



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**



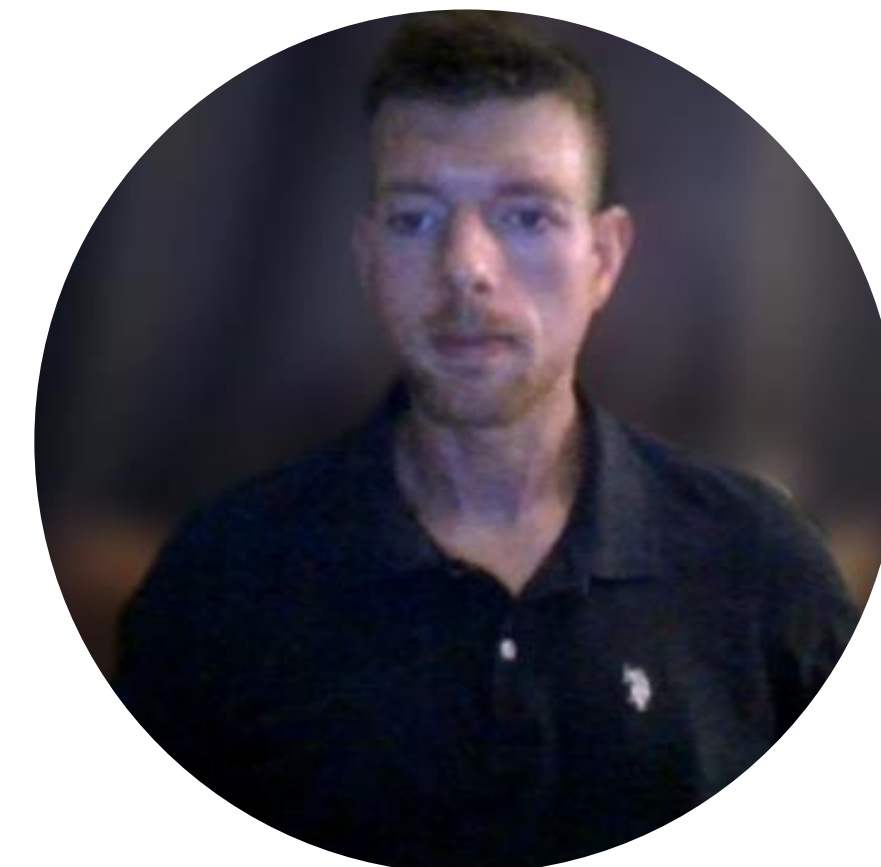


# Introduction

---



- Emerging trends in cybersecurity are becoming increasingly 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

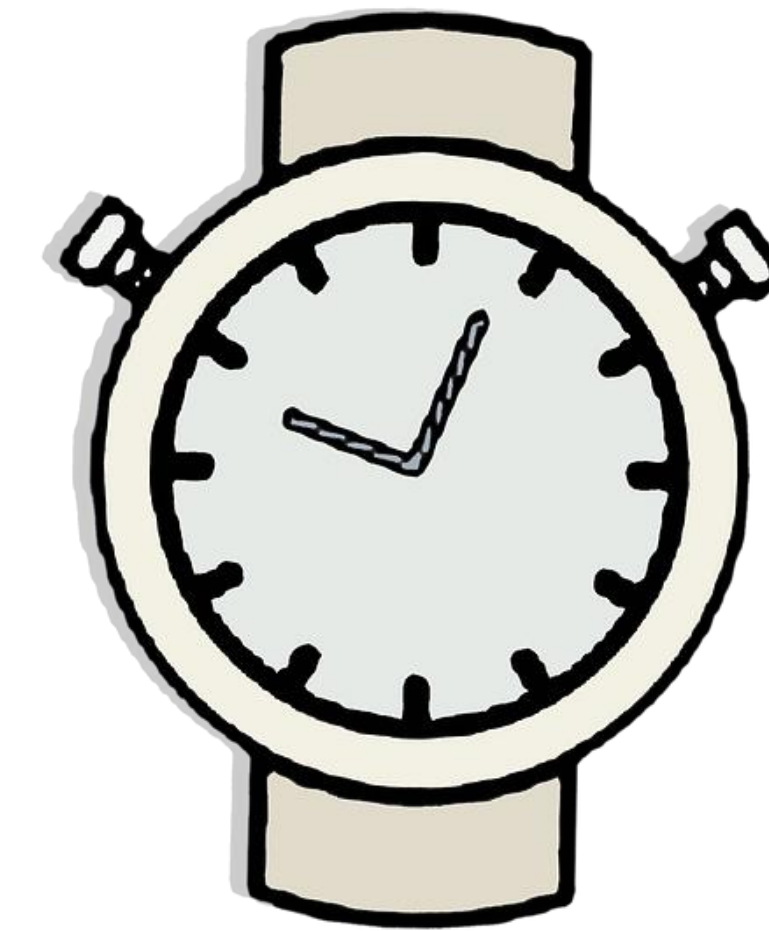


# Problem Statement

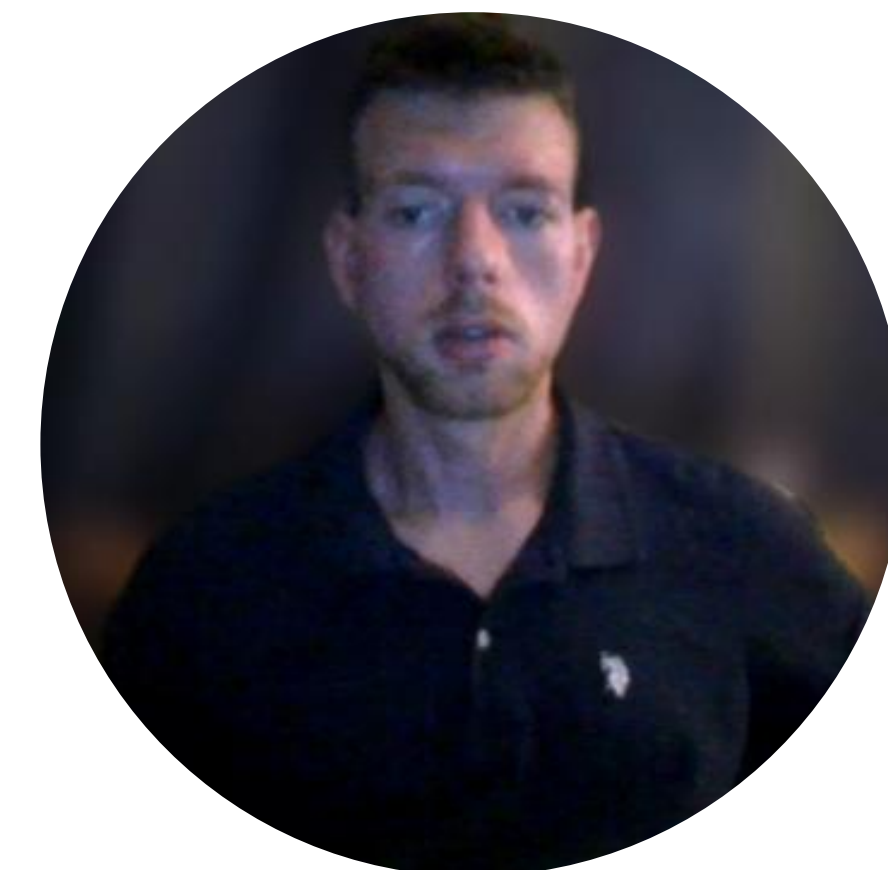
---



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

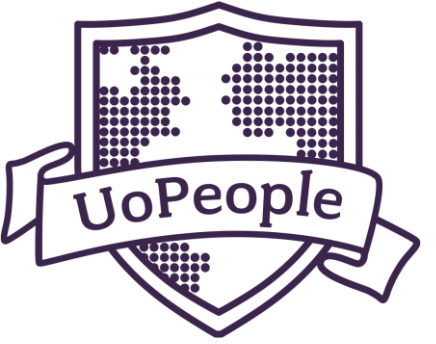


- Require expertise
- Need to keep up with emerging threats

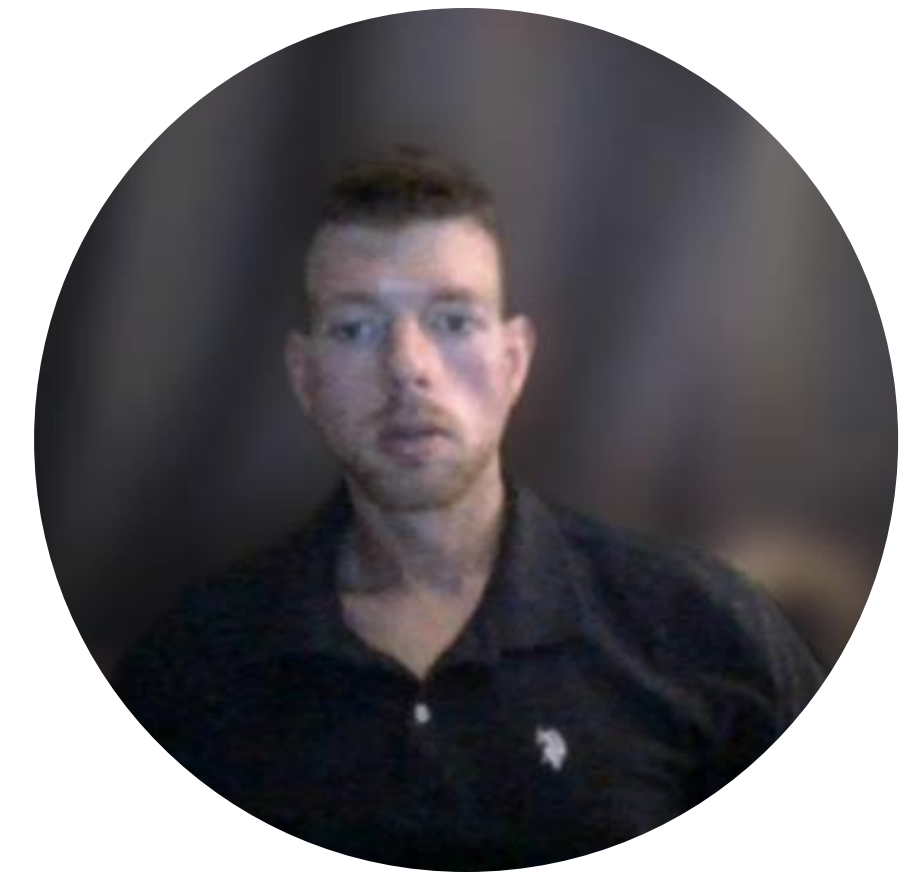


# Proposed Solution (Project Objective)

---



- 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



File Machine View Input Devices Help

Activities package

Oct 12 19:12

localhost / localhost / ca: MSIT5910\_Capstone/log Capstone Project by Mid: +

https://localhost/phpmyadmin/index.php?route=/sql&db=capdata&table=osint&pos=0

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 Date

Edit Copy Delete 1 2024

Check all With selected:

Show all Number of rows: 25

Query results operations

Print Copy to clipboard

Bookmark this SQL query

Label:

Bookmark this SQL query

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

# Results



File Machine View Input Devices Help  
Activities package  
Oct 12 19:12

localhost / localhost / ca: MSIT5910\_Capstone/log Capstone Project by Mich

https://localhost/phpmyadmin/index.php?route=/sql&db=capdata&table=osint&pos=0

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 Data

Edit Copy Delete 1 2024

Check all With selected:

Show all Number of rows: 25

Query results operations

Print Copy to clipboard

Bookmark this SQL query

Label:

Bookmark this SQL query

Console

XAMPP 8.0.30-0

Welcome Manage Servers Application log

Server	Status
MySQL Database	Running
ProFTPD	Running
Apache Web Server	Running

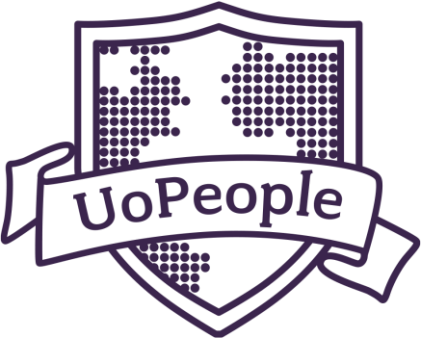
Start Stop Restart Configure

Start All Stop All Restart All

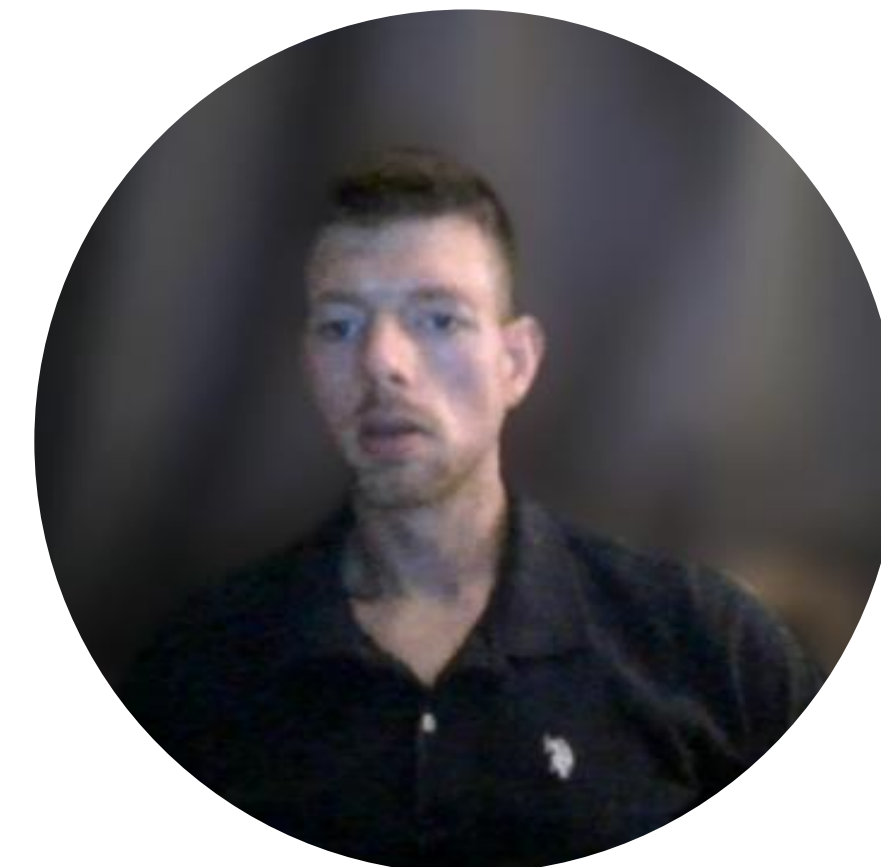


# Discussion & Potential Impact

---



- 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

A screenshot of a GitHub repository page for "MSIT5910\_Capstone" by user "Mcouchman2024". The repository is public and has 1 branch (main), 0 forks, and 0 stars. The file list includes CVE.txt, Capstone Handbook.pdf, OS.txt, README.md, combined.txt, conn.php, consolidate.py, and consolidate.sh. The README.md file was updated 3 hours ago. The right sidebar shows the "About" section with no description, website, or topics provided, and the "Releases" section with no releases published.

Mcouchman2024 / MSIT5910\_Capstone

Type / to search

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

MSIT5910\_Capstone Public

Pin Unwatch 1 Fork 0 Star 0

main 1 Branch Tags

Go to file

Add file Code

About

No description, website, or topics provided.

Readme Activity 0 stars 1 watching 0 forks

Releases

No releases published  
[Create a new release](#)

Packages

No packages published

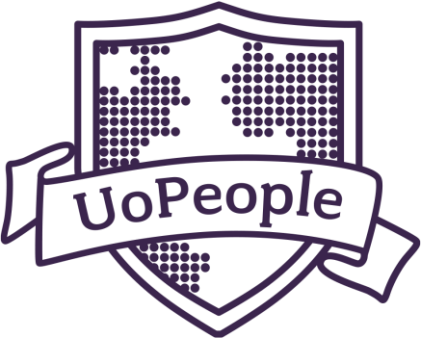
File	Action	Time
CVE.txt	Add files via upload	2 weeks ago
Capstone Handbook.pdf	Add files via upload	2 weeks ago
OS.txt	Add files via upload	2 weeks ago
README.md	Update README.md	3 hours ago
combined.txt	Add files via upload	2 weeks ago
conn.php	Add files via upload	2 weeks ago
consolidate.py	Add files via upload	2 weeks ago
consolidate.sh	Add files via upload	2 weeks ago

[https://github.com/Mcouchman2024/MSIT5910\\_Capstone](https://github.com/Mcouchman2024/MSIT5910_Capstone)

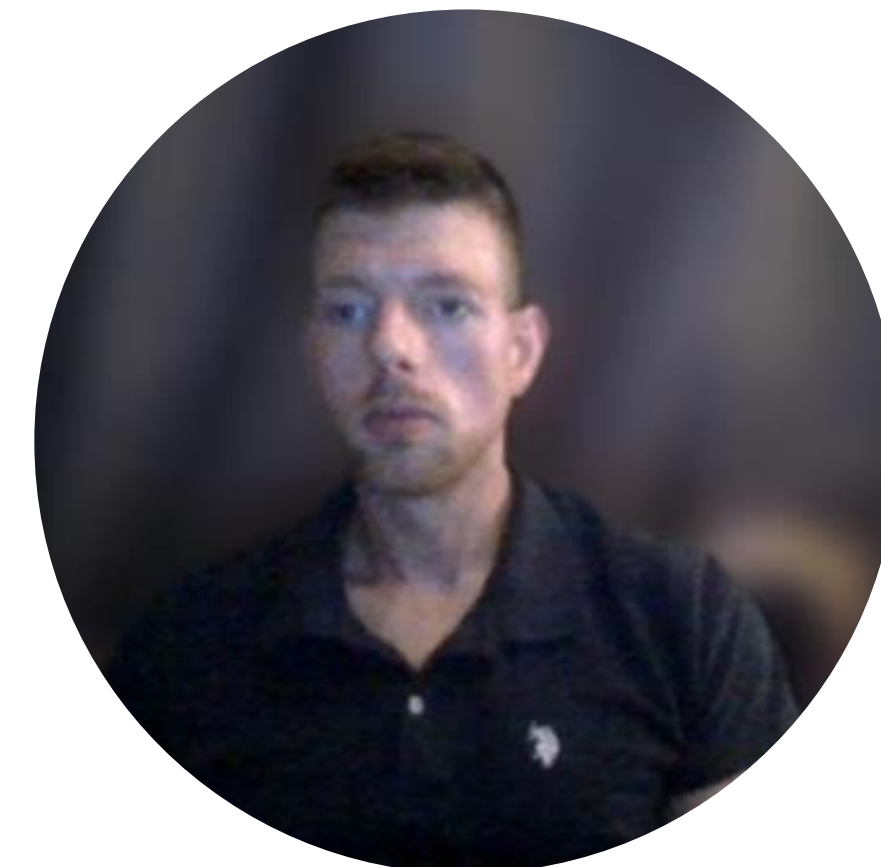


# Potential Impacts Cont'd & Conclusion

---



- 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](http://www.UoPeople.edu) | [info@UoPeople.edu](mailto: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\\_GOyWDszXTGELoKBISFgNWqmxyjhoOpHrrm32dXVG4UOj08oKSnvkNv50](https://www.sciencedirect.com/science/article/pii/S2214212620308620?casa_token=6arg-y6I9O4AAAAA:npUluJIdyXM9gMGUz-I_GOyWDszXTGELoKBISFgNWqmxyjhoOpHrrm32dXVG4UOj08oKSnvkNv50)