INSE – 6140 – Malware Defenses and Application Security

WINTER – 2024

Instructor: Dr. Makan Pourzandi

Project Proposal

Project Title: Ghidra Extension for Identification, Analysis, and Mitigation of OS Command Injection Vulnerabilities

Project Description: Our project aims to develop a specialized Ghidra extension with a primary focus on identifying and mitigating OS command injection vulnerabilities within binary code. This extension will target insecure functions commonly associated with such vulnerabilities.

Team Members and Responsibilities:

	Student ID	Name	Responsibilities
1	40235325	Rakshith Raj Gurupura Puttaraju	• Set up the development environment. • Share acquired knowledge with the team. • Collaborate with team for extension development and mitigation
2	40059335	Mustafa Talha Ucar	• Lead in developing the custom Ghidra extension Share acquired knowledge with the team. • Identify and analyze insecure functions. • Contribute to the overall extension design
3	40234542	Rahul Ravi Hulli	• Create vulnerable binaries for testing. • Validate extension results with practical testing. • Work on mitigation strategies for identified vulnerabilities

Timeline:

Phase	Duration	Key Activities
Tool Exploration	Feb 6 - Feb 12	Explore Ghidra, set up the development environment
Extension Development	Feb 13 - Feb 26	Develop and refine the Ghidra extension
Binary Creation	Feb 27 - Mar 12	Generate vulnerable binaries for testing
Validation	Mar 13 - Mar 26	Collaboratively validate extension results
Mitigation Strategies	Mar 27 - Apr 2	Work on mitigation strategies for identified vulnerabilities
Documentation	Apr 3 - Apr 9	Prepare comprehensive documentation
Final Presentation	Apr 10	Showcase the extension's capabilities and findings