College of Engineering

R&D Expo

University of North Texas

SENIOR DESIGN

Spring 2026

COLLEGE OF ENGINEERING
Department of Computer Science & Engineering

CYBERSECURITY
Senior Design Abstracts
Spring 2026

UNT COLLEGE OF ENGINEERING

Baneberry
by PseudoRoot

Team Members

Ryan Nation
Asil Elsharafi
Shayan Baniasadi

External Sponsors/Mentors

N/A

Internal Sponsors/Mentors

Pradhumma Srestha

Abstract

Modern security assessments increasingly rely on automation to streamline decision-making,generate results, and support security improvements. While tool execution can beautomated,selecting which tools to run and when remains largely heuristic-driven.

This project explores a decision-driven approach to automating network reconnaissance workflowsby introducing a modular framework that selects tools based on observations from target systems.Network scan results are parsed into structured asset inventories, from which features such as open ports and detected services are extracted. These features are used to inform a machine learning model that predicts appropriate next steps in the assessment process.

The system integrates scanning, parsing, and decision logic into a unified pipeline while operating under predefined constraints that promote human oversight, legal scope awareness, and target-specific testing. This work demonstrates the feasibility of using lightweight machine learning models to guide tool orchestration and highlights opportunities for more adaptive, data-drivensecurity assessment methodologies.

UNT COLLEGE OF ENGINEERING

Team Members

Astro Pryor
Bakr Alkhalidi
Grant Stautzenberger
Elli Gould
Jay Hernandez

External Sponsors/Mentors

Internal Sponsors/Mentors

Dr. Pradhumna Shrestha

Abstract

In professional environments there are many different ways they can be attacked. The 2 that we focused on were office macros and ransomware. Many businesses still rely on Microsoft Office macros and threats can spread quickly before detection or response. Ransomware is a rapidly growing cyber threat that encrypts files and demands payments. Small businesses are especially vulnerable due to limited security resources and budget constraints.

We built two dummy viruses to test against our antiviruses, a macroware and a ransomware. The macroware is a VBA-based file generator that is meant to exhaust CPU resources. The ransomware can recursively search through directories that encrypts files using AES encryption with added safeguards and a simulated delivery method. We created lightweight macroware and ransomware antiviruses in Python that use static analysis, dynamic analysis of files and processes, behavioral monitoring (mass file changes, rapid file renaming), an automatic quarantining system, and a logging system. These antiviruses would then be run from a GUI created in Tkinter that would allow the antiviruses to run scans and inspect files without technical expertise.

The antivirus programs we created were able to successfully monitor for, detect, mitigate, and quarantine the dummy viruses that were used to infect the test computer. The mitigation script for the macro attack successfully detected the attack happening and stopped the process that was causing the file creation.

Our main goal of this project was to create an effective program to combat both macro attack and ransomware viruses. This was accomplished by developing two Python antivirus programs with specific detection specification, automatic quarantining of malicious files or programs, and testing these systems against dummy viruses. By combining these programs a GUI, we have effectively created a program that can protect from real-world virus attacks.

CyberCapstone
Security Pass

Team Members

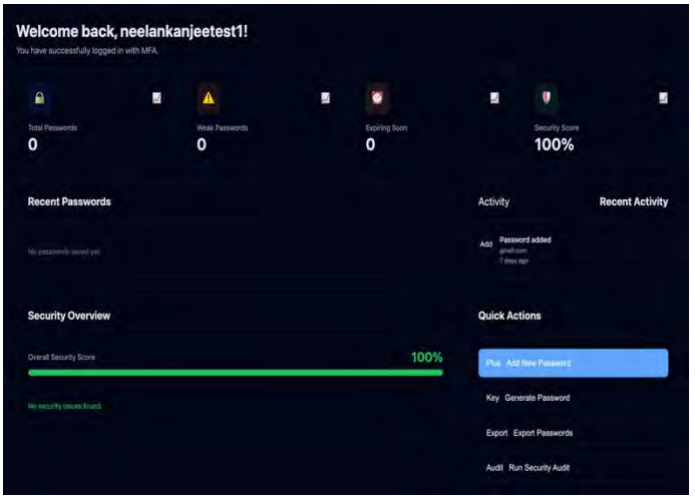
Neelan Kanjee
Will Woods
Sahib Mann
Arnav KC
Darius Stinson

External Sponsors/Mentors

N/A

Internal Sponsors/Mentors

Dr. Pradhumna Shrestha



Abstract

SecurityPass is a modern, Web-Based Password Manager that was created for a Senior Design Project. The goal of the SecurityPass project was to demonstrate how the latest in Cybersecurity and DevSecOps can be used to protect passwords (and other credentials). The project has an architecture that uses a Client-Encrypted Vault for storing User Credentials. This is done using AES-256-GCM Encryption and Argon2id Key Derivation. The project includes all the core features necessary for a secure password management solution including; Encrypted Credential Storage, Password Generation, Multi-Factor Authentication Support, Secure Storage, Cross Platform Access via Web Browser, and an Easy-to-use Interface. Additionally, we have included Cloud Deployment support through AWS, Containerized Backend Hosting, and Domain Configuration through Cloudflare. As well as creating the Application, this project also focused on implementing secure software engineering throughout the entire DevSecOps lifecycle

UNT | COLLEGE OF ENGINEERING

CyberOracle - Secure Gateway for AI Compliance and Data Protection

CyberOracle

Team Members

Bishesh Dulal
Niall Chiweshe
Pradip Sapkota
Quoc Nhan Tra

External Sponsors/Mentors

Internal Sponsors/Mentors

Dr. Pradhumna Shrestha

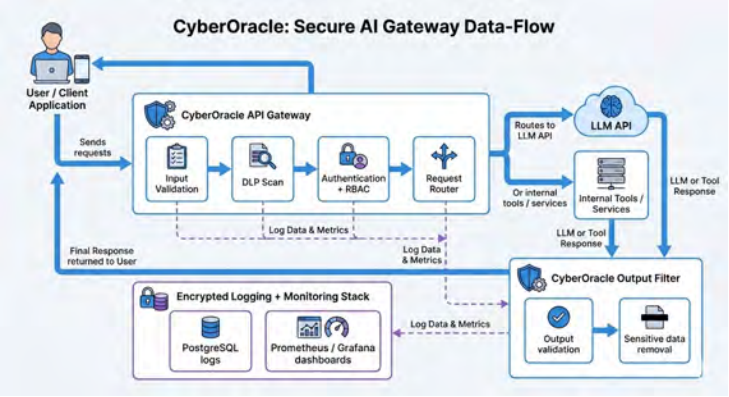
Abstract

The CyberOracle system is designed to provide a secure AI gateway for enforcing data protection and regulatory compliance in AI-driven workflows. The platform monitors, analyzes, and controls interactions with AI models to prevent the exposure of sensitive information and ensure adherence to security policies. CyberOracle integrates data loss prevention (DLP), role-based access control (RBAC), secure logging, and real-time monitoring to create a centralized defense layer for organizations using large language models.

The system continuously inspects incoming requests for sensitive data such as personally identifiable information (PII) and protected health information (PHI), applying automated redaction or blocking mechanisms when violations are detected. All interactions are securely logged and stored in a database, enabling auditing, traceability, and compliance reporting. CyberOracle also incorporates authentication and authorization mechanisms using JWT and API keys to enforce strict access control across different user roles.

To enhance visibility, the platform provides an interactive dashboard that visualizes system activity, security events, and compliance metrics in real time. Integrated monitoring tools track anomalies, trigger alerts, and support incident response through automated notifications. Additionally, the system includes red-team testing capabilities to simulate adversarial attacks such as prompt injection, ensuring continuous evaluation and improvement of AI security defenses.

By combining proactive threat detection, policy enforcement, and comprehensive monitoring, CyberOracle enhances the security, transparency, and compliance of AI applications. The platform enables organizations to safely leverage AI technologies while protecting sensitive data and maintaining regulatory standards.



A real-time AI security gateway for DLP enforcement, monitoring, and compliance.

UNT COLLEGE OF ENGINEERING

CyberPulse: A Real-Time Threat Visualization Dashboard

Team Members

Aishat Arawole
Ali Akhtar
Waad Elkenin
Grishab Mishra
Victoria Omosowon

External Sponsors/Mentors

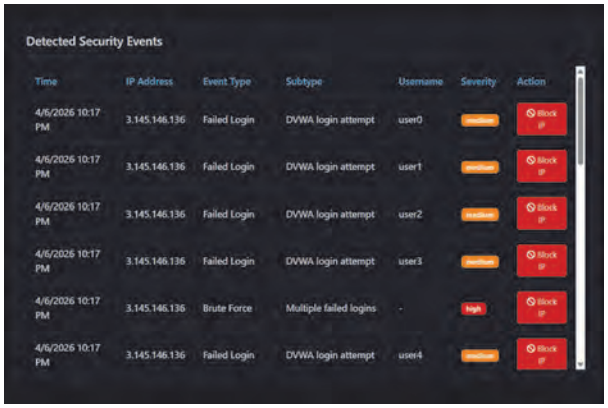
N/A

Internal Sponsors/Mentors

Dr. Pradhumna Shrestha

Abstract

CyberPulse is a live threat visualization dashboard developed as part of a virtual Security Operations Center (SOC). It allows security analysts to monitor web application attacks in real time, including SQL injection, XSS, and brute force attempts. The system is hosted on an AWS EC2 instance and consists of a Flask API backend that receives attack data from custom detection scripts targeting a vulnerable web application (DVWA). The Flask API generates security alerts, supports manual IP blocking/unblocking, and serves JSON data to the frontend dashboard. The dashboard automatically refreshes attack feeds, color? codes events by severity, provides IP blocking controls, and generates downloadable PDF reports. Attack events and blocked/unblocked IPs are stored in a local SQL database for persistence.



UNT COLLEGE OF ENGINEERING

Team Four Star-File Scanner

Team Members

Orion Vialpando
Luis David
Joe Strickland
Emmanuel Moonga

External Sponsors/Mentors

Internal Sponsors/Mentors

Dr. Pradhumna Shrestha

Abstract

The File Scanner Web Application is a Flask-based web tool designed to help users safely upload and analyze files for potential malware and viruses. When a file is uploaded through the web interface, the application automatically renames it with a unique identifier to prevent conflicts, saves it to a secure upload folder, and immediately passes it through a custom scanning module powered by the VirusTotal API. Scan results are returned in real time and cached in memory, showing users a color-coded status indicating whether a file is clean or infected, along with a SHA256 hash and a detailed scan summary. Each scanned file also generates a downloadable report for future reference. Users can view all uploaded files and delete them at any time, which also removes the associated report and clears the cached scan data. The application is built with Python, Flask, and Werkzeug for secure file handling.

UNT | COLLEGE OF ENGINEERING

Team Members

Gavin Hecke, Appar Thebe, Chuma Ejekute-Obi, Jacob Libres, and Jaylin Nwigwe

External Sponsors/Mentors

Internal Sponsors/Mentors

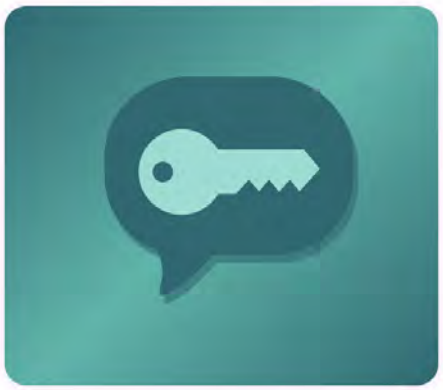
Dr. Pradhumna Shrestha

Abstract

This project presents the design and implementation of a malware scanner capable of detecting, mitigating, and reporting malicious files and processes. This scanner primarily focus on detection, this system emphasizes proactive mitigation by terminating harmful processes, quarantining suspicious files, and restricting malicious. The scanner also provides comprehensive logging and reporting features for transparency and auditability. Additional functionalities include a user-friendly interface for manual scanning, and a dashboard for monitoring system activity and historical events. Overall, the project demonstrates a scalable and security-focused approach to improving system protection through automated threat response and continuous monitoring. The backended portion uses SHA-256 And VirusTotal API to analyze files, rate severity, and support audit logging.

UNT COLLEGE OF ENGINEERING

Cipher_Chat - KCCA Security



Team Members

Annette Camacaro
Carlos Bonilla
Corinee Resendiz
Kyle McWilliams

External Sponsors/Mentors

N/A

Internal Sponsors/Mentors

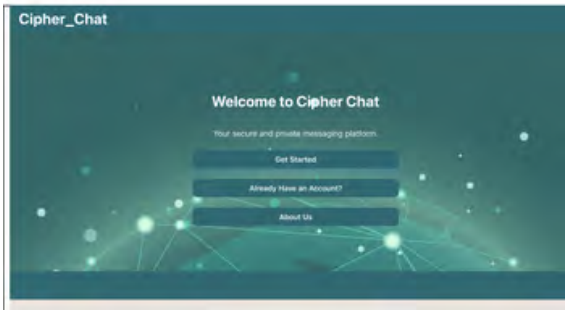
Dr. Pradhumna Shrestha

Abstract

Cipher_Chat is a secure messaging application designed to provide private and reliable communication through modern encryption and secure system design. The platform protects user data by ensuring that all messages, file attachments, and voice communications are end-to-end encrypted, preventing access from servers or unauthorized third parties. It addresses common issues found in traditional messaging platforms, such as centralized data storage, metadata exposure, and user activity tracking.

The application includes features such as secure login and account creation, multi-factor authentication, encrypted file sharing, voice memos, and ephemeral messaging, which allows messages to automatically delete after a specified period of time. It also incorporates monitoring and logging mechanisms to track system performance and detect potential security issues.

Cipher_Chat is designed to redefine how people communicate securely by giving users full control over their data, with the assurance that no unauthorized parties can access or store their information. The platform follows a decentralized, peer-to-peer (P2P) communication model, enabling users to communicate securely in real time without relying on centralized systems. Built with a strong emphasis on privacy and security, Cipher_Chat aims to meet professional standards for protecting sensitive user data while providing a consistent and user-friendly experience.



UNT COLLEGE OF ENGINEERING

SafeByte

Team Members

Poojah Mirkhelker
Akshith Raparthi
Madison Rodriguez
Edward Tomlinson
Khalil Webb

External Sponsors/Mentors

Internal Sponsors/Mentors

Dr. Pradhumna Shrestha

Abstract

SafeByte is a demonstration that simulates different attacks that could happen to a web application. It is designed be able to attack the web application first and then be able to enable the corresponding defense to those attacks. The system processes HTTP requests using socket programming and stores user data in a database. The system runs at constant high speeds, offers live updates from the dashboard page, and also has a live logging page to be able to detect when a user successfully logs into the app, when a user unsuccessfully logs in, and also what attack and defense is currently being ran. The attacks consist of a cross site scripting attack, an SQL injection, and a DDos attack. The application was intentionally designed with insecure input handling to simulate the common vulnerabilities between these attacks.

UNT COLLEGE OF ENGINEERING

WhisprTunnel - Secure File Sharing & Storage Application

Team Members

Jeovani Martinez
Amaanullah Shahim
Mason Schaefer
Muhammud Elsell

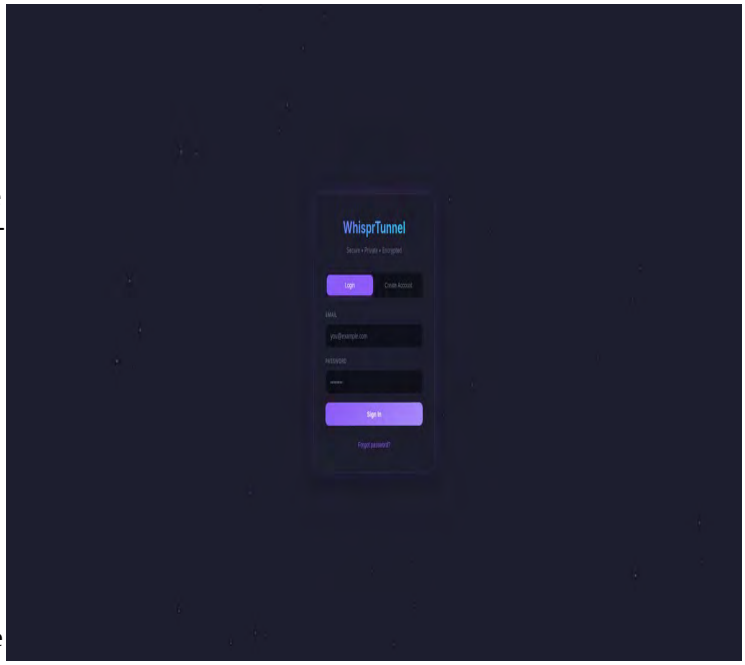
External Sponsors/Mentors

Internal Sponsors/Mentors

Dr. Pradhumna Shrestha

Abstract

The WhisprTunnel Secure File Sharing & Storage application is intended to solve common issues with file sharing platforms. Some of these issues include not having robust enough security features to keep user accounts and their data protected properly on the web. Additionally, anonymous file sharing capabilities aren't offered much, which is a useful market to users who want an application where they can securely store their data, as well as sharing it with others, and the receiver doesn't need an account to download the data. Furthermore, our database also employs parameterized database queries to prevent modern SQL injection attacks, combined with real-time threat detection from our ClamAV integration into our file scanning upon user upload. WhisprTunnel utilizes a per-user file and folder storage, ensuring separation between users. We implemented TOTP MFA authentication that doesn't use external APIs and is a locally generated QR for secure MFA setup. Dual SHA-256 hashing on the server-side & client-side for file integrity verification before and after file upload. We collect comprehensive audit logging for security event tracking combined with file retention policies with automatic expiration and cleanup through our RESTful API architecture. Password account creation uses bcrypt to hash user passwords on account creation for user safety and zero-trust. Additional features of our application allows users to preview files in the browser that they upload with multiple supported file types supported for viewing. Some of the security middleware that we have in place to protect against malicious traffic includes, but isn't limited to: XSS protection, HPP prevention, CORS configuration, SQL SSL support in production environment, API, authentication, upload endpoints are all rate limited. Our WhisprTunnel File Sharing application aims to help users find a secure platform to store and share their data with friends, family, and more in a safer, reliable way.



SPARROW

Team Members

Kevin
Jacob
Bhargav
Alessio
Lucero

External Sponsors/Mentors

Internal Sponsors/Mentors

Dr. Pradhumna Shrestha

Abstract

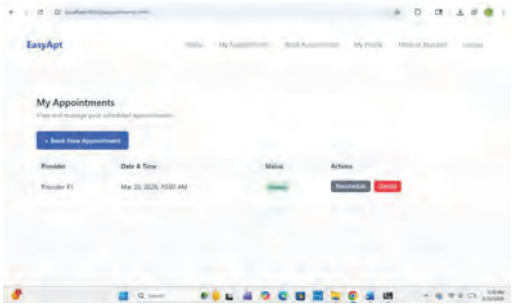
SPARROW Secure Messaging is designed to be a web application focused on providing secure and private communication between users. The system allows users to register, manage contacts, and exchange messages while ensuring data stays confidential with the use of encryption. Messages are encoded before transmission and stored securely to prevent any chances of unauthorized access.

SPARROW includes features such as user authentication, contact management, and QR key verification to ensure users are communicating with their designated user. This platform is built using web tech and deployed using containerization tools. This allows us to scale as we need and ensure users will have reliable communication at all times.

By combining secure messaging practices with a simple interface, SPARROW enhances user privacy and provides a reliable contribution for secure communication anywhere in the world.

UNT COLLEGE OF ENGINEERING

EasyAPT - Healthcare Appointment Scheduler



Team Members

Mason Rasberry
Efrain Castaneda-Reyes
Emil Karimov
Jesus Barco
Aiden Lambrecht

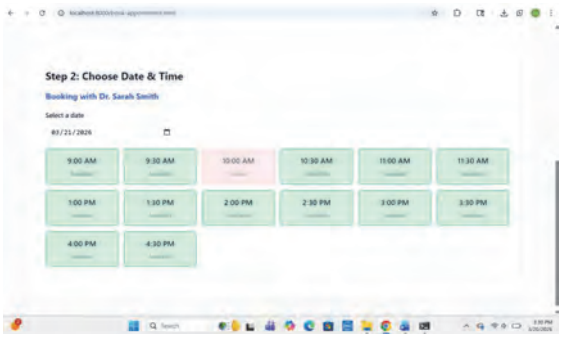
External Sponsors/Mentors

Internal Sponsors/Mentors

Dr. Pradhumna Shrestha

Abstract

EasyAPT is a web-based healthcare appointment scheduling system designed to improve efficiency, reduce no-shows, and enhance the overall experience for both patients and providers. The system allows patients to create accounts, search for healthcare providers, and book, reschedule, or cancel appointments through an intuitive interface. On the provider side, staff can manage availability, block time slots, and view daily or weekly schedules. EasyAPT is built using modern web technologies, including a FastAPI backend with SQLModel and a PostgreSQL database, ensuring scalability and reliability. Security is a key focus of the system, with features such as role-based authentication, encrypted data handling, and audit logging to protect sensitive patient information. Additionally, automated reminders are integrated to minimize missed appointments and reduce administrative workload. Overall, EasyAPT demonstrates how a secure and user-friendly scheduling platform can streamline healthcare operations and improve service delivery.



UNT COLLEGE OF ENGINEERING

Vision Quest - Cyber Training Platform

Team Members

Sydney Jones
Claire Pacquing
Dakshayani Mallu
Kylie Sutton

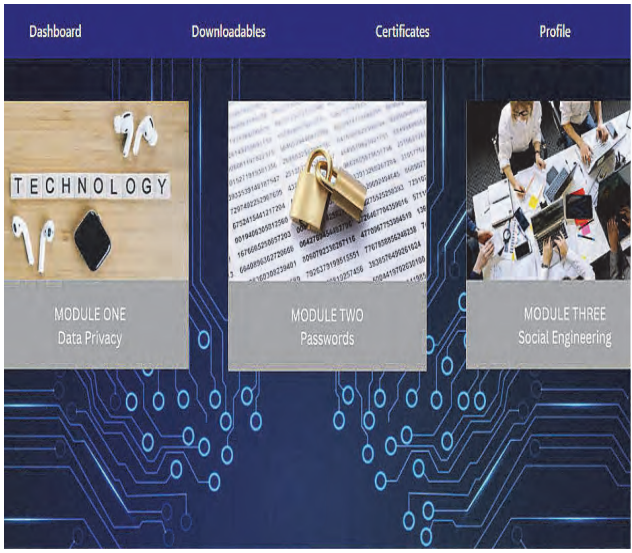
External Sponsors/Mentors

Internal Sponsors/Mentors

Dr. Pradhumna Shrestha

Abstract

Vision Quest is a secure web-based cybersecurity training platform that is built to address one of the most critical security vulnerabilities of an organization, its people. Many employees lack awareness of cybersecurity best practices including password hygiene, data privacy regulations, and social engineering threats like phishing. Vision Quest is designed to help organizations educate employees on these important security topics to help close this gap. Vision Quest has training modules that cover Data Privacy, Password Security, and Social Engineering. Each module includes a syllabus explaining the module content, videos on the module topic, and games to engage the user while also ensuring they understand module content. Once the training content is finished, employees must take the module quiz and earn a score of 80% or higher to earn the module completion certificate. User account information is stored in a secure MongoDB database and passwords are hashed before storage. The system tracks user training progress, quiz scores, streaks, and certificates, logging user actions across the platform. Vision Quest helps organizations strengthen the cybersecurity awareness of their employees.



UNT | COLLEGE OF ENGINEERING

@UNTEngineering

engineering.unt.edu
940-565-4300