Final Internship Reflection Paper

CYSE 368

Spring 2026

Student: Matthew Stone

Employer/Supervisor: Dr. Hans Peter-Plag

Organization: Earth Viability Center / Place4us Platform

Instructor: Teresa Duvall

Date: April 22, 2026

Table of Contents

1. Introduction 3
Organization Overview 3
Orientation and Initial Impressions 3
2. Management Environment 4
3. Major Work Duties, Assignments, and Projects 4
MOA Objective 1: Mycelia Cybersecurity Assessment 4
MOA Objective 2: Algedonic Channel Methodology 5
MOA Objective 3: MyFiles Cybersecurity Assessment 5
Graphic Design Contributions 6
Collaborative Intern Paper 6
4. Cybersecurity Skills Used 6
Pre-Existing Skills 6
Skills Learned on the Job 7
5. ODU Curriculum Preparation 7
6. Fulfillment of MOA Objectives 8
7. Most Motivating and Exciting Aspects 9
8. Most Discouraging Aspects 9
9. Most Challenging Aspects 10
10. Recommendations for Future Interns 10
11. Conclusion 11

Introduction

When I first came across the opportunity to intern with the Earth Viability Center and contribute to the Place4us platform I was very happy. I had been looking for an internship that would allow me to apply my cybersecurity knowledge in a context that felt meaningful and something that would help my career but The Earth Viability Center's mission, which centers on the long-term habitability of our planet for humans and animals alike, was exactly the kind of cause that deserves attention. I wanted to be part of something that mattered and this opportunity gave me that chance.

The three primary learning objectives I committed to through my signed Memorandum of Agreement reflect the core technical challenges the organization was facing at the time I joined. The first was to assess the cybersecurity posture of Mycelia, a posting service being developed to connect Virtual Community Centers and users on the Place4us platform, with the goal of identifying threats to user integrity and rights and proposing actionable mitigations. The second was to propose a formal methodology for handling messages submitted through the algedonic channel, which is the platform's mechanism for users to flag content that may be harmful, inaccurate, or otherwise in violation of the platform's guidelines. The third was to conduct a cybersecurity assessment of MyFiles, the feature that allows users to store and share files across the platform. Each of these objectives addressed a real and active vulnerability in the platform's security architecture, and each required me to bring both technical knowledge and careful thinking on problems that needed to be solved.

Organization Overview

The Earth Viability Center is an organization founded and led by Dr. Hans Peter-Plag, an earth scientist with decades of experience studying the conditions that make our planet viable as a

home for all living creatures. The organization's central argument is that the deterioration of Earth's habitability is the most serious and most consistently under talked about crisis facing humanity, and that addressing it requires both scientific involvement and broad human cooperation. The primary platform for that cooperation is Place4us, a social platform that Dr. Plag programmed all on his own and is designed to bring together people who share a commitment to addressing these challenges.

Place4us is not a conventional social media platform. It operates on a set of principles that stand in a stark contrast to the major commercial platforms most people use every day like Instagram or twitter. Hate speech and intolerance are prohibited and Disinformation and false information are actively monitored and removed. Most shockingly from a business perspective is that there are no advertisements anywhere on the platform. Dr. Plag has explained that he considers advertising to be one of the primary drivers of the overconsumption that accelerates environmental degradation, and he has chosen to build a platform that is free from that influence entirely. The platform is built on Linux and uses PHP as its primary server-side language, reflecting Dr. Plag's background as an experienced open-source developer.

The platform's target community is wide and far as anyone who cares about the planet's future and wants to engage seriously with others who share that concern, but it is specifically designed to attract people who are capable of good discourse and who are willing to engage with perspectives different from their own. The algorithmic echo chamber that characterizes most social media is something Dr. Plag has explicitly designed against. Users on Place4us are meant to encounter a range of viewpoints and not just the ones an algorithm determines they already agree with.

Orientation and Initial Impressions

My orientation to the internship was a zoom meeting that was very substantive. Dr. Plag introduced me to the platform's technical architecture, its codebase, and the specific areas he wanted me to focus on. I was one of four interns working with him during this period, and our group quickly established a rhythm of weekly video meetings supplemented by ongoing communication through Discord and email. My initial impression of the organization was one of genuine admiration. Dr. Plag had built something ambitious and principled mostly on his own, and the care he had put into every aspect of the platform's design was evident from the first time I explored it. I was also impressed by how seriously he took the security questions he had asked us to help address. He understood the risks even though he has no background in cybersecurity and he cared about the users who trusted his platform, and he wanted real solutions.

Management Environment

The management structure at Place4Us is pretty straightforward as Dr. Plag is the sole administrator and the founder of the platform, and he serves as the direct supervisor for all of the interns. There are no layers of middle management or no bureaucratic processes to navigate, and no ambiguity about who the leader is and for an intern, this structure has real advantages. It means that your work is seen directly by the person who matters most, and that feedback when it comes back comes from someone who has a complete understanding of the project and a genuine stake in its success.

Dr. Plag's supervisory style is direct and honest. He does not soften feedback unnecessarily, and he does not tell you something is good when he thinks it could be better however , at the same time, he is genuinely open to hearing what interns have to say. When my fellow interns

suggested changes to the platform's visual design and user interface during the first phase of the internship, he listened, engaging with their reasoning, and implemented the changes they recommended. That kind of responsiveness from a supervisor, especially from one who built the thing being critiqued, is not something to take for granted. It reflects a real commitment to improvement over ego.

The weekly meetings on Friday evenings were the primary formal structure of our work together. Each intern would share what they had accomplished in the previous week, what challenges they had encountered and what they planned to tackle in the coming week. Dr. Plag would respond with a lot of questions about what we were thinking about and gave us some good guidance from his big knowledge of most things related to the site. These meetings were productive and efficient without feeling rushed or too long and drawn out. Outside of the scheduled meetings we had some communication through Discord and email both of which worked well for a distributed team. The overall management environment was one that I found both motivating and professionally formative.

Major Work Duties, Assignments, and Projects

MOA Objective 1: Mycelia Cybersecurity Assessment

Mycelia is a posting service currently under development for the Place4us platform. Its purpose is to connect the platform's Virtual Community Centers with individual users, allowing for a richer and more structured form of community engagement than a standard social feed provides. From a cybersecurity standpoint, a posting service of this kind introduces a range of potential vulnerabilities that needed to be identified and addressed before the service could be safely deployed.

My work on the Mycelia assessment involved reviewing the planned architecture of the service, identifying the points at which user data could be exposed or integrity could be compromised, and proposing specific mitigation strategies for each risk identified. The key concerns I identified included the handling of user-submitted content and the potential safety risk of that, the authentication and authorization mechanisms governing access to community centers, the potential for injection attacks through input fields, and the risks associated with cross-site scripting in a platform that allows free user-generated content. For each of these concerns I developed mitigation recommendations grounded in established cybersecurity best practices, including input sanitization protocols, and role-based access controls.

This assessment was important to the organization because Mycelia represents a significant expansion of the platform's capabilities and its attack surface. A security failure in a new and somewhat anticipated feature could damage user trust in a way that would be very difficult to recover from, especially for a platform whose entire identity is built on being a trustworthy and transparent space. Getting the security architecture right from the beginning is far more efficient and less costly than attempting to patch vulnerabilities after they have been discovered or even worse, exploited.

MOA Objective 2: Algedonic Channel Methodology

The algedonic channel is the mechanism through which users on Place4us can flag content that they believe to be harmful or inaccurate or otherwise in violation of the platform's guidelines. The term algedonic refers to the pain-and-pleasure signaling concept from cybernetics, and in this context it describes the channel through which the community sends distress signals about content that is causing any harm. Designing a methodology for how those signals should be

received and acted upon was one of the most intellectually interesting assignments I undertook during the internship.

The methodology I developed and presented in collaboration with the other interns is a five-step distributed verification system. In Phase 1, users submit flags using structured categories, including factual inaccuracy, outdated information, broken or misleading links, missing context, and harmful content. Flags are recorded silently and not immediately shared with the content poster, because premature notification can allow bad actors to delete evidence or manipulate the review process before a fair assessment can happen like people who mass report content they don't agree with. In Phase 2, flags are aggregated using a tiered threshold system. One or two flags of the same type result in silent monitoring. Three to five flags of the same type trigger the content entering a peer review queue. Any flag categorized as dangerous or harmful is fast-tracked immediately regardless of the count. In Phase 3, the flagged content is routed to a trusted pool of peer reviewers acting like twitch moderators who have demonstrated a track record of good-faith and accurate participation similar to the editorial model used by Wikipedia. Reviewers determine whether the flag is legitimate and their decision determines whether the content is escalated, cleared, or sent to the site's admins in the event of a split decision.

In Phase 4, before the original poster is notified of any problem, the content itself is labeled publicly so that all readers can see that something is under review. A yellow label indicates the content is under review. A red label indicates that peer review has confirmed a problem. A black blurred overlay is applied in the most severe cases which requires readers to actively choose to view the content. In Phase 5, the poster is notified with a structured message that identifies the specific claim or section under scrutiny and cites the evidence reviewers used, and provides a clear pathway for correction and resubmission. The methodology also includes a flag integrity system to detect and penalize bad-faith flagging, and other attempts to weaponize the channel against legitimate speech.

This methodology was necessary to the organization because the existing approach to content moderation was essentially just super reactive and The platform's commitment to being free of disinformation and hate speech is only meaningful if there is a functioning and fair system for enforcing it, and the algedonic channel is the primary mechanism through which the community participates in that enforcement.

MOA Objective 3: MyFiles Cybersecurity Assessment

MyFiles is a feature on Place4us that allows registered users to upload and share files with the broader community. The concept is valuable and consistent with the platform's mission of enabling meaningful collaboration and information sharing. However, allowing users to upload arbitrary files to a web server is one of the more significant security challenges a developer can face, and the existing implementation had gaps that had to be addressed.

The most significant gap I identified was that the platform's existing file scanning functionality was unable to process certain file types. Proprietary formats such as Apple's Keynote presentation format, for example, could not be scanned by the current system. This meant that a malicious file in one of those unsupported formats could be uploaded to the platform without being detected, exposing other users to malware or to content that violated the platform's content policies. The only defense against this scenario under the existing system was peer review, which is not a security posture that a bigger growing platform can rely on.

The solution I researched and recommended and have previously discussed was the integration of a free and open-source antivirus engine that has been maintained by the open-source security community for many years called ClamAV. ClamAV is capable of scanning a wide range of file types, its virus definitions are regularly updated, and it can be integrated into server-side file handling workflows. I researched how ClamAV could be called from within the existing PHP codebase to scan uploaded files before they are accepted and stored, and I documented the integration pathway for Dr. Plag. As of the conclusion of my internship this integration remains a work in progress but the technical groundwork and implementation plan have been laid down at least. Also with the ClamAV work, I also researched encryption practices relevant to the secure storage of user data and authentication credentials. I investigated Transport Layer Security configuration best practices and I also researched Shamir's Secret Sharing, a cryptographic algorithm that allows an encryption key to be divided into multiple shares such that the original key can only be reconstructed when a minimum threshold of shares are combined. This approach is particularly relevant to key backup strategies in environments where no single person should have the sole access to critical secrets, and where the loss of any single backup could be absolutely terrible. I documented my findings and shared recommendations with Dr. Plag for consideration in the platform's long-term security planning.

Collaborative Intern Paper for Future Interns

One of the final projects of my internship was a collaborative written document that was made together with my fellow interns. This paper is intended to serve as a resource for future interns working with Place4us in an effort to provide an honest and thorough overview of the cybersecurity risks and vulnerabilities we identified during our time with the platform, along with the solutions and strategies we researched and developed in response. Writing collaboratively required navigating real differences in perspective and writing style, which was in and of itself a valuable professional experience. The paper covers all of the tasks that all of us did individually and collectively.

Cybersecurity Skills Used in the Internship

Pre-Existing Skills

Before beginning this internship, I had a foundation in core cybersecurity concepts that I was able to apply directly to the work from the start. My understanding of threat modeling and vulnerability assessment allowed me to approach the Mycelia and MyFiles assignments with a structured analytical framework. I was familiar with the general principles of secure web application development and the basic architecture of authentication and authorization systems. I also had a working understanding of cryptographic principles including symmetric and asymmetric encryption, hashing, and the general purpose of protocols like TLS, which gave me a starting point for the encryption research I conducted during the internship.

My ability to read and reason about code, even in languages I had not worked with extensively, also proved to be a pre-existing skill that was immediately useful. When I encountered the PHP codebase underlying the MyFiles feature, I was able to work through the logic of the existing code and identify its vulnerabilities without needing to become a proficient PHP developer first. This kind of code literacy in an unfamiliar language, at least well enough to reason about its

security implications, is something I had developed through my coursework and that paid off directly in this internship.

Skills Learned on the Job

The internship also required me to develop several skills and areas of knowledge that I did not have before I started. The most immediately necessary of these was a working familiarity with PHP. I had known essentially nothing about PHP before joining the organization, and I needed to understand it well enough to engage meaningfully with the existing MyFiles codebase. I found a free introductory PHP course on YouTube and worked through it systematically over the first few weeks of the internship. By the end of that process I was not a PHP developer, but I was able to read and reason about PHP code with enough confidence to do the security analysis my assignment required.

I also learned a great deal about the practical considerations involved in integrating open-source security tools into existing web application stacks. This is a different kind of knowledge than what you get from studying security concepts abstractly. It involves understanding how tools actually behave in real environments, what their limitations are, how they fail, and what the configuration choices mean in practice.

Shamir's Secret Sharing was another area of knowledge I developed during the internship that I had not studied in depth before. Understanding not just the algorithm itself but its practical applications in key management and backup strategy required working through both the mathematical foundations and the real-world use cases and that process deepened my understanding of cryptographic security in a way that was genuinely an addition to what I had learned in school.

Finally, the internship gave me practical experience with collaborative technical writing and documentation, which is a skill that is often underemphasized in academic cybersecurity programs but I found is essential in professional practice. Writing clearly about complex technical material for an audience that includes both technical and non-technical readers is hard but I got a lot of practice doing it during this internship.

ODU Curriculum Preparation

I would say that my coursework at ODU prepared me well for this internship and I was genuinely surprised at how directly applicable much of what I had studied turned out to be in a real professional context. The connections between classroom learning and on-the-job work were consistent and reinforcing throughout the experience.

The cybersecurity fundamentals courses I had taken gave me the vocabulary and conceptual framework I needed to engage with the security challenges at Place4us from the very beginning. When I sat down to assess the Mycelia architecture or analyze the MyFiles codebaseI had frameworks for thinking about threats, vulnerabilities and mitigations that I could apply directly. This made me more useful to the organization from the start than I might otherwise have been.

My coursework in network security was particularly relevant to the TLS research I conducted. Understanding the differences between TLS versions and the significance of cipher suite selection were all things I had covered in school and was able to build on during the internship rather than having to learn from scratch. That part of seeing concepts from the classroom show up as real decisions with real consequences in the world had a significant impact on how I understand and retain that material.

The ethical dimensions of cybersecurity that my coursework had touched on also turned out to be directly relevant. The discussions our intern team had about user data collection, guest flagging privileges, and the rights and responsibilities of platform users were not purely technical questions. They were ethical ones, and the frameworks I had encountered in my cybersecurity class helped me engage with them more thoughtfully than I might have otherwise.

There were also areas where the internship took me beyond what I had covered in the curriculum. Shamir's Secret Sharing was not something I had encountered in any of my courses. And the experience of writing and presenting technical documentation in a real professional context, with a real audience and real stakes, was something that coursework can prepare you for conceptually but it's not exactly a one to one replica. I wouldn't say these gaps were failures of the curriculum but simply reflections of the difference between academic preparation and professional practice, and they gave me a clear sense of the areas where I need to continue developing.

Fulfillment of MOA Learning Objectives

Looking back at the three learning objectives I committed to in my Memorandum of Agreement, I am satisfied that each was meaningfully addressed during the course of the internship, though the degree of completion varied across them.

The first objective which was assessing the cybersecurity posture of Mycelia and proposing mitigation actions, was fulfilled substantially. I conducted a thorough review of the planned service architecture to the best of my ability and produced documented recommendations for Dr. Plag's consideration. The assessment covered injection risks, authentication and authorization concerns, content security policy needs and cross-site scripting vulnerabilities. Whether all of those recommendations are ultimately implemented is obviously beyond my control but the assessment itself was completed to a standard I feel good about.

The second objective of proposing a methodology for the algedonic channel, was also fulfilled. The five-phase distributed verification methodology I developed with my fellow interns represents a genuine and substantive response to the challenge of community-based content moderation at scale. It is grounded in real precedents from other platforms and communities that have faced similar challenges, and it is designed to be both fair to content creators and protective of the broader community. The methodology was presented to Dr. Plag and received positively.

The third objective, assessing the cybersecurity of MyFiles, was partially fulfilled. I identified the core vulnerability which is the inability to scan certain file types for malware or policy-violating content and I proposed a concrete solution in the form of ClamAV integration with detailed documentation of the implementation pathway. However, the actual integration of ClamAV into the platform's codebase was not completed during my internship. I wasn't exactly entirely surprised given the scope of what a working integration requires, but it means that the objective was addressed at the level of assessment and planning rather than just the outcome which is an important distinction.

Across all three objectives, the internship gave me the opportunity to apply real cybersecurity knowledge to real problems in a way that had genuine stakes. That experience of working on something that matters for real people is one of the most valuable things an internship can offer, and this one delivered it.

Most Motivating and Exciting Aspects of the Internship

The single most motivating aspect of this internship was the sense that the work I was doing mattered. This is not something I take for granted. I've heard many internships involve tasks that feels like busywork that exists to keep an intern occupied rather than to advance a genuine organizational goal. That was never the case at the EVC. Every assignment I was given addressed a real vulnerability in the P4US platform used by real people who trusted it. That sense of genuine stakes was consistently motivating throughout the experience.

The algedonic channel methodology was particularly exciting to work on. The problem of content moderation is one of the defining challenges of the digital age, and being asked to develop a serious and structured response to it for a platform built on principles I genuinely believe in felt like exactly the kind of work I want to do. The five-phase system we developed was intellectually satisfying to build and felt like a real contribution to a hard problem.

The relationships I built with my fellow interns were also a source of genuine enjoyment and motivation throughout the internship. We worked well together, supported each other when things were difficult, and had a group dynamic that made the work more fun than it might otherwise have been. At certain points we had the opportunity to meet in person, which added a closeness to those relationships that video calls and Discord messages can't fully replicate. One particularly memorable moment came when one of my colleagues rejoined our group chat shortly after getting his wisdom teeth removed, still clearly feeling the effects of the laughing gas, and proceeded to say a series of things that had the rest of us laughing for the better part of an afternoon. Those moments are part of what makes a team feel like more than just a collection of people assigned to the same project.

Dr. Plag himself was a consistent source of motivation. His passion for the Earth Viability Center and for the platform he has built is not the performative enthusiasm of someone trying to sell something, he actually has the deep conviction of someone who has spent decades thinking seriously about a problem and who genuinely believes that what he is building can help address it. Being around that kind of authentic commitment has a way of raising your own standards and reminding you why the work matters.

Most Discouraging Aspects of the Internship

The most discouraging moments of the internship were not dramatic failures or interpersonal conflicts. They were quieter than that, and in some ways more instructive because of it. The primary source of discouragement was the occasional feeling that progress was slower than I wanted it to be, but the most discouraging parts of the internship were the times when brainstorming ideas couldn’t give me anything good to report.

There were also moments, particularly during the final phase of the internship when my responsibilities had expanded significantly, when I questioned whether I was contributing enough value to justify the trust Dr. Plag was placing in me. These doubts had a tendency to show up at the moments when I was most stretched between competing demands on my time and attention. Learning to manage that kind of self-doubt productively is still very much something I am still working on.

Most Challenging Aspects of the Internship

The most challenging aspect of the internship was time management, particularly during the final phase when the scope of my responsibilities had grown considerably. By that point I was simultaneously managing the ongoing cybersecurity work on all the tasks at hand like contributing to the algedonic channel methodology, creating visual graphics for the platform,

writing and collaborating on the intern resource paper, producing technical documentation, keeping up with my academic coursework, and fulfilling the hours of a part-time job. The challenge was not any one of them individually really but It was the cumulative weight of all of them together.

I learned during this period that time management is not simply a matter of working harder or staying more organized, though both of those things help. It is about developing a realistic and honest assessment of how long things actually take and actually building in contingency for the unexpected problems and being willing to communicate proactively with my supervisor when timelines are at risk. I did not always do those things as well as I should have during this internship, and the technical documentation I was responsible for producing fell slightly behind my own standards during the most demanding period. That feeling was uncomfortable, but it was also instructive in a way that classroom time management advice never quite achieves.

Recommendations for Future Interns

For anyone preparing to intern with the Earth Viability Center and the Place4us platform, spend some time with PHP before you start. The platform is built on PHP and while you do not need to be an expert, having a basic working familiarity with the language's syntax and common patterns before your first day will allow you to engage with the codebase that you have to download much more quickly than if you are learning from scratch. There are free and high-quality introductory PHP resources available online, and even ten to fifteen hours of preparation will make a meaningful difference. Also it would help familiarize yourself with Linux if you haven’t already, which is what Dr Plag uses for the site The MyFiles integration work is ongoing and understanding what the code says and how it is installed and configured on a Linux server, and how it can be called from within a PHP application will give you a significant head start on that work.

Be prepared to manage your time carefully. The internship has a way of expanding in scope as Dr. Plag gets a clearer sense of what you are capable of and as you become more invested in the work. IT needs good time management. Build realistic schedules, communicate early if you are falling behind, and do not wait until a deadline is already missed to ask for help or more time. Dr. Plag is a supervisor who genuinely values the perspectives and contributions of his interns, and the work you do here has the true chance of impacting someone else positively. It is a chance to engage seriously and to push yourself, and the experience is unbelievable.

Conclusion

When I began this internship, I was a cybersecurity student with a solid academic foundation and a genuine desire to apply what I had learned in a context that felt real and meaningful. What I did not fully anticipate was how substantially the experience would change my understanding of what cybersecurity work actually is and what it demands of the people who do it.

The main takeaway I carry from this internship is that cybersecurity is not a purely technical discipline because it looks at human behavior, and ethics, and the professionals who are most effective in it are those who can move fluidly across all three of those domains. My work all required me to think about the human context in which those solutions would operate and the ethical implications of the choices being made. That kind of integrated thinking is something I hope to continue developing for the rest of my career.

The influence of this internship on the remainder of my time at ODU will be significant. I come back to my coursework with a clearer sense of why the material matters and where it connects

to the problems that professionals in this field are actually working on. The gaps I identified between my academic preparation and the demands of the internship gave me a concrete agenda for what I want to focus on in my career. I intend to seek out more opportunities to do hands-on work with real systems.

The influence of this internship on my professional path is equally significant. I came in knowing that I wanted to work in cybersecurity but I left with a much more specific sense of what kind of cybersecurity work I want to do. Dr. Plag's vision for Place4us with his belief that technology can and should serve humanity's most important collective interests rather than extracting value from human beings is one I find deeply compelling and that I hope to find reflected in the organizations I work with throughout my career. His mentorship, honesty and his genuine investment in the growth of the interns he works with have set a standard for what a good professional relationship with a boss can look like. I am grateful for every part of this experience.