Corso di Laurea in Informatica

Security Smell: Una Systematic Literature Review

Prof. Fabio Palomba

Alessandro Tortora
Mat.: 0512106428

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

SCAN ME!

Introduzione e Background

Al giorno d’oggi lo sviluppo software sta assumendo un ruolo sempre più centrale in ambito informatico…

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Introduzione e Background

Al giorno d’oggi lo sviluppo software sta assumendo un ruolo sempre più centrale in ambito informatico…

Diventa indispensabile garantire la sicurezza dei sistemi sviluppati evitando i security smell

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Security Smell: Una Systematic Literature Review

Alessandro Tortora
Università degli Studi di Salerno

Introduzione e Background

I security smell sono difetti nella programmazione di codice che **possono** essere la causa di debolezze nella sicurezza di un sistema.

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Introduzione e Background

I security smell sono difetti nella programmazione di codice che **possono** essere la causa di debolezze nella sicurezza di un sistema.

Infatti non sempre portano a conseguenze negative, ma meritano comunque attenzione e, dove possibile, mitigazione.

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Security Smell: Una Systematic Literature Review

Alessandro Tortora
Università degli Studi di Salerno

Metodologia

Obiettivo:
Identificare le tipologie di security smell e le loro caratteristiche

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Metodologia

RQ1

Quali security smell sono stati definiti dalla letteratura esistente?

Obiettivo:
Identificare le tipologie di security smell e le loro caratteristiche

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Metodologia

Obiettivo:
Identificare le tipologie di security smell e le loro caratteristiche

RQ1

Quali security smell sono stati definiti dalla letteratura esistente?

RQ2

In quali infrastrutture, metodologie o tecniche di sviluppo sono più frequenti i security smell?

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Security Smell: Una Systematic Literature Review

Alessandro Tortora
Università degli Studi di Salerno

Metodologia

Obiettivo:
Identificare le tipologie di security smell e le loro caratteristiche

RQ1

Quali security smell sono stati definiti dalla letteratura esistente?

RQ2

In quali infrastrutture, metodologie o tecniche di sviluppo sono più frequenti i security smell?

RQ3

Quali tecniche si possono adottare per correggere il codice affinché non si presentino security smell?

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Security Smell: Una Systematic Literature Review

Alessandro Tortora
Università degli Studi di Salerno

Metodologia

Revisione sistematica della Letteratura

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Metodologia

Revisione sistematica della Letteratura

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Metodologia

Revisione sistematica della Letteratura

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Metodologia

sesa lab
SOFTWARE ENGINEERING
SALERNO

Revisione sistematica della Letteratura

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Security Smell: Una Systematic Literature Review

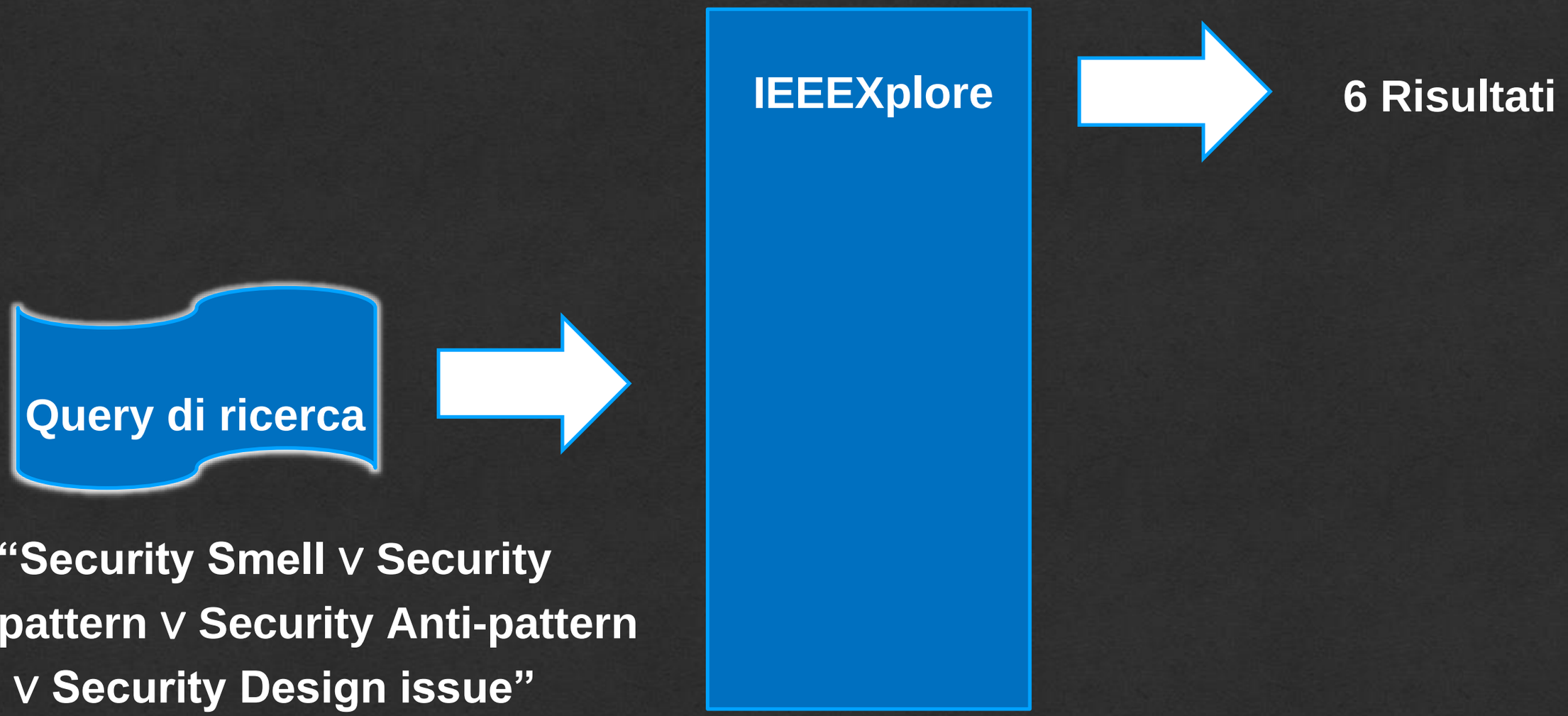
Alessandro Tortora
Università degli Studi di Salerno

Metodologia

“Security Smell V Security Antipattern V Security Anti-pattern V Security Design issue”

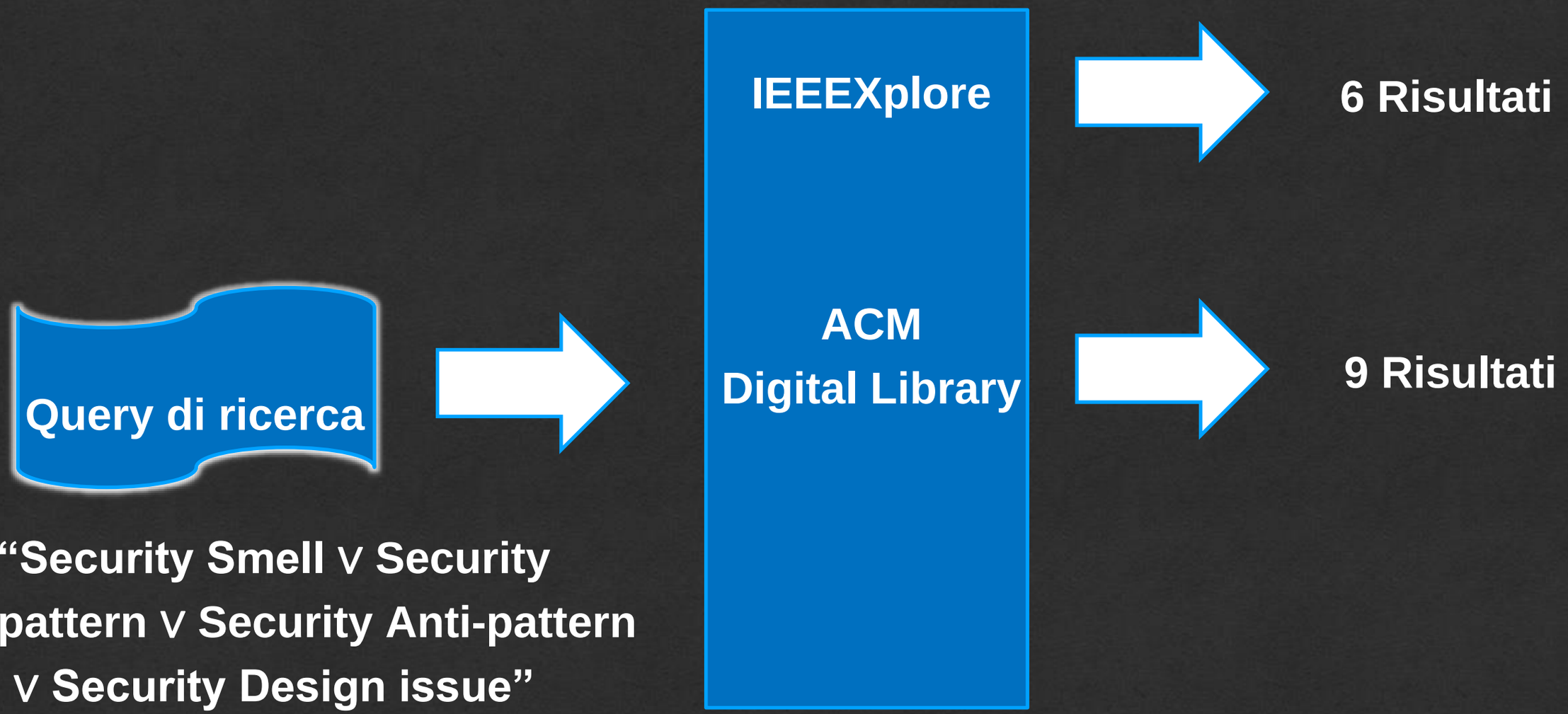
a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Metodologia



a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Metodologia

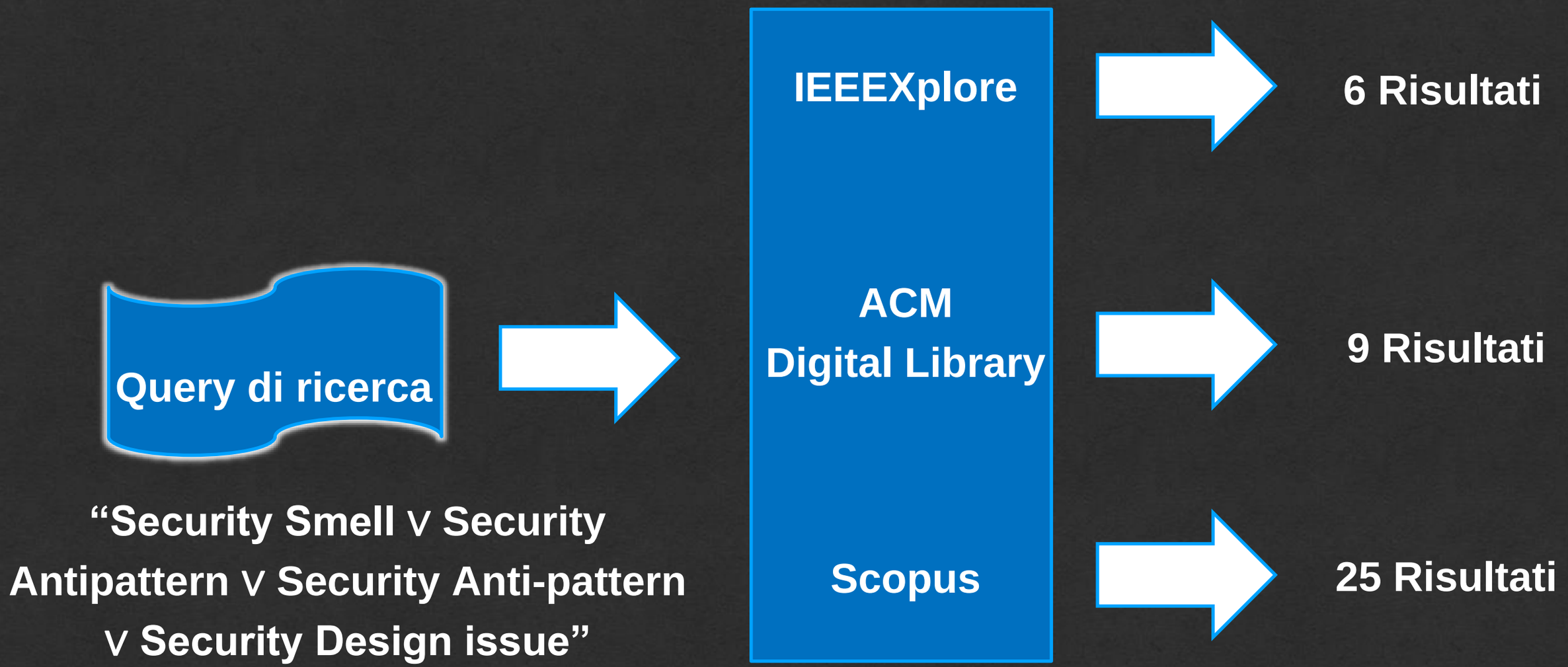


a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Security Smell: Una Systematic Literature Review

Alessandro Tortora
Università degli Studi di Salerno

Metodologia



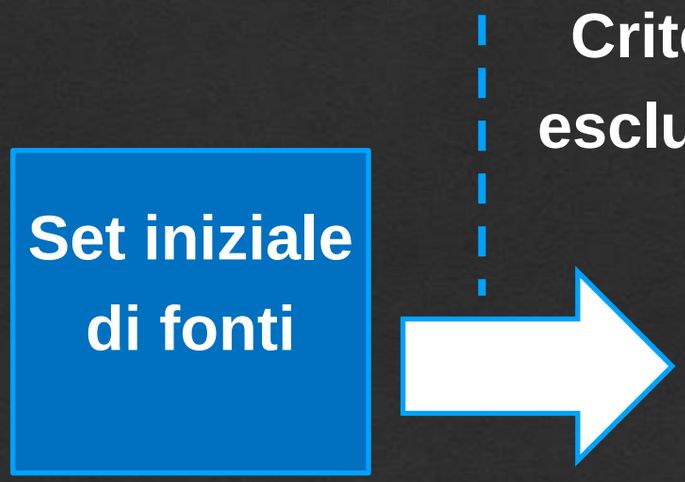
a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Metodologia

Set iniziale di fonti

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

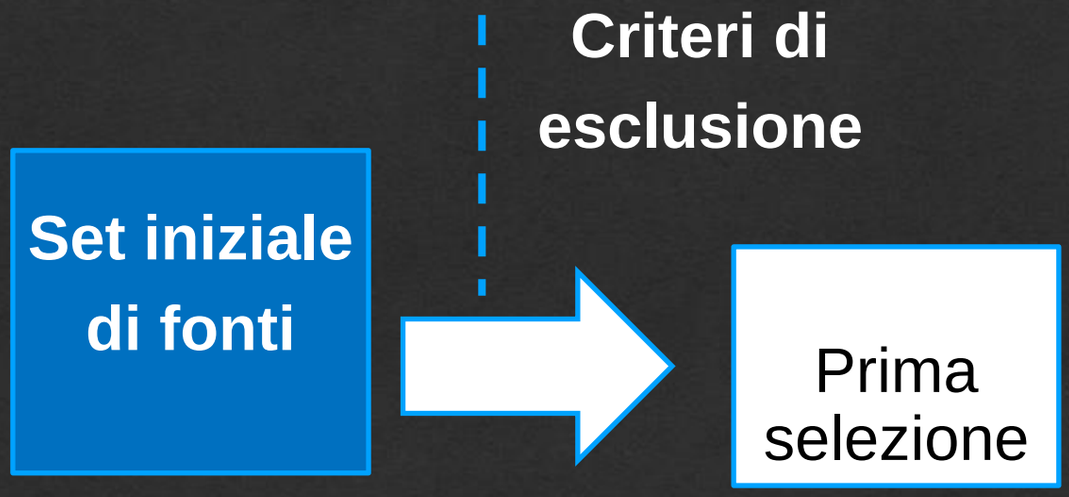
Metodologia



- Articoli non scritti in inglese
- Articoli con lunghezza inferiori a 7 pagine
- Documenti duplicati
- Articoli il cui testo non era disponibile
- Scarsa comprensibilità
- Non coerente con gli argomenti trattati
- Fonte non specificata

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Metodologia

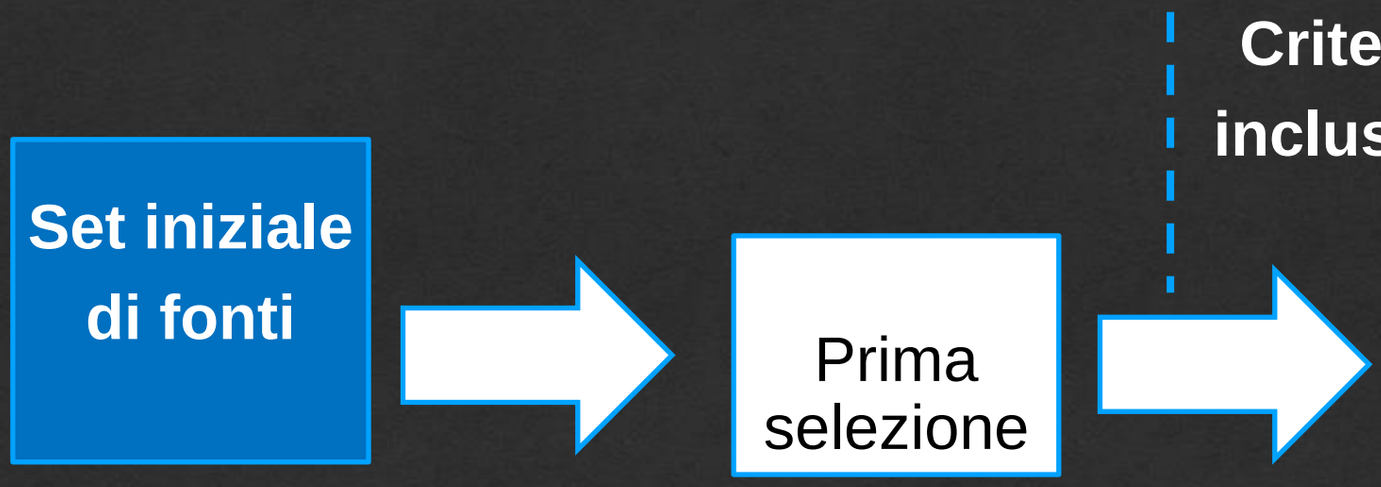


12 di 40 articoli passano alla fase successiva

- Articoli non scritti in inglese
- Articoli con lunghezza inferiori a 7 pagine
- Documenti duplicati
- Articoli il cui testo non era disponibile
- Scarsa comprensibilità
- Non coerente con gli argomenti trattati
- Fonte non specificata

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

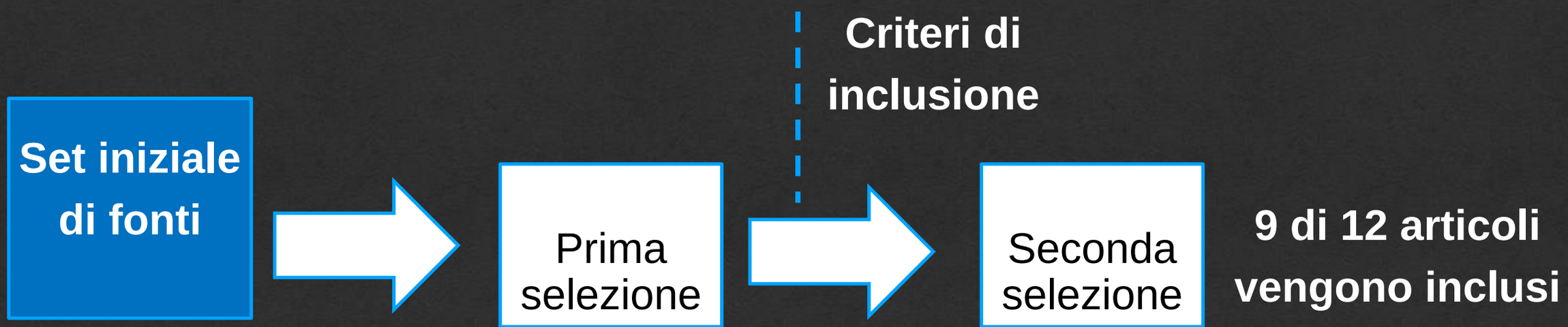
Metodologia



- Articoli che esplicitano quali security smell vengono trattati
- Articoli che esplicitano gli ambiti in cui i security smell sono stati riscontrati e la loro frequenza in essi
- Articoli che esplicitano tecniche per la risoluzione dei security smell

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Metodologia

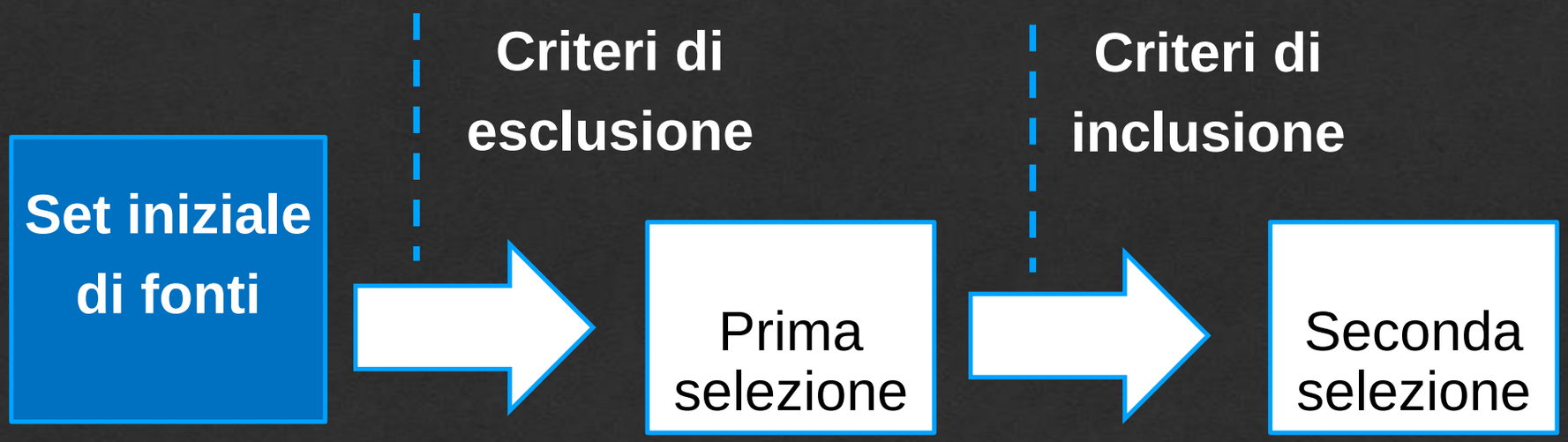


- Articoli che esplicitano quali security smell vengono trattati
- Articoli che esplicitano gli ambiti in cui i security smell sono stati riscontrati e la loro frequenza in essi
- Articoli che esplicitano tecniche per la risoluzione dei security smell

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Security Smell: Una Systematic Literature Review
Alessandro Tortora
Università degli Studi di Salerno

Metodologia



9 Risultati

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Risultati

RQ1:

Quali security smell sono stati definiti dalla letteratura esistente?

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Risultati

RQ1:

Quali security smell sono stati definiti dalla letteratura esistente?

Admin by default (CWE 250)
Password vuota (CWE 258)
Segreto hard-coded (CWE 259 – CWE 798)
Indirizzo IP senza restrizioni (CWE 284)
Commento sospetto (CWE 546)
Uso di HTTP senza SSL/TLS (CWE 319)
Nessun controllo di integrità (CWE 353)
Uso di algoritmi di crittografia deboli (CWE 326 – CWE 327)
Default mancante nella dichiarazioni di istruzioni switch-case (CWE 478)
Uso di assert (CWE 703)
Funzioni in lista nera (CWE 78 – CWE 330)
Sottoprocesso senza shell Uguale Vero (CWE 78)
Canale di trasporto non sicuro
Divulgazione di codice sorgente
Divulgazioni di informazioni sulla versione
Mancanza di controllo degli accessi
Reindirizzamenti HTTPS mancanti
HSTS mancante
Utilizzo di BCrypt con forza predefinita 10
Richieste illimitate durante invocazioni API

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Security Smell: Una Systematic Literature Review
Alessandro Tortora
Università degli Studi di Salerno

Risultati

RQ2:
In quali infrastrutture, metodologie o tecniche di sviluppo sono più frequenti i security smell?

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Risultati

RQ2:
In quali infrastrutture, metodologie o tecniche di sviluppo sono più frequenti i security smell?

IaC: Infrastructure as Code

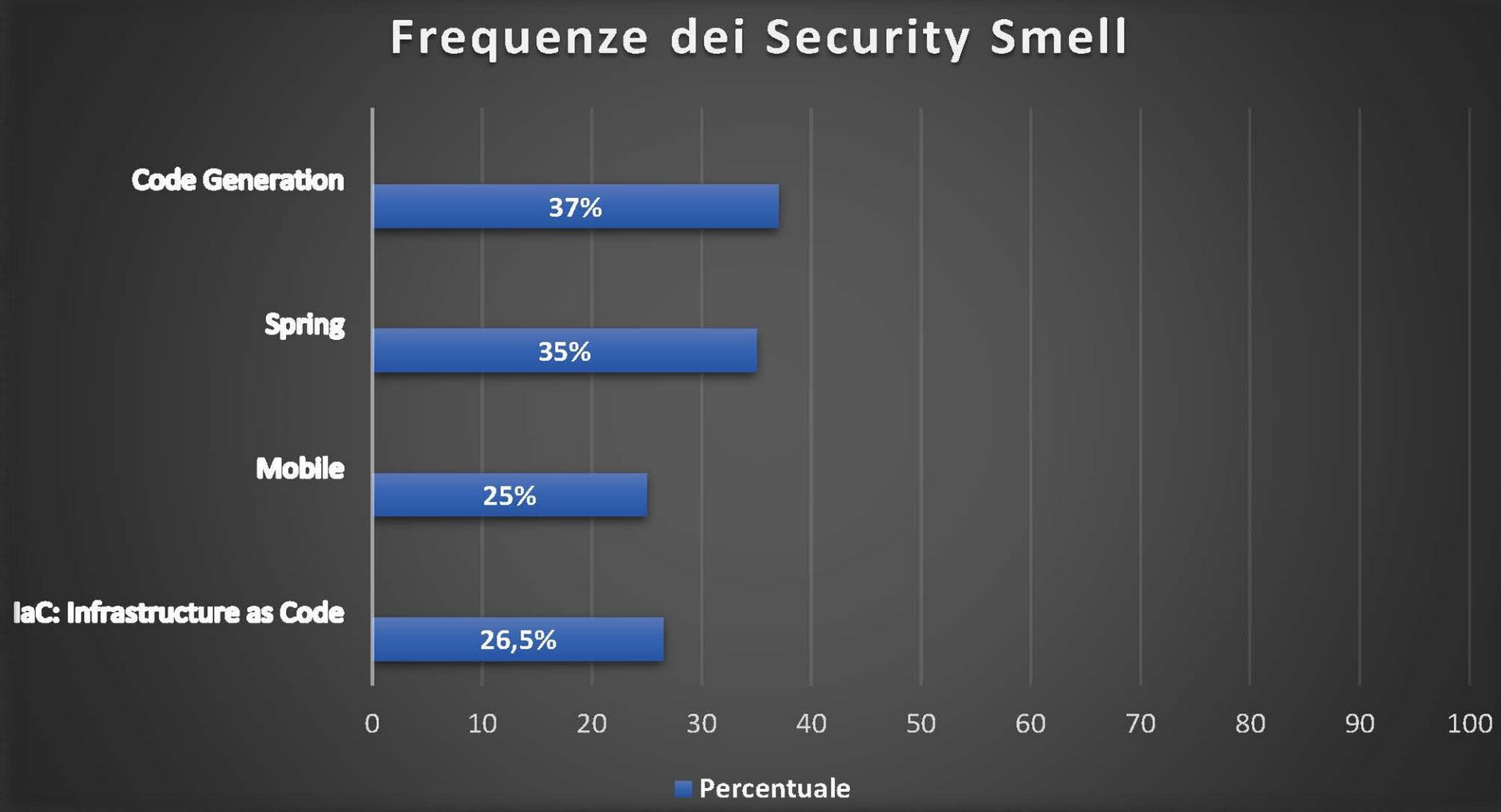
Mobile

Spring

Code Generation

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Risultati



Percentuale delle occorrenze dei security smell nelle varie categorie analizzate

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Security Smell: Una Systematic Literature Review

Alessandro Tortora
Università degli Studi di Salerno

Risultati

RQ3:
Quali tecniche si possono adottare per correggere il codice affinché non si presentino security smell?

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Risultati

RQ3:
Quali tecniche si possono adottare per correggere il codice affinché non si presentino security smell?

Essendo i security smell tutti distinti tra loro, le tecniche che si possono adottare per correggere il codice affinché essi non si presentino sono 20, come i security smell analizzati.

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Risultati

Esempio di tecniche risolutive

Security Smell 1: Admin by default

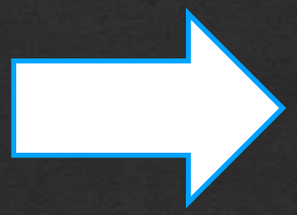
Si raccomanda ai professionisti di progettare ed implementare un sistema che, come impostazione predefinita, fornisca a qualsiasi entità il minor numero di privilegi necessari

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Risultati

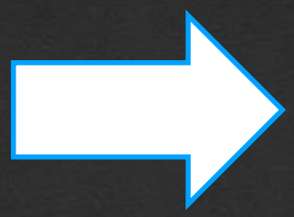
Esempio di tecniche risolutive

Security Smell 1: Admin by default



Si raccomanda ai professionisti di progettare ed implementare un sistema che, come impostazione predefinita, fornisca a qualsiasi entità il minor numero di privilegi necessari

Security Smell 2: Password vuota



Si raccomanda ai professionisti di utilizzare password forti, eliminando così la comparsa di password vuote

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Sviluppi futuri

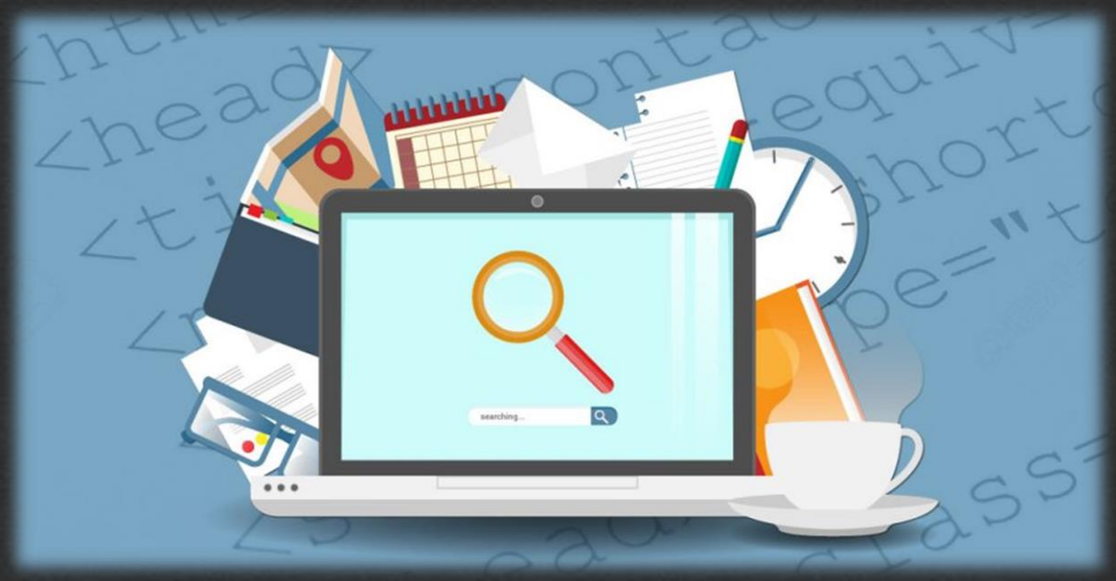
Ricerca di nuovi security smell

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Security Smell: Una Systematic Literature Review

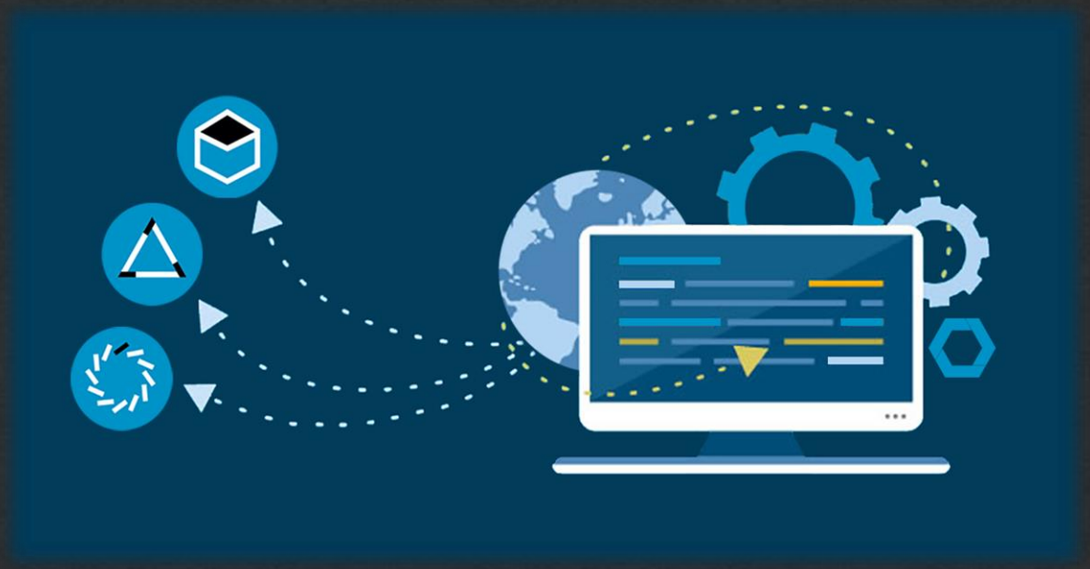
Alessandro Tortora
Università degli Studi di Salerno

Sviluppi futuri



Ricerca di nuovi security smell

Implementazione di un tool di identificazione per security smell



a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/

Security Smell: Una Systematic Literature Review

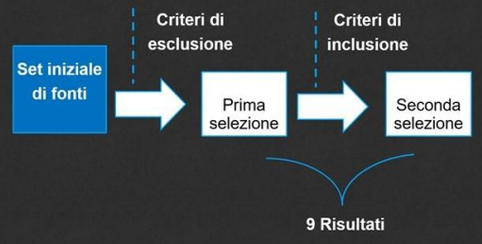
Alessandro Tortora
Università degli Studi di Salerno

Introduzione e Background

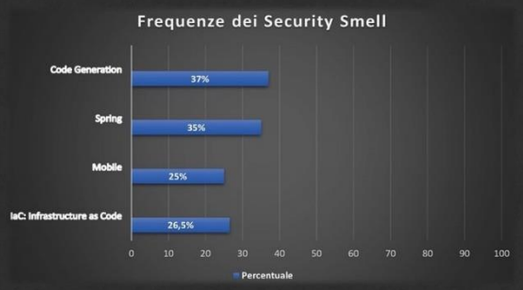
I security smell sono difetti nella programmazione di codice che **possono** essere la causa di debolezze nella sicurezza di un sistema.

Infatti non sempre portano a conseguenze negative, ma meritano comunque attenzione e, dove possibile, mitigazione.

Metodologia



Risultati



Percentuale delle occorrenze dei security smell nelle varie categorie analizzate

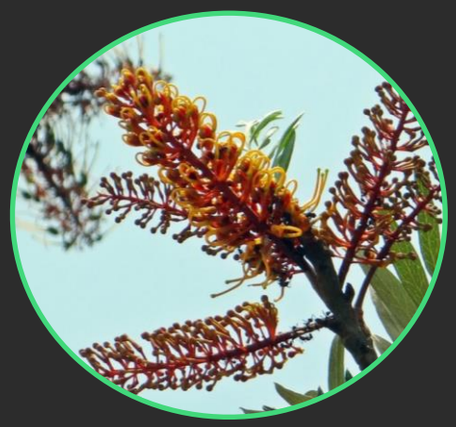
Sviluppi futuri

Ricerca di nuovi security smell

Implementazione di un tool di identificazione per security smell

treedom®
let's green the planet

Questa tesi ha contribuito a piantare un albero in Camerun



Security Smell: Una Systematic Literature Review

SCAN ME!

Grazie!

Alessandro Tortora

a.tortora91@studenti.unisa.it
https://github.com/AleTor00
https://www.linkedin.com/in/alessandro-tortora-8a32b4216/