ITS Academy
Adriano
Olivetti

Tecnico Superiore “Tecnico superiore per lo sviluppo software, web e l'analisi dei dati - Software & Web Developer”
BIENNIO 2024-26

[Rif. Pa 2024-22900/RER - CUP E61J24000820007]

approvata con Del. di Giunta Regionale DGR 1670/2024 del 29/07/2024 -
DD 19065/2024 del 17/09/2024 finanziata da FSE+ 2. Istruzione e formazione

Prova TEORICO-PRATICA

(minimo 24 punti - massimo 40 punti)

AMBITO [Architetture e infrastrutture per i sistemi di comunicazione]

Ferrara 16/07/2026

Dossier di lavoro di Andrea Melchiori

Brief di progetto	**Introduzione** La società SecureNet Cloud ha subito una serie di tentativi di intrusione. Il tuo compito è realizzare una Dashboard di Analisi Incidenti che legga un file di log in formato JSON, visualizzi le minacce in modo chiaro e utilizzi una logica di "Suggerimento AI" per fornire contromisure immediate al team di sicurezza.

	Queste le richieste, suddivise in task:
Task 1	Elaborazione Dati (Il "Motore" PHP) Dato il seguente set di dati JSON (simulato) per popolare la tua applicazione: [{"id": "EVT-001", "ip": "192.168.1.45", "tipo": "Brute Force", "pericolo": "Alto", "stato": "Rilevato", "data": "2026-03-26 08:30:12"}, {"id": "EVT-002", "ip": "10.0.0.12", "tipo": "SQL Injection", "pericolo": "Critico", "stato": "Bloccato", "data": "2026-03-26 09:15:45"}, {"id": "EVT-003", "ip": "172.16.254.1", "tipo": "Port Scanning", "pericolo": "Basso", "stato": "Monitorato", "data": "2026-03-26 09:40:00"}, {"id": "EVT-004", "ip": "185.220.101.34", "tipo": "DDoS Attack", "pericolo": "Critico", "stato": "Bloccato", "data": "2026-03-26 10:05:22"}, {"id": "EVT-005", "ip": "192.168.1.112", "tipo": "XSS Payload", "pericolo": "Medio", "stato": "Rilevato", "data": "2026-03-26 10:12:10"}, {"id": "EVT-006", "ip": "5.45.201.12", "tipo": "Malware Callback", "pericolo": "Alto", "stato": "Isolato", "data": "2026-03-26 10:25:55"}, {"id": "EVT-007", "ip": "10.0.5.88", "tipo": "Unauthorized Login", "pericolo": "Alto", "stato": "Rilevato", "data": "2026-03-26 10:45:30"}, {"id": "EVT-008", "ip": "88.150.12.4", "tipo": "Data Exfiltration", "pericolo": "Critico", "stato": "Bloccato", "data": "2026-03-26 11:00:01"}, {"id": "EVT-009", "ip": "192.168.1.200", "tipo": "Local Privilege Escalation", "pericolo": "Alto", "stato": "Rilevato", "data": "2026-03-26 11:15:18"}, {"id": "EVT-010", "ip": "172.16.0.5", "tipo": "ARP Spoofing", "pericolo": "Basso", "stato": "Monitorato", "data": "2026-03-26 11:30:44"}, {"id": "EVT-011", "ip": "45.33.22.11", "tipo": "Botnet Activity", "pericolo": "Medio", "stato": "Rilevato", "data": "2026-03-26 11:45:00"}, {"id": "EVT-012", "ip": "10.0.0.254", "tipo": "SSH Tunneling", "pericolo": "Alto", "stato": "Bloccato", "data": "2026-03-26 12:05:12"}, {"id": "EVT-013", "ip": "192.168.10.15", "tipo": "Phishing Link Click", "pericolo": "Medio", "stato": "Rilevato", "data": "2026-03-26 12:20:33"}, {"id": "EVT-014", "ip": "91.210.10.44", "tipo": "Credential Stuffing", "pericolo": "Alto", "stato": "Isolato", "data": "2026-03-26 12:40:55"}, {"id": "EVT-015", "ip": "172.16.254.10", "tipo": "Dictionary Attack", "pericolo": "Basso", "stato": "Bloccato", "data": "2026-03-26 13:00:10"}] Richiesta: Decodifica il JSON in PHP e crea una tabella che mostri gli incidenti. Logica Colore: Se il pericolo è "Critico", la riga deve lampeggiare o avere un bordo rosso marcato.

Task 2	Crea una sezione della dashboard chiamata "AI Security Consultant". - Quando l'utente clicca su un incidente, il sistema deve generare un "Consiglio AI" automatico. - Esempio di logica da implementare (Switch/If): *Se il tipo è Brute Force → Suggerire: "Attivare 2FA e blocco IP dopo 3 tentativi". Se il tipo è SQL Injection → Suggerire: "Utilizzare Prepared Statements (PDO) e sanitizzare gli input".
Task 3	- Realizza una dashboard Responsive con una barra laterale di navigazione. - Inserisci un grafico (anche statico o realizzato con CSS) che mostri la percentuale di minacce bloccate rispetto a quelle solo rilevate. - Area Prompt: Aggiungi un campo di testo dove l'analista può scrivere un comando per "Chiedere all'AI" un approfondimento su un IP specifico.
Task 4	- Generazione PDF Incident Report: Il sistema deve generare un PDF professionale che riassuma l'incidente selezionato, includendo l'indirizzo IP dell'attaccante e il consiglio tecnico generato dall'AI. - Security Lock: L'accesso alla dashboard è consentito solo tramite la password: Admin_Secure_2026.
Quesito 1	Perché è più efficiente scambiare dati tra un server Cloud e una Dashboard usando il formato JSON rispetto a un semplice file di testo o XML?
Quesito 2	Nel caso dell'incidente "SQL Injection" rilevato nel log, spiega come l'utilizzo di PDO in PHP avrebbe potuto prevenire l'attacco alla radice.
Durata	5 ore Inizio ore 9,00 - Termine ore 14,00
Risorse tecnologiche a disposizione delle candidate / dei candidati	File Json – esempio chiamata Ai – credenziali FTP – Filezilla – Visual Studio
Modalità di consegna degli elaborati	Consegnare in formato ZIP l'elaborato scritto con le domande e l'applicativo. Utilizzare PHP – Javascript – Java - Html

ITS Academy Adriano Olivetti

Svolgimento della prova

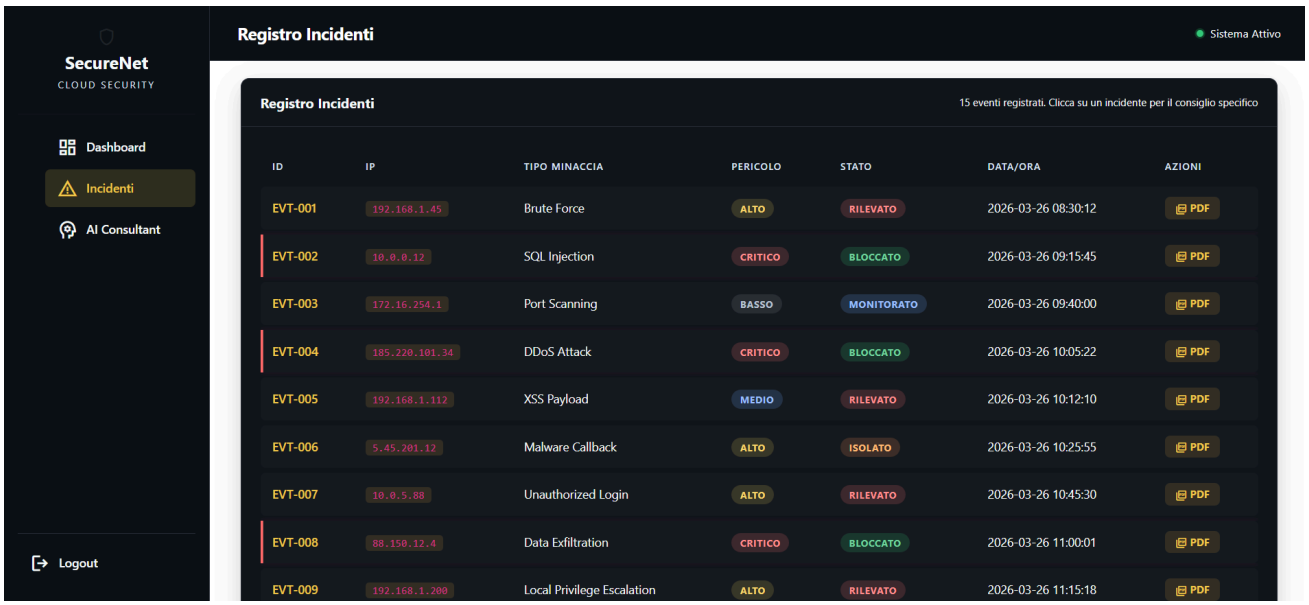
Task 1

Elaborazione Dati (Il "Motore" PHP)
Dato il seguente set di dati JSON (simulato) per popolare la tua applicazione:


```
[
  {"id": "EVT-001", "ip": "192.168.1.45", "tipo": "Brute Force", "pericolo": "Alto", "stato": "Rilevato", "data": "2026-03-26 08:30:12"},
  {"id": "EVT-002", "ip": "10.0.0.12", "tipo": "SQL Injection", "pericolo": "Critico", "stato": "Bloccato", "data": "2026-03-26 09:15:45"},
  {"id": "EVT-003", "ip": "172.16.254.1", "tipo": "Port Scanning", "pericolo": "Basso", "stato": "Monitorato", "data": "2026-03-26 09:40:00"},
  {"id": "EVT-004", "ip": "185.220.101.34", "tipo": "DDoS Attack", "pericolo": "Critico", "stato": "Bloccato", "data": "2026-03-26 10:05:22"},
  {"id": "EVT-005", "ip": "192.168.1.112", "tipo": "XSS Payload", "pericolo": "Medio", "stato": "Rilevato", "data": "2026-03-26 10:12:10"},
  {"id": "EVT-006", "ip": "5.45.201.12", "tipo": "Malware Callback", "pericolo": "Alto", "stato": "Isolato", "data": "2026-03-26 10:25:55"},
  {"id": "EVT-007", "ip": "10.0.5.88", "tipo": "Unauthorized Login", "pericolo": "Alto", "stato": "Rilevato", "data": "2026-03-26 10:45:30"},
  {"id": "EVT-008", "ip": "88.150.12.4", "tipo": "Data Exfiltration", "pericolo": "Critico", "stato": "Bloccato", "data": "2026-03-26 11:00:01"},
  {"id": "EVT-009", "ip": "192.168.1.200", "tipo": "Local Privilege Escalation", "pericolo": "Alto", "stato": "Rilevato", "data": "2026-03-26 11:15:18"},
  {"id": "EVT-010", "ip": "172.16.0.5", "tipo": "ARP Spoofing", "pericolo": "Basso", "stato": "Monitorato", "data": "2026-03-26 11:30:44"},
  {"id": "EVT-011", "ip": "45.33.22.11", "tipo": "Botnet Activity", "pericolo": "Medio", "stato": "Rilevato", "data": "2026-03-26 11:45:00"},
  {"id": "EVT-012", "ip": "10.0.0.254", "tipo": "SSH Tunneling", "pericolo": "Alto", "stato": "Bloccato", "data": "2026-03-26 12:05:12"},
  {"id": "EVT-013", "ip": "192.168.10.15", "tipo": "Phishing Link Click", "pericolo": "Medio", "stato": "Rilevato", "data": "2026-03-26 12:20:33"},
  {"id": "EVT-014", "ip": "91.210.10.44", "tipo": "Credential Stuffing", "pericolo": "Alto", "stato": "Isolato", "data": "2026-03-26 12:40:55"},
  {"id": "EVT-015", "ip": "172.16.254.10", "tipo": "Dictionary Attack", "pericolo": "Basso", "stato": "Bloccato", "data": "2026-03-26 13:00:10"}
]
```


Richiesta: Decodifica il JSON in PHP e crea una tabella che mostri gli incidenti.
Logica Colore: Se il pericolo è "Critico", la riga deve lampeggiare o avere un bordo rosso marcato.

Inserire screenshot della Tabella: Un'immagine della dashboard che mostri gli incidenti caricati, evidenziando la logica colore (bordo rosso o effetto lampeggiante) per gli eventi CRITICI



ITS Academy
Adriano
Olivetti

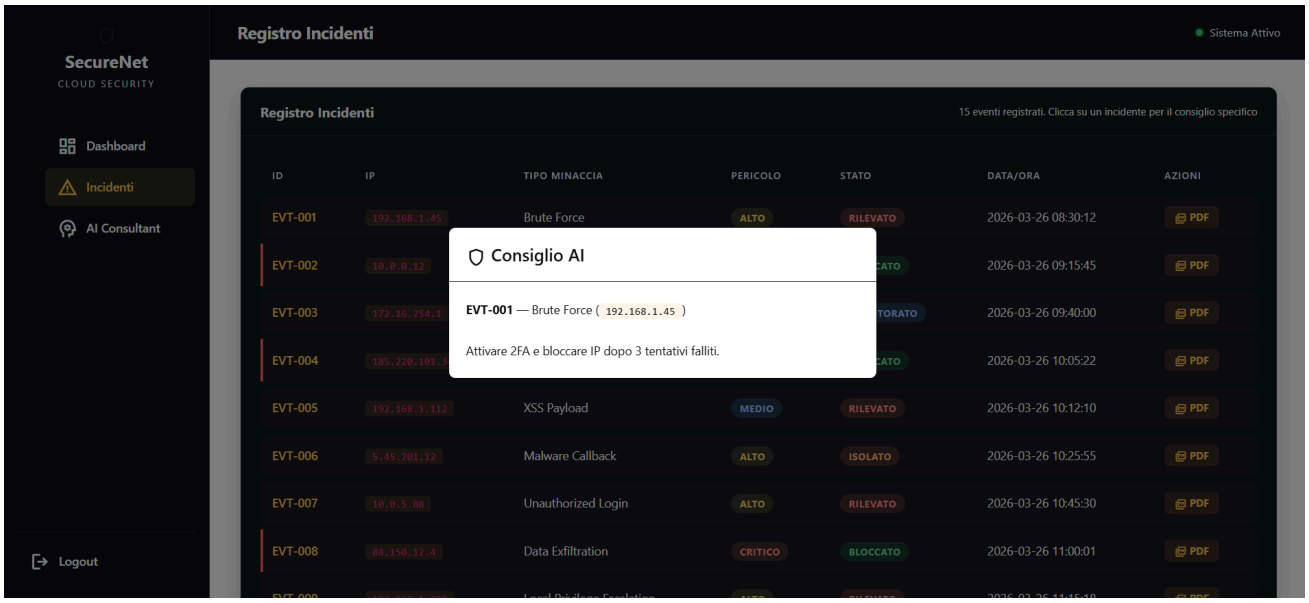
Task 2

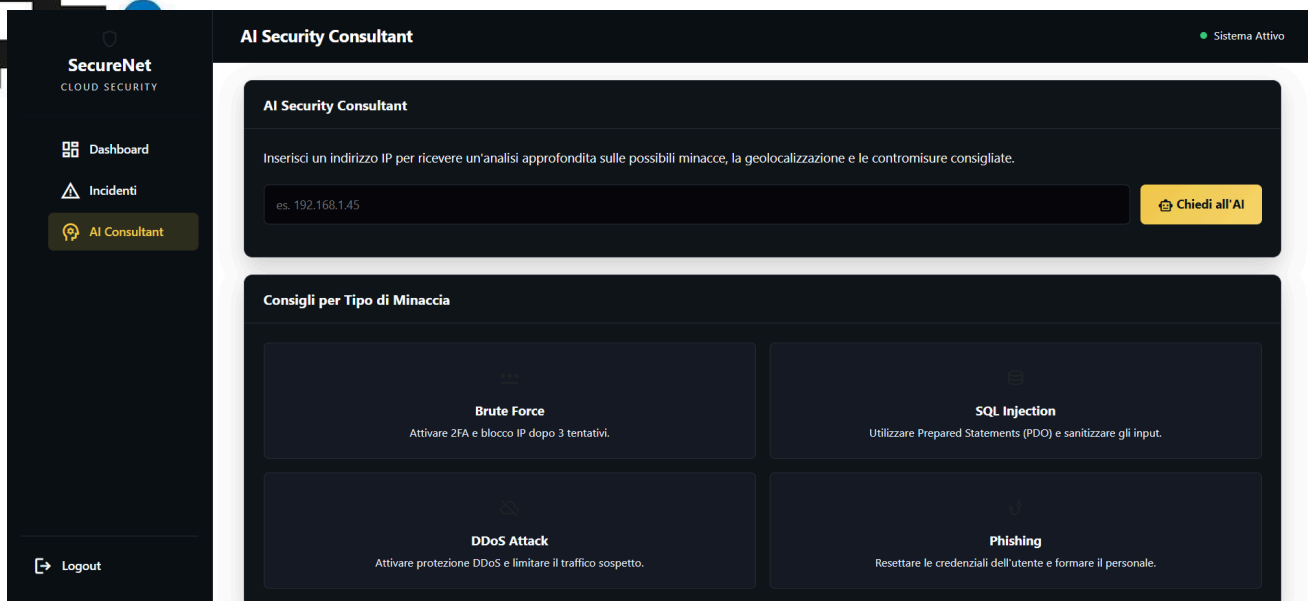
Crea una sezione della dashboard chiamata "AI Security Consultant".

- Quando l'utente clicca su un incidente, il sistema deve generare un "Consiglio AI" automatico.
- Esempio di logica da implementare (Switch/If): *Se il tipo è Brute Force → Suggerire: "Attivare 2FA e blocco IP dopo 3 tentativi".

  Se il tipo è SQL Injection → Suggerire: "Utilizzare Prepared Statements (PDO) e sanitizzare gli input".

Inserire un'immagine che mostri cosa succede quando si clicca su un incidente e come appare il box "AI Security Consultant" con il consiglio generato

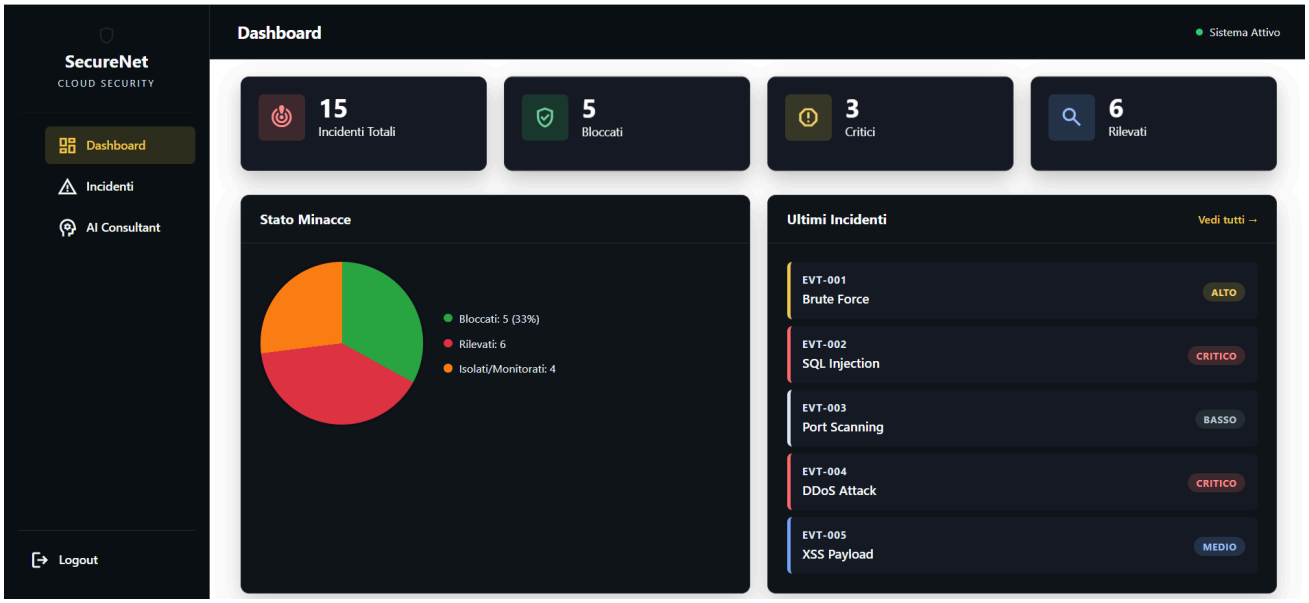



SecureNet
CLOUD SECURITY
Dashboard
Incidenti
AI Consultant
Logout
AI Security Consultant
Sistema Attivo
AI Security Consultant
Inserisci un indirizzo IP per ricevere un'analisi approfondita sulle possibili minacce, la geolocalizzazione e le contromisure consigliate.
es. 192.168.1.45
Chiedi all'AI
Consigli per Tipo di Minaccia
Brute Force
Attivare 2FA e blocco IP dopo 3 tentativi.
SQL Injection
Utilizzare Prepared Statements (PDO) e sanitizzare gli input.
DDoS Attack
Attivare protezione DDoS e limitare il traffico sospetto.
Phishing
Resettare le credenziali dell'utente e formare il personale.

Task 3

- Realizza una dashboard Responsive con una barra laterale di navigazione.
- Inserisci un grafico (anche statico o realizzato con CSS) che mostri la percentuale di minacce bloccate rispetto a quelle solo rilevate.
- Area Prompt: Aggiungi un campo di testo dove l'analista può scrivere un comando per "Chiedere all'AI" un approfondimento su un IP specifico.

Inserire screenshot della Dashboard Completa: Una vista d'insieme che mostri la barra laterale di navigazione e il layout adattivo



Task 4

- Generazione PDF Incident Report: Il sistema deve generare un PDF professionale che riassuma l'incidente selezionato, includendo l'indirizzo IP dell'attaccante e il consiglio tecnico generato dall'AI.
- Security Lock: L'accesso alla dashboard è consentito solo tramite la password: Admin_Secure_2026.

Inserire un'immagine o una scansione del report PDF professionale prodotto dal sistema, contenente l'ID incidente, l'IP dell'attaccante e il consiglio dell'AI.

Inserire anche il frammento di codice (es. gestione sessione o controllo POST) che verifica la password

ITS Academy
Adriano
Olivetti

SecureNet Cloud - Incident Report

ID Incidente: EVT-001

IP Attaccante: 192.168.1.45

Tipo di Minaccia: Brute Force

Livello di Pericolo: Alto

Stato: Rilevato

Data/Ora: 2026-03-26 08:30:12

Contromisure Immediate Consigliate

Attivare 2FA e blocco IP dopo 3 tentativi.

Analisi e Contromisure (AI)

Analisi dell'incidente

Tipo di minaccia: Brute Force
Indirizzo IP: 192.168.1.45
Livello di pericolo: Alto
Stato: Rilevato

Spiegazione della minaccia:
Un attacco Brute Force è un tipo di attacco informatico in cui un aggressore tenta di accedere a un sistema o a un'applicazione utilizzando una combinazione di username e password ripetutamente, sperando di riuscire a indovinare la combinazione corretta. Questo tipo di attacco può essere lanciato utilizzando strumenti di attacco specifici o software di cracking.

Impatto potenziale:
Un attacco Brute Force può avere un impatto significativo sulla sicurezza del sistema o dell'applicazione colpiti. Se l'aggressore riesce ad accedere al sistema o

```
```php
if ($_SERVER['REQUEST_METHOD'] === 'POST' && isset($_POST['password'])) {
    if ($_POST['password'] === DASHBOARD_PASSWORD) {
        $_SESSION['logged_in'] = true;
        header('Location: ' . $_SERVER['PHP_SELF']);
        exit;
    } else {
        $error = 'Password errata';
    }
}
```
```

ITS Academy
Adriano
Olivetti

Quesito 1

JSON è più efficiente perché: - è leggero e veloce da elaborare, molto più di XML - si legge facilmente sia da persone che da programmi - è nativo in JavaScript e ben supportato in PHP, quindi si integra subito con una dashboard - gestisce oggetti, array e valori senza tag inutili, a differenza di XML Rispetto a un file di testo, JSON organizza i dati con chiavi e valori chiari. Rispetto a XML, è più compatto e richiede meno codice per essere letto e scritto. In un ambiente Cloud questo si traduce in meno banda usata, tempi di risposta più rapidi e dashboard più facili da sviluppare.

ITS Academy
Adriano
Olivetti

Quesito 2

PDO previene la SQL Injection usando le query parametriche: invece di scrivere l'input dell'utente direttamente dentro la query, uso un placeholder (`?`) e passo il valore dopo, separatamente. ```php $stmt = $pdo->prepare("SELECT * FROM utenti WHERE username = ?"); $stmt->execute([$username]); ```
Così anche se qualcuno prova a mettere qualcosa come `' OR 1=1 --`, viene trattato solo come testo da cercare, non come comando SQL. Praticamente: - separa il codice SQL dai dati - blocca input malevoli che vorrebbero modificare la query - rende il tutto più sicuro senza troppo sforzo

Candidata/o [Nome e Cognome a stampatello]

……

Firma

……