Lab: Application Architecture and Logging

Jaiden Shoel, April 25th, 2025

Introduction and Materials

For this lab, we were supposed to set up logging for our localhost site using Loggly, which is a cloud-based log management service. This was supposed to be done using VScode and Docker to connect our app to Loggly and send logs for important system events like failed logins. Obviously though I experienced an unbearable debugging situation, which I still haven't been able to fix even after implementing Wyatt's advice through the email that I sent him about it, along with restarting all the way from week 1. Therefore I didn't complete the lab entirely but I do understand the goals and I am hoping to meet up to get this bug fixed at some point.

With this, the goals of the exercise was to show how logging can strengthen our web app's cybersecurity posture as centralized logging helps detect attacks, weird activities, and maintain forensic records.

The main tools required for the lab were:

Loggly (for managing and analyzing logs)

Our Localhost site

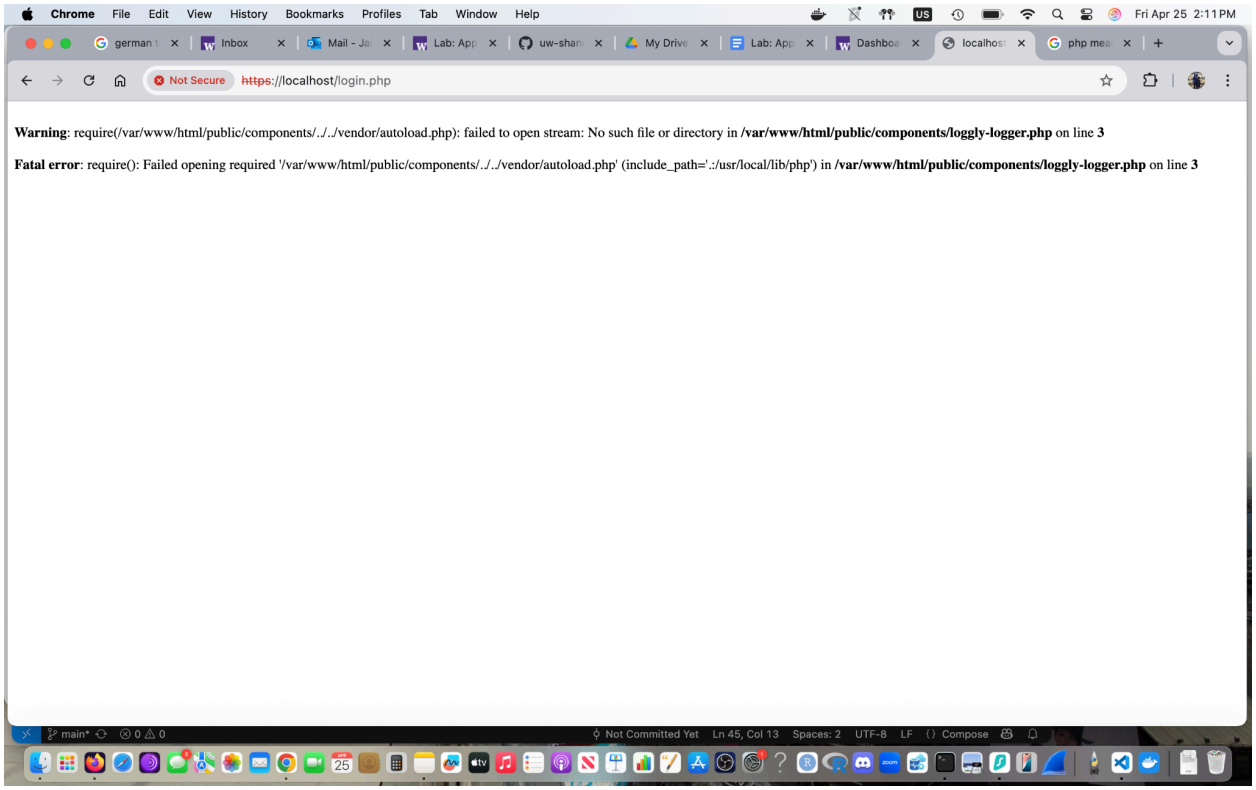
Docker and Docker Desktop

VSCode

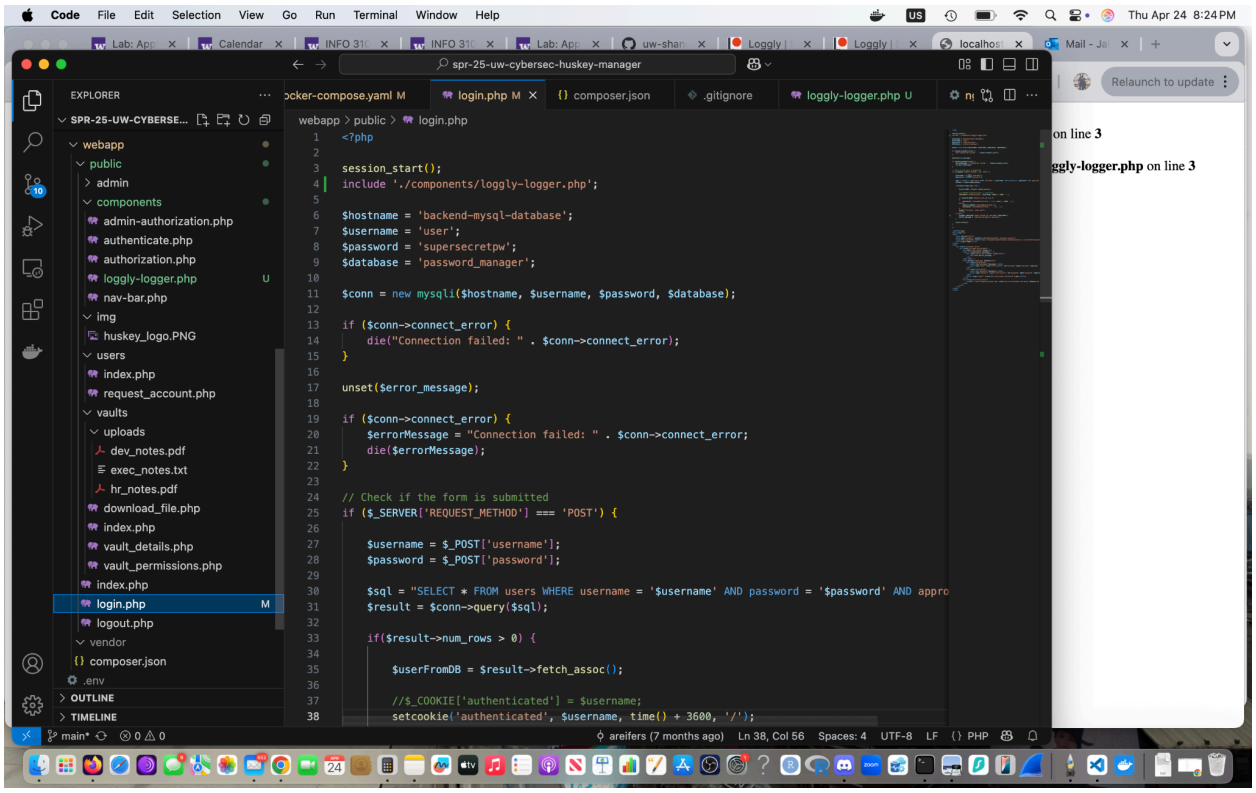
Steps to Reproduce

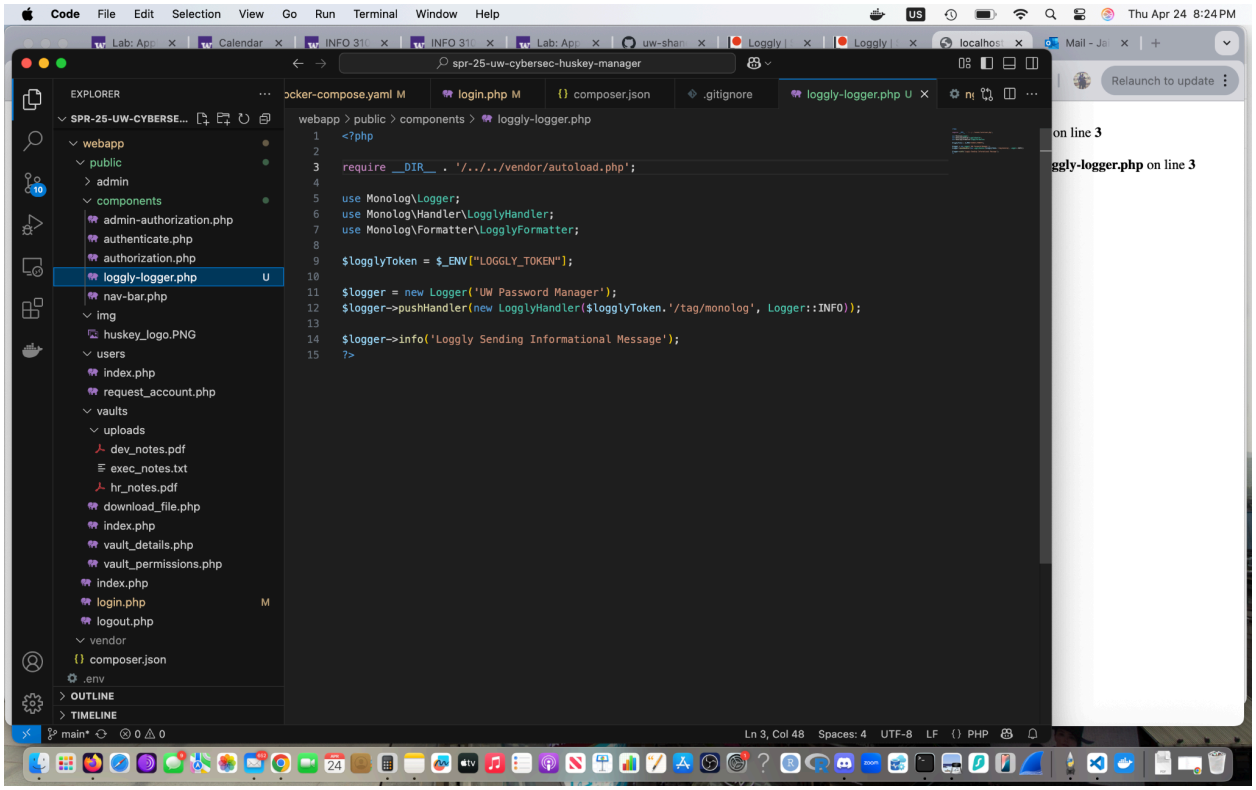
1. Create a Loggly Account
2. Retrieved the Customer Token from the Source Setup → Customer Tokens page.
3. Update relevant and said files stated in the README.txt at https://github.com/uw-shanemiller/spr-25-uw-cybersec-huskey-manager/tree/W4-Logging in VSCode
4. https://localhost/login.php would theoretically be all good to go.
5. Then Log Failed Login Attempts and Log Additional Events (for extra credit)

This is how far I got (Essentially only to the first half of step 4 in Part 2) before my frustrating bug error:



Pictures of VScode:





Class Principles

Question 1: The goal of cybersecurity is to protect assets. There are three ways we have discussed protecting assets. In terms of the methods we have discussed, how does logging help protect assets?

Through the methods we discussed and touched on, logging helps protect assets through prevention, detection, and response. First off, logging can prevent attackers if they know their actions are being monitored. Secondly, logging helps detect suspicious activity in real time, such as failed login attempts that could indicate a brute force attack. Finally, logging helps with the response protocol after a cyber incident. Logs give the ability to provide a top to bottom record from the beginning that helps us understand what happened, how it happened, and how to fix vulnerabilities. By having thorough logs, we ultimately strengthen all three protection strategies and increase the chance that attacks are spotted early and can be investigated thoroughly.

2. Where did you add logging? Why did you choose that location to add logging?

This question is not really applicable for me. However, if I did get loggly to work, I would add logging to failed login attempts in order to detect unauthorized access or possible brute force attacks. Successful logins to record legitimate access for auditing purposes. User logouts to track session endings and user activity patterns. And maybe password change requests, because changing a password is a sensitive action that should be monitored for security a lot of the time.

3. As we continue to enhance and secure the UW Password Manager application, what other user actions do you believe should be logged?

Off the top of my head I would say logging account creations could be of value in order to monitor new accounts for signs of suspicious activity. Additionally, failed password reset attempts can be of importance because it could signal attempts to take over an account. On that same token, changes to email addresses or linked accounts because these changes can compromise account security if not properly monitored. And finally, admin actions such as deleting users, resetting passwords, or changing roles would probably be of importance. For one, it can alert us if an admin may have been compromised, and two, it ensures accountability by keeping a record of any major system changes made by privileged users.

Hacker Mindset and Conclusion

While I didn't have the chance to fully complete this lab all the way through, I think one of the biggest things I learned from this lab and the class lectures and readings is how important it is to have logging set up early and thoughtfully in an application. Before this lab, I really thought of logging as something that was more for troubleshooting bugs, but now I realize it's also a major piece of cybersecurity. When we have good logging, it doesn't just help after an attack, but can actually work against the hacker mindset by making it much harder for attackers to stay invisible. A hacker usually wants to move through a system unnoticed, but if every action they take is being logged and flagged, it becomes a lot more difficult for them to succeed without getting caught.

However, I can also see how logging can be a weak spot if it's not properly secured. For example. if an attacker gains enough access, they could potentially spoof logs by flooding the system with fake events, or even delete important logs to cover their tracks. In our lab specifically, I would imagine this is easily achievable through maybe attacking the .env file where the Loggly token is stored, or compromising the Docker container itself (although somehow I achieved this already haha).

But all in all, the lessons from this lab definitely apply beyond just our lab and localhost site. In any system, whether it's a website, an API, or even internal company software, there should be a mindset and emphasis of treating logs like valuable evidence that needs to be protected. I said in my quiz response that logs are like security cameras. When you think of it this way, logs are only beneficial to have. Although, because logs can potentially be tampered with, it is probably a good practice to think about securing the logs themselves. Whether that's making sure they're encrypted to making them only accessible to authorized users. Logging is an amazing tool that we learned this past week, but it only works to it's ful potential if we treat it and utilize it like the security asset it is.