Final Internship Paper

Celeste Meraz-Luna

CYSE 368

April 19, 2026

Spring 2026

Professor Duvall

Earth Viability Center Inc.

Dr. Hans-Peter Plag

Introduction

I decided to intern with Earth Viability Center because I wanted a meaningful opportunity to apply what I have learned in cybersecurity to a real-world platform while gaining hands-on experience. As a student, I recognized that internships are one of the best ways to bridge academic knowledge with professional expectations. I wanted experience working in an internship where security, privacy, teamwork, and problem-solving all mattered. Since the internship focused just on cybersecurity aspects of the platform, it aligned well with both my educational background and long-term career goals.

According to the internship agreement, the purpose of the internship was to provide a meaningful educational experience that complemented my academic studies and career goals. This was exactly what I hoped to gain. The three main learning objectives I expected to achieve were:

1. Review user privacy protections while balancing the discoverability of users and their contributions.
2. Evaluate encryption methods for sensitive data stored in XML files and propose better protections.
3. Assess cybersecurity risks in the Confab messaging service and recommend improvements to better protect users.

Place4Us is an online platform designed to support communities, collaboration, blogging, and shared participation among users. The platform allows individuals to interact, post content, comment, and participate in community spaces. It allows users to create Virtual Community Centers (VCCs) which promises users a place to learn, collaborate, connect, and act. Users can join and contribute ideas to engage with one another. Because the platform relies on user

interaction, privacy and cybersecurity are especially important. Any platform that stores user information or allows communication between users must be designed carefully to reduce risks involving misuse, unauthorized access, or harmful content.

My internship began on January 23, 2026, and it required a minimum of 150 hours. In the beginning of the internship, I started with learning the purpose of the platform, attending the Zoom meetings, understanding the internship expectations, and becoming familiar with the technical environment. I also learned that the website was hosted through a Linux environment through IONOS, with development primarily in PHP and some JavaScript. Access to the xml files was provided through SSH keys, and I was able to work using my personal computer. My first impression of the internship was that it would require independence and self-motivation. Unlike my online courses, there was not always direct instruction or a clear list of steps to follow. Instead, I was expected to think critically, identify solutions, research unfamiliar topics, and contribute ideas. This created a realistic professional learning environment and helped me grow confidence over time.

Management Environment at the Internship

The management environment at the Earth Viability Center was supportive, flexible, and collaborative. I reported directly to Dr. Hans-Peter Plag, who served as my supervisor and mentor throughout the internship. He provided feedback and guidance through weekly reports, and team meetings, which helped guide my progress and professional development.

Weekly meetings were held through Zoom, where myself and other interns would discuss tasks, exchange ideas, and receive updates. These meetings created a safe environment where everyone was encouraged to speak openly and share perspectives. Early in the internship, I was somewhat hesitant to speak up, but over time I became more comfortable participating in

discussions and expressing my ideas. Rather than micromanaging, Hans-Peter encouraged interns to think independently and take initiative. This management style was effective because it promoted creativity, accountability, and confidence. It also reflected a real professional environment where employees are often to identify priorities, solve problems, and manage tasks with limited supervision.

Another positive aspect of the management environment was the emphasis on collaboration. Even though interns had individual responsibilities, many discussions involved shared ideas and teamwork. This helped create a learning atmosphere rather than a competitive one.

Major Work Duties, and Assignments

My major duties were centered around the three cybersecurity objectives listed in the internship agreement. Throughout the internship, I worked on privacy, security, and policy-related improvements for the Place4Us platform.

Terms of Use and Privacy Policies

One of my key responsibilities was helping improve the Terms of Use. I worked on clarifying responsibilities, acceptable behavior, privacy expectations, and platform policies. I proposed sections covering:

- Introduction and acceptance of terms
- Mission and community standards
- Privacy and data protection
- Information collected from users
- How information is used

- Data retention
- Misinformation and integrity
- Prohibited conduct

The original Terms of Use were shorter and more limited. My goal was to make the document clearer and more informative while keeping it concise enough that users would still read it. This task was important because users should understand how their information is handled and what standards apply when joining a platform.

XML File Security Review

Another responsibility I examined was risks involving sensitive information stored in the XML files, including names, email addresses, phones numbers, and passwords. I researched whether encrypting should be used and how stronger data protections methods could reduce risk. If sensitive XML files were exposed, user identities could be compromised, creating both trust and legal concerns. This task was necessary because stored user data is valuable to attackers and must be protected. This task helped me understand the importance of securing stored data, not just protecting public-facing systems.

Vulnerability Scan Findings

One of the interns performed a vulnerability scan on the platform. The report identified several issues that should be addressed. Based on the findings, I emphasized the importance of applying an HTTP Content Security Policy (CSP) header and the X-Content-Type-Options security header.

A Content Security Policy helps protect websites from malicious scripts and unauthorized content sources. It would be recommended to add the header, so it is sent with each HTTP

response, and be able to add the specific policies that are needed for the platform. It can reduce the risk of attacks such as Cross-Site Scripting (XSS). XSS is a client-side code injection attack where users insert malicious scripts into a website. Attackers are able to bypass any user input security and would also be able to gain sensitive information like email addresses, names, phone numbers and cookies from users on the platform. To mitigate this attack, it would be best to sanitize and validate any data before storing it in the xml files. Add a content security policy to block any untrusted sources. Also adding restrictions in the comment or post fields to prevent any uploads of malicious code. A restriction rule could be, no special characters and/or word count limit. It would also be best to do some pen-testing as much as possible using OWASP or burp suite. Open Worldwide Application Security OWASP is a nonprofit organization with the goal of improving software security. Burp Suite contains a set of tools for penetration testing.

The X-Content-Type-Options header, set to nosniff, helps prevent browsers from incorrectly guessing file types, which can reduce certain attacks vectors. This is recommended according to the vulnerability scan report by PentestTools. Without the Content-Type-Options header on the platform would also be vulnerable to XSS and/or phishing attacks.

User Experience and Platform Layout

Although my internship was focused on cybersecurity, I also observed the importance of usability and design. During the internship, the platform underwent layout improvements involving buttons, toggles, fonts, and section placement from one place to another to improve the visibility and appearance of the site.

Myself and the other interns believed that design plays a role in user trust, engagement, and retention even if our supervisor believes in functionality than appearance and design. If a

website feels cluttered, or difficult to use, users may leave or become frustrated. Users should be able to feel comfortable and not overwhelmed when navigating the platform. While functionality was a major priority for the supervisor, we were able to contribute ideas that balanced functionality with appearance. This experience taught me that cybersecurity and usability often overlap. Secure systems must also be understandable and accessible to users.

Specific Use of Cybersecurity Skills / Knowledge

Before the internship, I had academic knowledge of cybersecurity principles such as confidentiality, integrity, authentication, and vulnerabilities. During the internship, I applied and expanded that knowledge in practical ways.

Cross-Site Scripting (XSS)

One major topic I researched was Cross-Site Scripting (XSS). XSS is a vulnerability where attackers inject malicious scripts into websites through user input fields such as comments, posts or messages. If user input is not sanitized properly, harmful code can execute in another user's browser.

This can lead to:

- Theft of cookies or session tokens
- Exposure of personal information
- Account hijacking
- Unauthorized actions on behalf of users

To reduce XSS risks, I recommend:

- Sanitizing user input
- Validating submitted data

- Restricting dangerous character or scripts
- Applying Content Security Policy headers
- Performing security testing

Content Security Policy (CSP), evaluating risks of storing personal data in XML files, and balancing security with user functionality and privacy.

The internship changed my understanding of cybersecurity because it showed me that security decisions are not purely technical. If users believe their personal information is unsafe, they may stop using a platform entirely. They also involve usability, ethics, trust, governance, and communication.

How the ODU Curriculum Prepared Me

ODU prepared me well in foundational cybersecurity concepts. My coursework gave me an understanding of threats, risk management, secure systems, and technical terminology that helped me during the internship. I made several connections between school and the internship such as lessons on vulnerabilities connected directly to XSS research, the concepts of confidentiality connected to protecting stored user data, risk management principles connected to vulnerability scan findings, and governance and ethics concepts connected to Terms of Use and platform rules. Some experiences reinforced what I had learned, especially the importance of layered defenses and secure coding practices. However, the internship also introduced areas that are not fully experienced in school. I was able to work on a live platform rather than lab environments. I had the chance to work on open-ended assignments without exact instructions and draft policies that were applied to real users and balanced technical security with user experience. The internship also carried professional communication in a team setting, which is

an important skill to carry over into a professional environment. These experiences added practical value beyond coursework.

Outcomes Compared to Original Objectives

Objective 1: Review User Privacy Rights

This objective was fulfilled. I contributed to improving the Terms of Use and researched privacy expectations, anonymity concerns, discoverability, and policy improvements. In the Terms of Use I offered different sections that described topics of user privacy rights; Introductions & acceptance of terms, missions & community standards, fees, privacy & data protection, information we collects, how information is being used, data retention, misinformation and integrity, and prohibited conducts were some of the topics I presented to improve the terms of use. The first Terms of Use that was originally on the site lacked some important points that user should be advised of when creating an account on the platform. The Terms of Use were kept short to avoid the user from skipping the whole sections that contained the Terms of Use. Users usually skip important sections when signing up. Users only do what they are asked to type in but not read. This point can be backed up by thinking about how many times we, as users, do not read the terms and conditions when signing and entering our personal information on sites. Hans-Peter and the other interns also agreed to keep the Terms of Use in a short manner to not distract or bore the user and ensure it is read thoroughly.

Objective 2: Evaluate Encryption for XML Files

This objective was partially fulfilled. I identified the importance of protecting sensitive XML data and research encryption needs, although I also recognized encrypting as an area where I need to continue my growth. Although, if the XML files are not encrypted, it poses a risk of sensitive information being compromised or accessed externally. The files store personal data

like email addresses, names, and phone numbers. This sensitive data could be misused if it is accessed externally in the wrong hands. It would be a major concern if the information of an anonymous commenter was exposed to the public or leaked. Since the user is trusting that the platform protects their identity, it could lead to a major legal issue.

Most Motivating Aspects of the Internship

The most motivating aspect was contributing to a real platform where my ideas could influence improvements. Knowing that research on privacy or security might help actual users made the work meaningful. I also enjoyed collaborating with other interns in my major and hearing their ideas on cybersecurity topics. Since I'm completing my degree online, it was nice to interact with other students in real-time rather than just discussion posts in courses. Another exciting part was seeing how cybersecurity applies to real organizations rather than only textbook examples. This helped me gain an idea of how a cybersecurity position could look like in a professional setting.

Discouraging Aspects of the Internship

A discouraging aspect was sometimes feeling uncertain about where to begin because tasks were self-directed. Without step-by-step instructions, it occasionally took extra time to define priorities. We were advised to make a work plan, to help us and the supervisor know how we would navigate our task throughout the internship. Another discouraging moment was realizing that some areas such as encryption implementation were weaker areas in my knowledge. Which I think is fine because that just means there is room for growth. There were some other things and topics that other interns would describe, and I would think, how did they think about that or came up with that idea.

Most challenging Aspects of the Internship

The most challenging aspects of the internship were things that applied to myself as a intern. One of the aspects was taking initiative in an open-ended environment. This really helped me realize what I was able to offer as a cybersecurity student. Researching semi-familiar topics independently, translating technical risks into a business recommendation, building confidence to speak more during meetings and understanding both technical and policy dimensions of cybersecurity. These challenges were valuable growth experiences.

Recommendations for Future Interns

Future interns should prepare by learning Linux basics and SSH access. I think an important topic interns should feel comfortable with is, PHP. Future interns should review PHP and web application concepts. Understanding common web vulnerabilities like XSS and CSRF is also an essential skill users should have under their belt. I think also to get the most out of the internship, interns should have a basic understanding of data protections and encryption basics. Future interns should also be prepared for independent and self-directed work. Time management and self-discipline are very important skills interns need, not only for the internship, but these skills also carry over to the professional environment as well. Something else that would be greatly appreciated in the active meeting is participation, interns should be able to present and include their input in conversations. Lastly, writing skills for weekly reports is something interns should also be aware of, be ready to be able to communicate their plans and thoughts in these weekly reports.

Conclusion

My biggest takeaway from this internship is that cybersecurity is about protecting both systems and people. Technical defenses matter, but so do privacy rights, trust, communication, and responsible management. This experience will influence the rest of my time at ODU by

encouraging me to focus more deeply on web security, data protection, and practical cybersecurity skills. I now understand how classroom knowledge connects to professional environments. Professionally, this internship confirmed my interest in cybersecurity and showed me the importance of initiative, adaptability, and lifelong learning. It helped me identify strengths I can build on while also revealing areas where I want continued improvement. Overall, this internship was a valuable step in preparing me for a future career in cybersecurity.