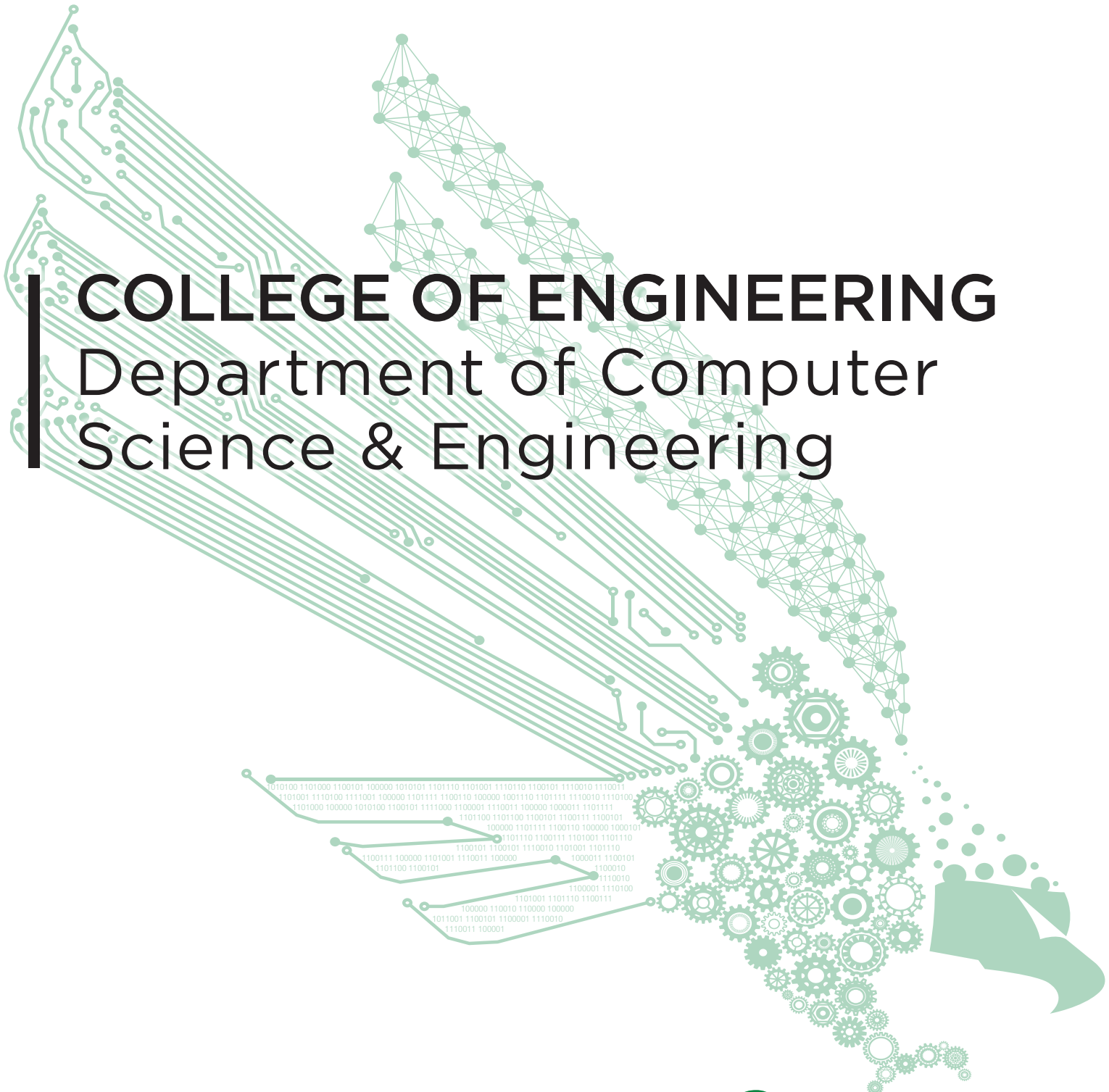




Senior Design Day Spring 2024



COLLEGE OF ENGINEERING

Department of Computer Science & Engineering

CYBERSECURITY

**Senior Design Abstracts
Spring 2024**



@UNTEngineering

engineering.unt.edu
940-565-4300

Gush



gush

Team Members

Alana Babilonia
Jessica Chibuzor-Muko
Ben Curtright
Kelsey Nichols
Tenbit Habtesillasie

External Sponsors/Mentors

Internal Sponsors/Mentors

Dr. Pradhumna Shrestha

Abstract

In recent years user privacy has been a growing concern in menstruapps where intimate data is stored. We've created GUSH in response, a socially oriented web app where user data privacy and security are the main design focus. User's data is protected with end-to-end encryption, limited Personally Identifiable Information, and a robust overall security architecture tested and reinforced throughout development.

GUSH is aimed at educating and empowering individuals about menstruation and reproductive health. It features comprehensive tracking tools and combines educational content with interactive forums. Healthcare professionals contribute to and authenticate content, ensuring reliability. GUSH creates a safe and inclusive space for all users, menstruators and non-menstruators, promoting open discussion and learning. Its tracking tools help users monitor menstrual cycles and health symptoms, integrating education for holistic health management. GUSH serves as both an educational hub and a personal health assistant, destigmatizing menstruation and offering verified expertise, making it an essential resource for health management.

LANCELOT

Lancelot: Cart Knight

CTRL+ALT+DEFEAT

Team Members

Caleb Heller
Rajan Pokharel
Julian Purgahn
James Bridge

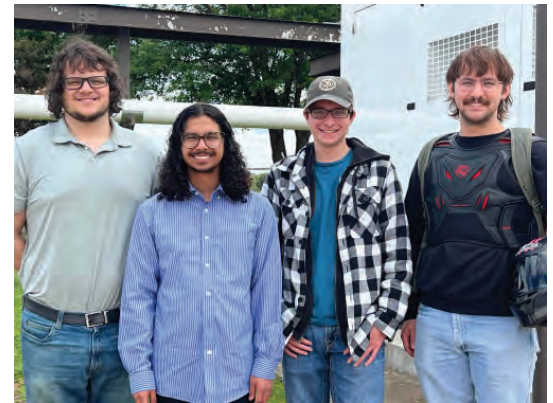
External Sponsors/Mentors

Internal Sponsors/Mentors

Dr. Pradhumna Shrestha

Abstract

With a growing reliance on technology in our society, many have turned to online shopping for convenience and simplicity in their transactions. With the rising demand for internet based shopping, protection of users becomes paramount to provide a secure and simple experience that the users can trust. With Lancelot, that is what we seek to provide. By creating our website from scratch, we can be in control of every level of security, and we can also utilize trusted solutions to provide a secure shopping experience. We provide federated authentication to ensure a secure log in into ones account. A secure payment system that the user can trust to ensure their money is handled correctly. And a minimalistic yet robust UI that provides the users with a trusted service that is able to be accessed across all devices.





VirtualATM by CyberCowboys

Team Members

Brian Granados
Jacob Hall
Ryan Fincher
Yohan Sanchez

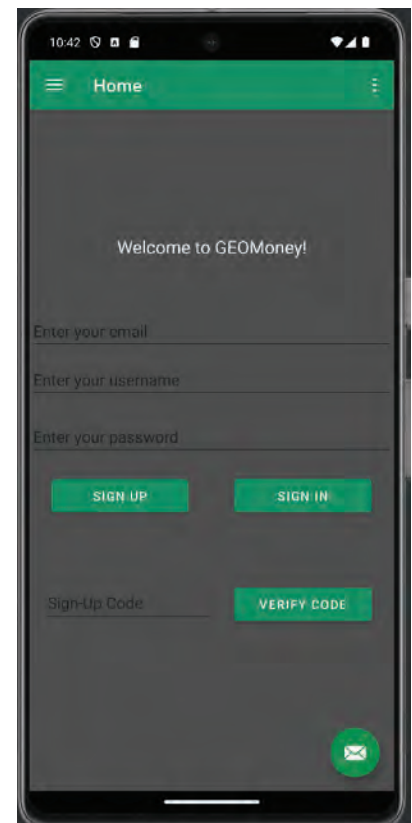
External Sponsors/Mentors

Internal Sponsors/Mentors

Dr. Pradhuma Shrestha

Abstract

Our project aims to create a secure method of transferring funds between parties by allowing the sender of funds to specify a pickup location via geolocation. This project shall be known as “VirtualATM”, an android application, wherein the sender will specify a location which the recipient of funds must travel to in order to complete the transfer. This innovative feature grants users an additional layer of security in their transfers, allowing senders the option of verifying that the intended recipient is actually the one who receives the transfer.





Cybrware

Team Members

Cody Savchenko
Brandon DeLuia
Tucker Hollenkamp
Ivan Navas

External Sponsors/Mentors

Internal Sponsors/Mentors

Dr. Pradhumna Shrestha

Abstract

Cybrware implements security at the software level by providing a tool that performs static code analysis, as well as malware analysis on a multitude of file types. Static code analysis is a proven secure coding practice that steps through each line of syntax without executing code. In today's world, testing code at runtime is insecure and bad practice. We help eliminate these insecure coding practices by alerting users of potential vulnerabilities and errors found in their code through detailed reports. Our tool is compatible with multiple file types including: Python, C/C++, Java, JavaScript, TypeScript, HTML, and PHP. We also offer file analysis through VirusTotal, a SaaS tool used to scan files or URLs for any traces of known malware.

We would like to thank Dr. Shrestha for providing us with all the resources needed to complete this project.

Project Name: VigilBoard

Team Name: VigilNet



Team Members

David Abbot
Isaac Bamidele
William Mahoney
Chance Currie

External Sponsors/Mentors

Internal Sponsors/Mentors

Dr. Pradhuma Shrestha

Abstract

The problem we are trying to solve is how to make something such as vulnerability scanning more streamlined and more user friendly.

VigilBoard solves this existing problem of vulnerability scanning through eliminating the need to know the command line as well as output only the information that is needed, but provides the technical details through logs that can also be viewed by those who are more knowledgeable about nmap and the security practices that come with network defense and security.

It's unique in the fact that anyone has the ability to use it in order to figure out what vulnerabilities are present on a scannable IP or URL. It helps the people and companies that use it by VigilBoard being able to streamline an important network security process that helps to simplify information to its users.

For those who are proficient with nmap (both on command line and GUI interface version of nmap) as well as have knowledge of or a good understanding of security standards for networking, it allows them to quickly gather vulnerability information through one tool instead of having to utilize multiple tools.

For those who may not be as technologically proficient, VigilBoard comes with an easy-to-understand GUI that will only present them with the information that is truly needed for a non-technical person to understand, and this information is output as an HTML page that can easily be viewed and stored as a log for later viewing purposes as needed.

VigilBoard is designed to be lightweight, multiplatform, and learnable by users who are not technically proficient in cybersecurity. However, the ability to fully interpret and act upon the outputs of the program will require varying levels of expertise in cybersecurity. The tool that we created meets the outlined requirements when compared to other vulnerability scanning tools.



We would like to thank our professor, Dr. Pradhuma Shrestha, for overseeing this project and mentoring us throughout the year.