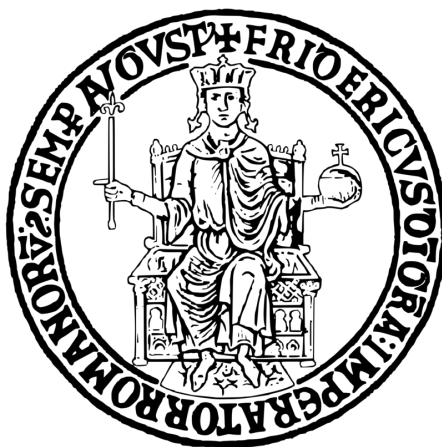


UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II



Scuola Politecnica e delle Scienze di Base
DIPARTIMENTO DI INGEGNERIA ELETTRICA E
TECNOLOGIE DELL'INFORMAZIONE
Corso di Laurea in Ingegneria Informatica
ELABORATO FINALE IN PROGRAMMAZIONE

Test di Sicurezza su Dispositivi Mobili: Generazione di Sequenze di Azioni con LLM e Analisi dei Flussi di Esecuzione

Candidato
Pietro Conte
Matr. N46006426

Anno Accademico 2023-2024

Alla persona che sono diventato

Indice

Introduzione	1
1 Attack Pattern e Execution Flow	3
1.1 Introduzione alle weakness e alle vulnerability	3
1.1.1 Organizzazione MITRE	5
1.1.2 NEO4J DESKTOP	7
1.2 Schema generale del Database	8
1.2.1 Relazione tra Vulnerability, Weakness, Attack Pattern e Attack Flow	9
1.3 Introduzione degli Execution Flow	11
2 Large Language Models	13
2.1 Strumenti di LLM a supporto del Testing	13
2.2 Il ruolo del Prompt Engineering	16
3 Analisi degli Execution Flow	21
3.1 Processo di Testing	21
3.2 Simulazione e Verifica dell'Execution Flow	29
3.2.1 Strumenti utilizzati	34

4 Conclusioni	36
4.1 Considerazioni finali	36
Bibliografia	38