

Piattaforma di Voto online

Autore: NemoSec

Data di pubblicazione: 12/09/2017

NOTA: SE SI VUOLE TESTARE IL PROGRAMMA, CAMBIARE LE STRINGHE DI CONNESSIONE NEL CODICE

Questo progetto mira a presentare un sistema di voto elettronico.

Lo scopo di questo progetto è presentare una piattaforma di voto che sia Sicura, Segreta e Libera, per questo è stato scelto un modello a codice aperto.

Il codice aperto permette a chiunque di poter verificare cosa fa il programma e, per garantire la sicurezza e la segretezza, si è scelto per operare tramite programma scollegato dal server centrale.

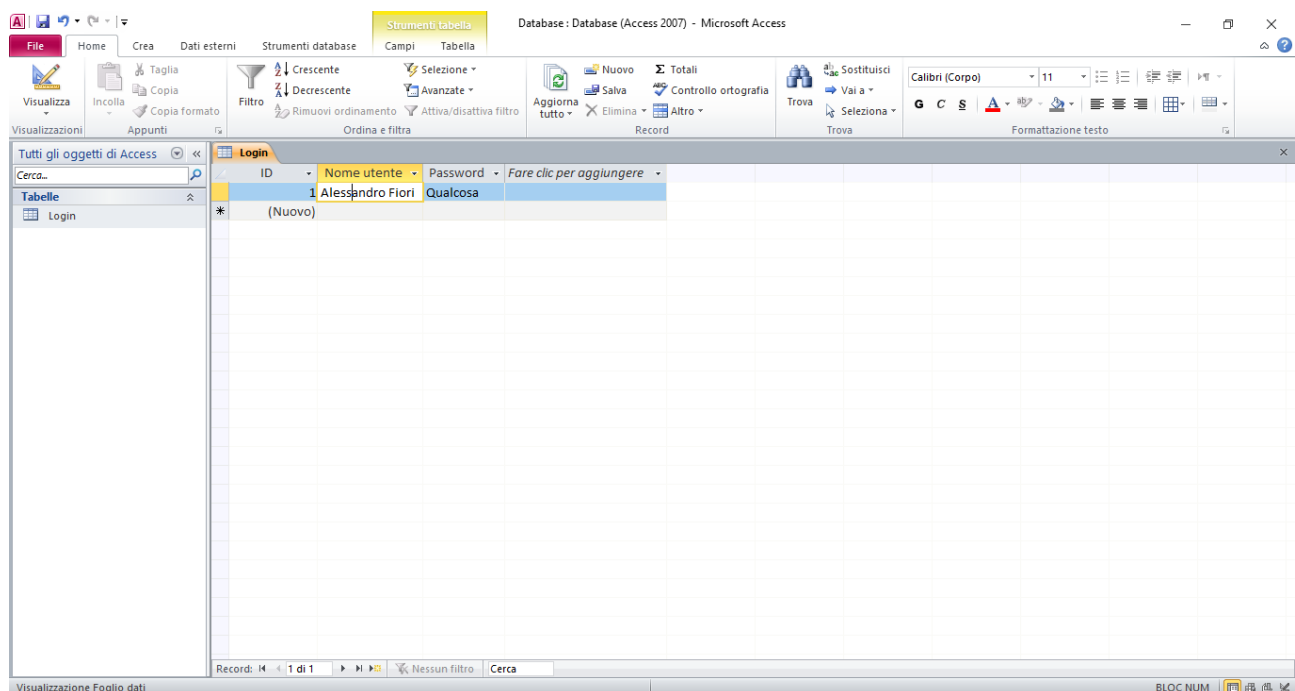
Vediamo, quindi, in cosa consiste questo software e cosa fa, partendo dal Database.

Il Database è un Access, pur sapendo che non è adatto per situazioni mission critical.

Questo perché, in caso si voglia utilizzare la piattaforma, si deve semplicemente cambiare il DB a cui punta il software, quindi questa versione è completa, ma OVVIAMENTE è un esempio di come funziona, e in caso modificarlo secondo le esigenze.

Il linguaggio di programmazione scelto per lo sviluppo è VB.NET, in futuro saranno disponibili esempi in molteplici linguaggi.

La prima tabella che analizziamo è la tabella Login:



ID	Nome utente	Password	Fare clic per aggiungere
1	Alessandro Fiori	Qualcosa	
(Nuovo)			

Questa tabella viene utilizzata dall'applicazione in fase di Login.

Applicazione: Aperta l'applicazione per la votazione online, si presenta davanti questa schermata:

Nome Utente:

Password:

Login

Il sistema di login può essere collegato ad altre piattaforme o Database, a seconda delle esigenze, in questo caso è collegato alla tabella “Login” contenuta nel database.

Il programma, effettua una prima connessione con il sistema di Login, solo ed esclusivamente per capire se l’utente che sta votando sia esistente oppure no.

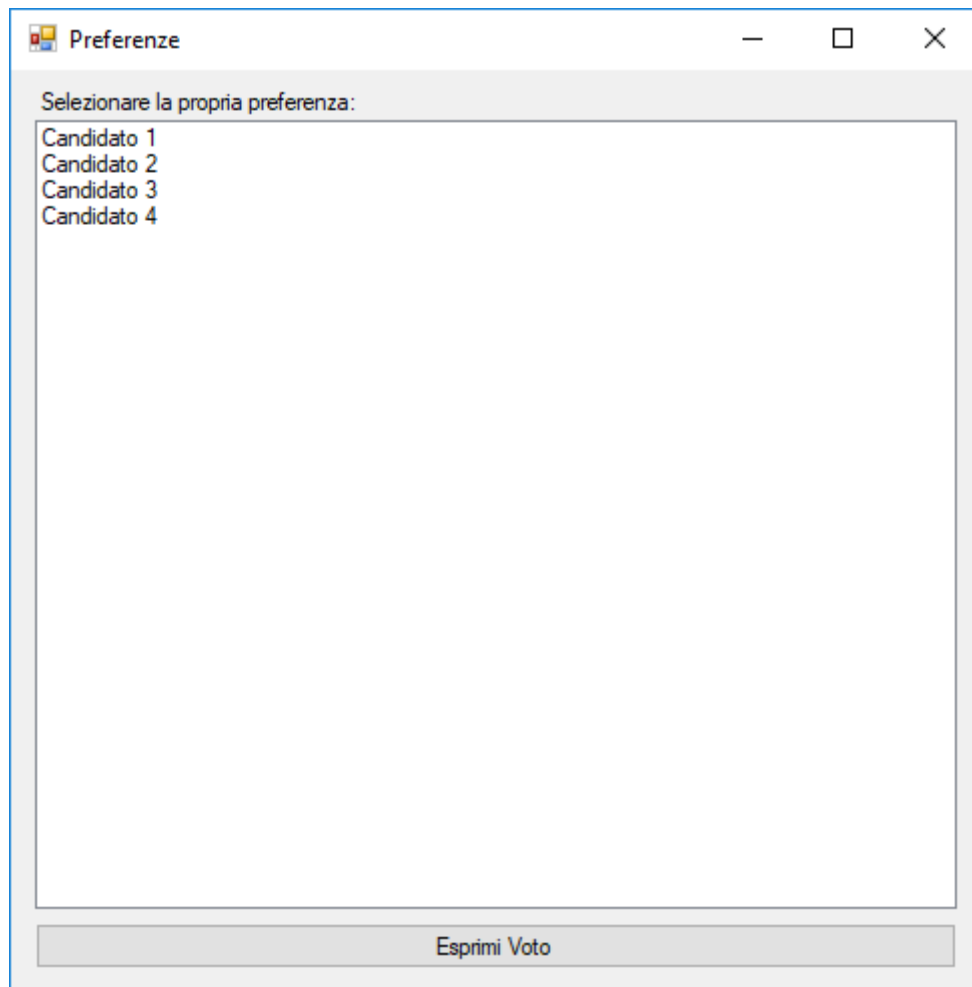
Questo rispecchia una specie di “cabina elettorale elettronica”, cioè questo è il momento in cui il cittadino va a votare e consegna la propria carta di identità.

Non appena il programma riconosce l’effettiva esistenza del cittadino, scarica dalla tabella “preferenze”, le preferenze disponibili al cittadino, un po’ come se, dopo aver consegnato la carta di identità, al cittadino fosse consegnata la scheda elettorale, e fosse nella cabina elettorale.

Lato Database, la tabella si presenta in questo modo:

ID	Preferenza	Fare clic per aggiungere
1	Candidato 1	
2	Candidato 2	
3	Candidato 3	
*	(Nuovo)	

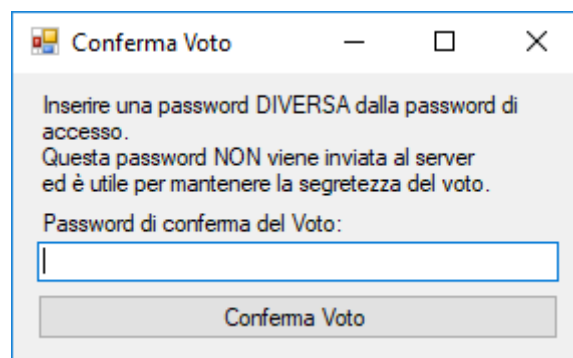
Questa è la schermata che appare al caricamento delle preferenze, il programma in questa fase effettua una seconda connessione al database:



Una volta selezionata la preferenza, il cittadino clicca su “Esprimi Voto”.

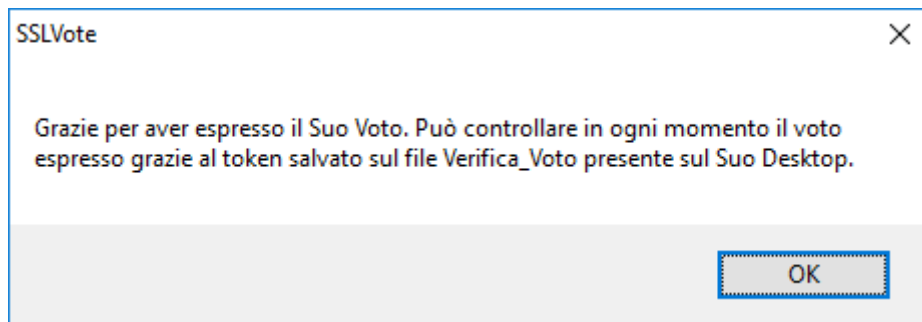
Il programma apre una maschera di conferma, chiedendo di inserire una password per generare un token il quale può essere utilizzato dall’utente per verificare il proprio voto.

Tale password non è la password di accesso al programma, la password non viene inviata al server.



Nel momento in cui l’utente conferma il proprio Voto, viene inserito il suo voto cifrato nella tabella delle votazioni e il proprio nome utente tra i votanti che hanno già espresso il voto.

Questo è il messaggio di conferma:



Il Database si presenta in questo modo:

Tabella Voti:

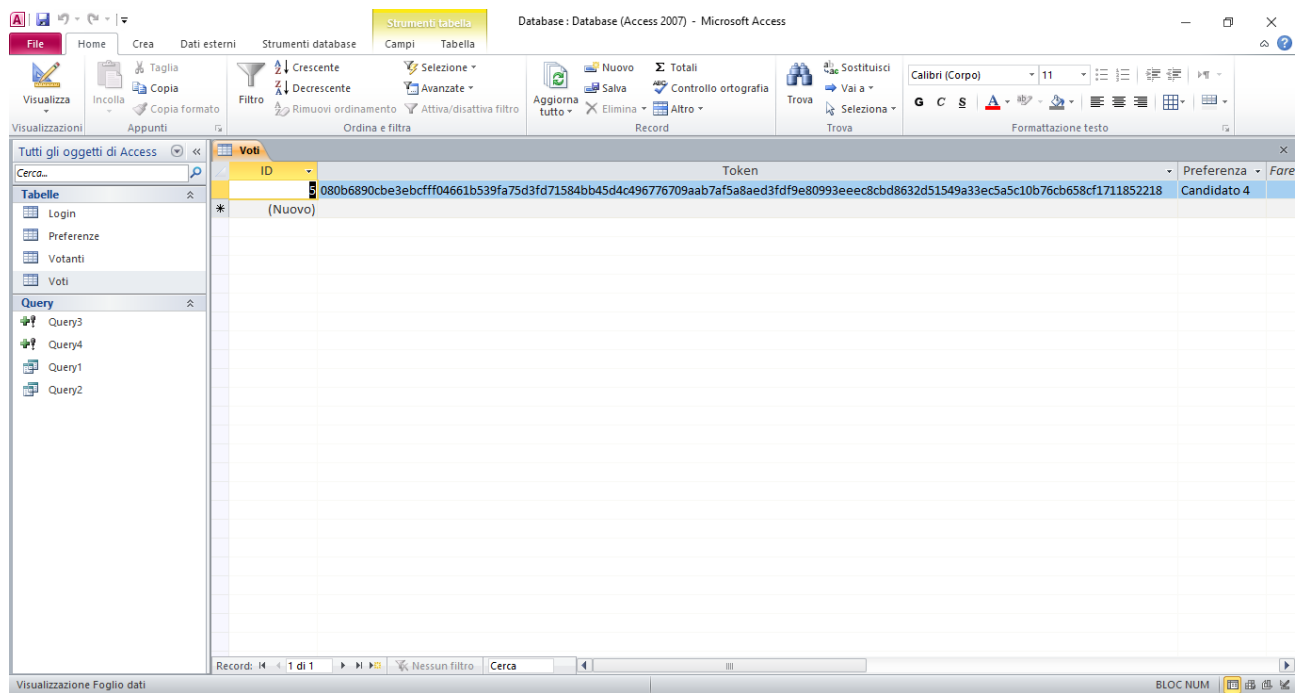
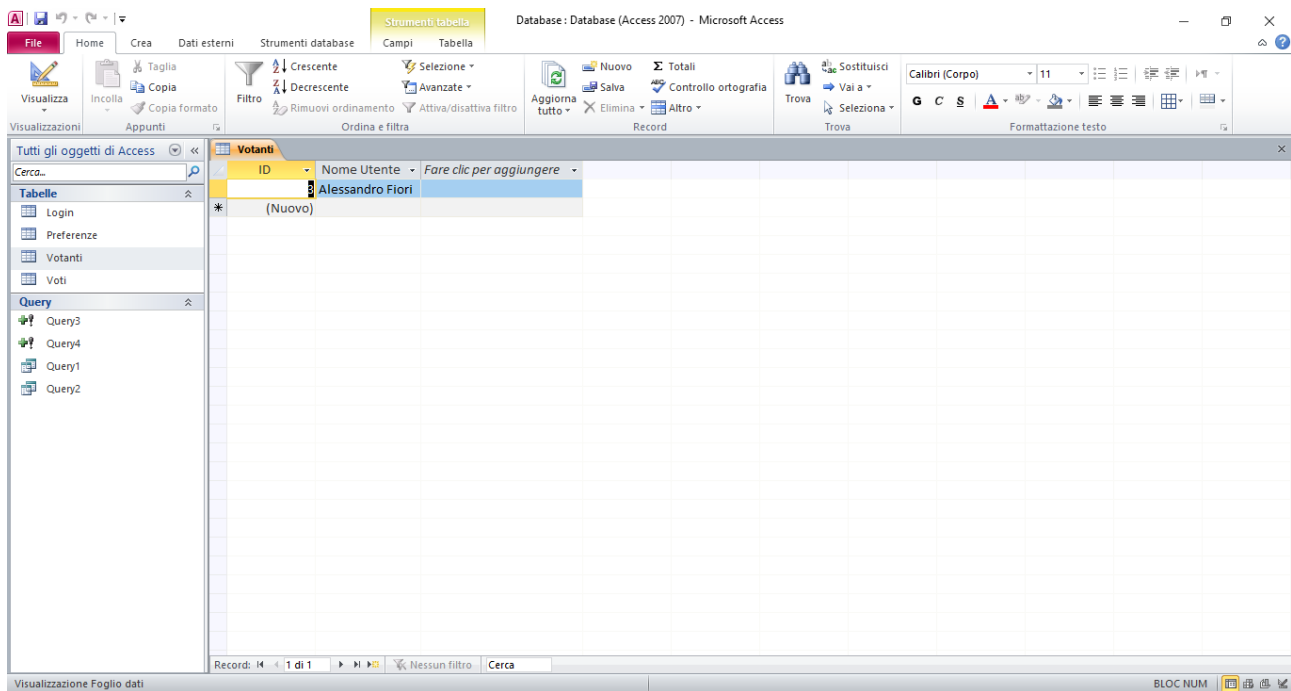
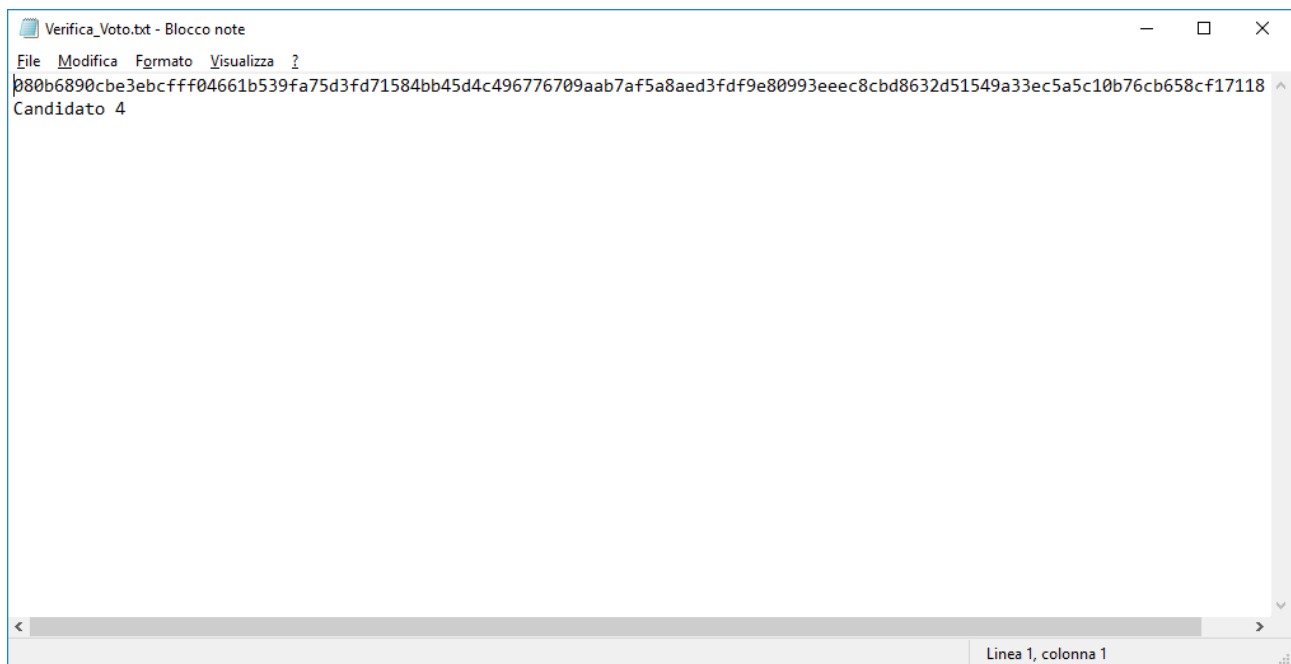


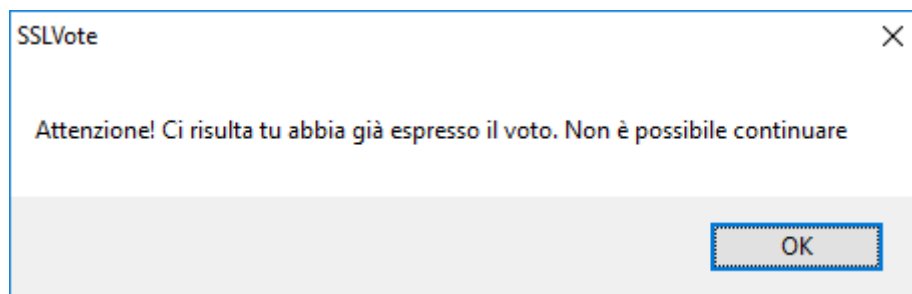
Tabella Votanti:



Così si presenta il file di Verifica Voto:



Nel caso in cui l'utente provasse a rivotare, il programma rifiuterebbe in quanto il nome utente è già presente nella tabella dei Votanti.



In sintesi:

Il programma simula a tutti gli effetti il funzionamento di una cabina elettorale.

Nome utente e password iniziale – L'Utente virtualmente si presenta al seggio, se ha già votato non può rivotare, altrimenti gli viene "consegnata" la scheda elettorale (la lista delle preferenze).

Una volta selezionata la preferenza è come se l'utente avesse segnato con la matita la propria preferenza, la password che genera il token rappresenta la scheda elettorale chiusa.

Il database registra il token+preferenza e il nome utente in due tabelle separate, senza registrare nessun altro dato, questo impedisce la profilazione dell'utente e quindi capire cosa ha votato.

Il token serve all'utente per verificare in qualunque momento, su eventuale sito web (questa funzione arriverà direttamente su programma in versioni future o verrà rilasciato un sito web di prova) o su programma la propria selezione, quindi può controllare la propria votazione, funzione impossibile attualmente con le cabine elettorali fisiche.

Le connessioni effettuate sono le seguenti:

Verifica le credenziali (Lettura – Attualmente le credenziali non hanno hash, è solo per prova)

Verifica voto (Lettura)

Lettura preferenze (Lettura)

Scrittura Voto (Scrittura)

Scrittura nome utente votante (Scrittura)

Tutte le operazioni di hash, operazioni interne ecc. (come anche evincibile da codice) sono operate internamente al programma, quindi sul PC dell'utente, questo per garantire il massimo della trasparenza.

E' attualmente in sviluppo un software anche per effettuare controlli incrociati e certificare le attività di Voto.

Contatti, suggerimenti, segnalazioni bug ecc.:

Alessandro Fiori – a.fiori@nemosec.com

Alessandro La Malfa - a.lamalfa@nemosec.com

NemoSec