Luca Antognarelli   
Alessio Panizzieri

**  
WEB  
SHOP**

**Indice**

* [Descrizione della piattaforma](#Descrizione_piattaforma)
* [Progettazione del database](#Progettazione_database)
  + [Specifiche](#Specifiche)
  + [Schema concettuale](#Schema_concettuale)
  + [Schema logico](#Schema_logico)
* [Funzionamento della piattaforma e query](#Funzionamento_piattaforma_query)
  + [Registrazione](#Registrazione)
  + [Login](#Login)
  + [Home page](#Home_page)
  + [Acquisto](#Acquisto)
  + [Modifica](#Modifica)
  + [Inserimento](#Inserimento)
  + [Profilo](#Profilo)

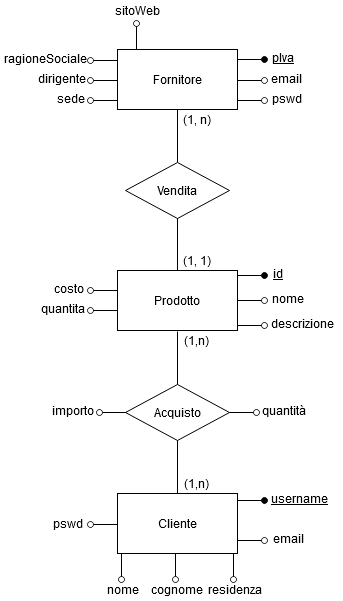
**Descrizione della piattaforma**

L’idea che c’è dietro alla piattaforma ‘A&P web shop’ è quella di realizzare una piattaforma di compravendita tra fornitori e clienti.  
Ogni fornitore, identificato univocamente dalla propria Partita IVA, produce una certa quantità di prodotti e li mette in vendita sulla piattaforma ad un determinato prezzo.  
Ogni cliente, identificato univocamente dal proprio username utilizzato al momento della registrazione, può consultare la piattaforma visualizzando tutti i prodotti disponibili e decidere di acquistarne uno o più in maniera semplice e veloce.  
Clienti e fornitori per poter usufruire dei servizi offerti dalla piattaforma dovranno registrarsi mediante email (che non potrà essere la stessa per più clienti e/o fornitori) e password; i clienti dovranno inoltre scegliere un username univoco, indicare il proprio nome, cognome e la loro residenza; i fornitori dovranno invece indicare, oltre alla loro email e password, la ragione sociale, la sede legale, il sito web ed il nominativo del dirigente.  
Grazie alla piattaforma sarà inoltre possibile, sia per i clienti che per i fornitori, tenere traccia dei propri acquisti (o vendite nel caso dei fornitori) consultando la pagina relativa al proprio profilo, nel quale saranno contenute quindi tutte le fatture.

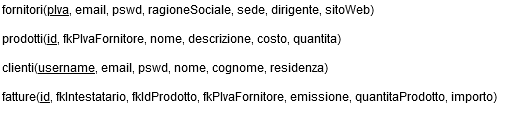
**Progettazione del database**

**Specifiche**  
Al fine della realizzazione, e successiva implementazione, della piattaforma risulta evidente la necessità di memorizzare le informazioni relative ai: clienti, fornitori e prodotti; ed individuarne le relazioni che li legano: clienti 🡪 acquisto 🡨 prodotti e prodotti 🡪 vendita 🡨 fornitori.  
Risulta inoltre necessario memorizzare permanentemente le informazioni relative alla compravendita di un prodotto, quali: l’intestatario 🡪 chi ha effettuato l’acquisto, l’emittente🡪 chi ha venduto un determinato prodotto, il prodotto acquistato, in che quantità, l’importo totale relativo (costo del prodotto \* quantità acquistata) e la data in cui è avvenuto l’atto.

**Schema concettuale**

****

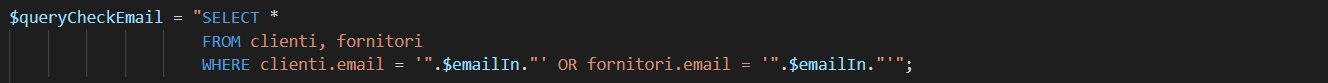
**Schema logico**

****

**Funzionamento della piattaforma e query**

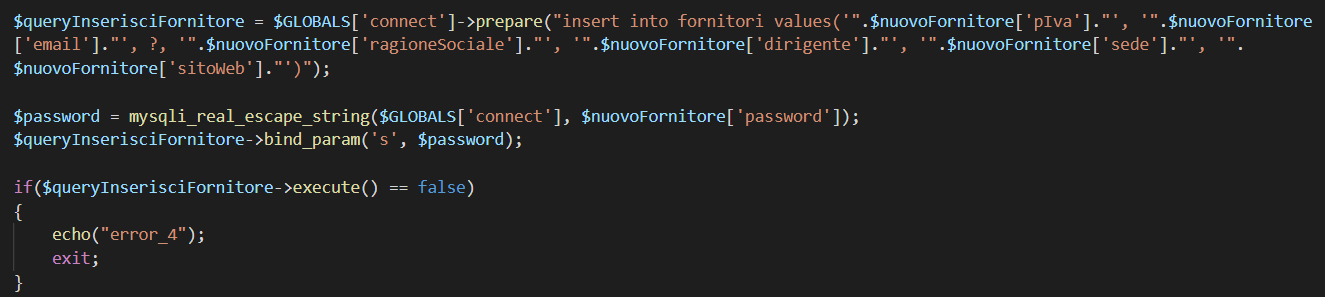
La piattaforma ‘A&P web shop’ prevede al suo interno l’esistenza di due tipologie di profili, profondamente diversi tra loro: profilo cliente e profilo fornitore.  
*Profilo cliente*: al momento della registrazione è richiesto l’inserimento: di un username che non sia già in uso, email, password ed alcuni dati personali quali: nome, cognome e residenza. Una volta effettuato il login si ha accesso alla home page della piattaforma nella quale sono presenti tutti i prodotti per cui è possibile effettuarne l’acquisto (quantità disponibile > 0) scegliendone la quantità, se dovesse essere inserita una quantità non valida verrà notificato il problema ed annullata la procedura d’acquisto. Nella pagina relativa al profilo cliente sono presenti le informazioni del cliente, con la possibilità di visualizzare tutte le fatture degli acquisti effettuati.  
*Profilo fornitore*: al momento della registrazione è richiesto l’inserimento: della partita iva, email, password ed alcuni dati relativi al fornitore quali: ragione sociale, collocamento della sede legale, nominativo del dirigente e sito web. Una volta effettuato il login si ha accesso alla home page della piattaforma nella quale sono presenti tutti i prodotti messi in vendita, con la possibilità di modificarne: nome, descrizione, costo e quantità disponibile. Nella pagina relativa al profilo fornitore sono presenti le informazioni del fornitore, con la possibilità di visualizzare tutte le fatture delle vendite effettuate.

**Registrazione**La registrazione avviene separatamente per fornitori e clienti, mediante form dedicate, con la possibilità di scelta all’apertura della pagina.  
A seguito dell’inserimento dei dati utili alla registrazione da parte di un cliente o un fornitore, questi ultimi vengono inviati al server con una particolare accortezza per la password che subisce inizialmente un’azione di crittografia basata sull’hashing, nello specifico SHA-256, e successivamente prima dell’inserimento dei dati nel db, al fine di evitare iniezioni di codice malevole, viene utilizzata una tecnica di query-prepare. Viene inoltre controllato che l’email inserita non sia già presente nella piattaforma, oltre che l’username nel caso di un cliente e della partita IVA nel caso di un fornitore.   
Seguono due delle query utilizzate:  
  
Query controllo unicità email:

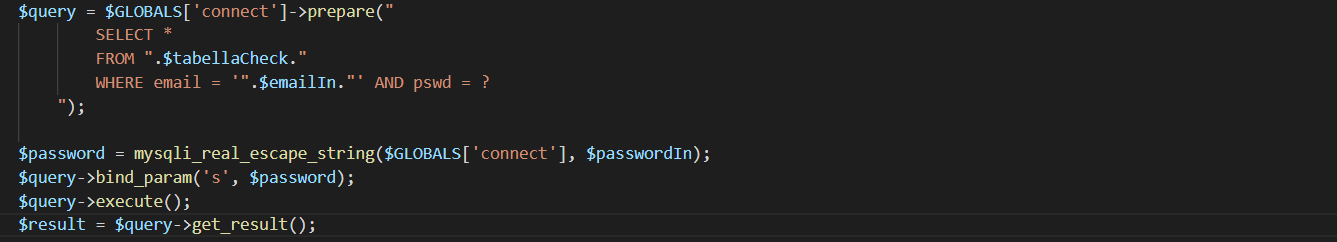


In cui $emailIn rappresenta l’email inserita al momento della registrazione.

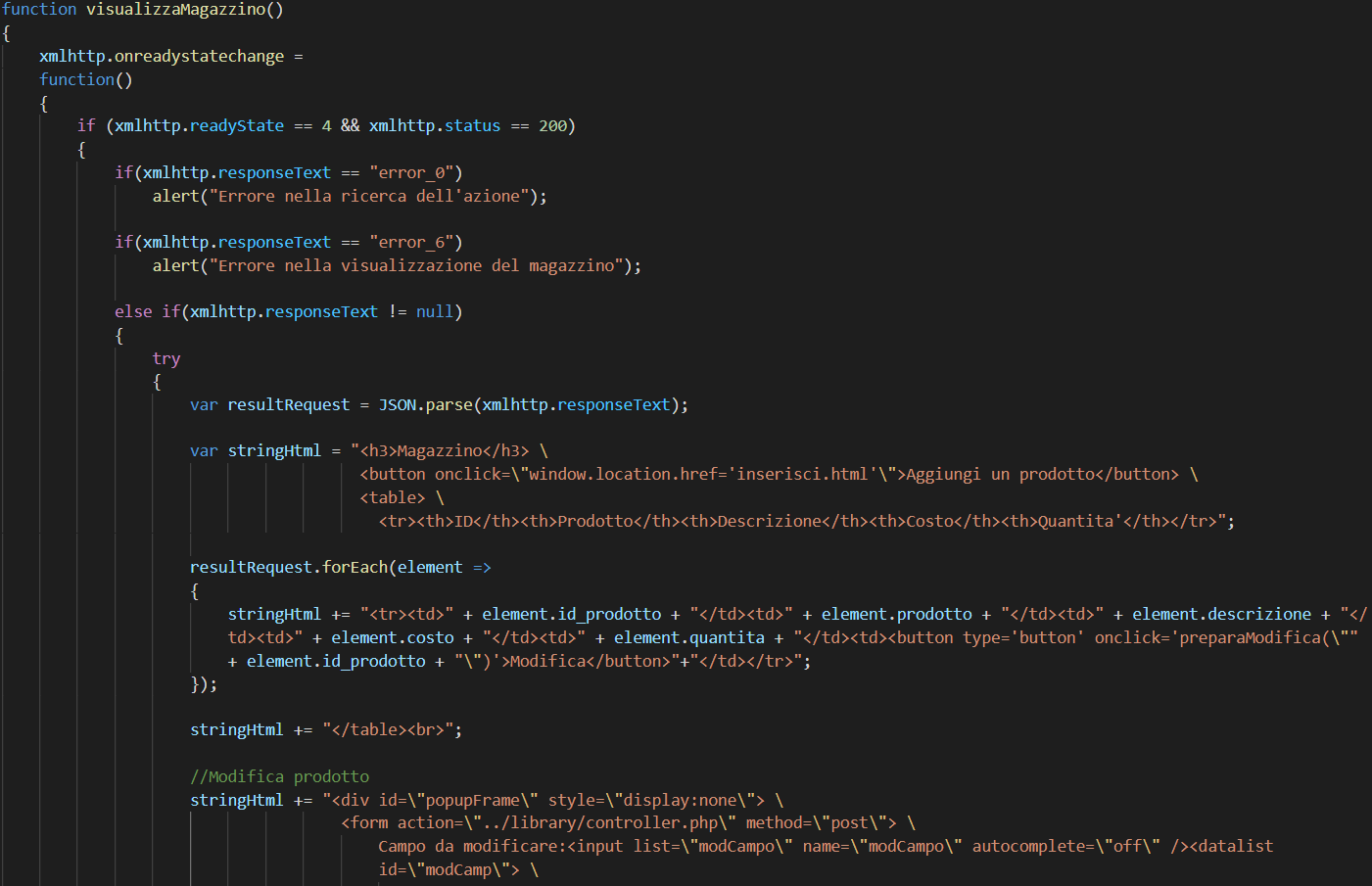
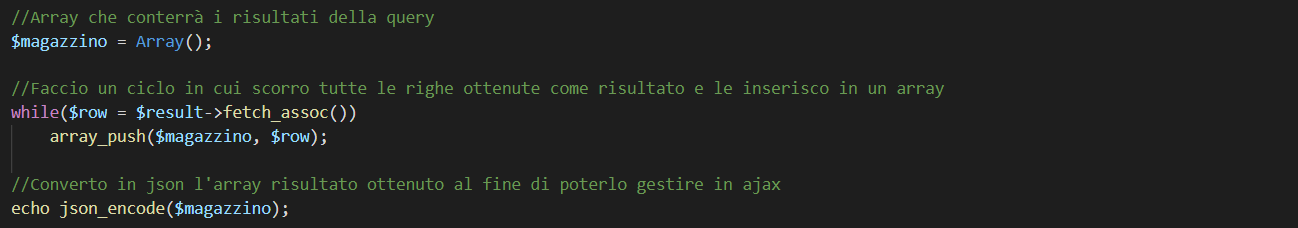
Query-prepare ed esecuzione query d’inserimento dati di un fornitore nel db:

 In cui: $GLOBALS[‘connect’] rappresenta la stringa di connessione al db, $nuovoFornitore[‘dato’] rappresenta un array associativo contenente i dati del fornitore da registrare nella piattaforma.  
Il carattere ‘?’ nella query serve per evitare azioni d’injection, viene ricostruita mediante le funzioni *myqli\_real\_escape\_string* e nello specifico *bind\_param* assegna il valore inserito per il quale si vuole evitare un’azione d’injection (password crittografata), successivamente alla ricostruzione della query viene eseguita.

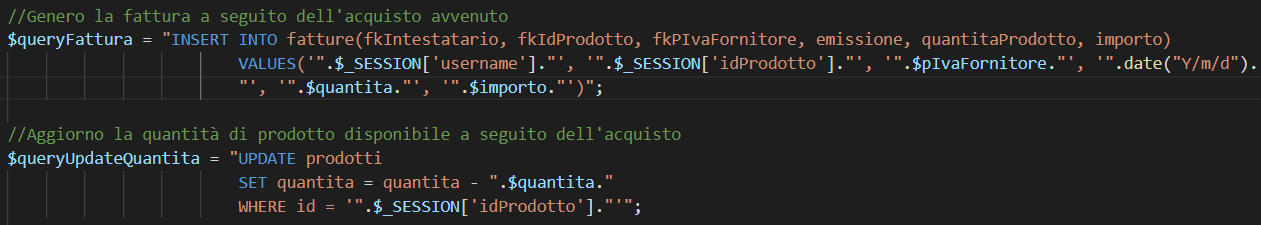
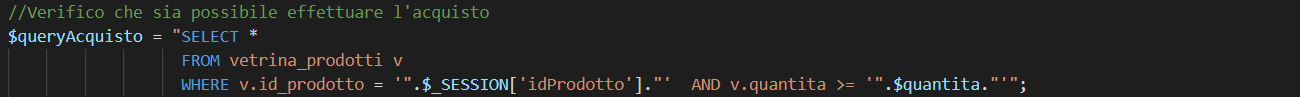
**Login**  
Avviene sia per i clienti che per i fornitori mediante l’email e la password, avendo entrambi i dati memorizzati in due tabelle differenti mediante una funzione controllo l’appartenenza dei dati inseriti ai clienti o ai fornitori, nel caso non vi fosse una corrispondenza l’utente viene invitato ad effettuare la registrazione di un nuovo account mediante il reindirizzamento presso la pagina di registrazione.  
Come per la registrazione, al fine di garantire la sicurezza della piattaforma, la password subisce una crittografia basata sull’hashing, nello specifico SHA-256 e successivamente, precedentemente l’esecuzione della query di controllo dei dati viene eseguita un’azione di query-prepare per prevenire tentativi d’injection.  
Segue la query di login:

 In cui: $tabellaCheck assume il valore ‘clienti’ se si deve effettuare il login di un cliente o ‘fornitori’ se si deve effettuare il login di un fornitore, $emailIn e $passwordIn sono l’email e la password (cifrata) inserite.  
A seconda del tipo di account loggato viene creata una sessione contenente valori utili alla gestione delle azioni di acquisto (se clienti l’username) e modifica dei prodotti (se fornitori partita iva), oltre che il tipo di utente loggato, ‘clienti’ o ‘fornitori’, e l’email, con la quale è possibile controllare se l’utente ha già effettuato il login nel caso in cui chiuda per errore la scheda non dovrà effettuare nuovamente il login; mantenere dati utili in sessione permette inoltre di gestire il caricamento dinamico delle pagine: home e profilo.

**Home page**  
Il caricamento della home page della piattaforma avviene dinamicamente attraverso uno script che utilizza la tecnologia AJAX, Asynchronous JavaScript and XML, basata su uno scambio di dati in modalità asincrona tra client e server che permette l’aggiornamento dinamico di porzioni di pagina, non interferendo quindi con eventuali altre azioni svolte dall’utente sulla pagina.  
Nel caso della home page, a seconda del tipo di account loggato, indicato dalla variabile in sessione, viene gestito il caricamento dinamico della pagina:  
*clienti*: viene visualizzato l’elenco di tutti i prodotti in vendita con le rispettive informazioni, accanto ad ognuno è presente un bottone che avvia la procedura d’acquisto, richiedendo la quantità del prodotto d’acquistare e confermando l’acquisto, se la quantità inserita è disponibile, viene notificato l’avvenuto acquisto e generata la corrispettiva fattura, che comporta la diminuzione della quantità disponibile del prodotto in accordo alla quantità acquistata.  
*fornitori*: viene visualizzato l’elenco dei prodotti in vendita appartenenti al fornitore che ha effettuato il login, accanto ad ognuno è presente un bottone che avvia la procedura di modifica. Quest’ultima si svolge inserendo in sessione l’id del prodotto, potendo così gestirne la modifica, selezionando attraverso l’apposito form il campo da modificare ed assegnandoli un nuovo valore, potendo così comporre e generare la query di modifica.  
Seguono una porzione dello script basato su AJAX che gestisce il caricamento dinamico della pagina e query di modifica:

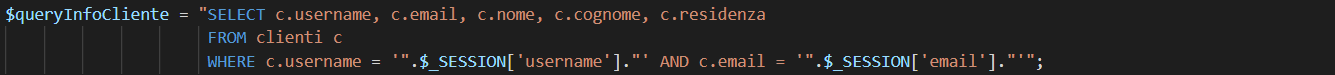
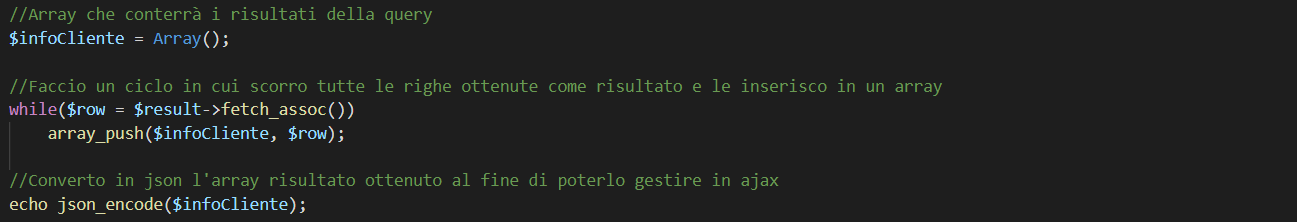
  
  
  
In cui la variabile xmlhttp è un oggetto XMLHttpdRequest che permette di gestire la comunicazione asincrona tra client e server. Attraverso *open* setto in GET l’azione da eseguire al server, così da avviare la procedura che mi porterà a comporre dinamicamente la pagina, attraverso *send* richiamo invio in GET la stringa con l’azione da eseguire al server e successivamente attraverso *readyState* e *status* controllo che la connessione al server sia andata a buon fine. Lato server in php compongo la risposta in formato JSON:   


e lato client attraverso *JSON.parse* decodifico la risposta al fine di ottenere i dati grazie ai quali nel ciclo successivo compongo dinamicamente la pagina.

**Acquisto**  
L’effettuazione di un acquisto è divisa in due parti: inizialmente il cliente sceglie il prodotto da acquistare, successivamente indicando la quantità conferma l’acquisto.  
Al momento della scelta del prodotto vengono inseriti in sessione l’id del prodotto selezionato ed il suo costo, utili alla successiva creazione della fattura e calcolo del costo complessivo.  
  
Quando l’utente indica la quantità che desidera acquistare e conferma l’acquisto viene avviata una procedura che controlla inizialmente se la quantità inserita è disponibile, se così non fosse viene notificato il problema al cliente, altrimenti viene calcolato il costo complessivo (costo \* quantità) e generata la fattura relativa all’atto di compravendita avvenuto. Ad acquisto avvenuto viene aggiornata la quantità residua disponibile del prodotto coinvolto.  
Seguono le query di generazione della fattura ed aggiornamento della quantità di prodotto disponibile:  
  
In cui $importo è dato da:  
  
Con la seguente query è avvenuto precedentemente il controllo della quantità richiesta che deve essere <= alla quantità disponibile, così da permettere l’avvio di tutta la procedura d’acquisto:  


**Modifica**  
La modifica di un prodotto da parte di un fornitore è divisa in due parti: il fornitore sceglie il prodotto da modificare, successivamente mediante l’apposito form sceglie il campo da modificare, gli assegna un nuovo valore e conferma la modifica. E’ possibile modificare qualsiasi campo eccetto l’id.  
Con la prima fase viene inserito in sessione l’id del prodotto da modificare:  
  
Con la seconda fase vengono inviati al server il campo ed il nuovo valore da assegnarlo, così da poter comporre una query dinamica per l’aggiornamento del dato del prodotto desiderato.  
Segue la query mediante la quale avviene l’aggiornamento del valore:  


**Inserimento**  
L’inserimento di un nuovo prodotto da parte di un fornitore avviene mediante una pagina ed un form dedicati. Viene richiesta la compilazione di tutti i campi previsti ed attraverso il click sul bottone viene inserito il nuovo prodotto all’interno del db.  
Segue la query d’inserimento:  


**Profilo**  
La pagina del profilo viene caricata dinamicamente a seconda della tipologia di account loggato mediante uno script in AJAX. Vengono visualizzate le informazioni relative all’account, con la possibilità inoltre di visualizzare le fatture associate all’account mediante una funzione AJAX che ne permette l’ottenimento ed inserimento all’interno della pagina.  
Segue la query d’ottenimento delle informazioni di un cliente e la composizione dei dati in formato JSON da inviare al client:  
  
  
Segue una frazione della funzione AJAX che si occupa del composizione delle informazioni da visualizzare nella pagina del profilo:  
