

Ramzi Alkaifi

October 4, 2026

Earth Viability Center / Place4Us

Reflection #3

The last 50 hours on my internship I was more used to the work compared to the start of my internship. After the first 50 hours I still tried to learn Place4Us, how it works, and what I should investigate and learn. The last 50 hours I knew Place4Us much better and could concentrate on the focus more on security and privacy instead of the Point of Learning. Still, the Point of Learning was User Roles and Authorities, but I also investigated User Privacy, MyFiles, GAI Detection, encryption, password safety, error handling, security logging, backup, and recovery.

One of the most important things I learned over these last 50 hours was that roles and authorities are crucial to ensuring Place4Us is secure. I learned Place4Us distinguishes platforms-level and VCC-level authorities. This clarified why access control can be complicated when a platform contains multiple communities, as well as multiple administrators in each community. I explored which pages displayed authorities and roles in Place4Us and realized that some displayed information about users without clearly indicating their Place4Us roles and authorities.

I also explored previous access control studies to gain a better understanding of roles that had been studied for the platform, which led me to design an authority process, including requesting, approval, assigning, utilizing, monitoring, reviewing, and removing an authority.

I continued to study more about privacy and its relation to cybersecurity. I studied privacy and canceling accounts, privacy settings, discoverability, login information, and log history. What I learned that seemed interesting to me was that security information collection has potential privacy issues. Log history can be good for tracking activity, but control of who views the logs and for how long it needs to be considered. This was remarkably interesting for me because I thought of privacy and cybersecurity to be quite separate, but they are not entirely exclusive.

A second area I was investigating was encryption and password security. I further investigated the analysis on Place4Us of the previous research questions about encryption and did a bit more research around the question of whether old passwords are stored or not to prevent password reuse. From this research I found that no, the old passwords should not just be stored as un-encrypted or in a reversing way. This backtracked from my results of researching roles and authorities, as encrypting/decrypting keys is just another example of an object that should only be accessible by the users that need to access it.

Along the way of my research, I also found PHP errors on other Place4Us pages. One of them revealed internal server paths, internal filenames, and internal line numbers. It was particularly interesting because it is a real thing that I saw as a user of this platform and not just something I read in a cybersecurity magazine. I understand that ordinary users should see only a simple error message while there can be more internal data stored in logs for programmers to fix these errors. Finding such an example on a real platform brought my knowledge of these errors in the context of the real system.

Another valuable experience that occurred in my last hours was experiencing the Place4Us data-loss. Some of the reports and data were lost – including two previous progress reports of mine.

Because of this I did a little research into backup and recovery and thought more about what should happen once data is lost. Backups are not enough. Data must be backed up with up-to-date information, protected, and tested for backup to be effective. There should also be a plan in place to identify the cause, restoring the right backup, testing to ensure the correct backup was restored, notifying the proper parties, and documenting the incident. The hands-on experience made this topic much more relevant to me than just learning about backups in the classroom.

GAI Detection was something I also kept working on in this project group. Rather than solely searching for more indicators of GAI, I worked on thinking about what steps should be taken after an indicator is uncovered. A learning I had was that an indicator should not get automatically taken as a sign that something must be created by an AI. Before confirming, there should be extra checks and human review.

Conclusion

In summary, my final 50 hours put into practice a lot of the things I worked on for the remainder of the internship. I entered the internship being unclear about the platform and what I should be doing, but I was able to independently research problems, apply that to cybersecurity, and make recommendations at the end of the internship. The biggest thing I have learned over the course of the internship is that sometimes cybersecurity is not so easy as just identifying a problem, but more about having a good understanding of a system, asking the right questions, and understanding what isn't clear.

By completing my 150 hours of internship, I had the opportunity to practice what I have learned from my cybersecurity courses on a real platform. I further advanced my skills in research,

communication, and problem-solving. I am now familiar with the interconnections between access control, privacy, encryption, logging, error handling, and backup and recovery.