

Sprint Dokument

Sammanfattning

Webbsidans syfte är att sälja pennor över nätet. Sidans huvudfunktioner är som följer: Möjligheten att köpa produkter, använda sig av en shoppingvagn, lämna recensioner och även att skapa en användare på sidan. Till hemsidan används HTML, CSS, Javascript och sedan PHP för att anropa databasen. Servern, som drivs av en Raspberry Pi, består av LAMP med MySQL som databasmotor.

Användarfall

Administratör:

- Kan ändra befintliga varor och lagersaldo i butiken, samt byta ut och redigera hemsidan och databasen.
- Har möjligheten att ta bort olämpliga recensioner som lagts på produkter.

Kund:

- Kan bläddra bland varor i butiken.
- Kan lägga till varor i en kundvagn som sparas mellan sessioner.
- Det som finns i kundvagnen går att köpa förutsatt att allt finns i lager.
- För köpta varor kan en recension med betyg 1 till 10 lämnas på produktsidan.
- Varje kund har möjligheten att skapa en användare i butiken. Utan inloggning får kunden endast bläddra bland varor.
- Skapade användare kan tas bort. Detta inkluderar tidigare beställningar och recensioner.

System Arkitektur

Till hemsidan används HTML, CSS, Javascript och sedan PHP för att anropa databasen. Servern, som drivs av en Raspberry Pi, består av LAMP med MySQL som databasmotor.

Produkt- och kategorisidan

Vid vald kategori visas en sammanställning av alla produkter som finns tillgängliga i den kategorin. Varje produkt kan antingen köpas via denna sida eller produktsidan, knapparna är desamma. För att se mer information om en produkt klickar man på respektive produktlänk. På denna sida visas en bild på produkten samt följande punkter visas:

- Produkttyp,
- Färg,
- Pris,
- Lagerstatus,
- Artikelnummer.

Recensioner

Under produktinformationen ska en sammanställning av alla recensioner med namn, kommentar och betyg visas som en lista. När en användare är inloggad finns även möjligheten att skriva en recension på en köpt vara. Endast en recension per användare och produkt är tillåten.

Användarsidan

På användarsidan kan kunden se en sammanställning av alla produkter som kunden har köpt och vad varje produkt kostade när beställningen gjordes. På denna sida finns även knappar för att logga ut och ta bort användare.

Kundvagnen

I sidan för kundvagnen visas en sammanställning av alla produkter som finns i kundvagnen i form av en lista med produktnamn, antal och totalt pris för produkten. För varje produkt i listan finns knappar för att öka eller minska antal samt ta bort produkten helt. Tillsammans med denna lista visas totalsumman för alla produkter, samt knappar för att tömma kundvagnen eller slutföra beställningen.

Administratörsidan

För att komma åt administratörsidan används samma inloggningssida som för vanliga användare. Dock kommer administratören dirigeras bort från den vanliga användarsidan. På denna sida kan administratören radera produkter, radera kommentarer, ändra lagersaldo samt ändra pris på produkter. Här finns även en länk som leder till PHPmyAdmin.

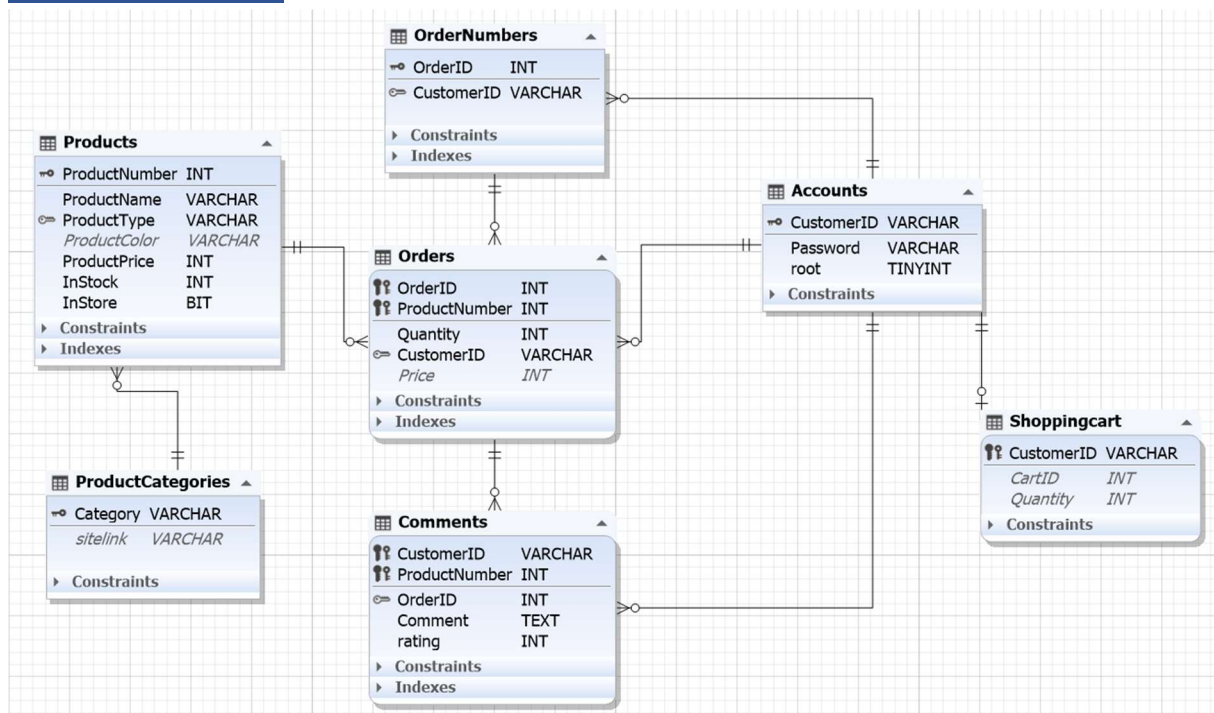
Nuvarande Backlog

ID	Uppgift	Typ	Prio.	Status	Sprint	Kommentar
1	Skapa LAMP server	Server	Hög		S0	
2	Simple hemsidayout	Front end	Hög		S0	
3	Skapa Databas	Databas	Hög		S0	
4	Interaktiv sidayout	Front end	Låg		S0	
5	Produktsida	Front end	Medel		S0	
6	Köplayout	Front end	Låg		S0	
7	Skapa Produktstruct	Databas	Hög		S1	
8	Koppla Databas till Sida	Front end	Hög		S1	
9	Php script till databas	Front end	Medel		S1	
10	Shoppingvagn/Recension layout	Databas	Medel		S1	
11	Byta ut placeholder element	Front end	Låg		S1	
12	Gemensam meny för hemsidan	Front end	Medel		S2	
13	Lägg till Användarfunktionalitet	Front end/databas	Medel		S2	
14	Lägg till shoppingvagn	Front end/databas	Hög		S2	
15	Lägg till köpfunktionalitet	Front end/databas	Hög		S2	
16	Byt ut alla bilder	Front end	Låg		S2	

Grupp 1 – Oskar & Robin

17	Möjlighet att skapa användare	Front end	Låg		S2	
18	Krypterade lösenord i databasen	Databas	Låg		S2	
19	Produktkategorier	Databas	Medel		S2	Istället för bara strängar i Products så har vi foreign key till en tabell.
20	Produktlänkar från databasen	Front end	Låg		S2	
21	Lägg till recensionsfunktionalitet	Front end/databas	Hög		S3	
22	Möjlighet att rensa och redigera varukorgen	Front end	Medel		S3	
23	Avregistrering	Front end	Låg		S3	Alla beställningar och information om en användare ska tas bort
24	Köpa produkt med olika antal	Front end	Låg		S3	Möjligheten att välja antal av en vara som ska läggas i varukorgen
25	Tömma varukorgen	Front end	Låg		S3	
26	Sida för kategorier	Front end	Låg		S3	En sida där alla produkter inom en kategori visas som en lista.
27	Sida för administratör	Front end	Hög		S3	
28	Admin funktionalitet	Front end/databas	Hög		S3	
29	Php sessioner	Front end	Medel		S3	
30	Generella Klasser för knappar och formulär	Front end	Låg		S3	
31	Error meddelanden	Front end	Låg		S3	Felmeddelanden ska ges vid felaktig inloggning och om recension läggs på ej köpt vara.
32	Antal varor i kundvagnen	Front end	Låg		S3	En siffra som visar hur många varor man har i kundvagnen.
33	Finslipad frontend	Front end	Låg		S3	Mer enhetlig design

Databas schema



Testfall

Användare

ID	Testfall	Handling	Förväntat resultat	Resultat	Ok	Not
1	Öppna sidan	Gå till http://90.224.160.35/	Hemsidan skall visas i webbläsaren.	Hemsidan visas		
2	Titta på produkterna	Välj en av kategorierna och välj en av tre produkter.	Den valda produkten skall visas.	Vald produkt visas		
3	Skapa en användare	Välj "Användarsida" och fyll i formuläret.	En användare skall skapas.	Användaren skapas		
4	Logga in	Välj "Användarsida" och ange dina uppgifter och tryck "Logga in".	Du bör se din användarsida med ordrar.	Inloggningen sker		
5	Logga ut	Välj "Inloggad som" och tryck "Logga ut".	Du bör loggas ut och returnera till hemvyn.	Utloggningen sker		
6	Genomför ett köp	Välj en produkt och tryck på knappen "Köp".	Produkten skall hamna i din kundvagn.	Produkten läggs till		
7	Placera en order	Gå till kundvagn och tryck på knappen "Slutför köp"	En order skall skapas och kundvagnen skall tömmas.	Ordern är betald		
8	Radera användare	Välj "Användarsida" och tryck på "Ta bort konto"	Kontot tas bort och användaren loggas ut	Kontot är raderat		
9	Lämna en recension	Tryck på knappen "Lämna en recension" och fyll i formuläret.	Din recension skall visas under produkten.	Recensionen visas		

Administratör

Testfall	Handling	Förväntat resultat	Resultat	Ok	Not
Logga in som admin.	Välj "Användarsida" och ange adminuppgifter och tryck "Logga in"	Du bör se adminsidan och inte den vanliga sidan för användare.	Inloggningen sker		
Logga ut.	Välj "Inloggad som" och tryck "Logga ut".	Du bör loggas ut och returnera till hemvyn.	Utloggningen sker.		
Adminfunktioner.	Välj "Användarsida" och fyll i ett formulär och tryck på dess knapp.	Knappen skall utföra det önskade kommandot.	Kommandot utförs.		
PHPmyAdmin.	Välj "Användarsida" och tryck på knappen märkt "PHPmyAdmin".	Du skall omdirigeras till 90.224.160.35/phpmyadmin	PHPmyAdmin nås.		

Systembegränsningar och förbättringar

Systemets begränsningar:

Hemsidan är endast formaterad för högupplösta datorskärmar. Inte mycket tid har lagts ner på att göra hemsidans innehåll flexibelt beroende på vilken webbläsare eller enhet användaren kan tänkas använda. Som följd av detta kan text sticka ut ur respektive behållare, samt att element kan uppfattas som deformerade. Dock är de mest nödvändiga segmenten angivna i procentenheter, med undantaget av vissa höjder angivna i pixlar. I nuläget har därför inga katastrofala designfel observerats.

Begränsningar i funktionaliteten inkluderar faktumet att förlorade lösenord inte går att återställa utan att redigera databasen direkt. Vid fallet då en användare, eller administratör, glömmer bort sitt lösenord blir det en relativt komplicerad process att skapa ett nytt hashat lösenord och byta ut det mot det gamla lösenordet.

Angående databasen och den bakomliggande strukturen till hemsidan är det teoretiskt möjligt att lägga till en kommentar på en produkt som köpts av en annan användare. Dock går det inte att lägga till en kommentar om produkten inte finns med i en befintlig beställning. Tills vidare är detta problem löst via kontroller i PHP, men en striktare databas-struktur hade önskats.

Det är även möjligt att utföra diverse attacker på både databasen och andra användare. En användare kan skicka in en recension som innehåller skadlig kod eller länkar till andra hemsidor. Och inga skydd finns mot SQL injektioner, förutom faktumet att en traditionell injektion för att komma åt andra användare inte är möjlig p.g.a. jämförelse med hashade lösenord. Sist men inte minst är ingen trafik mellan en användare och servern krypterad, vilket innebär att både sessionsdata och lösenord skickas i klartext.

Förbättringsområden:

Det går alltid att införa nya funktioner till hemsidan. Först och främst vore mobilanpassning en stor förbättring. Det går även att ändra källkoden för att få en mer enhetlig design genom alla sidor. För användare och administratörer saknas funktioner som att byta och återställa sitt lösenord, vilket är omöjligt just nu eftersom lösenord inte lagras i klartext.

För servern kan ett SSL certifikat lösa problemet med kryptering. Till servern kan även förberedda anrop implementeras för att förhindra injektioner, dock löser inte detta problemet med kod i recensionerna. För att begränsa vad som kan skrivas i recensionerna måste först och främst de tecken som kan finnas i en recension filtreras. Detta inkluderar alla tecken som tillhör syntaxen i HTML, CSS och javascript.

Det går även att förbättra hårdvaran som driver hemsidan och databasen. Än har inga tester utförts med ett stort antal användare, men om ett stort antal förfrågningar ska hanteras samtidigt krävs med stor sannolikhet snabbare hårdvara med fler än en processorkärna.

Länkar till verktyg

Git: <https://github.com/OskarHavo/D0018E-Hemsida>

Hemsidan: <http://90.224.160.35/>