



UNIVERSITÀ DEGLI STUDI DI MILANO - BICOCCA  
Dipartimento di Informatica, Sistemistica e Comuni-  
cazione  
Corso di Laurea in Informatica

# Piattaforma web per la ricerca automatica di vulnerabilità in file binari

**Relatore:** Prof. Claudio Ferretti

**Correlatore:** Dott.sa Martina Saletta

**Tesi di Laurea di:**  
Andrea Consonni  
Matricola 900116

**Anno Accademico 2024-2025**

*Vorrei esprimere i miei più sentiti ringraziamenti al **prof. Claudio Ferretti**, alla **Dott.sa Martina Saletta** e al **prof. Giovanni Denaro** per il costante supporto, la disponibilità e i preziosi consigli offerti durante tutto il percorso di tesi.*

*Un ringraziamento speciale va alla **mia famiglia**, che con il suo supporto incondizionato mi ha permesso di affrontare con serenità questo percorso di studi.*

*Sono profondamente grato anche **a tutti i miei amici**, il quale costante sostegno mi ha accompagnato e incoraggiato lungo tutto il percorso universitario*

**Abstract**  
TODO

# Indice

<b>1</b>	<b>Introduzione</b>	<b>2</b>
1.1	Struttura della relazione . . . . .	2

# Capitolo 1

## Introduzione

In un mondo sempre più digitalizzato ed interconnesso, la tematica della sicurezza informatica ha assunto sempre più un'importanza chiave in ogni processo di sviluppo software. La potenziale presenza e lo sfruttamento di una vulnerabilità all'interno di un'applicazione da parte di un'attaccante potrebbe avere conseguenze disastrose: dall'escalation di privilegi all'accesso non autorizzato a dati sensibili, compromettendo quindi l'integrità e la confidenzialità di quest'ultimi. È quindi fondamentale che i potenziali rischi per la sicurezza siano considerati sin dai primi momenti del processo di sviluppo. Effettuare un'analisi di sicurezza approfondita risulta quindi fondamentale nell'evitare che potenziali vulnerabilità persistano all'interno del programma; tuttavia, questo processo si complica notevolmente quando l'analista è in **solo possesso del file binario** e non ha accesso al codice sorgente dell'applicazione. In questo caso, l'analista non solo dovrà avere ampie competenze specifiche in ambito di reverse engineering, ma dovrà essere in grado di utilizzare tool e framework che potrebbero avere un'interfaccia a primo impatto ostica, richiedere conoscenze di scripting o di tematiche di sicurezza avanzate oppure avere un costo elevato, il quale potrebbe non rientrare nei limiti di budget prefissati. Questa tesi propone l'implementazione di una piattaforma web per l'analisi di file binari denominata **Binoculars**; la quale si prefigge l'obiettivo di semplificare il processo di analisi di sicurezza su file binari ELF compilati per architettura x86 tramite un'interfaccia semplice ed intuitiva, permettendo anche ad analisti con competenze di sicurezza non specialistiche di effettuare una prima valutazione del programma, la quale potrà poi essere approfondita tramite analisi più specifiche. La piattaforma si basa su **angr**, un toolkit open-source multi-architettura per l'analisi binaria, per eseguire automaticamente diverse tipologie di analisi statiche e dinamiche, sul framework python **Flask** per l'implementazione di una REST API progettata per comunicare i risultati dell'analisi e sul framework javascript SvelteKit, il quale si occupa della strutturazione delle pagine web della piattaforma e della presentazione dei risultati dell'analisi all'utente.

### 1.1 Struttura della relazione

La relazione è articolata nei seguenti capitoli:

- **Capitolo 2: Stato dell'arte:** Questo capitolo presenta una rassegna di alcune tecniche, metodologie e soluzioni esistenti per l'analisi di file binari. Verrà evidenziato l'approccio adottato per affrontare il problema della ricerca di vulnerabilità e i rispettivi limiti di ogni soluzione presentata.

- **Capitolo 3: Metodologie utilizzate:** Questo capitolo discute i fondamenti teorici che costituiscono la base delle analisi implementate dalla piattaforma. Saranno discussi in dettaglio sia i concetti di **disassembling** e **decompiling** sia le metodologie di analisi statica e dinamica utilizzate per effettuare la ricerca delle vulnerabilità. Verranno inoltre forniti degli esempi per illustrarne il funzionamento.
- **Capitolo 4: Analisi implementate:** Questo capitolo illustra nel dettaglio le analisi implementate all'interno della piattaforma. Verrà descritto come ciascuna tecnica di analisi porti al rilevamento di una vulnerabilità e quali classi di vulnerabilità ogni tecnica è in grado di rilevare.
- **Capitolo 5: Tecnologie utilizzate:** Questo capitolo presenta in dettaglio le tecnologie e i framework scelti per l'implementazione della piattaforma. Saranno presentati sia i componenti del backend sia le tecnologie adottate per lo sviluppo del frontend.
- **Capitolo 6: Architettura della soluzione:** Questo capitolo descrive l'architettura generale della piattaforma Binoculars. Verrà illustrato il modello architetturale della soluzione, illustrando le interazioni fra i vari componenti e come essi collaborano per presentare all'utente il risultato dell'analisi richiesta.
- **Capitolo 7: Sperimentazione** Questo capitolo presenta le varie sperimentazioni effettuate sulla piattaforma al fine di validarne l'accuratezza. Per ogni tecnica di analisi implementata, verranno presentati i programmi che sono stati utilizzati al fine di validare l'efficacia e l'accuratezza dell'analisi e i risultati prodotti da quest'ultima.
- **Capitolo 8: Conclusioni:** Questo capitolo presenterà le conclusioni finali del lavoro. Saranno inoltre esposte le limitazioni e le problematiche incontrate durante l'implementazione della piattaforma e i suoi possibili sviluppi futuri.