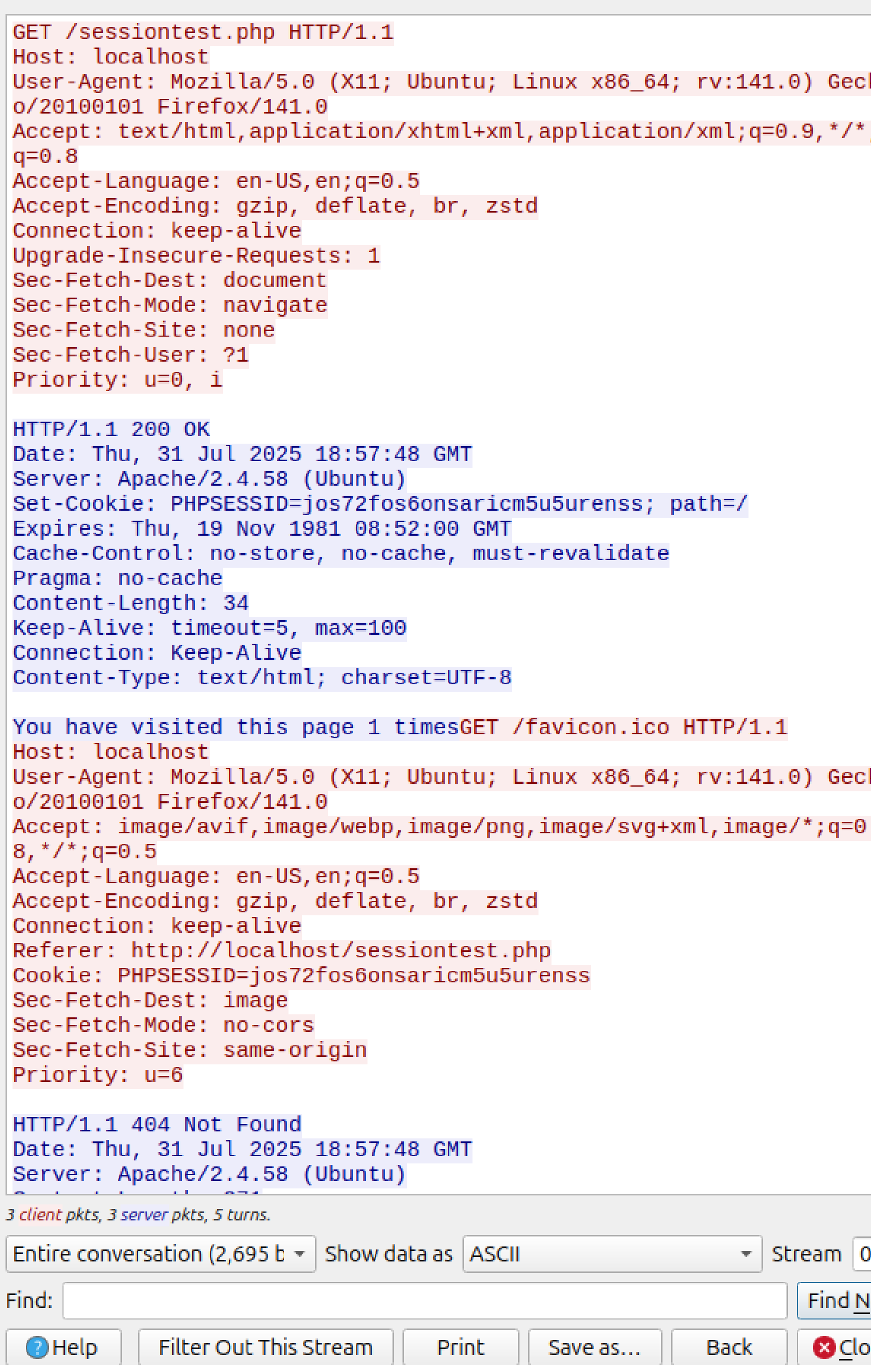
You have visited this page 1 times



You have visited this page 1 times

Figure 2: Firefox

1b: Wireshark Observations The session is set in the first screenshot then



```
GET /sessiontest.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:141.0) Geck
o/20100101 Firefox/141.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br, zstd
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i

HTTP/1.1 200 OK
Date: Thu, 31 Jul 2025 18:57:48 GMT
Server: Apache/2.4.58 (Ubuntu)
Set-Cookie: PHPSESSID=jos72fos6onsaricm5u5urenss; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 34
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

You have visited this page 1 timesGET /favicon.ico HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:141.0) Geck
o/20100101 Firefox/141.0
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.
8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br, zstd
Connection: keep-alive
Referer: http://localhost/sessiontest.php
Cookie: PHPSESSID=jos72fos6onsaricm5u5urenss
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Priority: u=6

HTTP/1.1 404 Not Found
Date: Thu, 31 Jul 2025 18:57:48 GMT
Server: Apache/2.4.58 (Ubuntu)
```

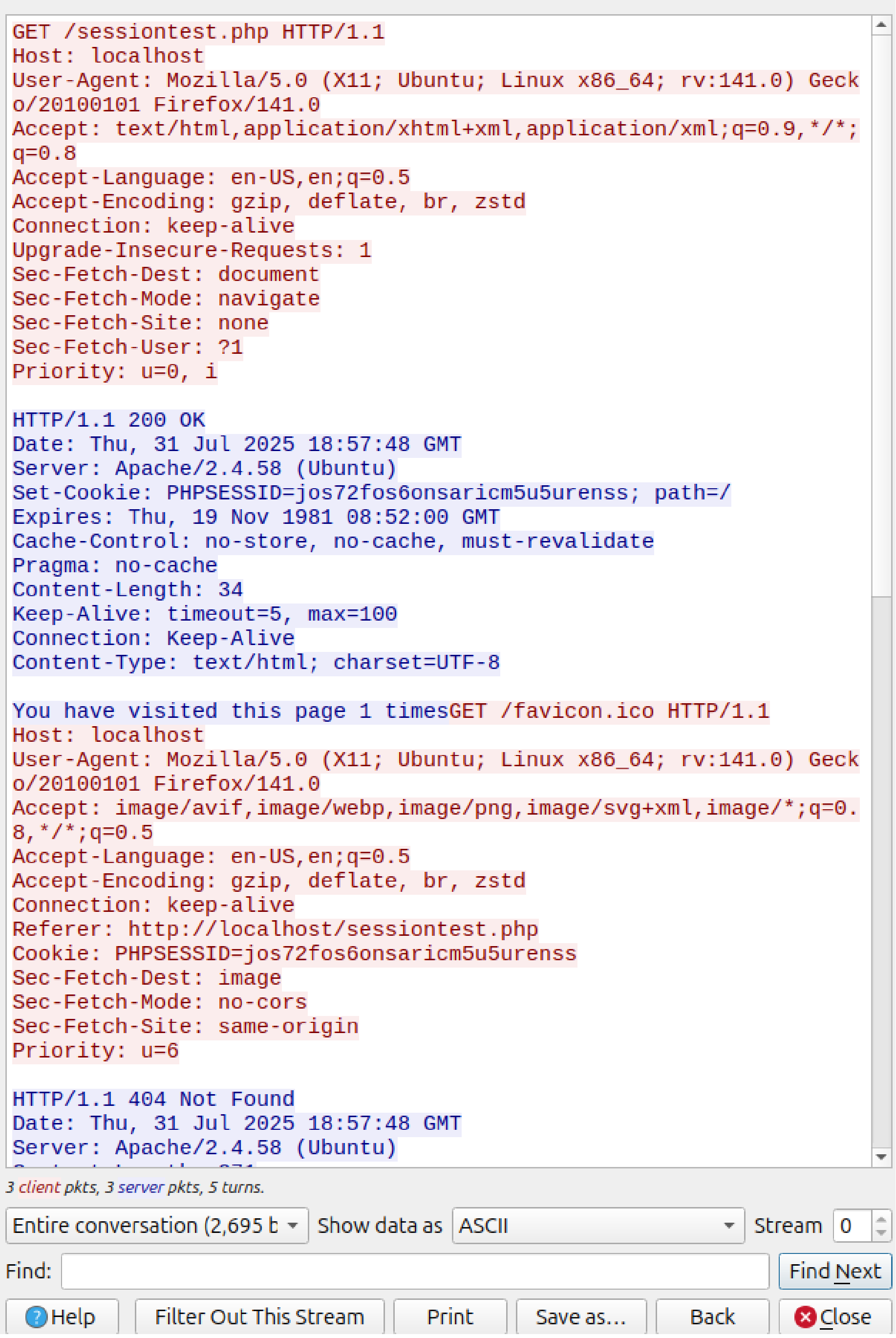
3 client pkts, 3 server pkts, 5 turns.

Entire conversation (2,695 b Show data as ASCII Stream 0

Find:

the cookie is held in the second one.

1c: Session Hijacking

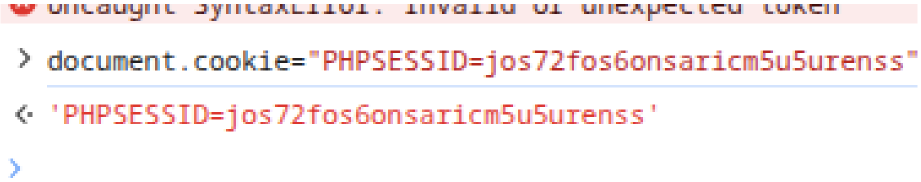


```
GET /sessiontest.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:141.0) Gecko/20100101 Firefox/141.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br, zstd
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i

HTTP/1.1 200 OK
Date: Thu, 31 Jul 2025 18:57:48 GMT
Server: Apache/2.4.58 (Ubuntu)
Set-Cookie: PHPSESSID=jos72fos6onsaricm5u5urenss; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 34
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

You have visited this page 1 timesGET /favicon.ico HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:141.0) Gecko/20100101 Firefox/141.0
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br, zstd
Connection: keep-alive
Referer: http://localhost/sessiontest.php
Cookie: PHPSESSID=jos72fos6onsaricm5u5urenss
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Priority: u=6

HTTP/1.1 404 Not Found
Date: Thu, 31 Jul 2025 18:57:48 GMT
Server: Apache/2.4.58 (Ubuntu)
```

3 client pkts, 3 server pkts, 5 turns.

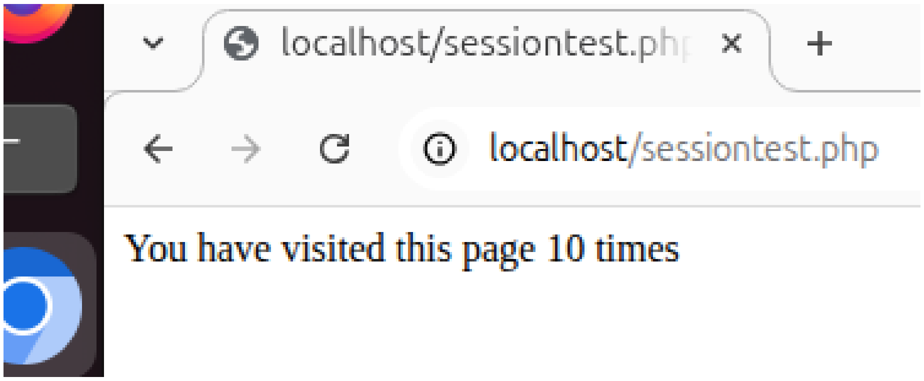
Entire conversation (2,695 b · Show data as ASCII · Stream 0

Figure 3: Second



```
Uncaught SyntaxError: Invalid or unexpected token
> document.cookie="PHPSESSID=jos72fos6onsaricm5u5urenss"
< 'PHPSESSID=jos72fos6onsaricm5u5urenss'
>
```

Figure 4: Cookie

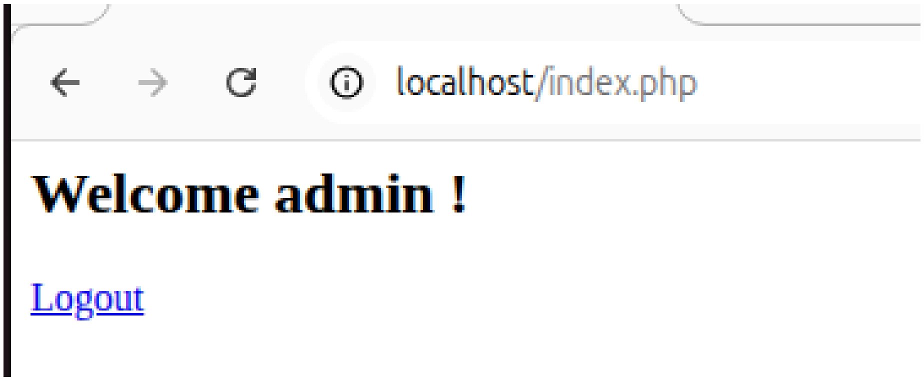


You have visited this page 10 times

Figure 5: Attack

Task 2: Insecure Session Auths

2a: Revised Login System with Sessions I revised the login system from lab 3 to have a logout button and check the users authication to avoid bypassing the form.php page. The first screenshot is a successful login.

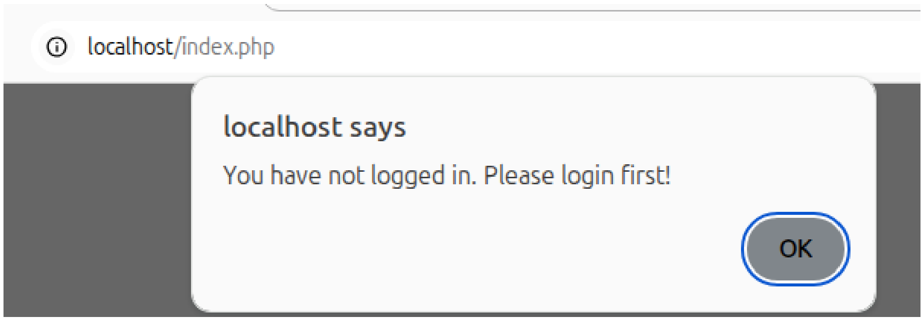


Welcome admin !

Logout

Figure 6: Sucessful Login

This is when you try to redirect to index.php without logging in.

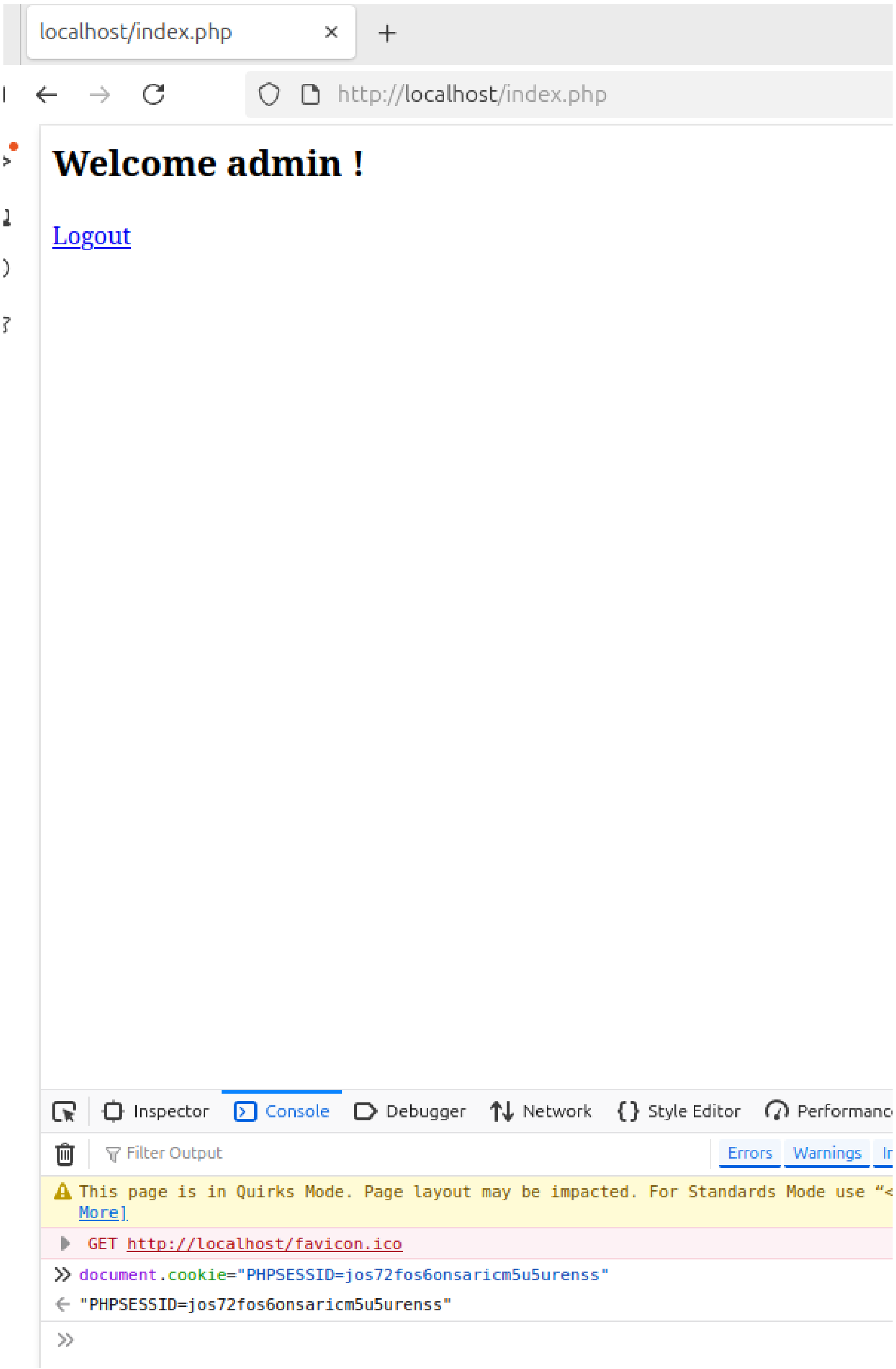


localhost says

You have not logged in. Please login first!

Figure 7: Skipping form.php

2b: Session Hijacking pt 2 In this task, I took the cookie from the chrome browser (I was logged in on this browser). After getting the cookie, I set it as my cookie in the Firefox browser and I didn't have to login on form.php at all.



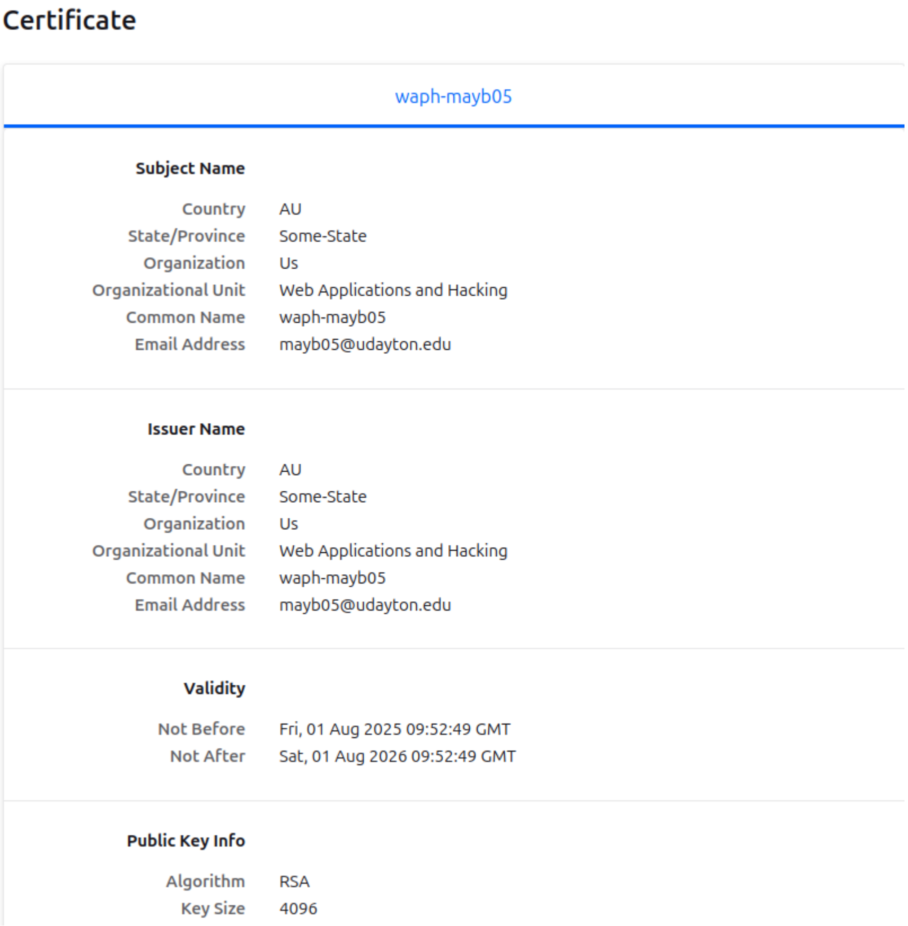
Welcome admin !

Logout

```
This page is in Quirks Mode. Page layout may be impacted. For Standards Mode use “<
More]
GET http://localhost/favicon.ico
>> document.cookie="PHPSESSID=jos72fos6onsaricm5u5urenss"
<- "PHPSESSID=jos72fos6onsaricm5u5urenss"
>>
```

Task 3: Secure Sessions

3a: Data Protection and Setup I setup this part by generating an ssl key to be able to use https which is more secure than http.



Certificate

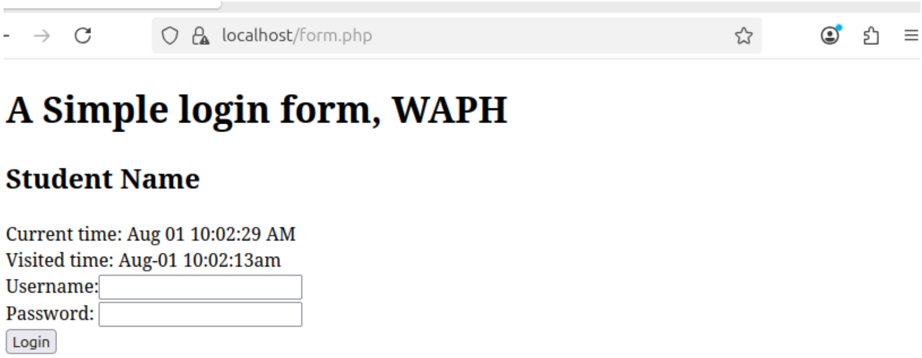
waph-mayb05

Subject Name	
Country	AU
State/Province	Some-State
Organization	Us
Organizational Unit	Web Applications and Hacking
Common Name	waph-mayb05
Email Address	mayb05@udayton.edu
Issuer Name	
Country	AU
State/Province	Some-State
Organization	Us
Organizational Unit	Web Applications and Hacking
Common Name	waph-mayb05
Email Address	mayb05@udayton.edu
Validity	
Not Before	Fri, 01 Aug 2025 09:52:49 GMT
Not After	Sat, 01 Aug 2026 09:52:49 GMT
Public Key Info	
Algorithm	RSA
Key Size	4096

Figure 8: SSL Key

3b: Securing Against Session Hijacking I revised my index.php to secure the cookies so they could not be easily found.

3c: Defense in Depth This task required me to adjust my index.php to store the browser information to avoid session hijacking. If the browser info doesn't match, hijacking is detected.

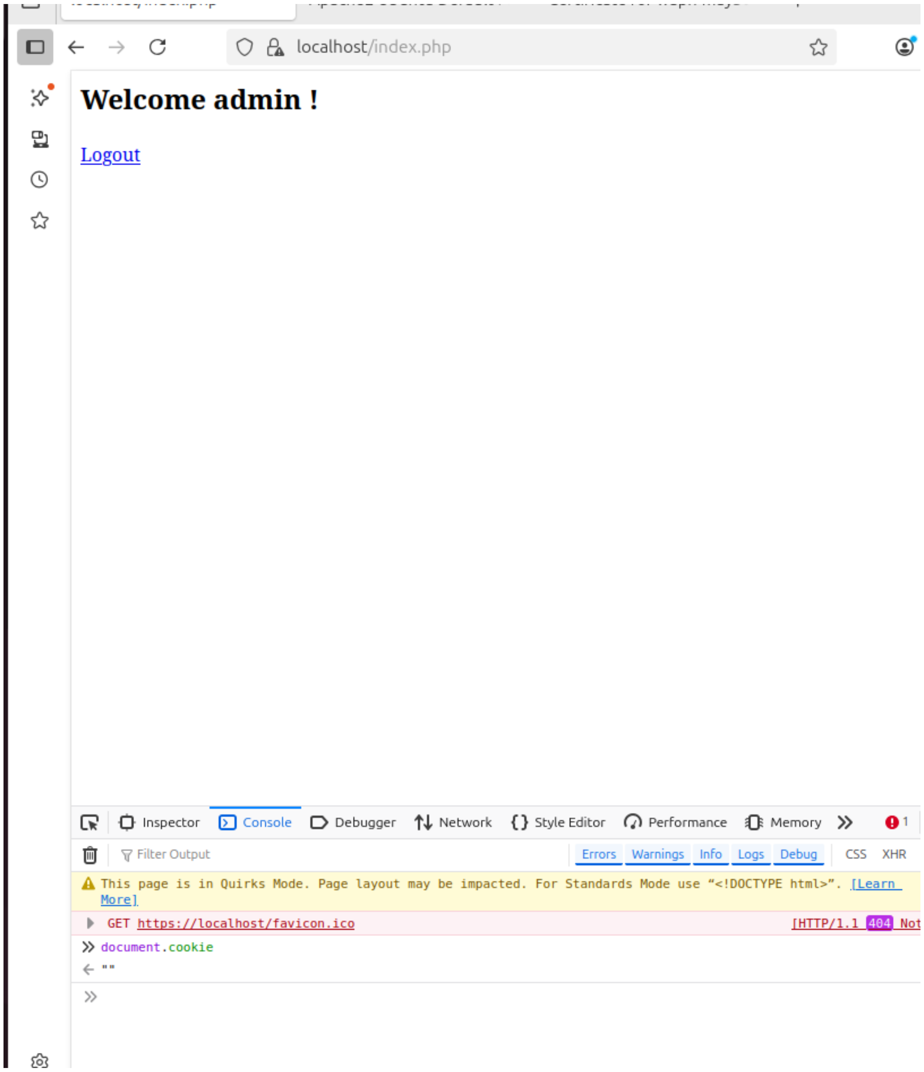


A Simple login form, WAPH

Student Name

Current time: Aug 01 10:02:29 AM
Visited time: Aug-01 10:02:13am
Username:
Password:

Figure 9: Index.php

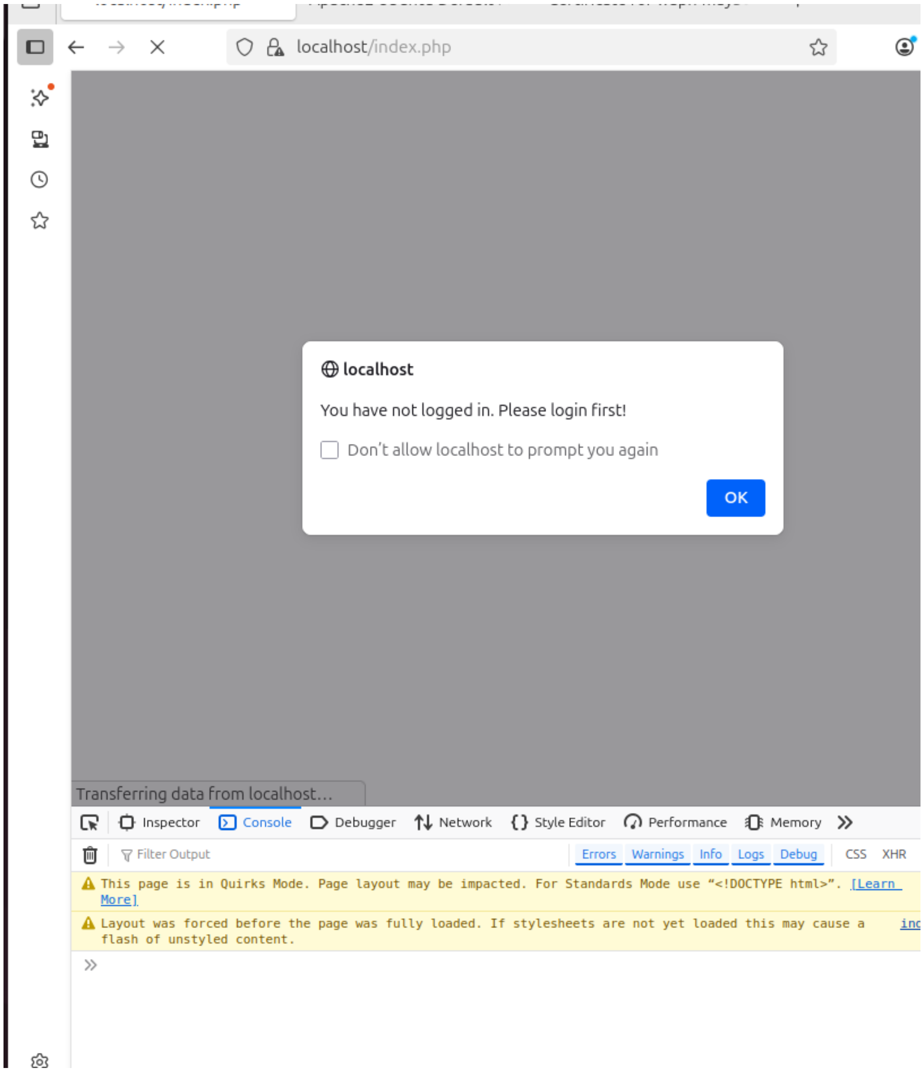


Welcome admin !

Logout

```
This page is in Quirks Mode. Page layout may be impacted. For Standards Mode use “<!DOCTYPE html>”. [Learn More]
GET https://localhost/favicon.ico                                   [HTTP/1.1 404 Not
>> document.cookie
<- ""
>>
```

Figure 10: Secure



You have not logged in. Please login first!

☐ Don't allow localhost to prompt you again

```
This page is in Quirks Mode. Page layout may be impacted. For Standards Mode use “<!DOCTYPE html>”. [Learn More]
Layout was forced before the page was fully loaded. If stylesheets are not yet loaded this may cause a flash of unstyled content.
```

Figure 11: Prevention!