NOME: **Raffaele** COGNOME: **Ruggeri** MATRICOLA: **1934646** TITOLO: **MalwareTotal** DATA: **24/06/2022**

Software utilizzati

Il DB è stato realizzato con il DBMS MySQL workbench.

L'applicazione è stata realizzata con Python (Django framework) + javascript + html + css (bootstrap framework)

1. Progettazione concettuale

1.1. Requisiti strutturati e organizzati

Si vuole realizzare la base di dati di un forum che è in grado di analizzare dei file, con il fine di rilevare minacce per la sicurezza.
Un utente può registrarsi alla piattaforma fornendo e-mail, username, nome, cognome e password.
Ogni sezione ha un proprio nome, un contenuto e può essere aperta solo da un utente amministratore.
Inoltre un utente amministratore deve essere anche un utente staff e avere più di 1000 punti
Il forum permette a tutti gli utenti con almeno 1000 punti di aprire dei topic in una determinata sezione.
Ogni topic ha un proprio titolo, un contenuto, uno stato (attivo/disattivato), la data di creazione e può essere commentato da un utente iscritto alla piattaforma.
Il topic deve avere sempre come argomento una minaccia nota nella base di dati.
Un utente dispone inoltre di un proprio stato (attivo/disattivato) e ha un proprio punteggio che consente di classificare gli utenti e la loro attività sulla piattaforma.
Tutti gli utenti possono caricare dei file, tuttavia solo l'amministratore può caricare più di 10 File.
Sui file già caricati, l'utente potrà eseguire molteplici scansioni sfruttando i diversi tipi di engine di analisi della piattaforma.
L'applicazione vuole dare all'utente la possibilità di avere un visione dettagliata di ogni scansione effettuata da quando si è registrato alla piattaforma.
Di ogni file sottoposto vengono salvate le informazioni principali quali: il file stesso, l'hash, il nome, il peso e l'autore (se presente).
Durante l'analisi di un file devono essere memorizzate alcune informazioni, ad esempio se un file contiene una o più minacce, l'engine di analisi utilizzato, il tipo di analisi effettuata, i report e la data di scansione.
Ogni informazione memorizzata durante i processi di analisi, viene in seguito resa reperibile dal database se l'utente vuole accedervi.
Nella base di dati si vuole avere una parte che viene aggiornata solo a seguito di procedure automatiche e programmate, ed è quindi statica dal punto di vista dell'utente, questa parte è composta da:

- L'elenco delle CVE
  - per ogni CVE salviamo i campi: nome, tipo, data e tutti i riferimenti (insieme di link)
- Le definizioni delle minacce
  - per ogni minaccia salviamo i seguenti campi: nome, categoria e tipo.
  - Salviamo anche quali CVE sono sfruttate da ogni minaccia.
- I dati relativi ad ogni engine di analisi statica e dinamica

- ovvero i nomi, le versioni e i linguaggi di programmazione con cui sono scritti e il produttore (software house) dell'engine stesso.

- I dati dei produttori
  - di cui si vogliono mantenere le informazioni principali, ovvero nome e nazione di origine.

Glossario dei termini

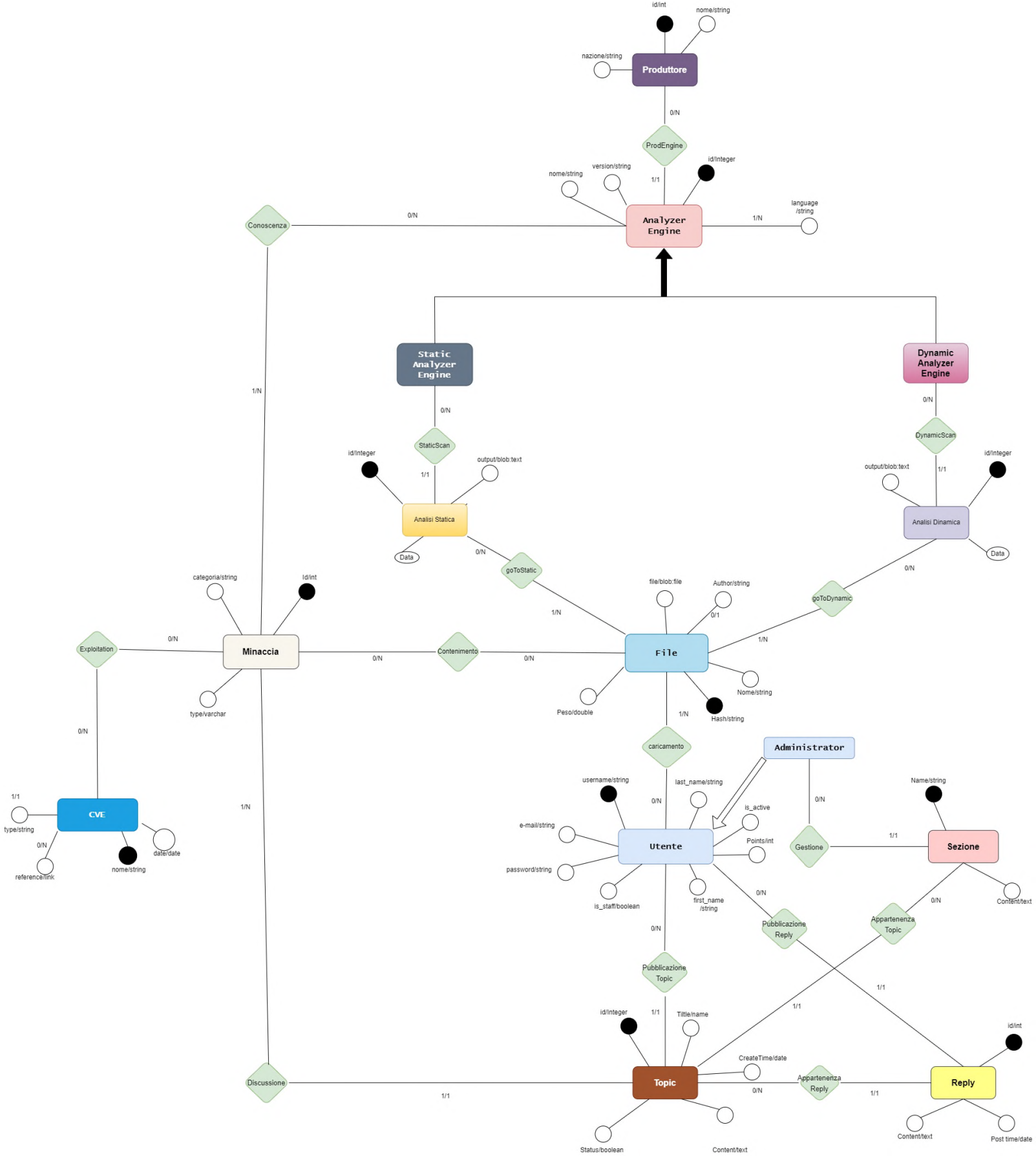
TERMINE	DEFINIZIONE
Minaccia	Qualunque cosa possa effettuare azioni malevole o danneggiare sistemi e le funzioni di sicurezza
Hash	Stringa cifrata tramite una funzione matematica uni-direzionale (non invertibile).
Malware	Software malevolo in grado di effettuare azioni malevole o non volute dall'utente
Reply	Commento ad un topic
CVE	Vulnerabilità nota ("Common Vulnerabilities and Exposures").
Language	Linguaggio di programmazione
Analyzer	Software in grado di verificare se un file in input è una minaccia di sicurezza ("engine di analisi").
Analisi statica	L'insieme delle operazioni che hanno lo scopo di trovare informazioni sul file, senza però eseguirlo.
Analisi dinamica	L'insieme delle operazioni che hanno lo scopo di trovare informazioni su file in esecuzione (processo/i).
Debugging	Studio approfondito dell'esecuzione di un programma, spesso al fine di trovare bug e/o capirne il funzionamento
Link	Percorso di una risorsa nella rete.
Reference	Riferimento ad una risorsa tramite link ad una risorsa o esterna o interna al server.
Report	Resoconto di una o più operazioni. Necessario per compattare le informazioni e renderle disponibili all'utente.

NOME: **Raffaele** COGNOME: **Ruggeri** MATRICOLA: **1934646** TITOLO: **MalwareTotal** DATA: **24/06/2022**

TABELLA DEI REQUISITI MINIMI

A.	Lo schema ER iniziale raccoglie 11 entità + 2 derivanti da una generalizzazione + 1 derivante da una relazione ISA. Lo schema ER finale raccoglie 13 entità.
B.	Administrator **IS A** Utente ← relazione ISA. Analisi statica e analisi dinamica sono le analisi ← generalizzazione.
C.	Lo schema ha vari cicli ad es tra Utente, sezione, Topic, Reply.
D.	Su tutti gli archi dello schema ER sono espressi i vincoli di cardinalità.
E.	Attributo facoltativo è l 'author' dell'entità File. Attributi multivalore sono references dell'entità CVE e language dell'entità Analyzer.
F.	Abbiamo 5 vincoli esterni, di cui 2 sulla stessa entità.
G.	Le specifiche includono indicazioni sui volumi per entità e relazioni. Vedi pag. 16.
H.	Le specifiche includono il carico di lavoro delle query con indicazioni di frequenza. Vedi pag. 19/20.

1.1. Diagramma dello schema concettuale


id/int
nome/string
nazione/string
Produttore
0/N
ProdEngine
id/Integer
version/string
nome/string
1/1
Analyzer Engine
language /string
1/N
Conoscenza
0/N
1/N
Static Analyzer Engine
Dynamic Analyzer Engine
0/N
StaticScan
DynamicScan
id/Integer
output/blob:text
1/1
Analisi Statica
Analisi Dinamica
Data
goToStatic
goToDynamic
categoria/string
Id/int
Exploitation
Minaccia
Contenimento
File
type/varchar
file/blob:file
Author/string
0/1
Nome/string
Peso/double
Hash/string
caricamento
Administrator
CVE
type/string
reference/link
nome/string
date/date
username/string
last_name/string
e-mail/string
password/string
is_staff/boolean
first_name /string
is_active
Points/int
Utente
Gestione
Sezione
Name/string
Content/text
Pubblicazione Reply
Appartenenza Topic
Pubblicazione Topic
Discussione
Topic
id/Integer
Tittle/name
CreateTime/date
Status/boolean
Content/text
Appartenenza Reply
Reply
id/int
Content/text
Post time/date

1.2. Dizionario dei dati dello schema concettuale

Entità	Descrizione	Vincoli Esterni	Identificatore
Administrator	Utente con massimi privilegi nel forum	Un amministratore deve essere un utente staff e avere più di 1000 punti	username
Analisi Dinamica	Debugging e controlli a tempo di esecuzione del file		id
Analisi Statica	Azione di controllo e scansione del contenuto del file		id
Analyzer Engine	Analizzatore di file		id
CVE	Common Vulnerabilities and Exposures		number
Dynamic Analyzer Engine	Analizzatore file in esecuzione		id
File	Dati sottoposti a scansione		hash
Minaccia	Software che influisce negativamente sul normale comportamento del dispositivo in cui si trova		id
Produttore	Chi ha realizzato il language o l'analyzer engine		id
Reply	Commento in risposta ad un ad altro commento o al topic stesso		id
Sezione	Categoria che contiene vari topic	Una sezione può essere aperta solo da un Utente administrator.	name
Static Analyzer Engine	Analizzatore di file non in esecuzione		id
Topic	Argomento di discussione	Un topic può essere aperto solo da un user con più di 1000 punti	id
Utente	Cliente che utilizza la piattaforma web		username

Relazione	Descrizione	Entità Associate	Vincoli Esterni
Appartenenza Reply	Associa il topic con il reply che ne fa parte	Topic, Reply	
Appartenenza Topic	Associa la sezione ai topic che ne fanno parte	Sezione, Topic	
Caricamento	Associa il file all'utente che lo ha caricato	File, Utente	Un utente non admin non deve poter caricare più di 10 file
Conoscenza	Associa un Analyzer alle minacce che questo conosce	Analyzer Engine, Minaccia	
Discussione	Associa ogni topic alla minaccia che discute	Minaccia, Topic	
StaticScan	Associa l'analisi statica allo static analyzer che effettua l'analisi		
DynamicScan	Associa l'analisi dinamica allo dynamic analyzer che effettua l'analisi	Analisi Dinamica, Dynamic Analyzer	
Exploitation	Associa ogni minaccia alle relative CVE che sfrutta	Minaccia, CVE	
Gestione	Associa l'amministratore alla sezione che gestisce	Administrator, Sezione	
goToDynamic	Associa il file analizzato all'analisi dinamica	Analisi Dinamica, File	
goToStatic	Associa il file analizzato all'analisi statica	Analisi Statica, File	
ProdEngine	Associa ogni Produttore all'Analyzer Engine che ha prodotto	Produttore, Analyzer Engine	
Pubblicazione Reply	Associa l'utente ai Reply che ha pubblicato	Utente, Reply	
Pubblicazione Topic	Associa l'utente ai topic che ha pubblicato	Utente, Topic	

1.3. Tabella dei volumi

Concetto	Tipo (E/R)	Volume
Produttore	E	200
Analyzer Engine	E	50
Static Analyzer Engine	E	25
Dynamic Analyzer Engine	E	25
Analisi Dinamica	E	4 000
Analisi Statica	E	4 000
File	E	8 000
Minaccia	E	99 999
CVE	E	200 000
Utente	E	1000
Administrator	E	5
Topic	E	200
Sezione	E	15
Reply	E	700
ProdEngine	R	50
Prodlanguage	R	200
Conoscenza	R	125 000

goToStatic	R	4 000
goToDynamic	R	4 000
staticScan	R	4 000
dynamicScan	R	4 000
Caricamento	R	8 000
Exploitation	R	5 550 000
Discussione	R	200
Pubblicazione Topic	R	200
Pubblicazione Reply	R	700
Gestione	R	15
AppartenenzaTopic	R	200
AppartenenzaReply	R	700

1.4. Tabella delle operazioni in base al carico dell'applicazione previsto

Identificativo	read/write	Descrizione	Frequenza accessi	Tipo (I/B)
OP1	write	Caricamento di un File	500/giorno	I
OP2	write	Iscrizione di un Utente	20/giorno	I
OP3	write	Analisi di un File	500/giorno	I

OP4	write	Rimozione di un Utente	20/giorno	I
OP5	write	Aggiunta di un Analyzer	10/anno	I
OP6	write	Aggiornamento delle Minacce note all'Analyzer	5/giorno	B
OP7	write	Aggiornamento dell'elenco delle CVE	5/giorno	B
OP8	write	Creazione di un nuovo Topic	10/giorno	I
OP9	write	Aggiunta di un Reply	100/giorno	I
OP10	read	Cambio password	50/giorno	I
OP11	read	Lettura dei Reply	10000/giorno	I
OP12	read	Accesso all'account utente	600/giorno	I
OP14	read	Lettura dati di analisi	1500/giorno	I
OP13	write	Modifica di un reply	10000/giorno	I
OP15	read	Visione delle minacce conosciute da un Analyzer	50/giorno	I
OP16	read	Lettura informazioni riguardanti una minaccia	10000/giorno	I
OP17	read	Visione di un Topic	400/giorno	I
OP18	read	Lettura informazioni file	10000/giorno	I
OP19	write	Modifica di un topic	100/giorno	I

1.6 Tavole dei valori

OP1 Caricamento di un File

Concetto	Costrutto	Accessi	Tipo
File	Entità	1	S
Caricamento	Relazione	1	S

OP2 Iscrizione di un Utente

Concetto	Costrutto	Accessi	Tipo
Utente	Entità	1	S

OP3 Analisi di un File

Concetto	Costrutto	Accessi	Tipo
goToStatic/goToDynamic	Relazione	1	S
Analisi	Entità	1	S
Contenimento	Relazione	1	S
staticScan/dynamicScan	Relazione	1	S

OP4 Rimozione di un Utente

Concetto	Costrutto	Accessi	Tipo
Utente	Entità	1	S
Dati Utente Aggiuntivi	Entità	1	S
Caricamento	Relazione	1	S
Sezione	Entità	0/N	S
Reply	Entità	0/N	S
Administrator	Entità	0/1	S

OP5 Aggiunta di un Analyzer

Concetto	Costrutto	Accessi	Tipo
Analyzer	Entità	1	S
Conoscenza	Relazione	1	S
Static Analyzer Engine/Dynamic Anlyzer Engine	Entità	1	S

OP6 Aggiornamento delle Minacce note all'Analyzer

Concetto	Costrutto	Accessi	Tipo
Analyzer Engine	Entità	1	L
Minaccia	Entità	1	L
Conoscenza	Entità	1	S

OP7

Concetto	Costrutto	Accessi	Tipo
CVE	Entità	k	S

K = numero di cve da aggiornare

OP8 Creazione di un nuovo Topic

Concetto	Costrutto	Accessi	Tipo
Topic	Entità	1	S

OP9 Aggiunta di un Reply

Concetto	Costrutto	Accessi	Tipo
Reply	Entità	1	S

OP10 Cambio password utente

Concetto	Costrutto	Accessi	Tipo
Utente	Entità	1	S
Administrator	Entità	0/1	S

OP11 Lettura dei Reply

Concetto	Costrutto	Accessi	Tipo
Reply	Entità	1	L

OP12 Accesso all'account utente

Concetto	Costrutto	Accessi	Tipo
Utente	Entità	1	L
Administrator	Entità	0/1	L

OP13 Modifica di un Reply

Concetto	Costrutto	Accessi	Tipo
Reply	Entità	1	S

OP14 Lettura dati di analisi

Concetto	Costrutto	Accessi	Tipo
Analisi	Entità	1	L
AnalisiToEngine	Relazione	1	L
FileToAnalisi	Relazione	1	L

OP15 Visione delle minacce conosciute da un Analyzer

Concetto	Costrutto	Accessi	Tipo
Analyzer Engine	Entità	1	L
Static Analyzer Engine/Dynamic Analyzer Engine	Entità	1	L
Conoscenza	Relazione	K	L
Minaccia	Entità	K	L

K = numero di minacce conosciute dall'analyzer engine

OP16 Lettura informazioni riguardanti una minaccia

Concetto	Costrutto	Accessi	Tipo
Minaccia	Entità	1	L
Exploitation	Relazione	k	L
Cve	Entità	k	L

K = numero di cve exploitate dalla minaccia

OP17 Visione di un Topic

Concetto	Costrutto	Accessi	Tipo
Topic	Entità	1	L
Reply	Entità	k	L

K = numero di reply presenti in un topic

OP18 Lettura informazioni file

Concetto	Costrutto	Accessi	Tipo
File	Entità	1	L
Minaccia	Entità	1	L
Contenimento	Relazione	1	L
Analisi Statica/dinamica	Entità	1	L
goToStatic/goToDynamic	Relazione	1	L
Caricamento	Relazione	1	L
Utente	Entità	1	L

OP19 Modifica di un topic

Concetto	Costrutto	Accessi	Tipo
Topic	Entità	1	L
Reply	Entità	k	L

K = numero di reply presenti in un topic

2. Ristrutturazione dello schema concettuale

Eliminazione della relazione is-a

(METODO 1)
Inglobo l'entità figlia 'administrator' nell'entità padre 'utente' aggiungendo un attributo 'is_superuser' booleano, che serve a distinguere l'amministratore da un utente normale e inserendo un vincolo di integrità esterno:
Un Utente con isAdmin == False non deve poter gestire una sezione.

Eliminazione delle generalizzazioni

(METODO 1)

Inglobo le entità figlie 'Dynamic Analyzer Engine' e 'Static Analyzer Engine' nell'entità padre 'Analyzer Angine', aggiungendo un attributo 'type', che permette di mantenere la distinzione tra analizzatore dinamico e statico.

Di conseguenza anche le entità "analisi dinamica" e "analisi statica", devono essere unite nell'entità "analisi", in questo caso per distinguere il tipo di analisi sarà sufficiente leggere l'attributo "type" del "Dynamic Analyzer Engine" associato.

Partizionamento verticale

Viene effettuato un partizionamento verticale sull'entità utente per scelta di progetto, si dividono gli altri dati dell'utente dai "points" per rendere le query che richiedono quel dato di più rapida esecuzione. Infatti nella base di dati si considera la necessità di confrontare spesso i punteggi degli utenti tra di loro, e anche la necessità di effettuare join e query innestate direttamente con la nuova entità "dati utente aggiuntivi", per risalire rapidamente al punteggio di un utente.

Eliminazione degli attributi multivalore

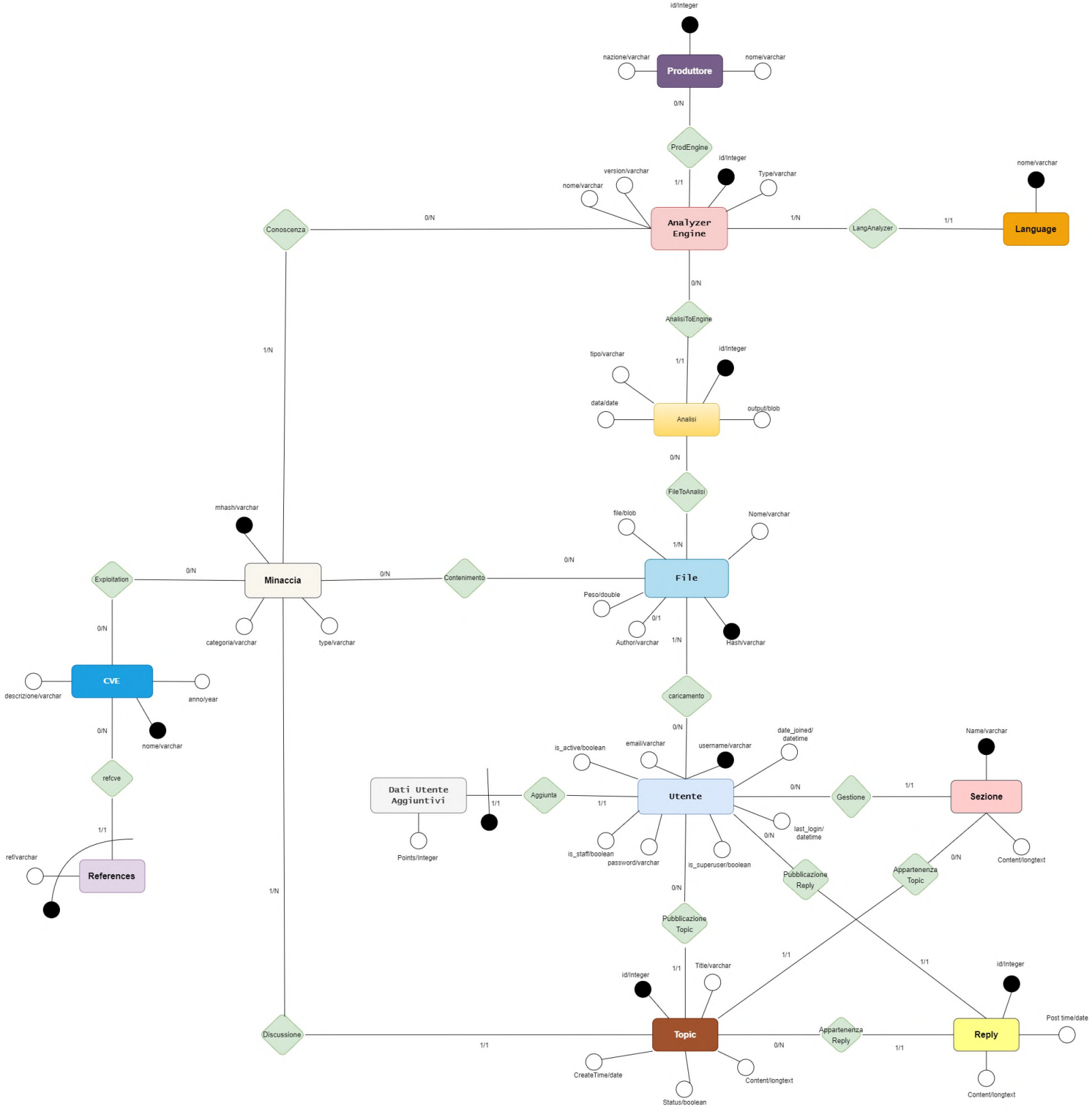
L'attributo "references" dell'entità "CVE" può avere da 0 a N valori, dato che non è rappresentabile in uno schema relazionale, dobbiamo eliminare l'attributo e aggiungere una nuova entità "References" e una relazione "refCVE".

L'attributo "language" dell'entità "Analyzer" può avere da 0 a N valori, anche in questo caso è necessario eliminare l'attributo e aggiungere una nuova entità "Lang" e una relazione "LangAnalyzer".

Mapping dei domini

Ad ogni attributo è stato associato il corretto dominio sulla base dei tipi supportati dal DBMS in uso (MySql workbench).

2.1. Diagramma ER ristrutturato


id/Integer
nazione/varchar
Produttore
nome/varchar
0/N
ProdEngine
id/Integer
version/varchar
nome/varchar
1/1
Type/varchar
nome/varchar
Conoscenza
0/N
Analyzer Engine
1/N
LangAnalyzer
1/1
Language
0/N
AnalisiToEngine
1/N
tipo/varchar
1/1
id/Integer
data/date
Analisi
output/blob
0/N
FileToAnalisi
mhash/varchar
file/blob
Nome/varchar
1/N
Exploitation
0/N
Minaccia
0/N
Contenimento
0/N
File
Peso/double
0/1
categoria/varchar
type/varchar
Author/varchar
1/N
Hash/varchar
0/N
CVE
descrizione/varchar
anno/year
0/N
nome/varchar
caricamento
0/N
refcve
1/1
ref/varchar
References
is_active/boolean
email/varchar
username/varchar
date_joined/ datetime
Name/varchar
Dati Utente Aggiuntivi
1/1
Aggiunta
1/1
Utente
0/N
Gestione
1/1
Sezione
Points/Integer
last_login/ datetime
0/N
is_staff/boolean
password/varchar
is_superuser/boolean
Pubblicazione Reply
Appartenenza Topic
0/N
Content/longtext
0/N
Pubblicazione Topic
1/1
Title/varchar
1/1
1/1
id/Integer
1/N
Discussione
1/1
Topic
0/N
Appartenenza Reply
1/1
Reply
Post time/date
CreateTime/date
Content/longtext
Status/boolean
Content/longtext

2.2. Dizionario dei dati ristrutturato

Entità	Descrizione	Identificatore	Vincoli Esterni
Analisi	Azione di controllo del file	id	
Analyzer Engine	Analizzatore di file	id	
CVE	Common Vulnerabilities and Exposures	number	
File	Dati sottoposti a scansione	hash	
Minaccia	Software che influisce negativamente sul normale comportamento del dispositivo in cui si trova	id	
Produttore	Chi ha realizzato l'analyzer engine	id	
Reply	Commento in risposta ad un ad altro commento o al topic stesso	id	
Sezione	Categoria che contiene vari topic	name	Una sezione può essere aperta solo da un utente con più di 1000 punti
Language	Linguaggi di programmazione utilizzati in un analyzer engine	id	
Topic	Argomento di discussione	id	Un topic può essere aperto solo da un Utente con più di 1000 points o staff
Utente	Cliente che utilizza la piattaforma web	username	Un amministratore deve essere un utente staff con più di 1000 punti.
Dati Utente Aggiuntivi	Dati utente aggiuntivi	Utente	
References	links associati alla cve	cve,ref	

Relazione	Descrizione	Entità Associate	Vincoli Esterni
Appartenenza Reply	Associa il topic con il reply che ne fa parte	Topic, Reply	
Appartenenza Topic	Associa la sezione ai topic che ne fanno parte	Sezione, Topic	
Caricamento	Associa il file all'utente che lo ha caricato	File, Utente	Un utente non admin non deve poter caricare più di 10 file
Composizione	Associa Analyzer con i linguaggi di programmazione utilizzati	Analyzer Engine, languages	
Conoscenza	Associa un Analyzer alle minacce che questo conosce	Analyzer Engine, Minaccia	
Discussione	Associa ogni topic alla minaccia che discute	Minaccia, Topic	
Exploitation	Associa ogni minaccia alle relative CVE che sfrutta	Minaccia, CVE	
Gestione	Associa l'amministratore alla sezione che gestisce	Administrator, Sezione	
ProdEngine	Associa ogni Produttore all'analyzer Engine che ha prodotto	Produttore, Analyzer Engine	
Pubblicazione Reply	Associa l'utente ai Reply che ha pubblicato	Utente, Reply	
Pubblicazione Topic	Associa l'utente ai topic che ha pubblicato	Utente, Topic	
AnalisiToEngine	Associa l'analisi statica all'analyzer che effettua l'analisi	Analisi, Analyzer Engine	
FileToAnalisi	Associa il file caricato all'analisi effettuata	File, Analisi	
Refcve	Associa alle cve i links di referenza	CVE, References	

Aggiunta	Mantiene i dati aggiunti dell'utente in relazione con l'utente stesso	Utente, Dati Utente Aggiuntivi	

Vincolo esterno	Descrizione
v1	Un utente non admin non deve poter caricare più di 10 File
v2	Un utente admin deve essere anche utente staff
v3	Un utente admin deve avere più di 1000 punti
v4	Un topic può essere aperto solo da un Utente con più di 1000 points
v5	Una sezione può essere aperta solo da un Utente admin.

3. Tabella dei volumi

Concetto	Tipo (E/R)	Volume
Produttore	E	200
Language	E	30
Analyzer	E	50
Analisi	E	8 000

File	E	8 000
Minaccia	E	99 999
CVE	E	200 000
Utente	E	500
Dati Aggiuntivi Utente	E	500
references	E	1000
Topic	E	200
Sezione	E	15
Reply	E	700
ProdEngine	R	50
LangAnalyzer	R	100
Conoscenza	R	125 000
fileToAnalisi	R	8 000
AnalisiToEngine	R	8 000

Caricamento	R	8 000
Exploitation	R	5 550 000
Discussione	R	200
Pubblicazione Topic	R	200
Pubblicazione Reply	R	700
Gestione	R	15
AppartenenzaTopic	R	200
AppartenenzaReply	R	700
Refcve	R	100 000
Aggiunta	R	500

4. Tabella delle operazioni in base al carico dell'applicazione previsto

Identificativo	read/write	Descrizione	Frequenza accessi	Tipo (I/B)
OP1	write	Caricamento di un File	500/giorno	I
OP2	write	Iscrizione di un Utente	20/giorno	I
OP3	write	Analisi di un File	500/giorno	I
OP4	write	Rimozione di un Utente	20/giorno	I
OP5	write	Aggiunta di un Analyzer	10/anno	I
OP6	write	Aggiornamento delle	5/giorno	B

		Minacce note all'Analyzer		
OP7	write	Aggiornamento dell'elenco delle CVE	5/giorno	B
OP8	write	Creazione di un nuovo Topic	10/giorno	I
OP9	write	Aggiunta di un Reply	100/giorno	I
OP10	read	Cambio password utente	50/giorno	I
OP11	read	Lettura dei Reply	10000/giorno	I
OP12	read	Accesso all'account utente	600/giorno	I
OP13	write	Modifica di un reply	10000/giorno	I
OP14	read	Lettura dati di analisi	1500/giorno	I
OP15	read	Visione delle minacce conosciute da un Analyzer	50/giorno	I
OP16	read	Lettura informazioni riguardanti una minaccia	10000/giorno	I
OP17	read	Visione di un Topic	400/giorno	I
OP18	read	Lettura informazioni file	10000/giorno	I
OP19	write	Modifica di un topic	100/giorno	I

2.3 Tavole dei valori

OP1 Caricamento di un File

Concetto	Costrutto	Accessi	Tipo
File	Entità	1	S
Caricamento	Relazione	1	S

OP2 Iscrizione di un Utente

Concetto	Costrutto	Accessi	Tipo
Utente	Entità	1	S
Dati utente aggiuntivi	Entità	1	S

OP3 Analisi di un File

Concetto	Costrutto	Accessi	Tipo
FileToAnalisi	Relazione	1	S
Analisi	Entità	1	S
Contenimento	Relazione	1	S
AnalisiToEngine	Relazione	1	S

OP4 Rimozione di un Utente

Concetto	Costrutto	Accessi	Tipo
Utente	Entità	1	S
Dati Utente Aggiuntivi	Entità	1	S
Caricamento	Relazione	1	S
Sezione	Entità	0/N	S
Reply	Entità	0/N	S

OP5 Aggiunta di un Analyzer

Concetto	Costrutto	Accessi	Tipo
Analyzer	Entità	1	S
Conoscenza	Relazione	1	S

OP6 Aggiornamento delle Minacce note all'Analyzer

Concetto	Costrutto	Accessi	Tipo
Analyzer	Entità	1	L
Minaccia	Entità	1	L
Conoscenza	Entità	1	S

OP7 Aggiornamento dell'elenco delle CVE

Concetto	Costrutto	Accessi	Tipo
CVE	Entità	k	S
References	Entità	k	S
RefCve	Relazione	k	S

K = numero di riferimenti per una cve

OP8 Creazione di un nuovo Topic

Concetto	Costrutto	Accessi	Tipo
Topic	Entità	1	S

OP9 Aggiunta di un Reply

Concetto	Costrutto	Accessi	Tipo
Reply	Entità	1	S

OP10 Cambio password utente

Concetto	Costrutto	Accessi	Tipo
Utente	Entità	1	S

OP11 Lettura dei Reply

Concetto	Costrutto	Accessi	Tipo
Reply	Entità	1	L

OP12 Accesso all'account utente

Concetto	Costrutto	Accessi	Tipo
Utente	Entità	1	L

OP13 Modifica di un Reply

Concetto	Costrutto	Accessi	Tipo
Reply	Entità	1	S

OP14 Lettura dati di analisi

Concetto	Costrutto	Accessi	Tipo
Analisi	Entità	1	L
AnalisiToEngine	Relazione	1	L
FileToAnalisi	Relazione	1	L

OP15 Visione delle minacce conosciute da un Analyzer

Concetto	Costrutto	Accessi	Tipo
Analyzer	Entità	1	L
Conoscenza	Relazione	k	L
Minaccia	Entità	k	L

K = numero di minacce conosciute da un analyzer

OP16 Lettura informazioni riguardanti una minaccia

Concetto	Costrutto	Accessi	Tipo
Minaccia	Entità	1	L
Exploitation	Relazione	k	L
CVE	Entità	k	L

K = numero di cve sfruttate da una data minaccia

OP17 Visione di un Topic

Concetto	Costrutto	Accessi	Tipo
Topic	Entità	1	L
Reply	Entità	k	L

K = numero di reply presenti in un topic

OP18 Lettura informazioni file

Concetto	Costrutto	Accessi	Tipo
File	Entità	1	L
Minaccia	Entità	1	L
Contenimento	Relazione	1	L
Analisi	Entità	1	L
FileToAnalisi	Relazione	1	L
Caricamento	Relazione	1	L
Utente	Entità	1	L

OP19 Modifica di un topic

Concetto	Costrutto	Accessi	Tipo
Topic	Entità	1	L
Reply	Entità	k	L

K = numero di reply presenti in un topic

Si decide di cambiare nel modello relazionale alcuni nomi per interfacciarsi con gli standard del framework Django.

2. Traduzione diretta al modello relazionale

```
Produttore(id, nome, nazione)
-----------------------------------------------------------------------------------
Analyzer(id, nome, version, produttore, tipo)
Analyzer[produttore] ⊆ FK  Produttore[id]
-----------------------------------------------------------------------------------
Conoscenza(minaccia, analyzer)
Conoscenza[analyzer] ⊆ FK  Analyzer[id]
FK Conoscenza[minaccia] ⊆  Minaccia[mhash]
-----------------------------------------------------------------------------------
Minaccia(mhash, nome, descrizione, tipo)
-----------------------------------------------------------------------------------
Contenimento(minaccia, files)
Contenimento[minaccia] ⊆ FK Minaccia[mhash]
Contenimento[files] ⊆ FK files[fhash]
-----------------------------------------------------------------------------------
Exploitation(minaccia, cve)
Exploitation[minaccia] ⊆ FK Minaccia[mhash]
Exploitation[cve] ⊆ FK CVE[nome]
-----------------------------------------------------------------------------------
CVE(nome, descrizione, anno)
-----------------------------------------------------------------------------------
refCVE(cve, ref)
refCVE[cve] ⊆ FK CVE[nome]
-----------------------------------------------------------------------------------
Analisi(id, analyzer, datatime, tipo, output)
Analisi[analyzer] ⊆ FK Analyzer[id]
Analisi[files] ⊆ FK files[fhash]
-----------------------------------------------------------------------------------
fileToAnalisi(files, analisi)
fileToAnalisi[files] ⊆ FK files[fhash]
fileToAnalisi[analisi] ⊆ FK Analisi[id]
-----------------------------------------------------------------------------------
```

```
---------------------------------------------------------------------------------------
files(fhash, nome, fdati, peso, autore)
---------------------------------------------------------------------------------------
Caricamento(utente, files)
Caricamento[files] ⊆ FK files[fhash]
Caricamento[utente] ⊆ FK Utente[username]
---------------------------------------------------------------------------------------
Utente(username, isAdmin, email, first_name, last_name, is_superuser, is_staff, is_active, date_joined, last_login, password)
---------------------------------------------------------------------------------------
DatiUtente(utente, points)
DatiUtente[utente] ⊆ FK Utente[username]
---------------------------------------------------------------------------------------
Sezione(nome, content, utente)
Sezione[utente] ⊆ FK Utente[username]
---------------------------------------------------------------------------------------
Topic(id, title, utente, sezione, clickCount, createTime, status, content, minaccia)
Topic[minaccia] ⊆ FK Minaccia[mhash]
Topic[utente] ⊆ FK Utente[username]
Topic[sezione] ⊆ FK Sezione[nome]
---------------------------------------------------------------------------------------
Reply(id, topic, utente, content, postTime)
Reply[utente] ⊆ FK Utente[username]
Reply[topic] ⊆ FK Topic[id]
---------------------------------------------------------------------------------------
Lang(id, nome, version, descrizione)
---------------------------------------------------------------------------------------
LangAnalyzer(analyzer, lang)
LangAnalyzer[analyzer] ⊆ FK Analyzer[id]
LangAnalyzer[lang] ⊆ FK Lang[id]
```

3.3 Carico dell'applicazione a seguito della riformulazione in schema relazionale rimane invariato.

L’applicazione raggiunge il massimo del carico durante l’esecuzione delle operazioni 11, 13, 14, 16, 18 che sono tuttavia operazioni che coinvolgono poche tabelle, e con pochi campi, infatti anche portando l’applicazione a massimo carico previsto, le prestazioni del sito saranno comunque sufficienti a soddisfare le richieste di tutti gli utenti.

L’operazione con più carico in assoluto è visualizzare per ogni minaccia la cve associato e per ogni cve i links di riferimento. Tuttavia questa operazione non viene permessa dalla web app, anche perché non è in alcun modo utile all’utente vedere queste informazioni tutte insieme.

In generale le operazioni permesse dalla web app sono tutte controllate e non generano carico e sforzo computazionale (in base al numero dei records previsti nella tabella dei volumi).

4. Ristrutturazione dello schema relazionale tenendo conto del carico dell'applicazione

Non è necessario ristrutturare ulteriormente lo schema relazionale, in quanto le operazioni effettuate più di frequente sulla base di dati sono tutte operazioni che richiedono pochi accessi. Il carico dell’applicazione è quindi bilanciato e permette un uso efficiente delle risorse.

5. Specifica del database in SQL

```
create table Auth_user(
    id Integer primary key auto_increment,
    username varchar(40) not null,
    password varchar(100) not null,
    first_name varchar(100) not null,
    last_name varchar(100) not null,
    is_superuser tinyint(1) not null,
    is_staff tinyint(1) not null,
    is_active tinyint(1) not null,
    date_joined datetime not null,
    last_login datetime not null
);

create table Produttore(
    id Integer primary key auto_increment,
    nome varchar(30) not null,
    nazione varchar(50) not null
);
create table Lang(
    id integer primary key auto_increment,
    nome varchar(30) not null,
    version varchar(20) not null,
    descrizione longtext not null
);
create table Files(
    fhash varchar(100) primary key,
    nome varchar(500) not null,
    fdati blob not null,
    peso integer not null,
    autore varchar(50)
);
create table Analyzer(
    id Integer primary key auto_increment,
    nome varchar(30) not null,
    version varchar(20) not null,
    produttore Integer not null,
    type varchar(20) not null,
    foreign key (produttore) references  Produttore(id)
);
```

```
create table LangAnalyzer(
     analyzer Integer not null,
     lang integer not null,
     foreign key (analyzer) references Analyzer(id),
     foreign key (lang) references Lang(id),
     primary key (analyzer, lang)
);
create table Minaccia(
    mhash varchar(100) primary key,
    nome varchar(30) not null,
    categoria varchar(30) not null,
    tipo varchar(20) not null
);
create table Conoscenza(
    minaccia varchar(100)  not null,
    analyzer Integer not null,
    foreign key (minaccia) references Minaccia(mhash),
    foreign key (analyzer) references Analyzer(id),
    primary key (minaccia, analyzer)
);
create table CVE(
    nome varchar(30) primary key,
    descrizione longtext not null,
    anno year not null
);
create table RefCVE(
    cve varchar(30) not null,
    ref varchar(400) not null,
    foreign key (cve) references CVE(nome),
    primary key (cve, ref)
);
create table Contenimento(
    minaccia varchar(100)  not null,
    files varchar(200) not null,
    foreign key (minaccia) references Minaccia(mhash),
    foreign key (files) references Files(fhash),
    primary key (minaccia, files)
);
```

```
create table Exploitation(
    minaccia varchar(100)  not null,
    cve varchar(30) not null,
    foreign key (minaccia) references Minaccia(mhash),
    foreign key (cve) references CVE(nome),
    primary key (minaccia, cve)
);
```

```
create table Analisi(
    id Integer primary key auto_increment,
    analyzer Integer not null,
    datatime date not null,
    tipo varchar(10) not null,
    output blob,
    foreign key (analyzer) references Analyzer(id)
);
```

```
create table filesToAnalisi(
    files varchar(100) not null,
    analisi Integer not null,
    foreign key (files) references Files(fhash),
    foreign key (analisi) references Analisi(id),
    primary key (files, analisi)
);
```

```
create table DatiUtente(
    auth_user Integer primary key,
    points Integer not null,
    foreign key (auth_user) references Auth_user(id)
);
```

```
create table Caricamento(
    auth_user Integer not null,
    files varchar(100) not null,
    foreign key (auth_user) references auth_user(id),
    foreign key (files) references Files(fhash),
    primary key (auth_user, files)
);
```

```
create table Sezione(
    nome varchar(30) primary key,
    content longtext not null,
    auth_user Integer not null,
    foreign key (auth_user) references auth_user(id)
);
```

```
create table Topic(
    id Integer primary key auto_increment,
    title varchar(50) not null,
    auth_user Integer not null,
    sezione varchar(30) not null,
    createTime date not null,
    status boolean not null,
    content longtext not null,
    minaccia varchar(100)  not null,
    foreign key (minaccia) references Minaccia(mhash),
    foreign key (sezione) references Sezione(nome),
    foreign key (auth_user) references auth_user(id)
);
```

```
create table Reply(
    id Integer primary key auto_increment,
    topic Integer not null,
    auth_user Integer not null,
    content longtext not null,
    postTime date not null,
    foreign key (topic) references Topic(id),
    foreign key (auth_user) references auth_user(id)
);
```

VINCOLO ESTERNO 1: Un utente non admin non deve poter caricare più di 10 File

```
DELIMITER $$
USE `malwaretotal`$$
CREATE DEFINER=`root`@`localhost` TRIGGER `caricamento_BEFORE_INSERT` BEFORE INSERT ON `caricamento` FOR EACH ROW BEGIN
    if
        (
        select count(*)
        from caricamento c
        where NEW.auth_user = c.auth_user ) > 10 and (
            select au.is_superuser
            from auth_user au
            where au.id = NEW.auth_user
        ) = 0 then
            SIGNAL sqlstate '45001' set message_text = "No way ! You cannot do this !";
    end if;
END$$
```

VINCOLO ESTERNO 2: Un utente admin deve essere anche utente staff

```
DELIMITER $$
USE `malwaretotal`$$
CREATE DEFINER=`root`@`localhost` TRIGGER `auth_user_BEFORE_INSERT` BEFORE INSERT ON `auth_user` FOR EACH ROW BEGIN
    if new.is_superuser = 1 and new.is_staff = 0 then
        SIGNAL sqlstate '45001' set message_text = "Un account superuser deve anche essere staff!";
    end if;
END$$
DELIMITER ;
```

VINCOLO ESTERNO 3: Un utente admin deve avere più di 1000 punti

```
DELIMITER $$
USE `malwaretotal`$$
CREATE DEFINER=`root`@`localhost` TRIGGER `datiutente_BEFORE_INSERT` BEFORE INSERT ON `datiutente` FOR EACH ROW BEGIN
    if NEW.points < 1000 and (select is_superuser from auth_user where id = NEW.auth_user) = 1 then
        SIGNAL sqlstate '45001' set message_text = "Un account superuser deve avere più di 1000 punti!";
    end if;
END$$
DELIMITER ;
```

VINCOLO ESTERNO 4: Un topic può essere aperto solo da un Utente con più di 1000 points

```
DELIMITER $$
USE `malwaretotal`$$
CREATE DEFINER=`root`@`localhost` TRIGGER `topic_BEFORE_INSERT` BEFORE INSERT ON `topic` FOR EACH ROW BEGIN
    if new.auth_user in (select du.auth_user from datiutente du where du.points < 1000 ) then
        SIGNAL sqlstate '45001' set message_text = "Un topic può essere aperto solo da un utente con almeno 1000 punti";
    end if;
END$$
DELIMITER ;
```

VINCOLO ESTERNO 5: Una sezione può essere aperta solo da un Utente admin.

```
DELIMITER $$
USE `malwaretotal`$$
CREATE DEFINER=`root`@`localhost` TRIGGER `sezione_BEFORE_INSERT` BEFORE INSERT ON `sezione` FOR EACH ROW BEGIN
   if NEW.auth_user in (select au.id from auth_user au where au.is_superuser = 0 ) then
      SIGNAL sqlstate '45001' set message_text = "Una sezione può essere aperta solo da un utente admin";
   end if;
END$$
DELIMITER ;
```

NOME: **Raffaele** COGNOME: **Ruggeri** MATRICOLA: **1934646** TITOLO: **MalwareTotal** DATA: **24/06/2022**

```
-- descrivo la metà delle operazioni:
-- OP1 caricamento del file "sha256xxx","name","txt",3405691582,"C:/name.txt",20,"raff") dall'utente con id 0
INSERT INTO Files values ("sha256xxx","name","txt",3405691582,"C:/name.txt",20,"raff");
INSERT INTO Caricamento values (0,"sha256xxx");

-- OP2 Iscrizione dell'utente amministratore (password = 'pass', username = "hak", nome = "kali", cognome = "linux") con 2 email email_1@lib.net e email_2@lib.net
INSERT INTO auth_user values (NULL, password("pass"), NULL,  1, "hak", "kali", "linux", "r@root.net", 1, 1 , NULL);
INSERT INTO datiutente values ((SELECT max(ID) from auth_user), "linux", "kali", 0, 1,  STR_TO_DATE('1-01-2012', '%d-%m-%Y'));
INSERT INTO email values ("email_1@lib.net", (SELECT max(ID) from auth_user));
INSERT INTO email values ("email_2@lib.net", (SELECT max(ID) from auth_user));

-- OP3 Analisi di un del file con hash = "sha256xx", tramite analyzer con id = 4 e il report di analisi localizzato
-- in "C:/out.txt"
INSERT INTO analisi values (NULL, 4, NULL, "C:/out.txt");
INSERT INTO filetoanalisi values ("sha256xxx", (SELECT max(ID) from analisi));
-- se risulta una minaccia di id = N, si esegue anche la query
INSERT INTO contenimento values (N, "sha256xxx");
-- OP4 Rimozione di tutti i dati di un Utente con id = 10 (il file che va conservato senza chi l'ha caricato)
delete from reply where auth_user = 10;
delete from topic where auth_user = 10;
delete from sezione where auth_user = 10;
delete from caricamento where auth_user = 10;
delete from datiutente where auth_user = 10;
delete from email where auth_user = 10;
delete from utente where id = 10;
-- OP5 Aggiunta di un Dynamic Analyzer "newanalyzer v. 1.0", scritto in linguaggio "c++" e prodotto dal produttore con id = 5, che conosce solo 2 minacce
-- una con id = 5 e l'altra con id = 7
INSERT INTO analyzer values (NULL, "newanalyzer", 1.0, 5, "dynamic");
insert into conoscenza values (5, (SELECT max(ID) from analyzer));
insert into conoscenza values (7, (SELECT max(ID) from analyzer));
insert into langanalyzer values ((SELECT max(ID) from analyzer), "c++");
-- OP6 Aggiornamento delle Minacce note all'Analyzer con id = 2, aggiunta la conoscenza delle minacce 10 e 11 e rimozione della minaccia 7
insert into conoscenza values (7, 2);
insert into conoscenza values (7, 2);
delete from conoscenza where minaccia = 7 and analyzer = 2;
```

```
-- OP8 Creazione di un nuovo Topic "title1", contenuto = "discussione1", da parte dell'utente con id = 0,
-- riferito alla minaccia con id = 4, nella sezione = "trojan"
insert into topic values (NULL, "title1", 0, "trojan", 0, NULL, 1, "discussione1", 4);
-- OP9 Aggiunta di un Reply da parte dell'utente con id = 0, nel topic con id = 5, di contenuto = "contenuto"
insert into reply values (NULL, 5, 0, "contenuto", NULL);

-- dato che le operazioni base che fa il database sono tutte query molto semplici, adesso vado a creare altre 12 query
-- che soddisfano i requisiti richiesti ma che non vengono effettivamente utilizzante dalla web app (almeno non nella versione attuale).

-- query 1: ritorna il numero di utenti che hanno risposto in reply con contenuto "wow" nella sezione "Trojan"
select count(auth_user)
from Reply
where Reply.content = "wow" and Reply.topic in (
    select id
    from Topic
    where Topic.sezione = "Trojan"
);
-- query 2: ritorna il numero di utenti che hanno risposto in reply con contenuto "ciao" nella sezione
-- creata da un utente di nome = "nome" e cognome = "cognome"
select count(auth_user)
from Reply
where Reply.content = "ciao" and Reply.topic = (
    select id
    from Topic
    where Topic.sezione in (
        select nome
        from sezione
        where auth_user in (
            select auth_user
            from datiutente
            where nome = "nome" and cognome = "cognome"
        )
    )
);
```

```sql
-- query 3: ritorna i dati di tutti i file caricati dall'utente iscritto meno di recente
-- e che ha più di una email associata e ha più di 1000 points
select fhash,nome,estensione,magicNumber,fdati,peso,autore
from files
join caricamento
on files.fhash = caricamento.files
join auth_user
on auth_user.id = caricamento.auth_user
where date_joined = (select min(date_joined) from auth_user)
and (select count(email.email) from email where email.auth_user = auth_user.id) > 1
and (select points from datiutente where auth_user.id = datiutente.auth_user) > 1000;

-- query 4: ritorna i dati di tutti i file caricati dagli utenti che sono amministratori
select fhash,nome,estensione,magicNumber,fdati,peso,autore
from files
join caricamento
on files.fhash = caricamento.files
join auth_user
on auth_user.id = caricamento.auth_user
where auth_user.is_superuser = 1;

-- query 5: calcolare la media dei punti degli utenti che hanno caricato almeno un file, raggruppando per utenti staff e non staff
select avg(points)
from datiutente
join auth_user
on datiutente.auth_user = auth_user.id
where (
    select count(*)
    from caricamento
    where caricamento.auth_user = auth_user.id
) >= 1
group by auth_user.is_superuser;
```

```
-- query 6: calcolare la media dei punti degli utenti, che hanno pubblicato almeno 2 reply e non sono admin,
-- raggruppandoli per anno di iscrizione

select avg(points)
from datiutente
join auth_user
on datiutente.auth_user = auth_user.id
where auth_user.is_superuser = 0 and (
    select count(*)
    from reply
    where reply.auth_user = auth_user.id
) > 1
group by year(date_joined);

-- query 7: selezionare tutti i dati delle minacce, raggruppate per categoria, che sono state rilevate più della media
-- delle rilevazioni per quella stessa categoria e che exploitano almeno 2 cve

select *
from minaccia
where (
    select count(*)
    from exploitation
    where exploitation.minaccia = minaccia.mhash
) > 1
group by categoria
having nRilevazione > avg(nRilevazione);
```

```
-- query 8: seleziona il nome di tutte le cve scoperte nel 2001 e che hanno almeno una reference e
-- che sono exploitate da almeno 4 minacce

select nome
from cve
where anno = '2001' and (
    select count(*)
    from refcve r1
    where r1.cve = cve.nome
) >= 1 and (
    select count(*)
    from exploitation e1
    where e1.cve = cve.nome
) >= 4;

-- query 9: seleziona tutti i topic, che riguardano una minaccia di categoria "ransomware", e a cui appartiene almeno un
-- reply pubblicato in data successiva al '16/06/2022'

select *
from topic
where topic.minaccia in (
    select id
    from minaccia
    where minaccia.categoria = "ransomware"
) and (
    select count(*)
    from reply
    where reply.topic = topic.id and reply.postTime > '16/06/2022'
)>= 1;
```

```
-- query 10: seleziona tutti i nomi dei linguaggi di programmazione usati dai produttori di nazionalità italiana
select nome
from lang
where lang.id in (
    select la.lang
    from langanalyzer la
    where analyzer in (
        select a.id
        from analyzer a
        where a.produttore in (
            select p.id
            from produttore p
            where nazione = "italia"
        )
    )
);

-- query 11: conta quanti analyzer ci sono per (produttore, language) espludendo quelli prodotti dai produttori
-- con nome più lungo di 10 caratteri

select count(*)
from analyzer join langAnalyzer
on analyzer.id = langAnalyzer.analyzer
where (
    select char_length(p1.nome)
    from produttore p1
    where p1.id = analyzer.produttore
) <= 10
group by (analyzer.produttore, langAnalyzer.lang);
```

```sql
-- query 12: selezionare tutte le email degli utenti che hanno meno di 100 punti e sono di sesso maschile

select E.email
from email E
where E.auth_user in (
    select DU.auth_user
    from dati_utente DU
    where DU.sesso = 1 and DU.points < 100
);

--  ne riscrivo 6 con le viste

-- query 1 (viste): ritorna il numero di utenti che hanno risposto in reply con contenuto "wow" nella sezione "Trojan"
create view v
as
select auth_user
from Reply
where Reply.content = "wow" and Reply.topic in (
    select id
    from Topic
    where Topic.sezione = "Trojan"
);
select count(auth_user) from v;

-- query 2: ritorna il numero di utenti che hanno risposto in reply con contenuto "ciao" nella sezione
-- creata da un utente di nome = "nome" e cognome = "cognome"
create view v2 as
select id
from Topic
where Topic.sezione in (
    select nome
    from sezione
    where auth_user in (
        select auth_user
        from datiutente
        where nome = "nome" and cognome = "cognome"
    )
);
```

```
select count(auth_user)
from Reply
where Reply.content = "ciao" and Reply.topic = ( select id from v2);

-- query 3: ritorna i dati di tutti i file caricati dall'utente iscritto meno di recente
-- e che ha più di una email associata e ha più di 1000 points

create view v3 as
select fhash,nome,estensione,magicNumber,fdati,peso,autore,auth_user.id id, auth_user.date_joined date_joined
from files
join caricamento
on files.fhash = caricamento.files
join auth_user
on auth_user.id = caricamento.auth_user;

select fhash,nome,estensione,magicNumber,fdati,peso,autore
from v3
where date_joined = (select min(date_joined) from auth_user)
and (select count(email.email) from email where email.auth_user = id) > 1
and (select points from datiutente where id = datiutente.auth_user) > 1000;

-- query 4: ritorna i dati di tutti i file caricati dagli utenti che sono amministratori
create view v4 as
select fhash,nome,estensione,magicNumber,fdati,peso,autore, is_superuser
from files
join caricamento
on files.fhash = caricamento.files
join auth_user
on auth_user.id = caricamento.auth_user;

select fhash,nome,estensione,magicNumber,fdati,peso,autore
from v4
where is_superuser = 1;
```

```sql
-- query 5: calcolare la media dei punti degli utenti che hanno caricato almeno un file, raggruppando per utenti staff e non staff
create view v5 as
select points, is_superuser
from datiutente
join auth_user
on datiutente.auth_user = auth_user.id
where (
    select count(*)
    from caricamento
    where caricamento.auth_user = auth_user.id
) >= 1;

select avg(points)
from v5
group by is_superuser;

-- query 6: calcolare la media dei punti degli utenti, che hanno pubblicato almeno 2 reply e non sono admin,
-- raggruppandoli per anno di iscrizione
create view v6 as
select points, date_joined
from datiutente
join auth_user
on datiutente.auth_user = auth_user.id
where auth_user.is_superuser = 0 and (
    select count(*)
    from reply
    where reply.auth_user = auth_user.id
) > 1;

select *
from v6
group by year(date_joined);
```

5. Realizzazione di un video che mostra il funzionamento dell'applicazione finale

Il video è presente nella cartella del progetto

6. Conclusione

Mi sono ispirato ad alcuni siti già esistenti: virustotal.com, exploit-db.com e inforge.net per questa idea.