Colegiul Național „Octavian Goga” Marghita, Bihor



WebShop

Categoria: pagini web

Concursul național de Informatică ”InfoEducație”

2-8 aug. 2015, Gălăciuc, Vrancea

Autor: **Tincău Mihai-Gabriel**

prof. coordonator: Coraș Zenovia

Cuprins

1. Introducere
2. Despre Bitcoin
3. Prezentare generală
4. Bibliografie

Introducere

Proiectul meu este o demonstrație a unui sistem de plăți prin Bitcoin (BTC) folosind API-ul oferit de Blockchain.info. Proiectul este prezentat sub formă de website alcătuit din 6 pagini (index, products, myaccount, my orders, login & register) și a fost creat folosind PHP, aspectul site-ului fiind făcut în html/css.

Despre Bitcoin

**Bitcoin** este un sistem de plată electronic descentralizat și o monedă digital creată în 2009 de Satoshi Nakamoto. Numele Bitcoin se referă de asemenea și la programul cu sursa deschisă pentru folosirea acestor monede, cât și la rețeaua peer-to-peer (de la egal la egal) pe care acesta o formează. Spre deosebire de majoritatea monedelor, Bitcoin nu se bazează pe încrederea într-un emitent central. Bitcoin folosește o bază de date distribuită peste noduri ale unei rețele de la egal la egal (peer-to-peer) pentru a inventaria tranzacțiile și se folosește de criptografie pentru a furniza funcții de bază pentru securitate cum ar fi asigurarea că bitcoinii nu pot fi cheltuiți decât de cel care îi deține și decât o singură dată.

Construcția monedei Bitcoin permite deținerea și transferul anonim de valoare. Bitcoinii pot fi salvați pe un computer personal sub forma unui *fișier portofel* sau pot fi stocați cu un serviciu de *portofel* a unei terțe părți, iar în ambele cazuri bitcoinii pot fi trimiși prin intermediul Internetului oricărei persoane cu o *adresă Bitcoin*. Topologia de la egal la egal și lipsa unei administrații central fac nefezabil ca o autoritate, un guvern, etc. să manipuleze valoarea Bitcoinului sau să introducă inflație prin producerea lor.

Bitcoin este una din primele implementări a conceputului numit „*criptomoneda*” (crypto currency), prima dată descries în 1998 de Wei Dai pe mailing listul Cyperpunk.

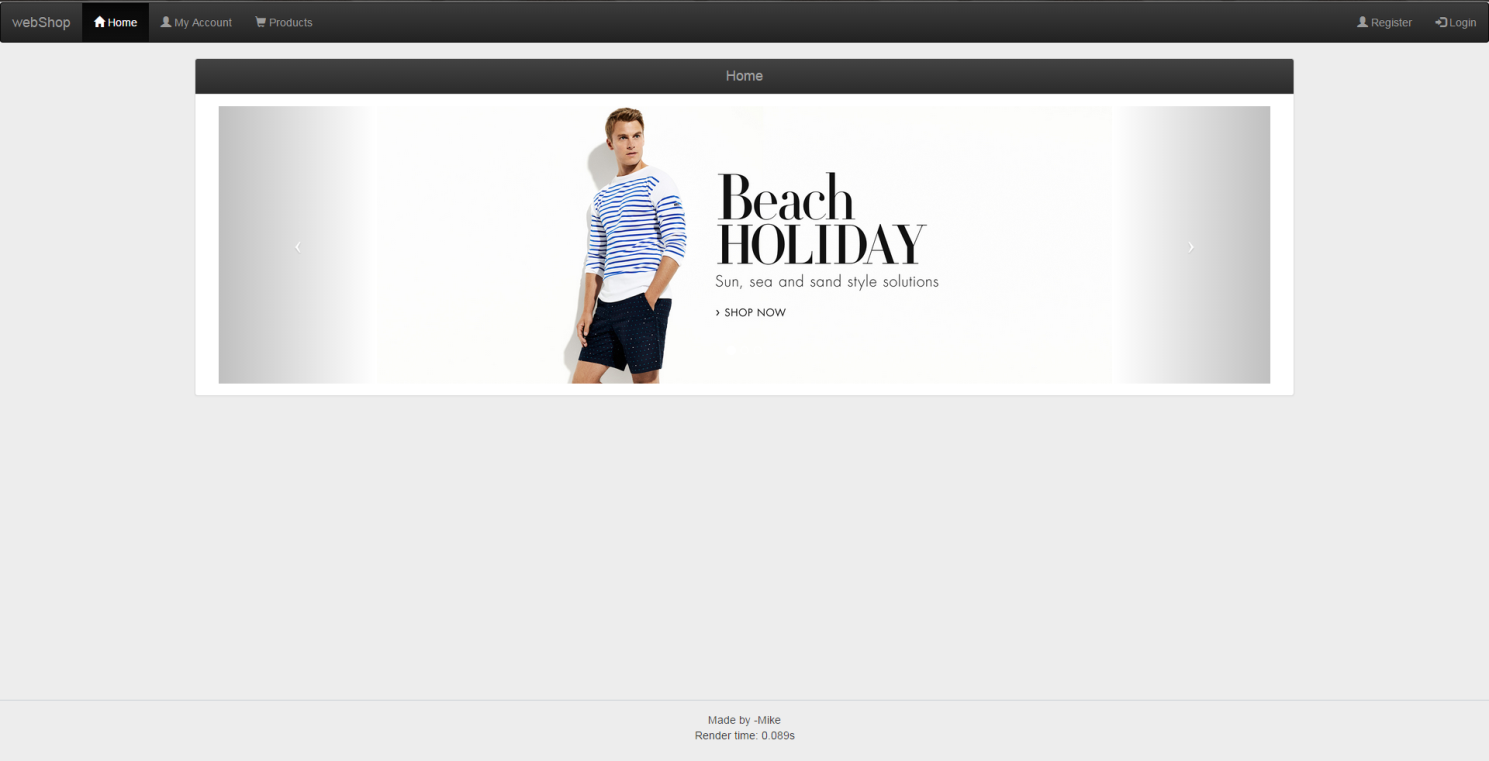
Orice persoană care participă la rețeaua bitcoin deține un portofel care conține un număr arbitrar de perechi de chei criptografice. Cheile publice sau *adrese* bitcoin funcționează ca punctul terminal de primire a tuturor plăților. Adresele nu conțin nicio informație despre deținătorul lor și sunt în general anonime. Adresele în formă care pot fi citite de om sunt șiruri de numere și litere aleatorii lungi de aproximativ 33 de caractere, întotdeauna începând cu cifra 1, de forma *175tWpb8K1S7NmH4Zx6rewF9WQrcZv245W*. Utilizatorii bitcoin pot deține multiple adrese, și de fapt pot genera noi adrese fără limite practice, deoarece generarea unei noi adrese necesită relative puțină putere computațională, echivalentul la a genera o pereche de chei public/private, și nu necesită niciun contact cu vreun nod din rețea. Crearea de adrese de unică folosință ajută la menținerea anonimatului utilizatorului.

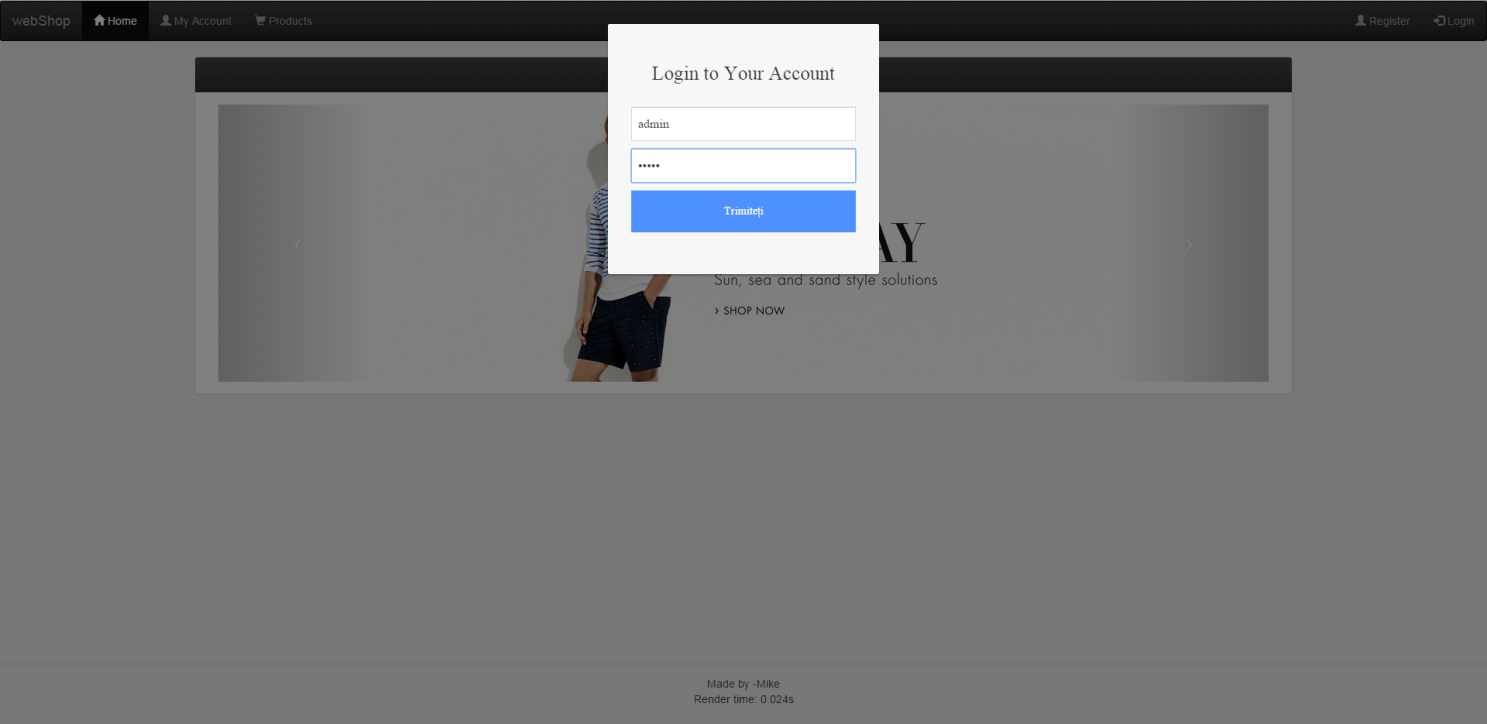
Bitcoinii conțin cheia publică a deținătorului actual (adresă). Când un utilizator *A* transferă o sumă către utilizatorul *B*, *A* renunță la proprietatea pe bitcoinii trimiși prin adăugarea cheii publice a utilizatorului *B* și semnându-i cu propria cheie privată. Acesta difuzează acești bitcoini cu un mesaj potrivit, *tranzacția*, în rețeaua bitcoin. Restul nodurilor din rețea validează semnăturile criptografice și sumele tranzacției înainte de a o accepta. Tranzacțiile sunt realizate prin intermediul unui „portofel Bitcoin” (Bitcoin wallet), o aplicație sau serviciu care se conectează la rețeaua Bitcoin și permite păstrarea și tranzacționarea monedei cu orice alt utilizator.

Prezentare generală

În crearea interfeței am apelat doar la HTML și CSS. Am folosit javascript pentru a calcula timpul luat pentru a încărca pagina, care poate fi văzut la sfârșitul paginii (în footer), iar PHP pentru restul funcțiilor.

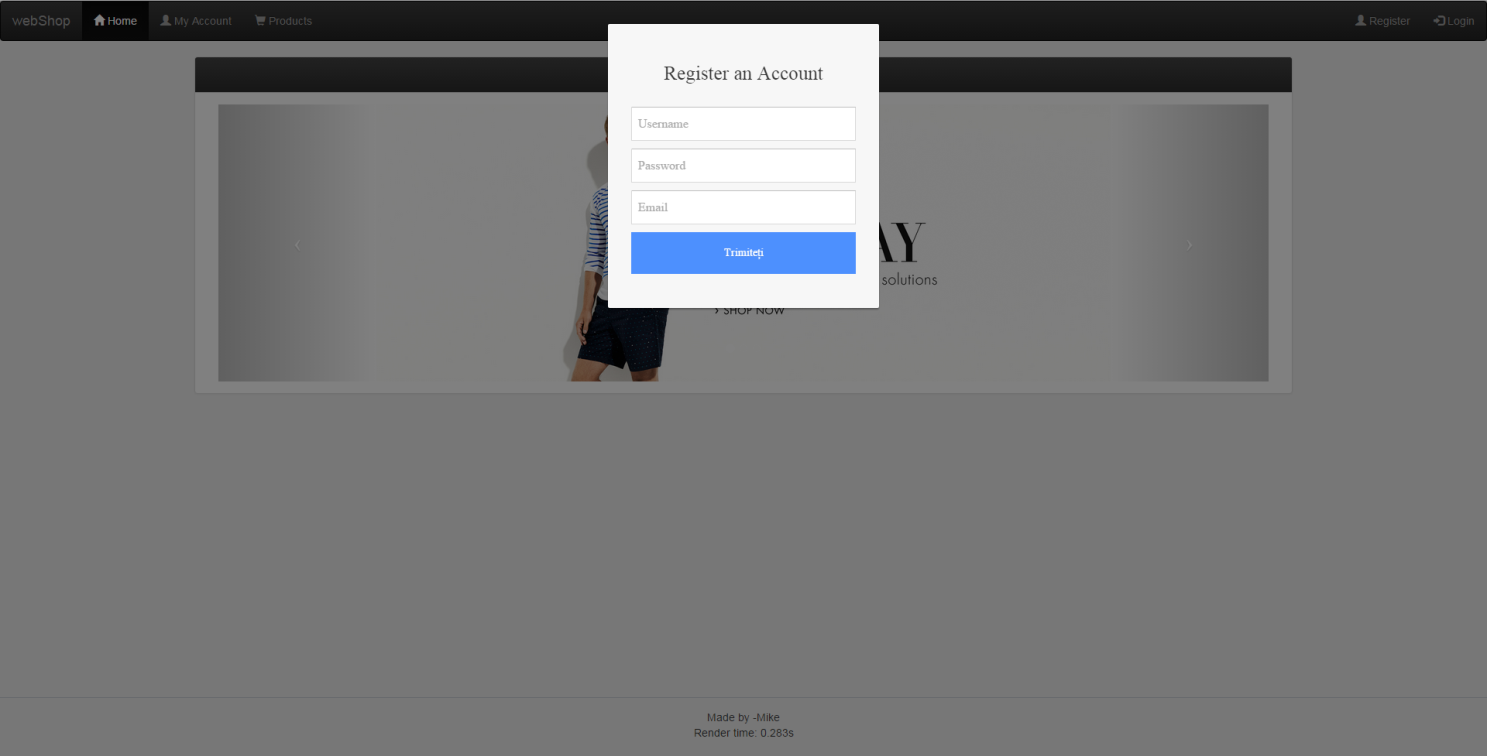
Pagina principală (**index.php**):



Pagina pentru autentificare (**login.php**):

Codul sursa pentru **login.php**:

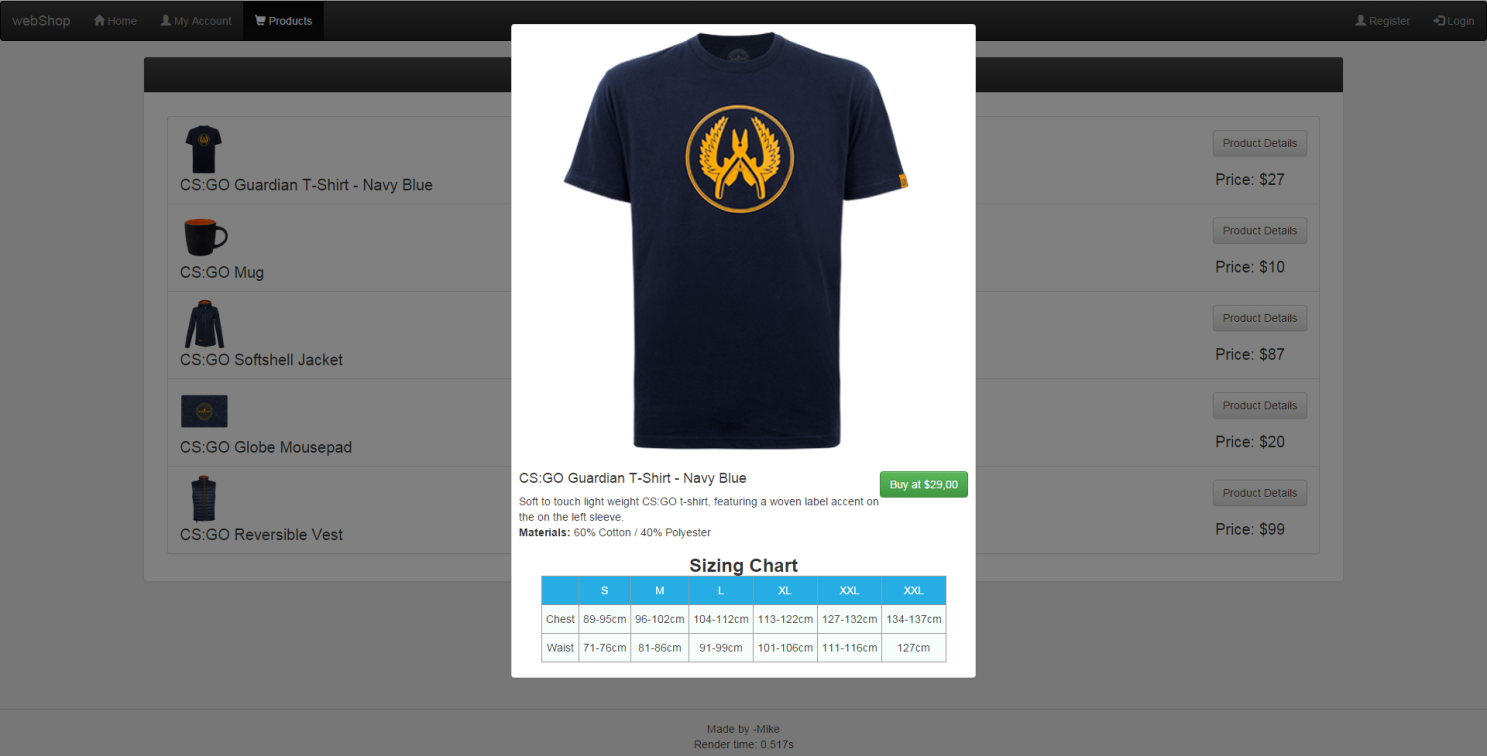
Pagina pentru înregistrare (**register.php**):



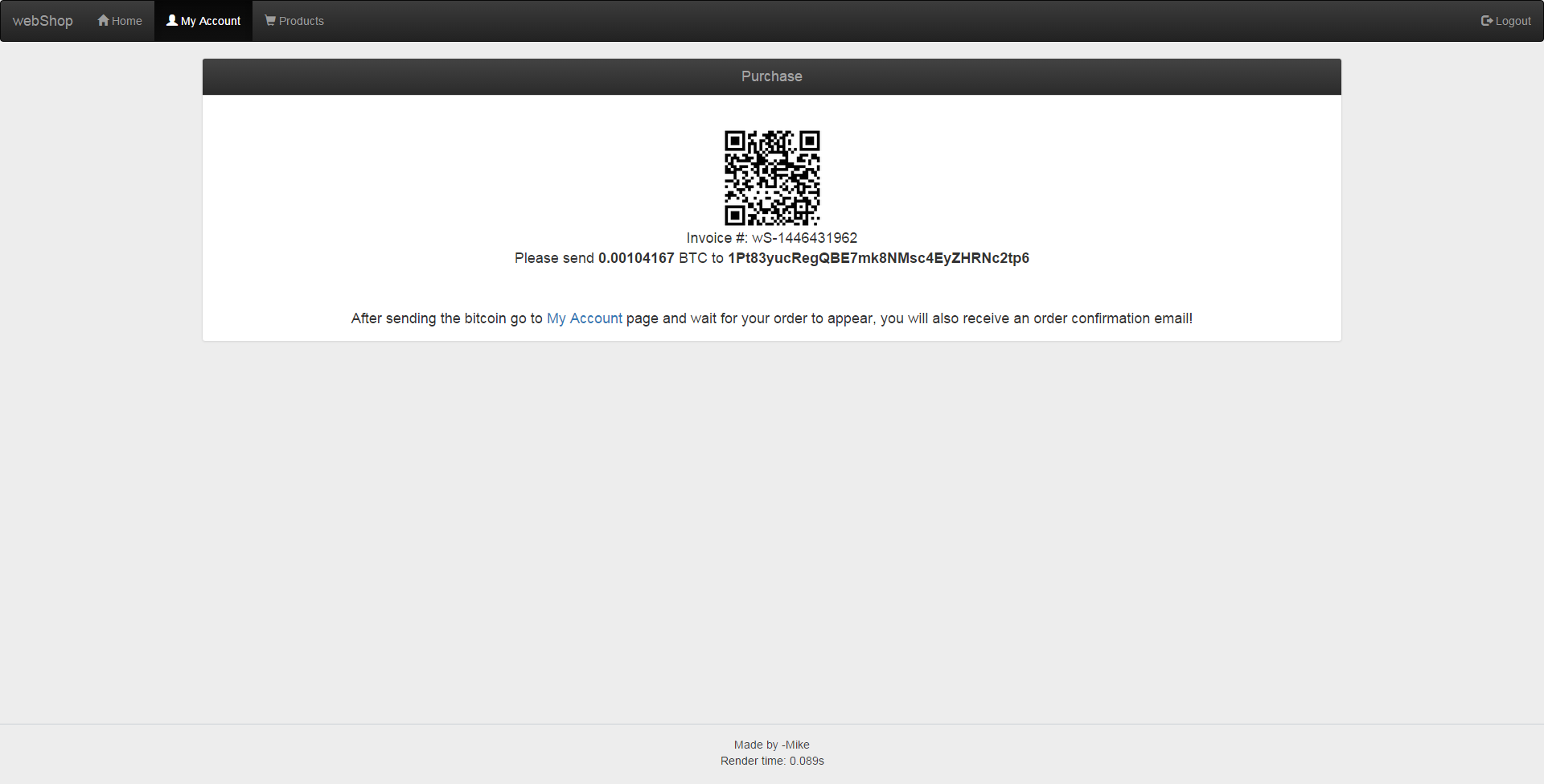
Codul sursă pentru **register.php**:

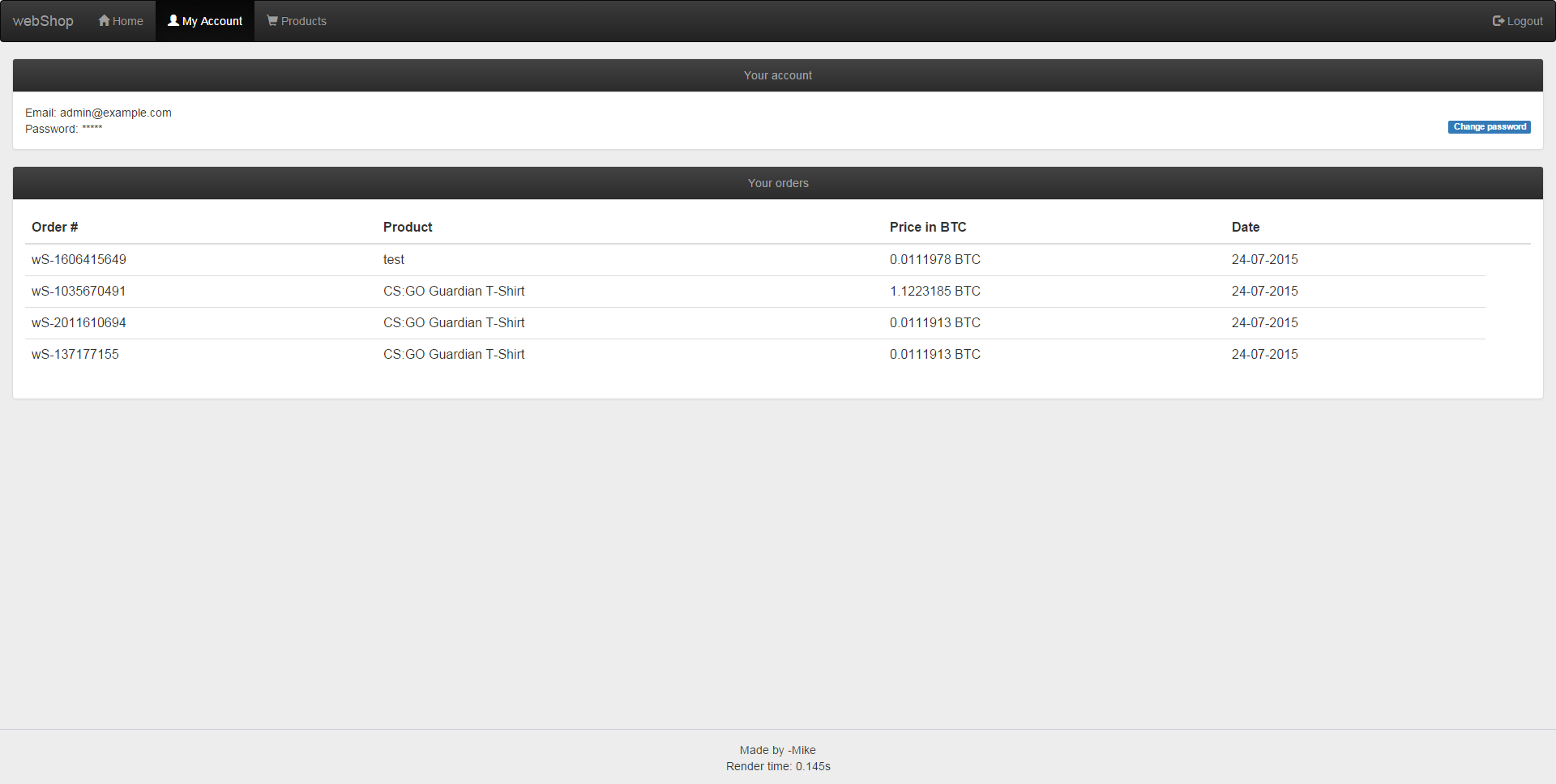


Pagina cu produse (**products.php**):

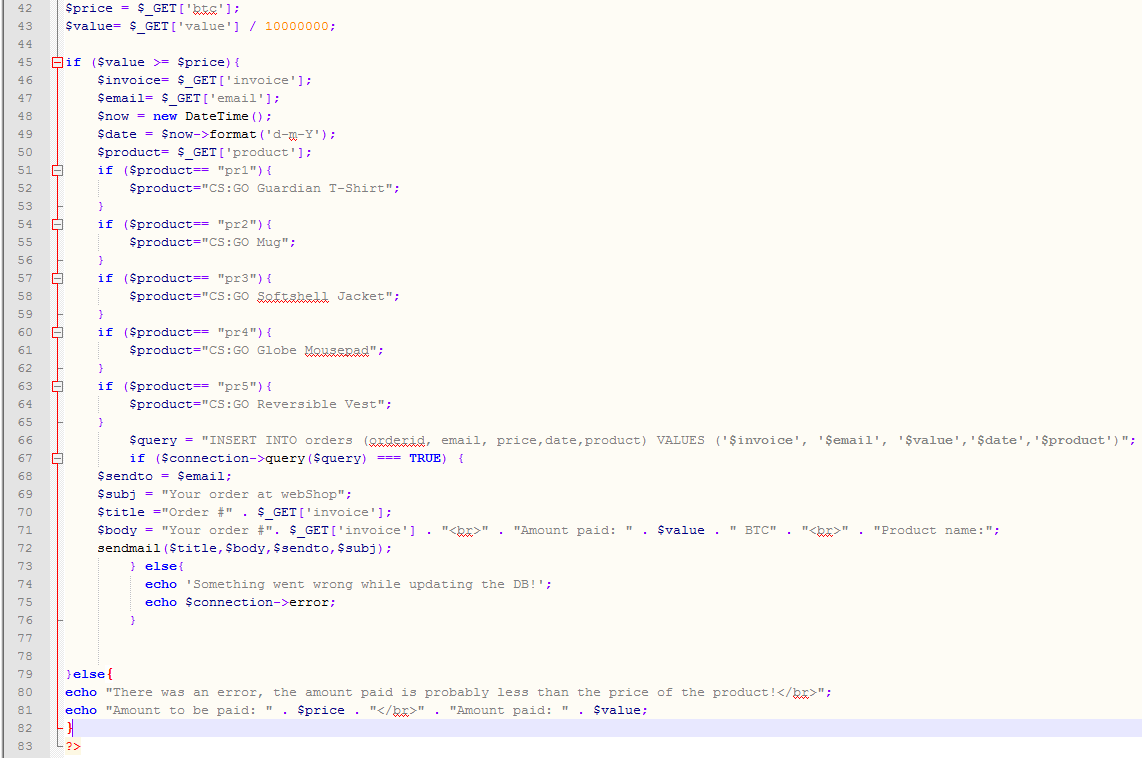


Pagina cu instrucțiunile pentru efectuarea plății (**purchase.php**):



Contul meu (**myaccount.php**):

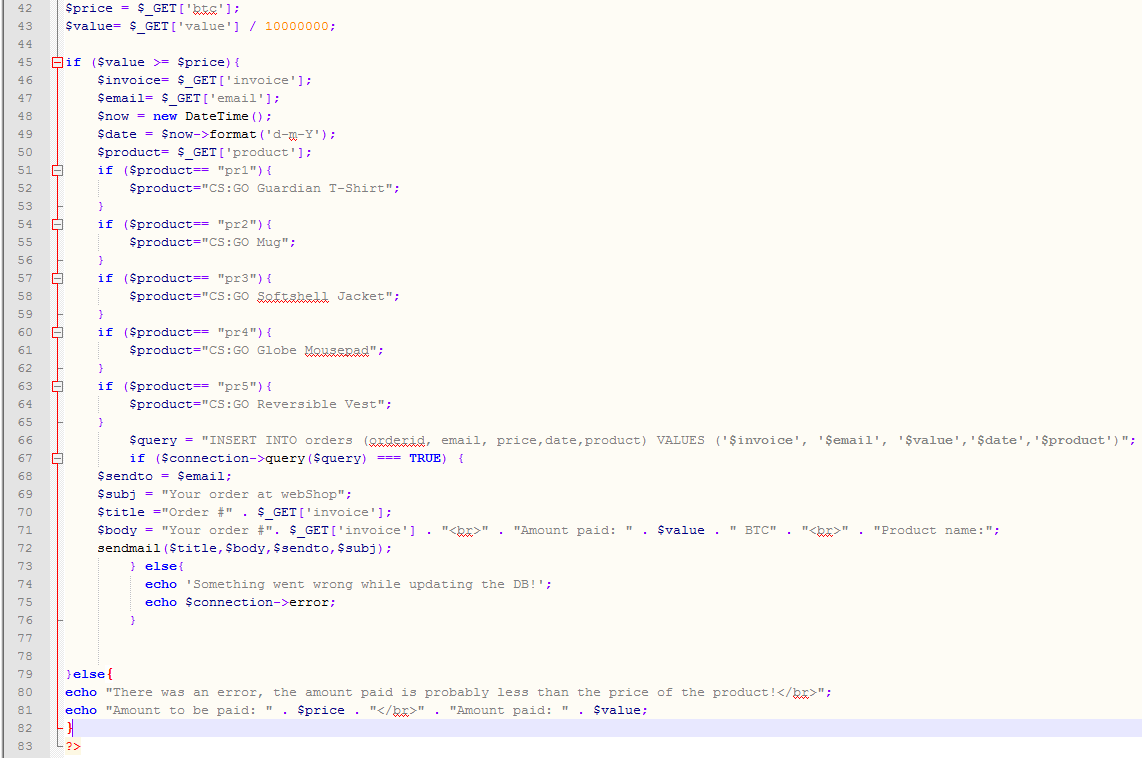
Schimbă parola (**pwchange.php**):



Cea mai importantă parte, **callback.php**, această pagină primește date de la **blockchain.info** atunci când o plată este procesată și ne dă de știre. Când primim aceste informații noi putem face orice vrem cu ele, le salvăm într-o bază de date, sau orice altceva, depinde de scopul în care acest sistem de plăți este folosit.



Verificăm dacă suma plătită este mai mare sau egală cu prețul produsului, dacă este, atunci putem considera plata efectuată cu succes, altfel afișăm un mesaj de eroare. Blockchain trimite aceste callback-uri până când primește un răspuns specific: \*ok\*



Surse electronice

<https://blockchain.info/en/api/api_receive>

<https://blockchain.info/en/api/blockchain_wallet_api>

<http://php.net/manual/en/index.php>