Corso di Laurea in Informatica

Identificazione di vulnerabilità SQL Injection tramite Taint Analysis: Analisi della letteratura e Confronto Empirico

Prof. Andrea De Lucia
Dott. Emanuele Iannone

Angelo Santangelo
Mat.: 0512112615

a.santangelo18@studenti.unisa.it

Introduzione e Background

La Sicurezza nelle applicazioni web è una preoccupazione.

a.santangelo18@studenti.unisa.it

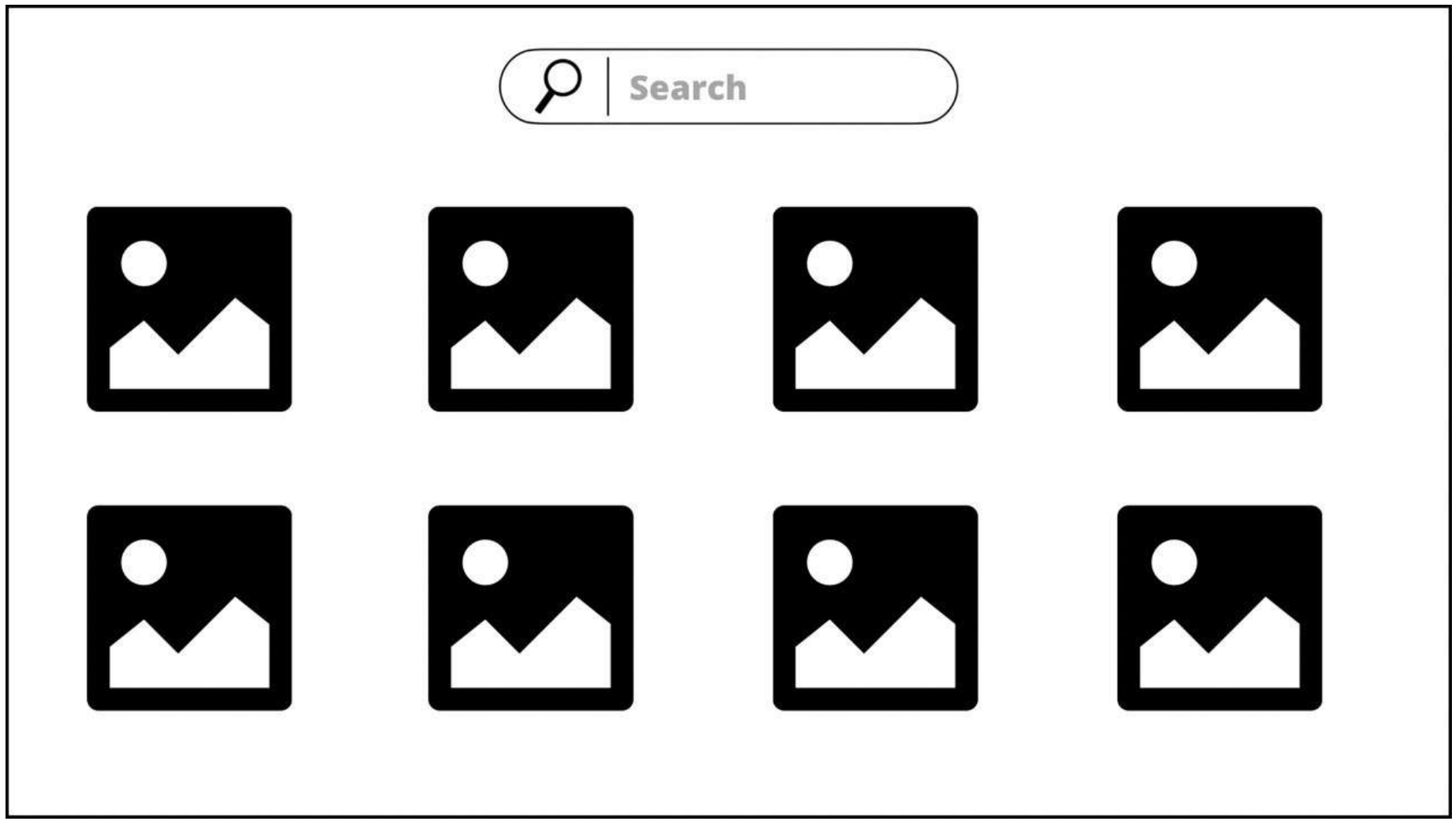
Identificazione di Vulnerabilità SQL Injection tramite Taint Analysis: Analisi della Letteratura e Confronto Empirico

Angelo Santangelo
Università degli Studi di Salerno

Introduzione e Background

SQL Injection al terzo posto nella lista delle 10 vulnerabilità più comuni.

Esempio:



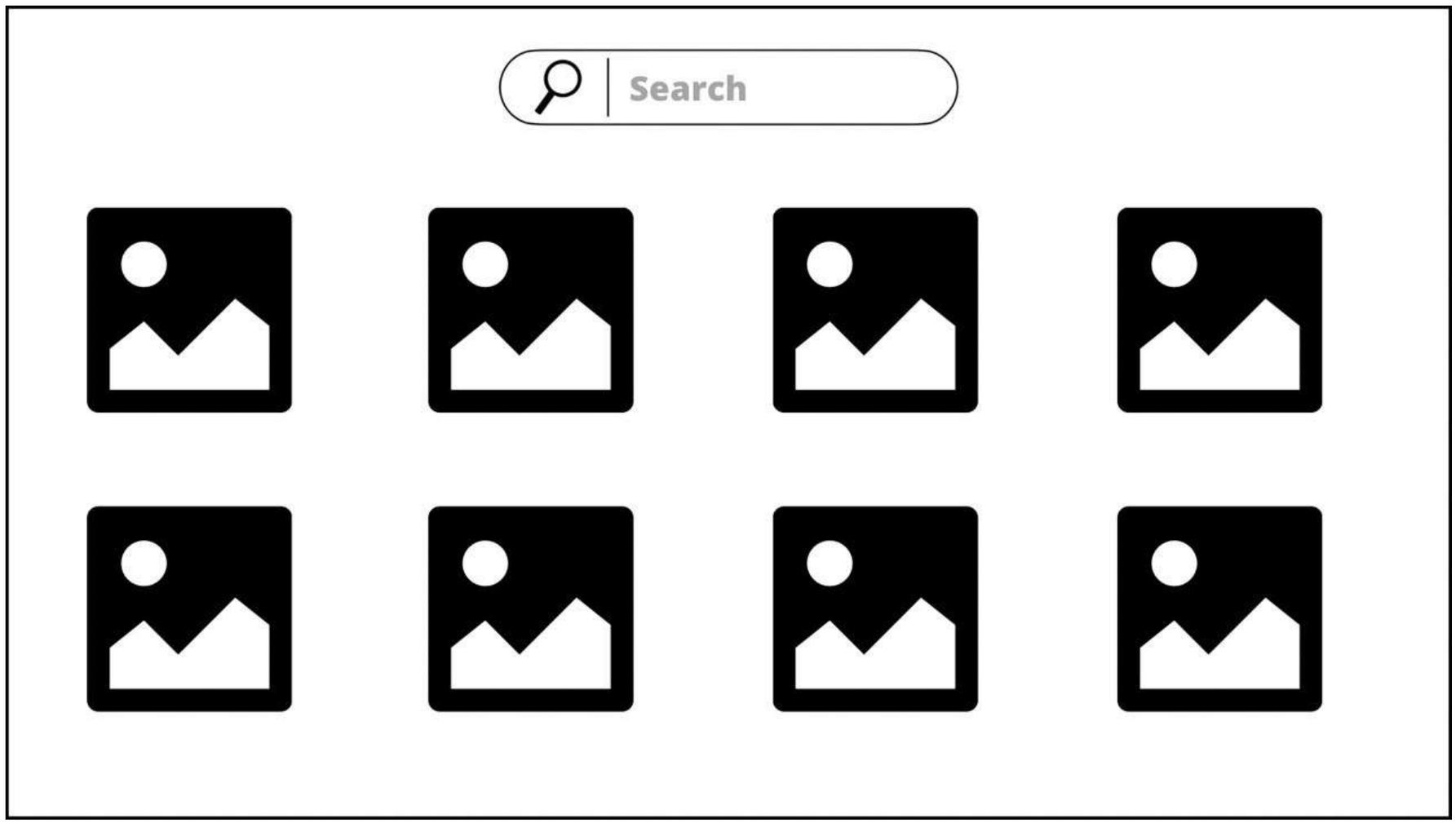
a.santangelo18@studenti.unisa.it

Introduzione e Background

Query:

“SELECT * FROM product WHERE categoria = ’’ + userInput

Esempio:



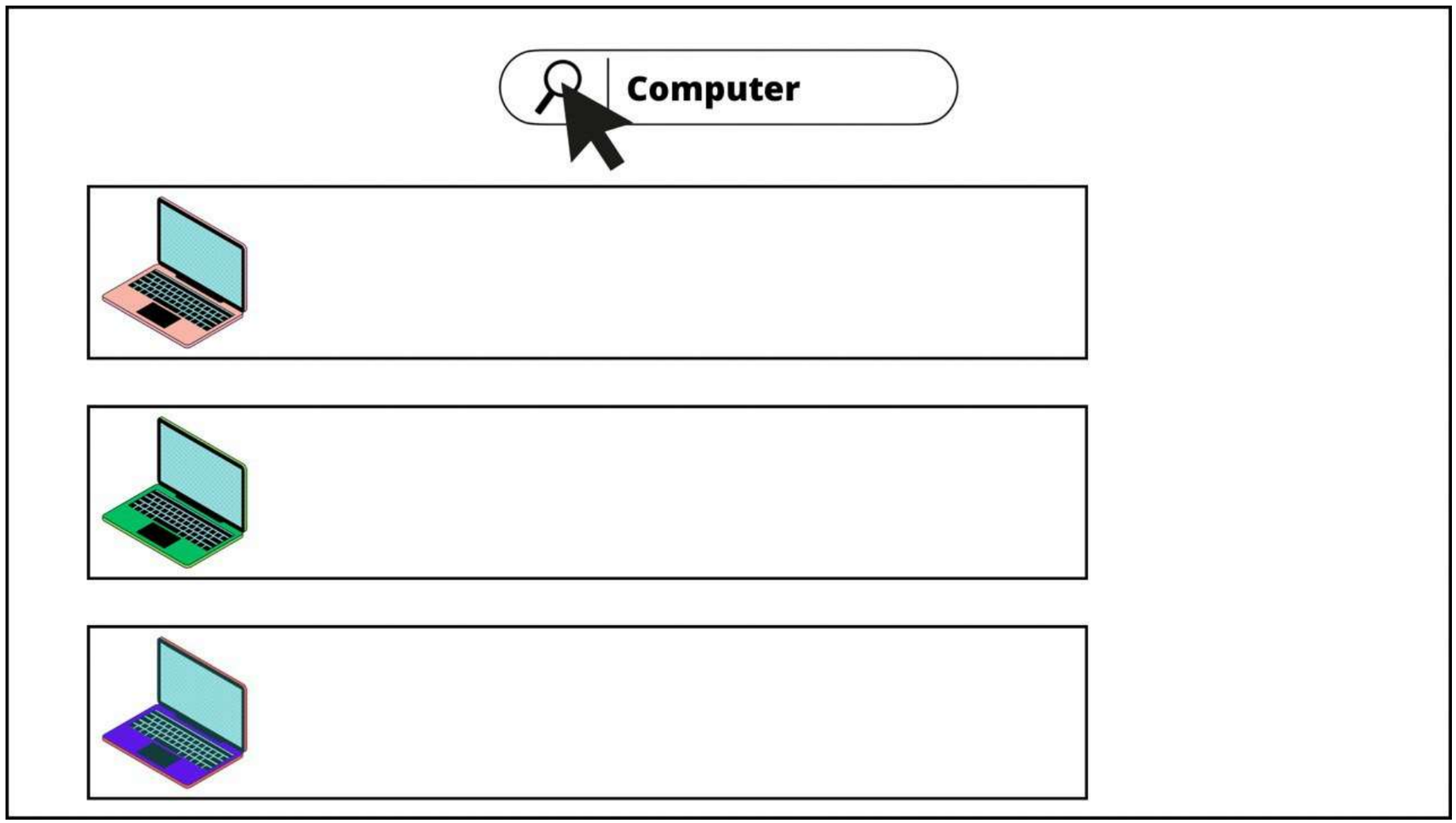
a.santangelo18@studenti.unisa.it

Introduzione e Background

Query:

“SELECT * FROM product WHERE categoria = ’’ + **userInput**

Esempio:



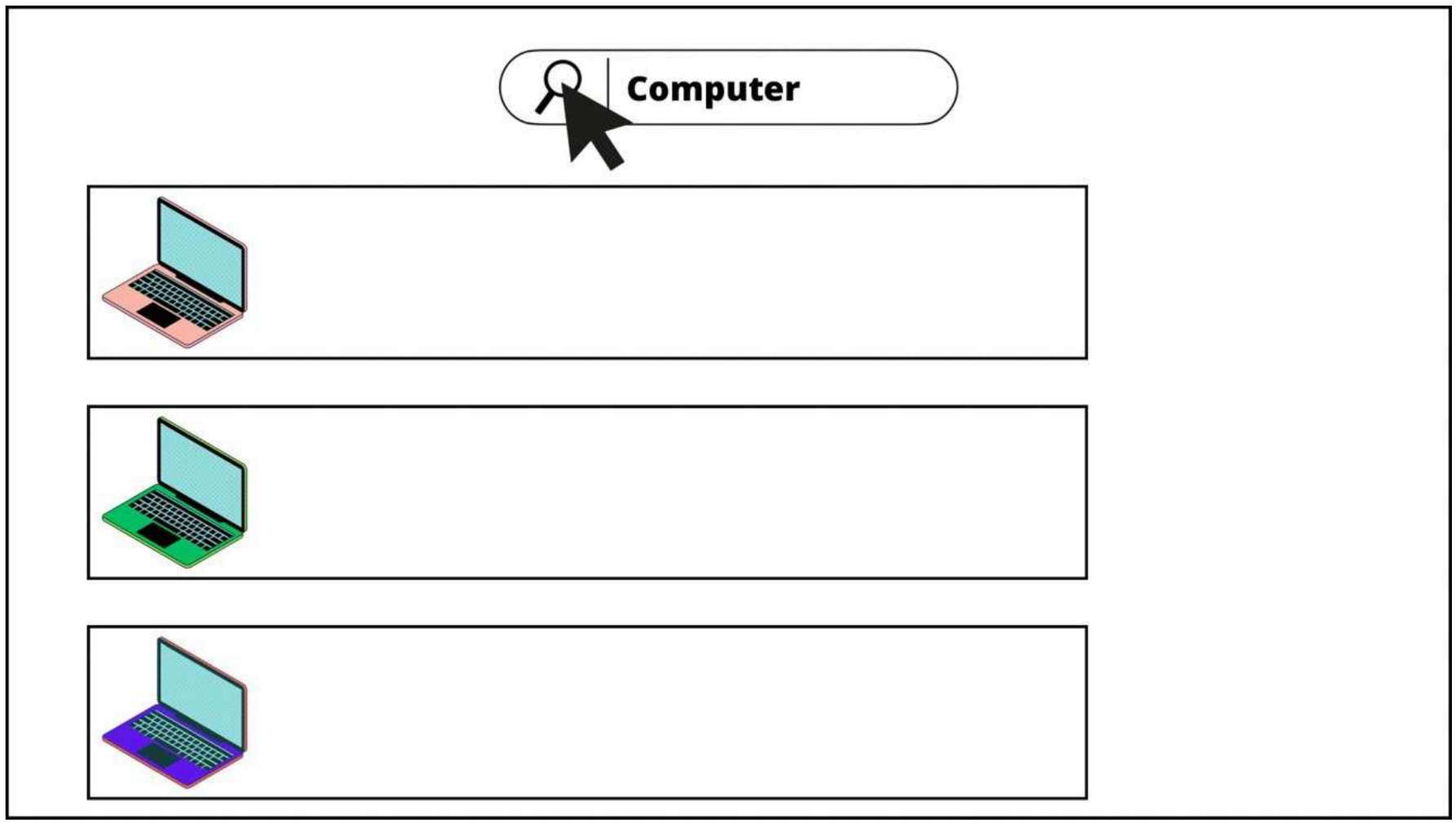
✉ a.santangelo18@studenti.unisa.it

Introduzione e Background

Query:

“SELECT * FROM product WHERE categoria =

Esempio:



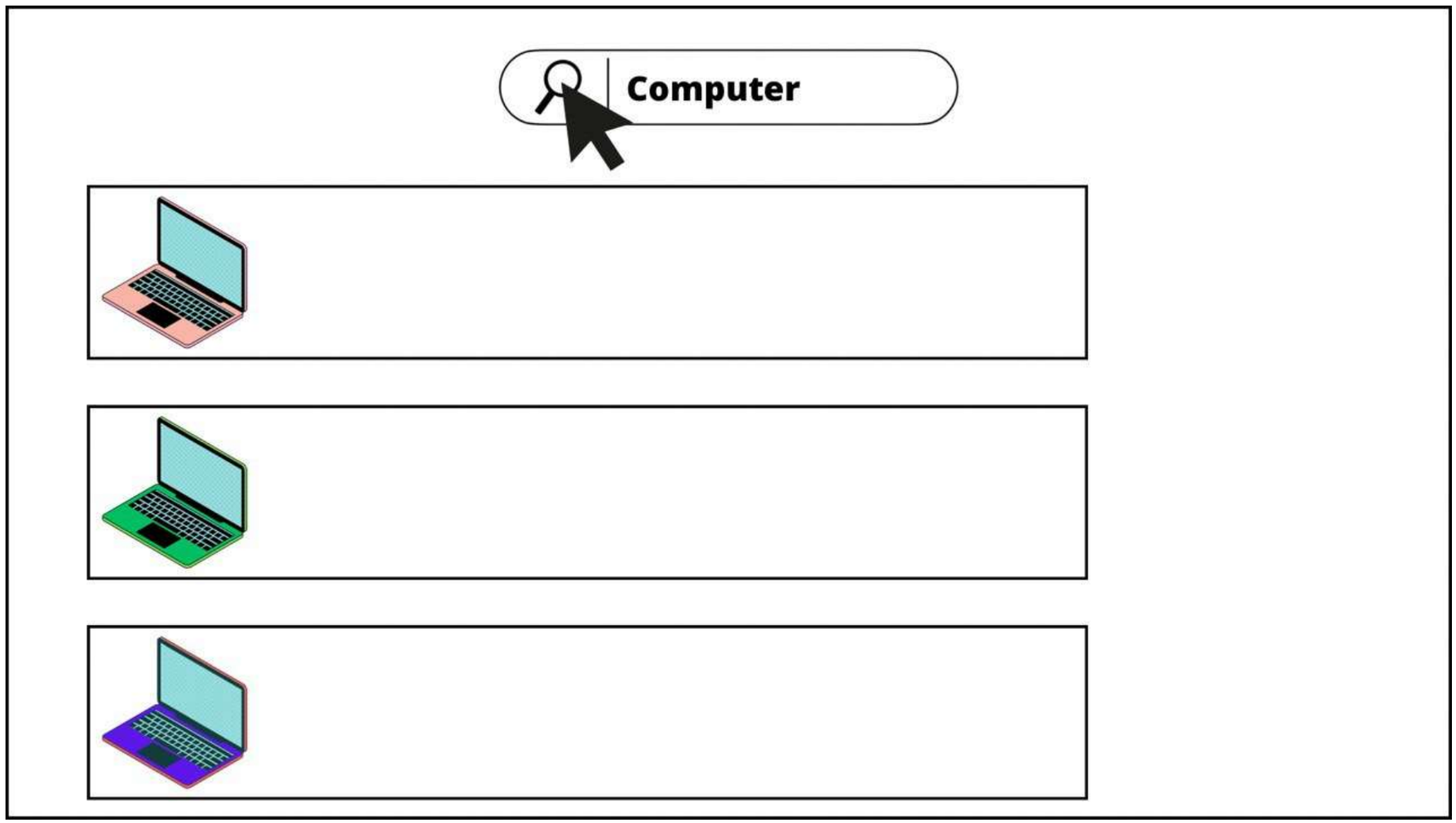
a.santangelo18@studenti.unisa.it

Introduzione e Background

Query:

“SELECT * FROM product WHERE categoria = **computer**

Esempio:

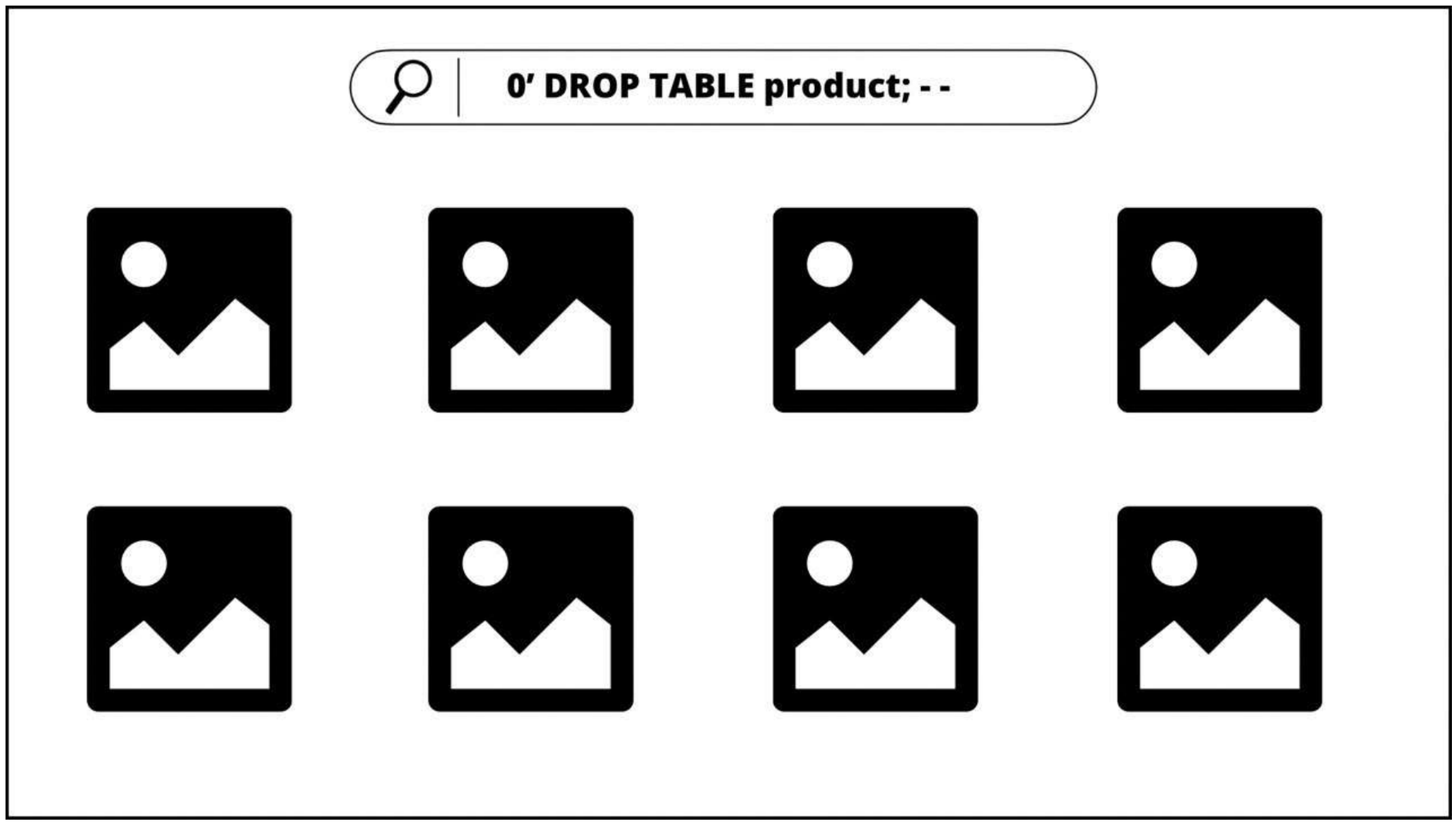


a.santangelo18@studenti.unisa.it

Introduzione e Background

Query:
“SELECT * FROM product WHERE categoria = ’’ + **userInput**

Esempio:



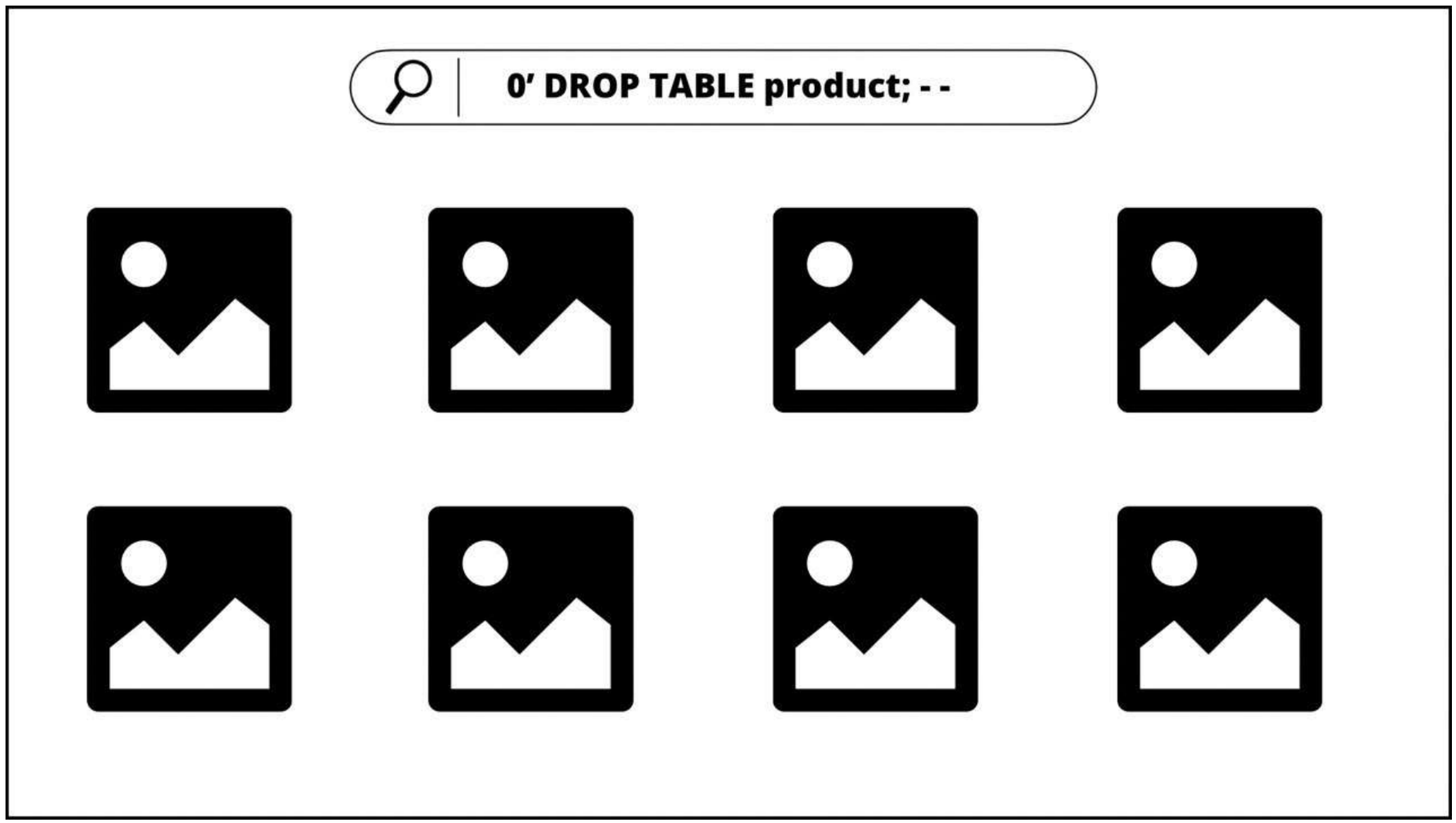
a.santangelo18@studenti.unisa.it

Introduzione e Background

Query:

“SELECT * FROM product WHERE categoria =

Esempio:



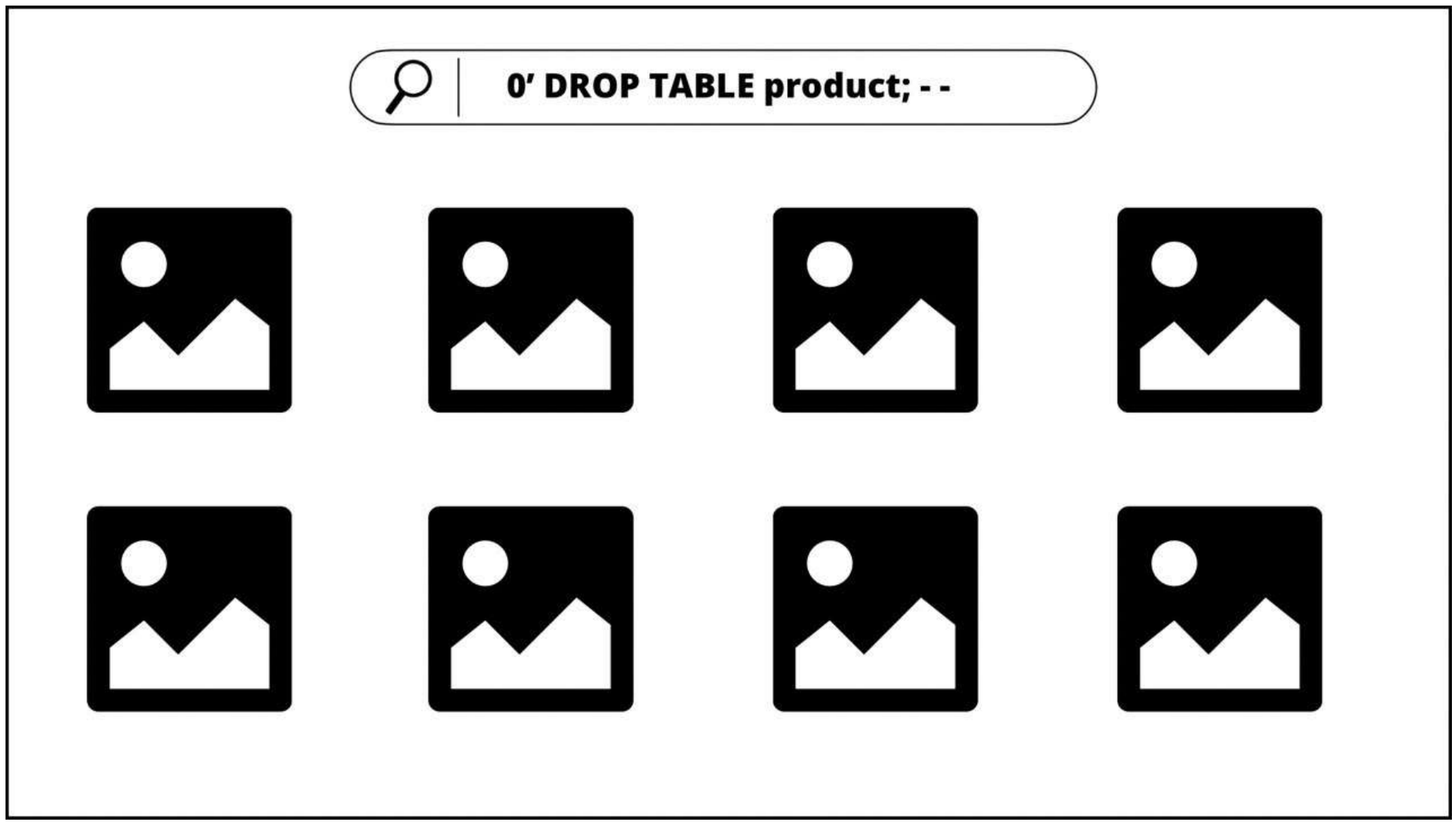
a.santangelo18@studenti.unisa.it

Introduzione e Background

Query:

“SELECT * FROM product WHERE categoria = **0’ DROP TABLE product; - -**

Esempio:



a.santangelo18@studenti.unisa.it

Identificazione di Vulnerabilità SQL Injection tramite Taint Analysis: Analisi della Letteratura e Confronto Empirico

Angelo Santangelo

Università degli Studi di Salerno

Introduzione e Background

Come si può evitare l’attacco?

Introduzione e Background

Come si può evitare l'attacco? ⟹ **Sanificazione**

✉ a.santangelo18@studenti.unisa.it

Introduzione e Background

Come si può evitare l'attacco? ⟹ **Sanificazione**

Query:

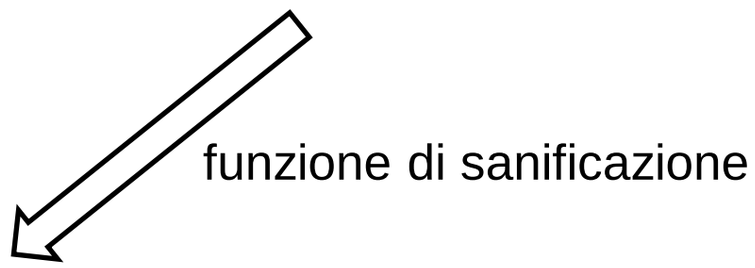
"SELECT * FROM product WHERE categoria = **0' DROP TABLE product;- -**

Introduzione e Background

Come si può evitare l'attacco? ⟹ **Sanificazione**

Query:

"SELECT * FROM product WHERE categoria = **0' DROP TABLE product;- -**



0 DROP TABLE product

✉ a.santangelo18@studenti.unisa.it

Introduzione e Background

Come si può evitare l'attacco? ⟹ **Sanificazione**

Query:
"SELECT * FROM product WHERE categoria = **0' DROP TABLE product;- -**

funzione di sanificazione

0 DROP TABLE product

Query:
"SELECT * FROM product WHERE categoria = **0 DROP TABLE product**

✉ a.santangelo18@studenti.unisa.it

Introduzione e Background

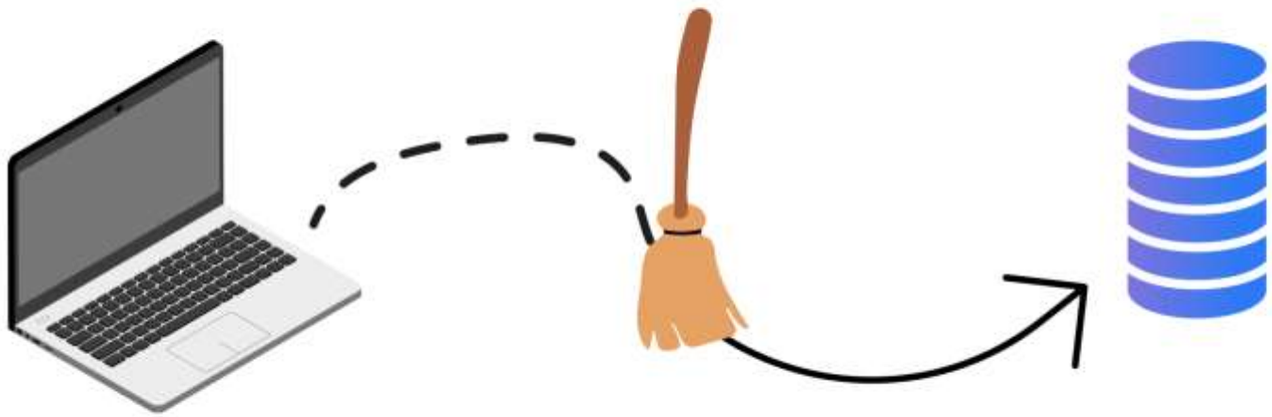
Tecnica che permette la sanificazione dell’input?

a.santangelo18@studenti.unisa.it
Angelo Santangelo
Università degli Studi di Salerno

Introduzione e Background

Tecnica che permette la sanificazione dell’input?

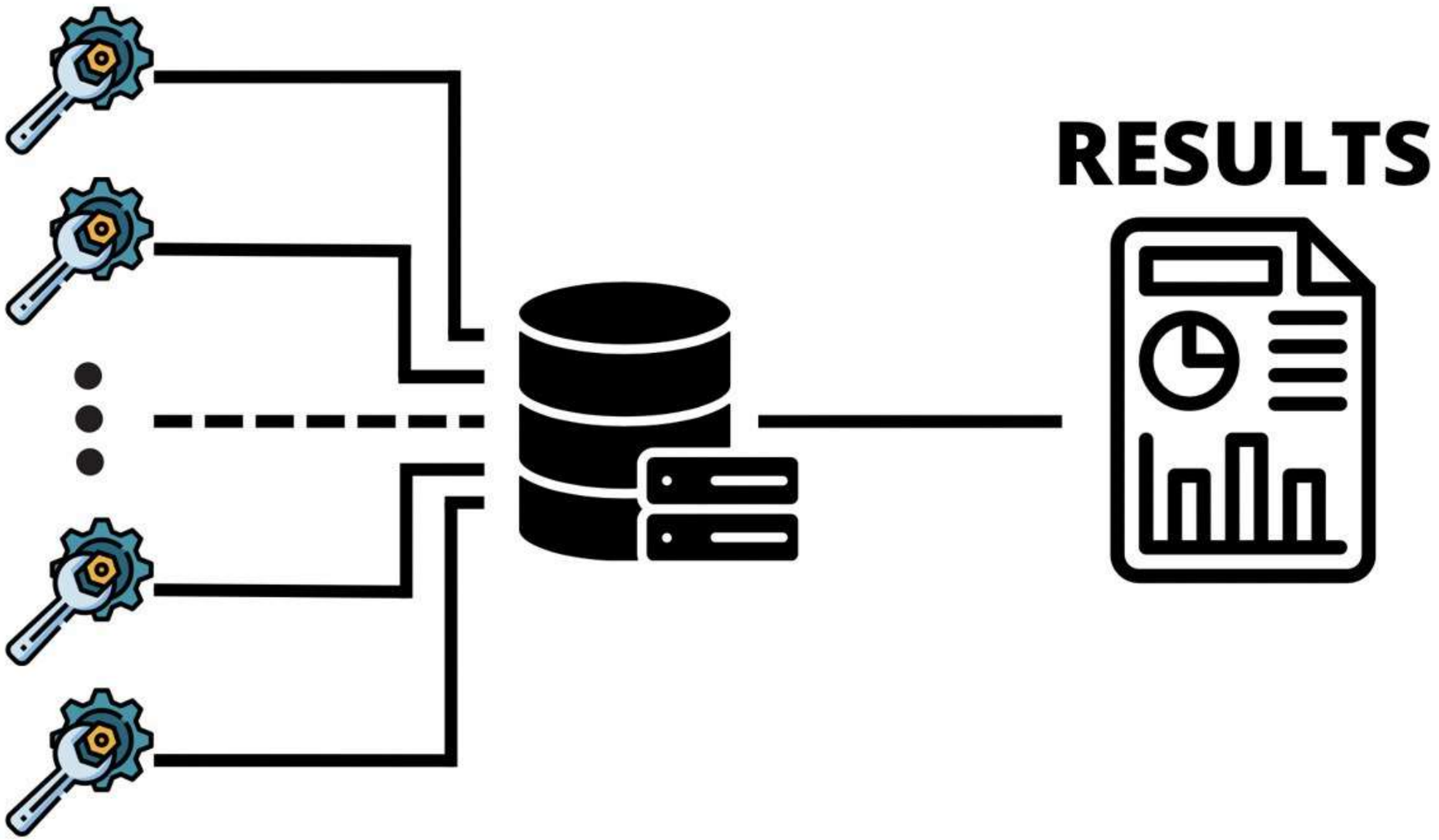
Taint Analysis:



a.santangelo18@studenti.unisa.it

Introduzione e Background

OBIETTIVO



✉ a.santangelo18@studenti.unisa.it

Identificazione di Vulnerabilità SQL Injection tramite Taint Analysis: Analisi della Letteratura e Confronto Empirico

Angelo Santangelo

Università degli Studi di Salerno

Metodologia

Query su Google Scholar, usando le seguenti keywords**:**

- Taint analysis
- SQL injection

a.santangelo18@studenti.unisa.it
Angelo Santangelo
Università degli Studi di Salerno

Metodologia

Query su Google Scholar, usando le seguenti keywords**:**

- Taint analysis
- SQL injection
- Tool – Benchmark – Suite

a.santangelo18@studenti.unisa.it
Angelo Santangelo
Università degli Studi di Salerno

Metodologia

Query su Google Scholar, usando le seguenti keywords**:**

- Taint analysis
- SQL injection
- Tool – Benchmark – Suite
- Java – PHP – Android

Angelo Santangelo
Università degli Studi di Salerno
a.santangelo18@studenti.unisa.it

Metodologia

Query su Google Scholar, usando le seguenti keywords**:**

- Taint analysis
- SQL injection
- Tool – Benchmark – Suite
- Java – PHP – Android

Numero di risultati ottenuti: **1300**

Metodologia

Query su Google Scholar, usando le seguenti keywords**:**

- Taint analysis
- SQL injection
- Tool – Benchmark – Suite
- Java – PHP – Android

Numero di risultati ottenuti: **1300**

Dopo **100** risultati, la rilevanza dei risultati diminuiva per l’obiettivo di tesi

Angelo Santangelo
Università degli Studi di Salerno
a.santangelo18@studenti.unisa.it

Metodologia

Criteri di Inclusione/Esclusione:

- [E]: non si fa menzione di SQL Injection
- [E]: non si fa menzione di Taint Analysis

Angelo Santangelo
Università degli Studi di Salerno
a.santangelo18@studenti.unisa.it

Metodologia

Criteri di Inclusione/Esclusione:

- [E]: non si fa menzione di SQL Injection
- [E]: non si fa menzione di Taint Analysis
- [I]: si presenta un tool di individuazione di SQL injection, tramite T.A.
- [I]: si presenta un dataset/benchmark

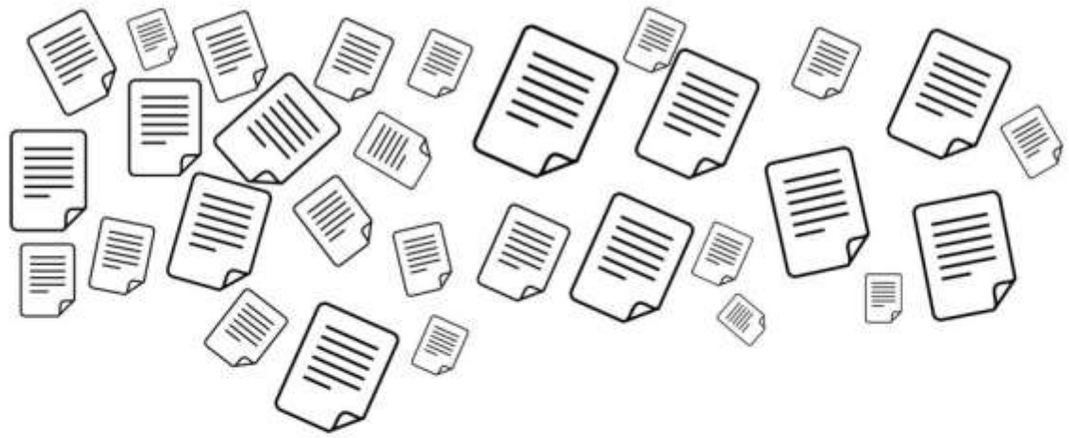
a.santangelo18@studenti.unisa.it
Angelo Santangelo
Università degli Studi di Salerno

Metodologia

Criteri di Inclusione/Esclusione:

- [E]: non si fa menzione di SQL Injection
- [E]: non si fa menzione di Taint Analysis
- [I]: si presenta un tool di individuazione di SQL injection, tramite T.A.
- [I]: si presenta un dataset/benchmark

Numero di risultati ottenuti: **30**



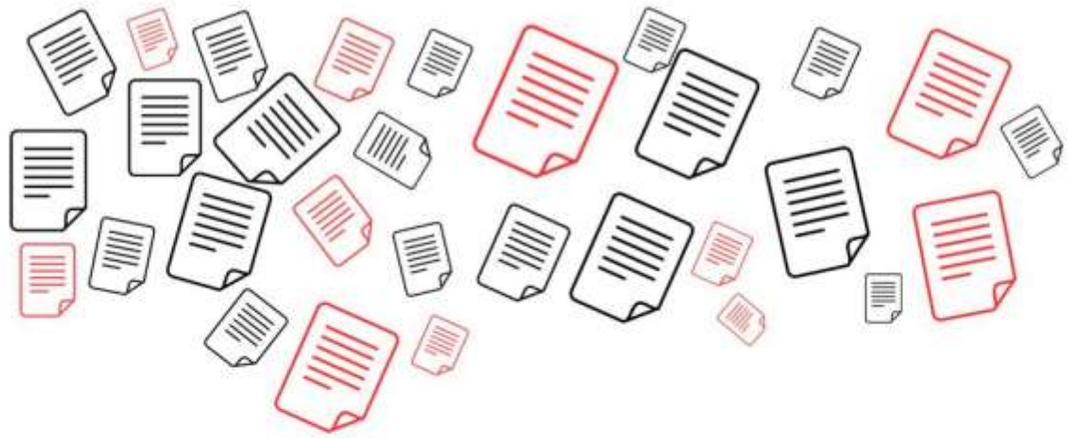
Angelo Santangelo
Università degli Studi di Salerno
a.santangelo18@studenti.unisa.it

Metodologia

Criteri di Inclusione/Esclusione:

- [E]: non si fa menzione di SQL Injection
- [E]: non si fa menzione di Taint Analysis
- [I]: si presenta un tool di individuazione di SQL injection, tramite T.A.
- [I]: si presenta un dataset/benchmark

Risultati rilevanti (a valle della lettura completa): **19**



a.santangelo18@studenti.unisa.it

Risultati

Domande di Ricerca:

- [**RQ1.1**]: quali tool esistono?

a.santangelo18@studenti.unisa.it

Risultati

Domande di Ricerca:

- [**RQ1.1**]: quali tool esistono?
- [**RQ1.2**]: quali sono i benchmark/dataset rilevati?

Angelo Santangelo
Università degli Studi di Salerno
a.santangelo18@studenti.unisa.it

Risultati

Domande di Ricerca:

- [**RQ1.1**]: quali tool esistono?
- [**RQ1.2**]: quali sono i benchmark/dataset rilevati?
- [**RQ2.1**]: che grado di eseguibilità/usabilità hanno i tool?

a.santangelo18@studenti.unisa.it
Angelo Santangelo
Università degli Studi di Salerno

Risultati

Domande di Ricerca:

- [**RQ1.1**]: quali tool esistono?
- [**RQ1.2**]: quali sono i benchmark/dataset rilevati?
- [**RQ2.1**]: che grado di eseguibilità/usabilità hanno i tool?
- [**RQ2.2**]: come sono le prestazioni dei tool?

a.santangelo18@studenti.unisa.it
Angelo Santangelo
Università degli Studi di Salerno

Risultati

Risultati del processo di Literature Review

RQ1.1 – Analisi dei Tool Esistenti

- Numero di tool identificati: **14**

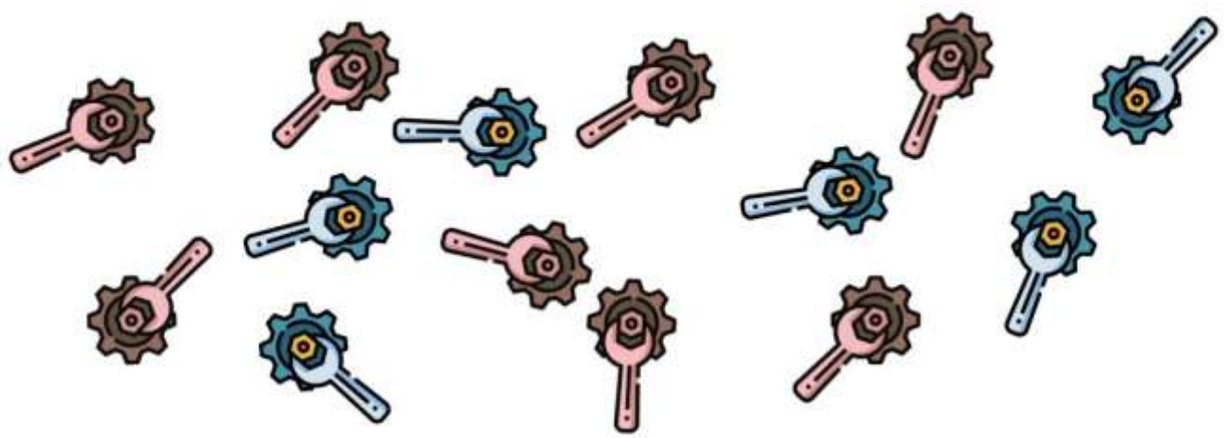
a.santangelo18@studenti.unisa.it

Risultati

Risultati del processo di Literature Review

RQ1.1 – Analisi dei Tool Esistenti

- Numero di tool disponibili online: **6**



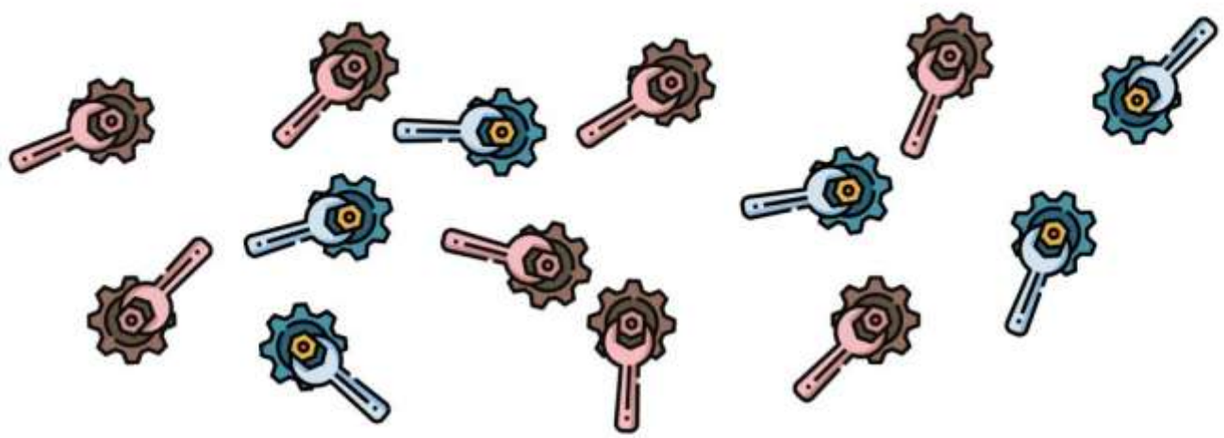
a.santangelo18@studenti.unisa.it

Risultati

Risultati del processo di Literature Review

RQ1.1 – Analisi dei Tool Esistenti

- Numero di tool disponibili online: **6**



RQ1.2 – Analisi dei Benchmark/Dataset Esistenti

- Numero di benchmark identificati e disponibili online: **4**

✉ a.santangelo18@studenti.unisa.it

Risultati Esecuzione Tool sui Benchmark

RQ2.1 – Usabilità / Eseguibilità dei Tool

3 Tool risultati eseguibili:

- SQL-Scan
- WAP
- RIPS

a.santangelo18@studenti.unisa.it
Angelo Santangelo
Università degli Studi di Salerno

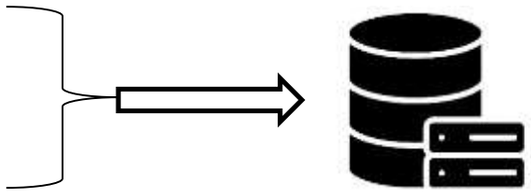
Risultati

Risultati Esecuzione Tool sui Benchmark

RQ2.1 – Usabilità / Eseguibilità dei Tool

3 Tool risultati eseguibili:

- SQL-Scan
- WAP
- RIPS



PHP-Vulnerability-Test-Suite

a.santangelo18@studenti.unisa.it

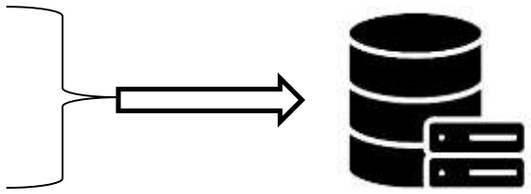
Risultati

Risultati Esecuzione Tool sui Benchmark

RQ2.1 – Usabilità / Eseguibilità dei Tool

3 Tool risultati eseguibili:

- SQL-Scan
- WAP
- RIPS



PHP-Vulnerability-Test-Suite

- **8.640** istanze **NO SQL Injection**
- **912** istanze **SÌ SQL Injection**

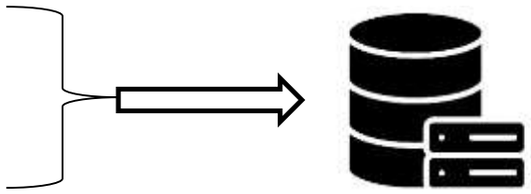
Risultati

Risultati Esecuzione Tool sui Benchmark

RQ2.1 – Usabilità / Eseguibilità dei Tool

3 Tool risultati eseguibili:

- SQL-Scan
- WAP
- RIPS



PHP-Vulnerability-Test-Suite

- **8.640** istanze **NO SQL Injection**
- **912** istanze **SÌ SQL Injection**

9.552

✉ **a.santangelo18@studenti.unisa.it**

Risultati

RQ2.2 – Prestazioni dei Tool

	WAP	RIPS
Precision	12%	15%
Recall	14%	22%
Accuracy	82%	81%
F1 - score	13%	16%
Tempo di esecuzione	1 ora e 18 minuti	43,705 secondi

a.santangelo18@studenti.unisa.it

Risultati

RQ2.2 – Prestazioni dei Tool

	WAP	RIPS
Precision	12%	15%
Recall	14%	22%
Accuracy	82%	81%
F1 - score	13%	16%
Tempo di esecuzione	1 ora e 18 minuti	43,705 secondi

WAP

RIPS

a.santangelo18@studenti.unisa.it

Risultati

RQ2.2 – Prestazioni dei Tool

	WAP	RIPS
Precision	12%	15%
Recall	14%	22%
Accuracy	82%	81%
F1 - score	13%	16%
Tempo di esecuzione	1 ora e 18 minuti	43,705 secondi

WAP  **RIPS** ⟹ **RIPS** 

✉ a.santangelo18@studenti.unisa.it

Identificazione di Vulnerabilità SQL Injection tramite Taint Analysis: Analisi della Letteratura e Confronto Empirico

Angelo Santangelo

Università degli Studi di Salerno

Conclusioni

COMMENTI

Documentazione chiara e semplificare (ridurre) il processo di installazione e configurazione del tool.

SVILUPPI FUTURI

Creazione di un modello di Machine Learning che decreti il vincitore.

Università degli Studi di Salerno

DIPARTIMENTO DI INFORMATICA

Corso di Laurea Triennale in Informatica

Anno accademico 2022/2023

Identificazione di Vulnerabilità SQL Injection tramite Taint Analysis: Analisi della Letteratura e Confronto Empirico

Grazie per l'attenzione!

Angelo Santangelo

a.santangelo18@studenti.unisa.it