UNIVERSITY OF THE PEOPLE
The Education Revolution

Automated Penetration Testing Procedures

A Capstone Project Report of MSIT 5910

Submitted by:

Michael Couchman (C10111672)

For the partial fulfilment of the requirements for the degree of

Master of Science in Information Technology

Supervised by:

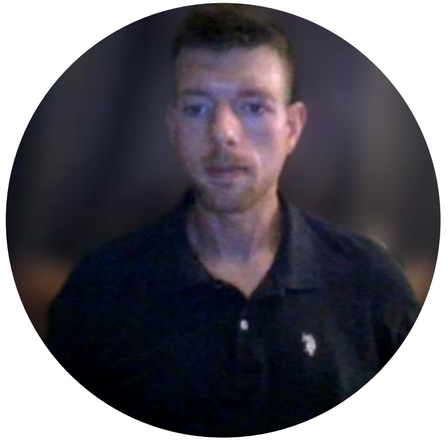
Dr. Shuchi Dhir

Department of CS and MSIT
University of the People,
Pasadena, CA 91101, United States

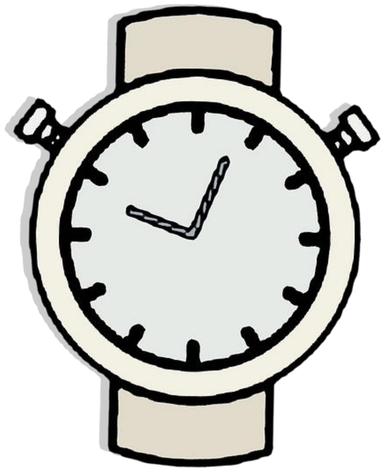
Term 1, September-October, 2024

Introduction

- Emerging trends in cybersecurity are becoming increasing advanced
- Potential for AI-enabled cyberweapons (Yamin et al., 2021) is an example of how emerging technologies pose greater threats
- Automated Penetration Testing performed successfully by Enoch et al. (2020) - HARMer

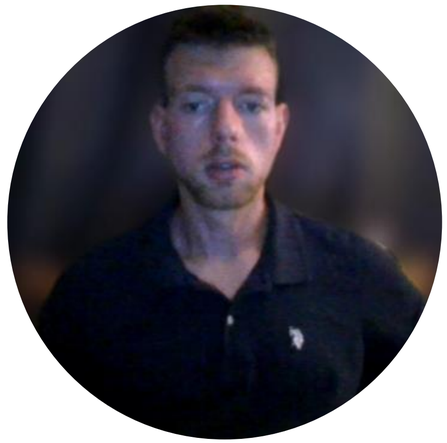


Problem Statement



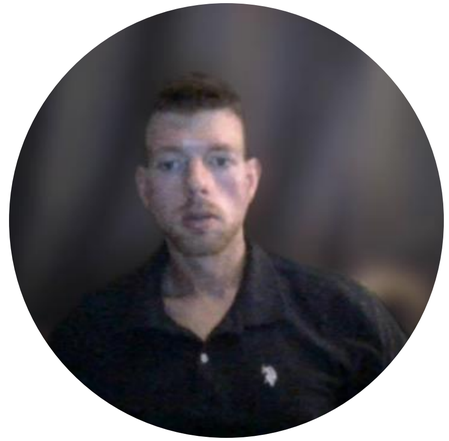
- Manual penetration testing procedures take up a lot of time and $$$

- Require expertise
- Need to keep up with emerging threats



Proposed Solution (Project Objective)

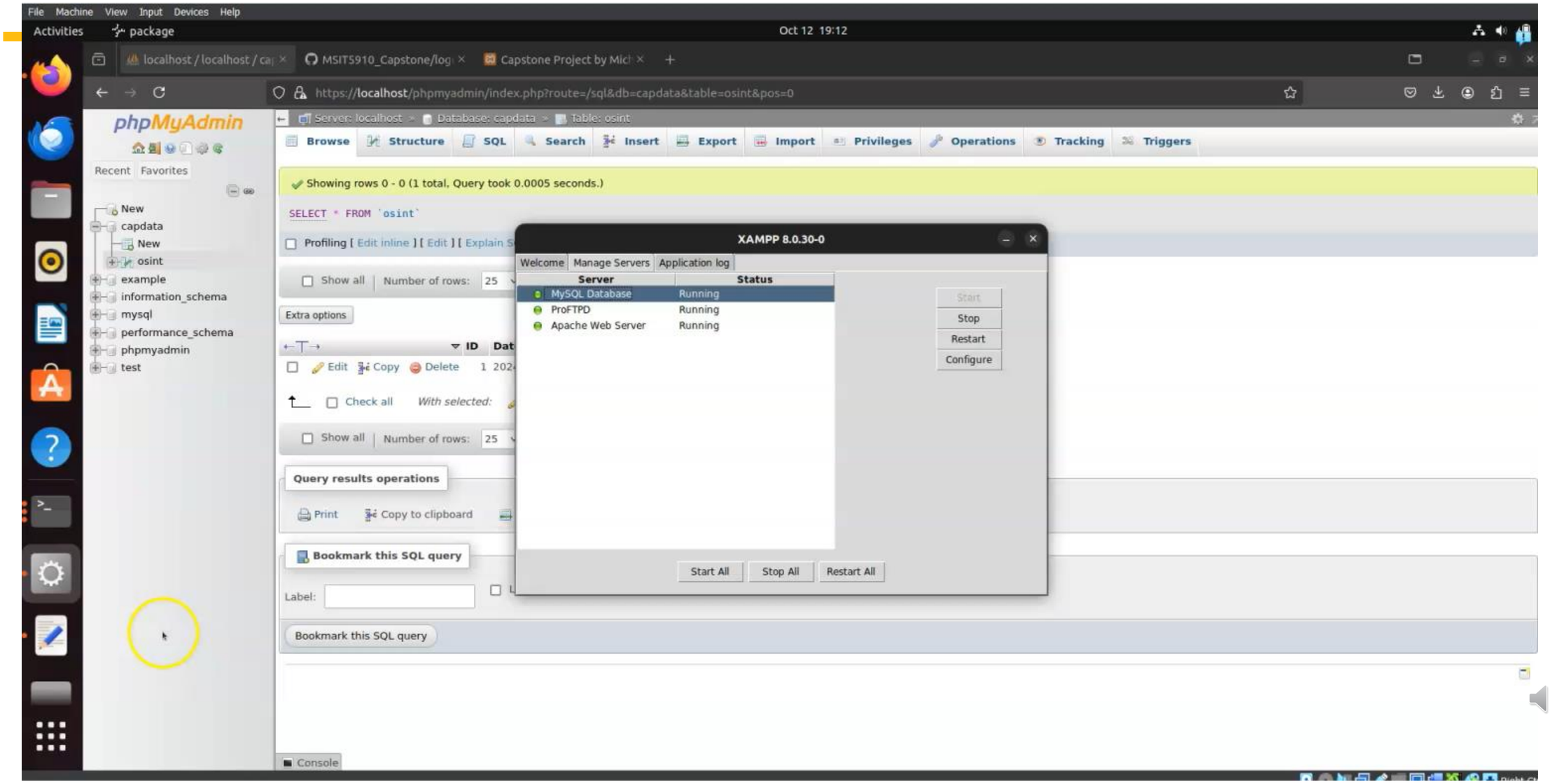
- Utilize automation to reduce time through scripting
  - Bash (Linux CLI)
  - SQL (Database)
  - PHP (API)
  - HTML, CSS (Webpage)



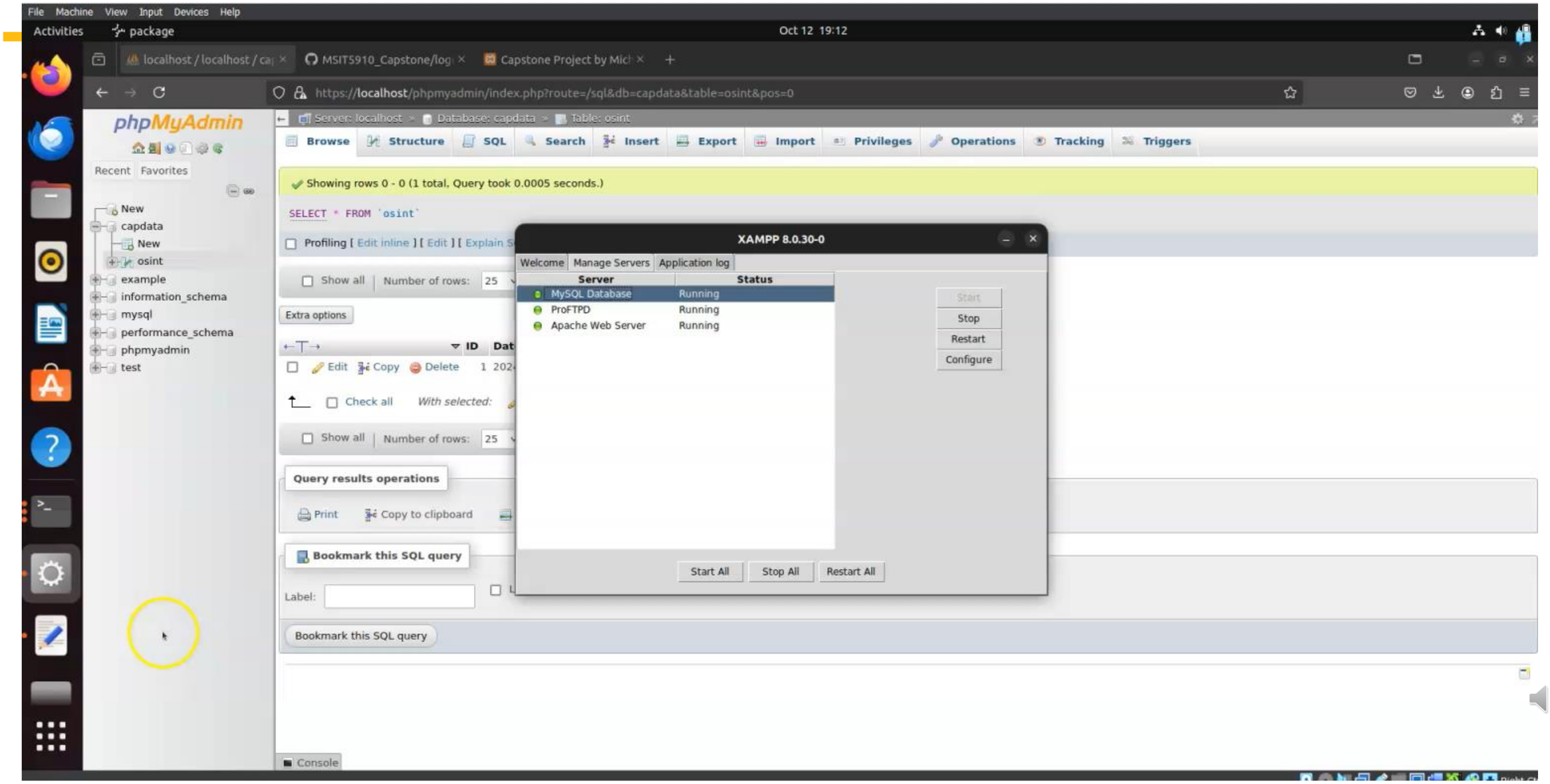
- Automate these elements to be able to:

- process scans over multiple target domains -> format relevant data -> upload to database -> present on web page

Methodology & Results

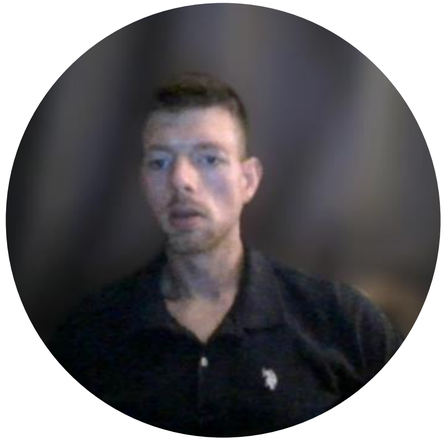


Results

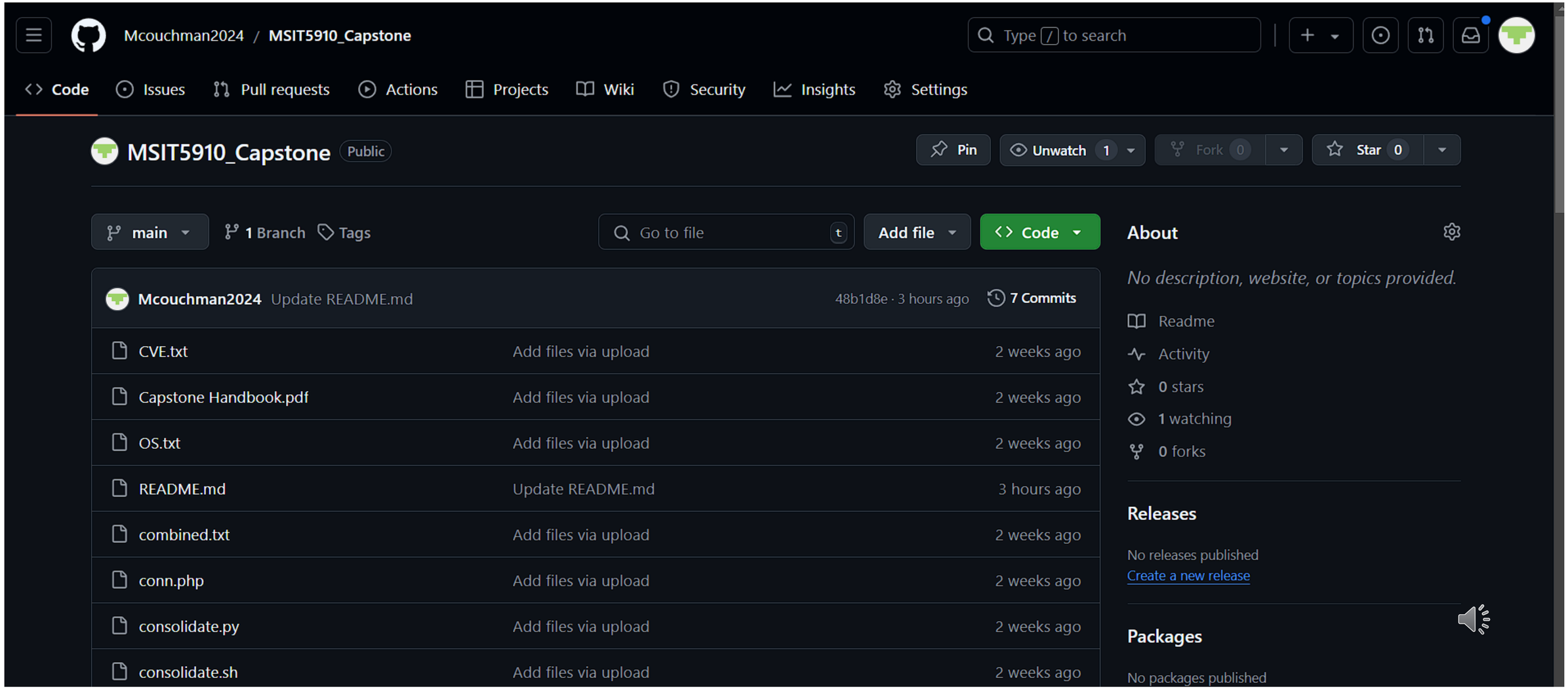

File Machine View Input Devices Help
Activities
package
Oct 12 19:12
https://localhost/phpmyadmin/index.php?route=/sql&db=capdata&table=osint&pos=0
phpMyAdmin
Recent Favorites
New
capdata
New
osint
example
information_schema
mysql
performance_schema
phpmyadmin
test
Server: localhost » Database: capdata » Table: osint
Browse Structure SQL Search Insert Export Import Privileges Operations Tracking Triggers
Showing rows 0 - 0 (1 total, Query took 0.0005 seconds.)
SELECT * FROM `osint`
Profiling [Edit inline] [Edit] [Explain S
Show all Number of rows: 25
Extra options
ID
Edit Copy Delete 1
Check all With selected:
Query results operations
Print Copy to clipboard
Bookmark this SQL query
Label:
Console
XAMPP 8.0.30-0
Welcome Manage Servers Application log
Server Status
MySQL Database Running
ProFTPD Running
Apache Web Server Running
Start
Stop
Restart
Configure
Start All Stop All Restart All

Discussion & Potential Impact

- Great potential to be expanded into more elaborate workflows that actually initiate attacks based on the information gathered.
- Could also be repurposed towards different goals (i.e. integrating OSINT database content)



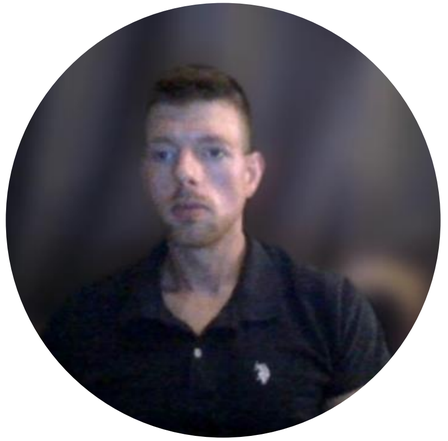
Code Accessible at GitHub



https://github.com/Mcouchman2024/MSIT5910_Capstone

Potential Impacts Cont’d & Conclusion

- The project implantation successfully achieved the goal of reducing the amount of time required in penetration testing procedures.
- The project allowed me to apply previously learned skills in software development, databases, programming languages, project management, and cybersecurity.



THANK YOU

www.UoPeople.edu | info@UoPeople.edu

References

- Enoch, S. Y., Huang, Z., Moon, C. Y., Lee, D., Ahn, M. K., & Kim, S. K. (2020). HARMer: Cyber-Attacks Automation and Evaluation. *IEEE Access.* https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9142179

- Guembe, B., Azeta, A., & Misra, S. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. *Applied Artificial Intelligence*. 36(1). https://www.tandfonline.com/doi/full/10.1080/08839514.2022.2037254

- Yamin, M. M., Ullah, M., Ullah, H., & Katt, B. (2021, March). Weaponized AI for cyber attacks. *Journal of Information Security and Applications*. 57. https://www.sciencedirect.com/science/article/pii/S2214212620308620?casa_token=6arg-y6I9O4AAAAA:npUluJIdyXM9gMGUz-I_GOyWDszXTGELoKBlSFgNWqmxyjhoOpHrrm32dXVG4UOj08oKSnvkNv50