Onderzoeks verslag DOOMotica

22 januari 2018

Inhoudsopgave

1 Domotica **3**

2 Website bouwen **3**

3 Hindernissen **3**
3.1 Afwezigheid docent 'Databases' . . . 3
3.2 hashen . . . 3
3.3 Cookies . . . 4

4 Centrale vraag **5**
4.0.1 Connectie . . . 6
4.0.2 Commando's . . . 6
4.0.3 Problemen . . . 7
4.1 spelltjes . . . 7
4.2 Tegeltjes . . . 7

5 Verantwoording gebruikte methodes **8**
5.1 Create user . . . 8
5.2 Inloggen . . . 8

6 Analyse van de gegevens **9**
6.1 Dataverzameling . . . 9
6.2 Analyse . . . 9
6.3 Deelconclusie/ aanbeveling . . . 9

7 Eindconclusie **10**

8 Aanbeveling **10**

9 bijlagen **11**

1 Domotica

De reden dat we dit project doen is zodat we de domotica in een huis zouden kunnen besturen. Hier voor maken we een webpagina waarop op onder andere de functies van Dahaus, spelletjes, tegeltjes voor je favoriete sites en nog wat andere tegeltjes voor je site geschiedenis.

2 Website bouwen

De opdracht voor de studenten is het maken van een website waar de gebruiker een account kan aanmaken en op dit account kan inloggen. Na het inloggen moet de gebruiker zijn favorieten site op de pagina kunnen zetten in de daar aangewezen tegels er voor. verder zijn er nog tegels voor de laatst bezochte sites. verder is er nog plek voor simpele spelletjes en als laatst moet de gebruiker Dahaus kunnen gebruiken.

De web applicatie heeft een aantal eisen:

- Er is een ERD opgesteld voor het Database Management Systeem.
- Voor de volgende functies worden PSD's opgesteld:
  - Login-functie
  - Create User-functie
  - Aanmaken tegels-functie
- Door gebruik te maken van XHTML, CSS en ASP.NET wordt de webapplicatie gerealiseerd

3 Hindernissen

3.1 Afwezigheid docent 'Databases'

In de afgelopen periode is de leraar voor het vak 'Databases' vier weken afwezig geweest. Dit heeft ervoor gezorgd dat de projectgroep tot week 7 geen les heeft gehad in de onderwerpen: Referentiële integriteit en de vragentaal 'SQL.

De studenten hebben dit geprobeerd op te vangen door zelf onderwerpen te verdelen van het lesplan en zelf uit te zoeken. Voor het assessment zijn alle lessen ingehaald en toegepast op de database.

3.2 hashen

hashen houd in dat je een wachtwoord zo vervormt met een speciaal algoritme dit kan alleen 1 kant op waardoor het originele wachtwoord niet terug te vinden is. Tenzij je een super computer heb, maar dan ben je nog steeds wel even bezig. Het probleem waar de studenten voor stonden was dat ze hier nog niet eerder mee hadden gewerkt. en dus zelf moesten kijken hoe het hashen werkt. nadenken te weten hoe het werkt deed hij het nog niet goed,

maar na stapsgewijs erdoor heen gelopen te zijn kwamen ze uiteindelijk bij het probleem. Dat na het ophalen van de database de Hash of wachtwoord niet eerst omgezet werd naar bytes. Waardoor de studenten de eerste 16 tekens als salt zagen en wat er na kwam als hash, maar dit hadden de eerste 16 bytes moeten zijn waardoor bij het vergelijken van beide gehashde wachtwoorden niet gelijk waren. Dit hebben De studenten simpel opgelost door het opgehaalde uit de database meteen om te zetten naar bytes.

3.3 Cookies

In de web-applicatie hebben de studenten cookies gebruikt om ervoor te zorgen dat gebruikers ingelogd blijven. Op basis hiervan is ook een Uitlog-knop gebouwd die de cookie moet terugzetten naar de huidige datum -1 dag. Na het drukken op de knop bleef de cookie bestaan en verwijderde de browser deze dus niet.

In de 9de week(!) kwamen de studenten erachter dat het aan de testbrowser lag. Deze verwijderde de cookies niet wanneer ze zijn verlopen, zelfs niet wanneer de gehele browser is afgesloten.

4 Centrale vraag

In hoe verre zijn De studenten instaat tot het bouwen van een webpagina. Dit houd in een site met inlog systeem die ook gekoppeld is aan een database en werkende functie heeft zoals Dahaus en spelletjes om te spelen voor de gebruiker. Verder wil de opdrachtgever hoe uitgebreid de studenten de webpagina kunnen maken en wat de studenten nog meer verzinnen om als extra dingen er op te zetten. Denk hierbij bijvoorbeeld aan extra functie als een muziek speler.

4.0.1 Connectie

De connectie met DaHaus is gemaakt met behulp van een TCP client. DaHaus is een TCP listener en om met een listener te verbinden moet je een TCP client gebruiken. Er is voor gekozen om de connectie met DaHaus alleen te maken als er een message verstuurd moet worden.

Nadat het bericht is verstuurd wordt de connectie ook meteen weer afgesloten. Het lukte namelijk niet om een connectie te openen en open te houden en op die connectie dan meerdere berichten te sturen en de connectie door middel van een event af te sluiten. Het open houden van de connectie gaf ook het probleem dat als de connectie niet goed werd afgesloten, dan crashde DaHaus. Terwijl nu de connectie automatisch wordt afgesloten waardoor er dus haast geen kans is op een crash van DaHaus.

Om het bericht naar DaHaus te sturen is er een NetworkStream nodig. Deze NetworkStream is aangemaakt door via de aangemaakte TCP client een stream te openen. Op deze stream is het mogelijk om een bericht naar plain text te encoden in ASCII en naar DaHaus te sturen in de vorm van Bytes. Als deze bytes zijn verstuurd moet het programma de reactie van DaHaus opvangen. De reactie van DaHaus is ook in plain text en wordt op de zelfde stream terug gestuurd.

Om deze reactie te lezen resetten de webapplicatie de bytes die de studenten gebruikten voor de message, deze worden dan gevuld met wat er van de stream gelezen wordt. Deze bytes worden dan weer terug gezet naar text. Deze text wordt dan in een string gezet en in de response textbox geprint.

De stream en client worden daarna nog niet gesloten. Eerst wordt de ëxit"message naar DaHaus gestuurd. Hierdoor sluit DaHaus de connectie zelf. Daarna wordt de client en de stream geclosed. Deze exit message wordt dan niet geprint, anders komt er na elk commando "Bye bye" geprint in de response textbox wat het alleen maar onnodig opvult. De stream en client worden dus pas geclosed nadat DaHaus zelf is geëxit. Als de exit message namelijk niet verstuurd werd dan zou de connectie toch nog blijven openstaan bij DaHaus en zou er even goed nog een nieuwe connectie worden gemaakt bij DaHaus bij een nieuwe message. Hierdoor zou er dan een ophoping aan connecties ontstaan bij DaHaus. Dit gaf in kleine tests geen problemen maar bij het opschalen van gebruikers zal het uiteindelijk te veel stress kunnen veroorzaken bij DaHaus.

4.0.2 Commando's

De commando's die naar DaHaus worden gestuurd kan het best via knoppen worden gedaan. Hierdoor hoeft de gebruiker dan namelijk niet alle commando's uit hun hoofd te kennen of op te zoeken. De makkelijkste optie was om 2 radiobutton lists te maken. Één radiobuttonlist om een object(lamp, window, heater, alle lampen of alle windows) te selecteren. De andere radiobuttonlist zou dan zijn voor de actie die de objecten moeten uitvoeren. Door een lange if else statement te maken is het daarmee mogelijk om voor elke combinatie het bijpassende commando te sturen. Om het commando op te sturen moet de gebruiker dan op de Send button drukken. Als er een ongeldige combinatie wordt gemaakt dan wordt dat in de Response textbox gezet, deze wordt dan niet naar DaHaus gestuurd. De heater wordt van temperatuur veranderd door de Heater en Heater Temp radio buttons te selecteren en in de heater textbox een value te geven. Deze wordt dan gecheckt of het wel een geldig getal is. Als dit getal

boven de 35 graden is, dan wordt dit veranderd in 35 graden, dat is namelijk de maximale waarde voor de heater. Zelfde gebeurd met onder de 12 graden, als er een getal onder de 12 ingevuld wordt, dan wordt de heater tot 12 graden gezet. Dat is dus de minimale waarde voor de heater.

4.0.3 Problemen

Bij de connectie maken met DaHaus zijn veel problemen opgetreden. Er is begonnen bij de commando's op te halen door middel van het "help"commando te sturen naar DaHaus via Putty, op blackboard stond hoe dit gedaan moest worden. Dit zelf leverde geen problemen op. Nu was er toegang tot alle commando's. Daarna moest gekeken worden hoe de connectie met DaHaus gemaakt kon worden. Dit werd gedaan door middel van een TCP client. Deze TCP Client creëren koste tijd om te begrijpen, maar gaf daarnaast geen problemen. Daarna is er uitgezocht hoe de commando's gestuurd konden worden. Dit is geprobeerd op meerdere manieren. Ten eerste werd geprobeerd commando's te sturen door een stream te openen en door middel van handmatig de bytes in de stream te sturen. En daarna de reactie te lezen. Hierbij bleef de stream steken op het lezen van de reactie. Het was niet gelukt om dit probleem op te lossen, er is geprobeerd de volgorde van acties te veranderen, maar verder is er geen informatie gevonden over waarom het niet werkte, er waren namelijk ook geen errors die konden uitleggen waarom de connectie vast liep, omdat dit niet werkte is er naar een andere manier gezocht. Deze manier bestond uit een StreamWriter en StreamReader, alleen hierbij trad hetzelfde probleem op. Daarna is er met behulp van Paul "peregrine"getroubleshoot waarom dit niet werkte. Na het proberen van communicatie tussen eigen gemaakte TCP clients en listeners, bleek dat dat wel werkte. Uiteindelijk is er uitgekomen dat het probleem heel simpel bleek. Er moest namelijk een extra regel in de string van het commando meegestuurd worden.

Het gemaakte programma dat commando's verstuurde was een makkelijk console programma dat na 1 commando meteen de connectie afsloot. Er moest dus nu een webpagina gemaakt worden die dan een beetje gebruiks vriendelijk is. Zoals als eerder al gezegd in het kopje Connectie was er eerst geprobeerd om een connectie te maken en open te houden totdat deze gesloten werd. Dit lukte dus niet.

4.1 spelltjes

De spelletjes die de studenten op de site moeten verwerken zijn simpele spelletjes voor de gebruiker om te spelen op de webpagina zelf. Er kunnen spelletjes op staan zoals:

4.2 Tegeltjes

De Tegeltjes die op de site verwerkt zitten zijn voor de gebruiker. Om zelf in te vullen met zijn of haar eigen favorieten websites.

5 Verantwoording gebruikte methodes

5.1 Create user

5.2 Inloggen

Voor het inlog gedeelte van het systeem zijn de studenten zelf gaan programmeren. Dit omdat de studenten dit een leuke uitdaging leek. Bij het maken van de inlog hebben de studenten een psd gemaakt zoals te zien is in Figuur 1. Het Programma is opgebouwd uit een aantal delen deze zijn Het ophalen van het wachtwoord uit de Database. Vervolgens het wachtwoord omzetten naar byte, daarna dan het opsplitsen van de Salt en de Hash. vervolgens de Slat voor het ingevulde wachtwoord zetten. Dit Wordt dan gehashed en als laatst word er vergeleken of de hash van het wachtwoord uit de database en het net gehashde wachtwoord het zelfde zijn, als dit zo is dan word er een cookie gemaakt die de gebruikersnaam onthoud en de gebruiker door stuurt naar de homepage. Wanneer dit niet het geval is krijgt de gebruiker een foutmelding dat het wachtwoord niet correct is. De code is te zien in Figuur 2.

6 Analyse van de gegevens

6.1 Dataverzameling

De Studenten hebben voor een groot deel gebruik gemaakt van de gegeven powerpoints van de lessen Webprogrammeren. ook hebben we een aantal dingen opgezocht op internet hier de links die we gebruikt hebben: `https://msdn.microsoft.com/en-us/library/ms525800(v=vs.90).aspx` (bekeken op 19-01-2018, Geschreven door Microsoft),
`https://stackoverflow.com/questions/13058574/check-if-cookie-exists`(Bekeken op 19-01-2018, geschreven door zmbq).

6.2 Analyse

De powerpoints waren van een betrouwbare bron. Ze komen namelijk van hun docent die ze les heeft gegeven in webprogrameren en het is ook 1 van de docenten die het project beoordeeld hierdoor weten de studenten ook meteen dat het op de manier gaat als de opdrachtgever wil. De eerste link is afkomstig van Microsoft een betrouwbare bron, omdat het programma waar de studenten hun webpagina op maken ook van Microsoft is. De Tweede links is van de site stackoverflow op deze site stellen mensen vragen over dingen waar ze niet uitkomen met hun programma's. De antwoorden zijn niet altijd betrouwbaar, maar in dit geval werkte het antwoord wel.

6.3 Deelconclusie/ aanbeveling

De studenten zijn er achtergekomen dat de powerpoints heel handig zijn om bij de hand te hebben voor als je ergens niet op komt. Verder zijn de voorbeelden van Microsoft handig om op te zoeken als je iets niet meer compleet weet. De site stackoverflow is handig als je weet wat je wilt alleen niet weet hoe je het uitvoert. De studenten zouden aanbevelen om zeker de powerpoints te gebruiken en als je het daar niet in kunt vinden kun je altijd nog internet raadplegen.

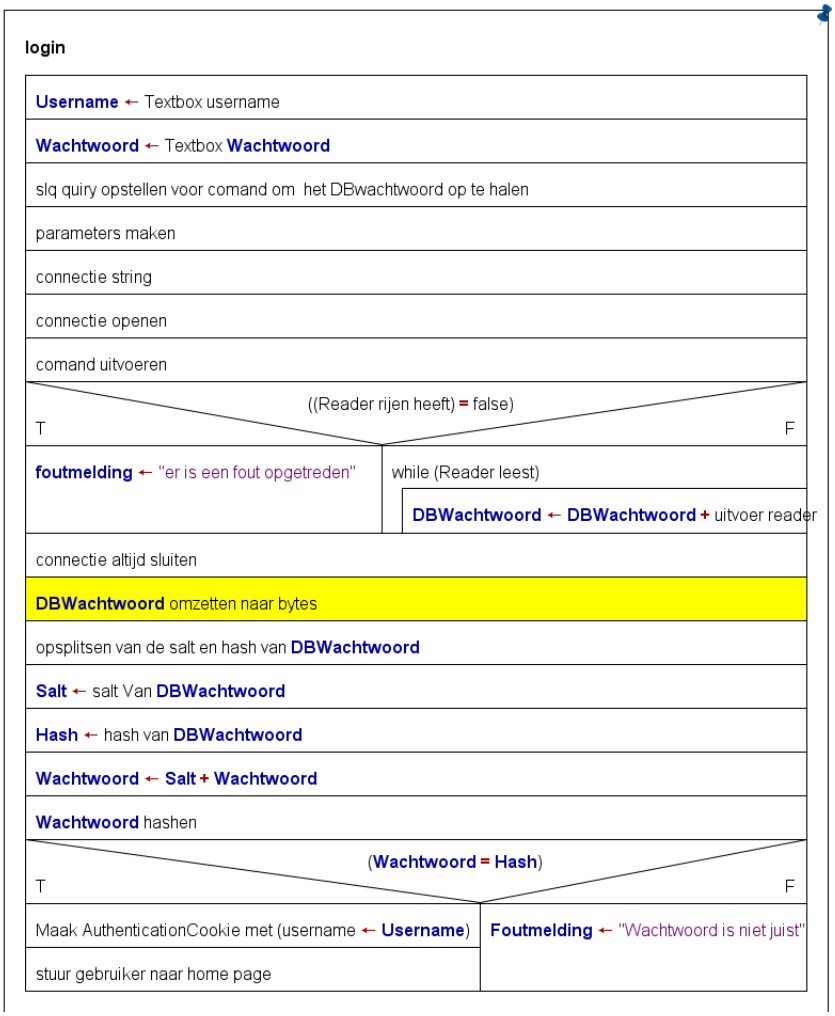
7 Eindconclusie

De studenten zijn er achter gekomen dat het meer werk is dan alleen maar een paar dingen op de pagina slepen zoals in de lessen werd gedaan om, maar dat er veel meer bij komt kijken bij een echte webpagina maken met alle eisen zoals beschreven staat in Hoofdstuk 2 staat beschreven. Verder is het handig als zoals bij de studenten gebeurde dat er een les als database uitvalt voor het begin van de periode dat je er zelf gewoon mee aan de slag gaat dan word je achterstand niet te groot.

8 Aanbeveling

De aanbeveling van de studenten is om het werk niet te onderschatten en op tijd er mee te beginnen zodat je tijd over kan houden voor extra dingen. Die je op je webpagina wilt zetten. Verder als er een les niet gegeven word om de één of andere reden zoek iemand die er het begrijpt en kan uitleggen en vraag om hulp wanneer nodig, ook aan je groepsgenoten. het is beter hulp te vragen dan het slecht product te leveren.

9 bijlagen



Figuur 1: psd van de Login

```
protected void btn_Login_Click(object sender, EventArgs e)
{
    string Wachtwoord = "";
    int RolNr;
    Connectie.ConnectionString = ConfigurationManager.ConnectionStrings["Harry"].ToString();
    Query.Connection = Connectie;

    Query.CommandText = "SELECT Wachtwoord, Rolnr FROM LID WHERE Gebruikersnaam = ? ";
    OleDbParameter Param1 = new OleDbParameter();
    Param1.Value = txt_Username.Text;
    Query.Parameters.Add(Param1);

    try
    {
        Connectie.Open();
        OleDbDataReader Leesding = Query.ExecuteReader();
        while (Leesding.Read())
        {
            Wachtwoord = Leesding["Wachtwoord"].ToString();
            RolNr = Convert.ToInt32(Leesding["Rolnr"]);
        }
    }
    catch (Exception exc)
    {
        lbl_gelukt.Text = exc.ToString();
    }
    finally { Connectie.Close(); }

    //converteren string naar bytes
    byte[] DBhash = Convert.FromBase64String(Wachtwoord);


    //AANMAKEN SALT VAN DBHASH
    byte[] DBsalt = new byte[16];
    Array.Copy(DBhash, 0, DBsalt, 0, 16);
    //Aanmaken en converten hash uit ww
    byte[] Controle_DBhash = new byte[20];
    Array.Copy(DBhash, 16, Controle_DBhash, 0, 20);
    string DBww = Convert.ToBase64String(Controle_DBhash);

    //HASHEN
    var pbkdf2 = new Rfc2898DeriveBytes(txt_Password.Text, DBsalt, 10000);
    byte[] CtHash = pbkdf2.GetBytes(20);
    string ControlePass = Convert.ToBase64String(CtHash);

    if (ControlePass == DBww)
    {
        //toevoegen cookie met username + lidnr
        HttpCookie Koekje = new HttpCookie("AuthenticationCookie");
        Koekje.Values.Add("Username", txt_Username.Text);
        Koekje.Expires = DateTime.Now.AddMinutes(20);
        Response.Cookies.Add(Koekje);

        //doorsturen naar home.aspx
        Server.Transfer("~/MEMBERS/Home.aspx");

    }

}
```

Figuur 2: Code van de login