Project 4
Inrichting Centrale bank

Achternaam, Voornaam:	Liu, Wen
Studentnummer:	0911282
School:	Hogeschool Rotterdam
Klas:	Ti 2A
Schooljaar:	2017-2018
Datum:	30 mei 2018
Bytegroep:	11

Inhoudsopgave

Inleiding

In opdracht van mijn project docenten, moet ik een verslag schrijven voor mijn individueel deel van mijn project. In mijn verslag komen 2 attributen per indicator uitgebreid te staan. De 2 indicatoren zijn: Voor de kwaliteit voor het product(A5) en kwaliteit voor het gebruik (A6). De 4 attributen die ik in mijn verslag verwerkt zijn: Security(product), Robuustheid(product), Vertrouwen(gebruik) en Tevredenheid(gebruik). De documenten en code worden geplaatst op github. De link naar github komt onder bijlage te staan.

1. Stappenplan:
   - Aller eerst onderzoeken
   - Kijken wat men gebruikt
   - Wat voor alternatieven er zijn
   - Vergelijken
   - Adviseren

2. Kwaliteit van het product
   Voordat je kan beginnen met een verslag moet er allereerst worden onderzocht wat er wordt bedoeld met bepaalde woorden. Robuustheid betekent stevig en sterk gebouwd.
3. Adviseren

1.1 Robuustheid

Voordat je kan beginnen met een verslag moet er allereerst worden onderzocht wat er wordt bedoeld met bepaalde woorden. Robuustheid betekent stevig en sterk gebouwd. Denk aan een brug. Hoe wordt die gemaakt, waarom gebruikt men geen hout in plaats van beton, wat voor technieken wordt er toegepast, enz. De geldautomaat moet niet alleen stevig en sterk zijn, maar ook weer bestendig, hittebestendig, lang mee kunnen en nog veel meer. De geldautomaat heeft een monitor, geld dispenser, bonnen printer en een RFID scanner. De belangrijkste component van de geldautomaat is de geld dispenser, Je wilt niet dat mensen makkelijk toegang verschaft naar de geld dispenser.

1.1.1 Robuustheid van geldautomaat (materiaal)

Voor de gehele geldautomaat kunnen we verschillende materialen gebruiken, zoals metaal, hout, plastic, enz.
Standaard gebruikt men metaal en plastic.[1]
Maar wat voor metaal, plastic en/of hout precies?
Metaal soorten zoals aluminium, ijzer, koper, chroom, zilver, lood, zink enz.
Om een echte geld automaat in elkaar te zetten zal er worden vergeleken tussen deze 3 metaal soorten: aluminium, ijzer en roest vrije staal.

Aluminium[2][3]
Aluminium is een metaal soort met een silver grijs kleur. Aluminium wordt gebruikt voor Verschillende dingen, zoals het maken van vliegtuigen, fiets, auto, blik, folie, ramen, deuren en noem maar op. Aluminium is een van de meest gebruikte metaal soorten en is recyclable (meest efficiënt). Het heeft een smelt punt van ongeveer 660 graden Celsius en roest niet makkelijk. De prijs hiervan is momenteel 1.03$/lbs.

Ijzer(Staal)[4][5]
Ijzer is een metaal soort met een grijs kleur. Ijzer wordt gebruikt voor auto’s, schepen en het bouwen van grote constructies. Het heeft een smeltpunt van 1538 graden Celsius. Recyclable.

Roest Vrije Staal [6][7]
Roest Vrije Staal (RVS) ook bekend als INOX is een metaal soort. RVS kan wel roesten, alhoewel het roestvrij staal heet. Het roest wel minder snel dan ijzer. Het wordt gebruikt om borden, draad, constructie materiaal, eetgerei, koelkast, microwave, wasmachine enz. te maken. De prijs hiervan is momenteel 1.68$/lbs.

Materiaal	Duurzaam	Weerbestendig	Hittebestendig	Duur/Goedkoop	Recyclable
Aluminium	X	X	X	Duur	X
Ijzer			X	Goedkoop	X
RVS	X	X	X	Duur	X
Hout				Goedkoop	X

1.1.2 Robuustheid geld dispenser
Er zijn verschillende manieren om een geld dispenser te maken. Voor mijn geld dispenser heb ik de keuze uit 3 modellen. De drie keuzen zijn:

- Motor systeem (LEGO Mindstorm)
- Motor systeem (Arduino)
- Zuignap (vacuum) systeem

In principe werken alle 3 modellen, maar ze verschillen in snelheid, functionaliteit, ontwerp en coderen, enz.
Het moet natuurlijk stevig en sterk zijn (robuust). Maar het moet ook snel en goed werken.
Vandaar de vragen:

- Is de geld dispenser stevig genoeg?
- Hoelang gaat die mee?
- Is die snel genoeg?
- Welk programmeertaal gebruikt het?

De geld dispenser bestaat uit een motor (roller) en een kastje.
Wat voor motor is goed voor een geld dispenser?
Wat voor opties zijn er ?
De keuze uit LEGO Mindstorms, een zuigsysteem of met motoren geschikt voor arduino.

LEGO Mindstorms NXT[8]
LEGO Mindstorms NXT is een programmeerbare robot kit gemaakt door Lego.
Je kan makkelijk simpele programma's maken op de NXT intelligent Brick. De NXT intelligent Brick is te vergelijken met een microcontroller, die speciaal gemaakt is voor lego. De NXT intelligent brick heeft een brede ondersteuning voor programmeertalen. Enkele hiervan zijn Java, C, C# , enz. (zie bijlage). Uit eigen ervaring werkt de lego Mindstorm wel, maar het programmeren hier van is als nog lastig ingeval je met eclipse IDE wilt werken. Ook was de geld dispenser met lego blokjes niet zo stevig. De batterijen in de NXT brick lopen ook best snel leeg, het is dus ook niet duurzaam.

Arduino systeem[9]

Het systeem is heel simpel en stevig. Er wordt gebruikt gemaakt van een Arduino Uno en 4 stukken motoren. Er wordt 4 bakken gemaakt om de bankbiljetten te zetten. De bakken worden eerst getekend in autodesk en daarna uitgesneden in de stadslab. Het is niet zomaar iets tekenen en uit snijden, maar op een manier dat ervoor zorgt dat de bakken stevig zijn en niet zomaar los vallen. Je kan bijvoorbeeld het snijden en daarna op elkaar lijmen, maar er is natuurlijk een steviger manier zoals het snijden zodat die in elkaar kan schuiven, dit zorgt ervoor dat je geld dispenser bakken en motoren stevig in elkaar zitten.
Hiervoor wordt er gebruik gemaakt van een motor. Voor de motor heb je best veel opties, men kan bijvoorbeeld een stepper motor, servo motor enz. gebruiken. Je hebt verschillende motoren die geschikt zijn voor de geld dispensers, maar ze verschillen allemaal in kwaliteit, snelheid, duurzaamheid, stevigheid, enz. De stepper motoren zijn geschikt voor langzame taken en de servomotoren voor snelle taken. De ideale voor een geld dispenser zou dus een servomotor zijn.

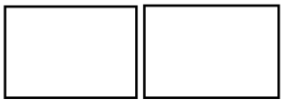
Vacuüm systeem
Het vacuüm systeem werkt heel goed, maar maakt best veel geluid en heeft veel voeding nodig. Er wordt gebruik gemaakt van een zuignap, die een voor een de biljetten moet kunnen oppakken en die vervolgens in de bak neerleggen. Het vacuüm systeem wordt bestuurd middels een Arduino. Met de vacuüm systeem kan je heel complexe geld dispenser ontwerpen, omdat je van alle materialen gebruik kunt maken. Je kan dus bijvoorbeeld overwegen om half lego te gebruiken, hout, plastiek, laser printer , enz. (wat men leuker vindt). Verder moet je zelf jouw Arduino programmeren en jouw ontwerp met elkaar koppelen. Dit kan dus veel tijd in beslag nemen.

Systeem	Stevig	Snel	Brede programmeertaal	Duurzaam
Lego		X	X	
Arduino motor	X	X	X	X
Zuignap/vacuüm			X	

Kwaliteitseisen (robuustheid)
- De geld dispenser moet gemaakt zijn van stevige materiaal? (bijv.hout)
- De geld dispenser moet tenminste tegen lichte stoten.
- De geld dispenser moet tenminste 2 maanden kunnen draaien.
- De geld dispenser moet zoveel mogelijk water dicht zijn (geen onnodig openingen).
- De geld dispenser maakt geen gebruik van batterijen maar een directe voeding

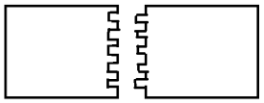
Advies robuustheid
Het is beter om een sterk materiaal te gebruiken zoals RVS, maar voor een prototype mag er best wel hout gebruikt worden. Hout is goedkoper en als het dik genoeg is in diameter, is het wel stevig. Ook is het belangrijk om nummer 2 toe te passen. De blokken uitsnijden zodat je ze precies in elkaar kan schuiven en daarna vast lijmen. Dit zorgt ervoor dat je geld dispenser stevig is en tegen paar klappen tenminste aan kan. Indien je toch met RVS werkt, raad ik je sterk aan om het te lassen en te verven. Een verflaag zorgt ervoor dat die minder snel roest dan zonder een verflaag. Vier bakken naast elkaar leggen in plaats van op stappelen, zorgt voor stevigheid. Tenzij je met een goede design komt voor opstappelen.

1.



2 blokjes lijmen

2.



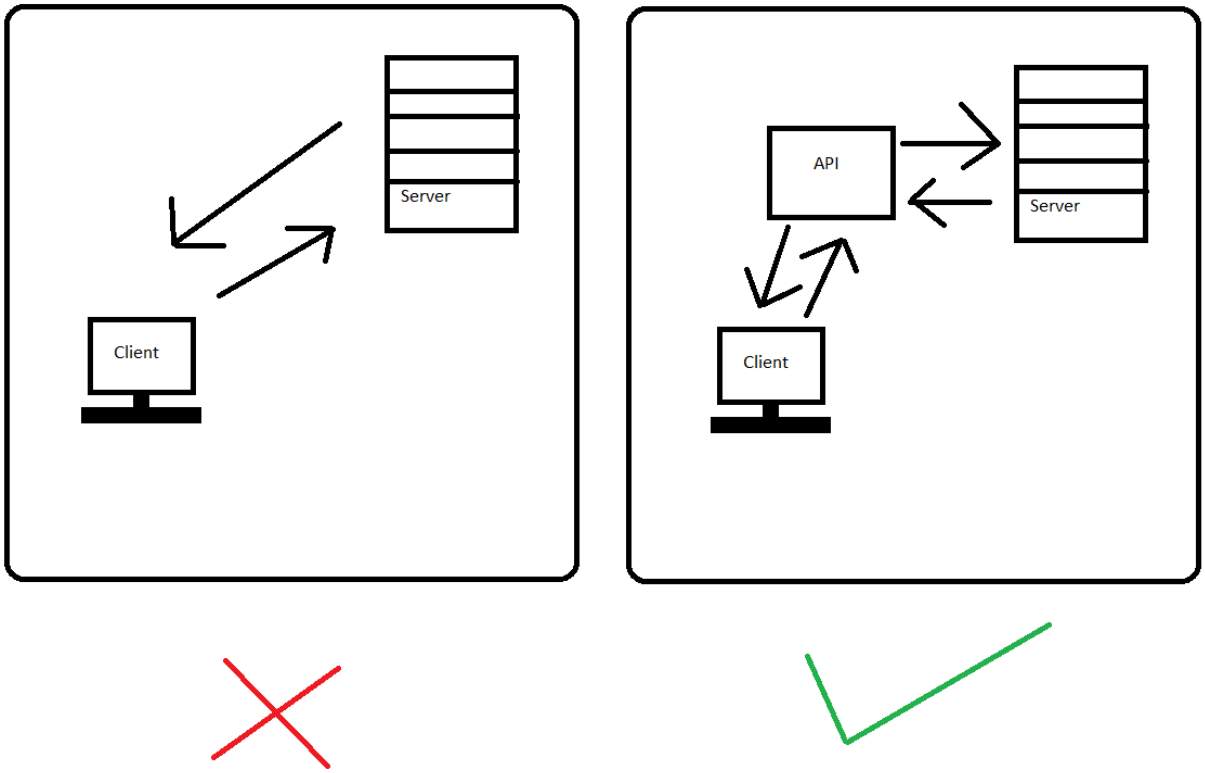
2 blokjes in elkaar schuiven
Daarna lijmen

1.2 Security (beveiliging)

Het is heel belangrijk dat de gebruikers veilig de geldautomaat kan gebruiken.
Onze geldautomaat is momenteel ook niet beveiligd (fysiek). Boosdoeners kunnen dus makkelijk aan onze usb poorten en hardwares komen. Ongebruikte usb poorten kunnen we liefst verwijderen of locken[10]. De usb poorten kunnen disabled worden op je computer door te gaan naar device manager en je usb poort selecteren en dan disablen. Er zijn ook softwares die men gebruikt om apparaten te whitelisten of blacklisten zodat onbekende apparaten geen toegang verschaft en bekende apparaten juist wel[11].
Waarop moeten de gebruikers en makers op letten ?
Enkele punten waarop er gelet moet worden zijn:

- Geen directe verbinding maken tussen server en client
- Skimmen
- SQL injection
- Versturen van data
- Slecht geschreven code
- Wachtwoord brute force (code)
- Database goed beveiligen

Verbinding tussen cliënt en server[12]
De verbinding tussen de cliënt en server is momenteel direct met elkaar verbonden. Dat is namelijk niet zo slim. Hackers kunnen dus nu gelijk binnen onze database binnen en onze gebruikers gegevens stelen en zelfs aanpassen. Om dit te voorkomen kunnen we gebruik maken van een Application Programming Interface (API) gebruiken. Het gebruik van een API zorgt niet alleen voor een beter beveiliging maar ook voor uitbreidbaarheid. Met de API kan je ook meerdere cliënten tegelijkertijd verbinden.Wat is een API en wat doet het ? Een API kan je vergelijken met een ober. Stel voor dat de keuken het systeem is en je de gebruiker een besteller is. De gebruiker besteld een gerecht en de ober geeft dat aan in de keuken, kort hierna brengt de ober de gekozen gerecht naar de gebruiker. De ober is dus niets anders dan een boodschapper (tussen persoon) die een request verstuurt naar de server en een antwoord terug geeft aan de gebruiker. Transport Layer Security[13] (TLS) is toepasbaar op een API. Verder kan met ook een API gebruiken om te authenticeren en autoriseren. TLS zorgt ervoor dat de communicatie tussen de cliënt en API en van API naar de server beveiligd wordt met encryptie. Hierdoor kunnen hackers niks met de data doen als die toch wordt onderschept.



Skimmen[14][15]
Wat is skimming?
Met skimming bedoelen we niet het verwijderen van het schuimlaag van vloeistof, maar het stelen van bankpas en wachtwoorden. De criminelen stelen de bankpasnummer en wachtwoorden op verschillende manieren. Met de gestolen informatie maken zij de bankpas na en maken misbruik ermee. Hierdoor kunnen zij geld pinnen met de verkregen informatie. Skimmers gaan op verschillende manieren te werk. Op geldautomaten en betaalautomaten plaatsen de criminelen opzetstukken/voorzetmondjes waarmee ze de magneetstrip van een betaalpas kunnen aflezen. Daarna wordt de pincode door middel van diverse trucs onderschept. Bijvoorbeeld door een camera die boven het toetsenbord is geïnstalleerd of simpelweg door over de schouder mee te kijken.

Hoe voorkom ik skimmen? [16][25]
Als bank is het aangeraden om gebruik te maken van EMV-chip in plaats van magneetstrip. EMV chip is een microprocessor chip dat namen en data van de gebruiker opslaat en beveiligd. Criminelen kunnen makkelijk bankpassen met magneetstrip makkelijk namaken, maar een bankpas met EMV-chip niet.
Let op mensen die te dichtbij staan, ze kunnen proberen uw pincode af te lezen.
Scherm met uw hand de pincode af. Bijna alle geldautomaten zijn tegenwoordig voorzien van een 'invoermond'. Let erop dat dit mondje er exact zo uitziet als de afbeelding op het scherm (hoewel op sommige geldautomaten de afbeelding niet staat). Elke andere invoermond kan een lezer bevatten die de magneetstrip op de pas leest. Valse frontjes lopen vaak minder soepel dan de echte. Komt uw pas een paar keer terug uit de geldautomaat? Dan kan het om een vals frontje gaan. Breek de transactie af en neem contact op met uw bank. Het is altijd veiliger om een automaat binnen een bank of winkel te gebruiken dan een betaalautomaat. Check uw banksaldo zeer regelmatig. Als er onbekende transacties wordt gedaan, moet je zo snel mogelijk je bankpas blokkeren.

SQL injection [17][18]
Wat is SQL injection?
SQL-injectie is een modus van de aanval die wordt gebruikt om corrupte een legitieme database query om vervalste gegevens te verstrekken. Script injectie is een aanval waarbij de aanvaller biedt program code om de server van de scripting engine.

Hoe gaan we SQL injection tegen?[19]
Enkele simpele manieren:
Voor programmeren welke functies gebruikt mogen worden.
Whitelisten van ingevoerde commands.(input validation).

Encryptie[20][21]
Encryptie is het versleutelen van berichten of informatie in een manier, zodat mensen niks kunnen doen met de informatie als het niet voor hun bestemd zijn. Stel voor dat persoon A een belangrijke bericht stuurt naar persoon B. Daarin stond zijn gebruikersnaam en wachtwoord van zijn bank rekening. Als dit wordt onderschept door iemand anders dan persoon B, kan die persoon (onbevoegden) er misbruik ervan maken. Als persoon A zijn/haar bericht had encrypt, kon de ander persoon niks ermee doen. De wachtwoord van persoon A is “2018”, maar met encryptie is die 8102 geworden. De persoon die het onderschept snapt dus niks ervan, maar persoon B wist wel van te voren hoe die het moest ontcijferen. Enkele bekende encryptie algoritmen zijn: Triple DES, RSA, Blowfish, twofish en AES.

Symmetrische encryptie[21][22]
Er zijn in de praktijk een aantal verschillende encryptie vormen. Met een symmetrische encryptie bedoeld men dat dezelfde sleutels worden gebruikt. Een bekend voorbeeld van een symmetrische encryptie is een versleuteld wachtwoord op de computer. De goede combinatie van cijfers en tekens zorgt ervoor dat alleen jij toegang hebt tot het apparaat. Maar een symmetrische encryptie is niet de beste encryptie. Het nadeel is dat het alleen werkt als niemand jouw sleutel in handen krijgt. Andere voorbeelden van symmetrische encryptie zijn: DES-algoritme, IDEA, RC4 enz.

Asymmetrische encryptie[22]
Asymmetrische encryptie werkt bijna hetzelfde als symmetrische. Het verschilt ligt bij de gebruikte sleutel om te encrypten en een ander sleutel voor het decrypten. Asymmetrische encryptie wordt ook wel public key encryption genoemd. Er zijn dus 2 sleutels, waarvan 1 de public key is en de andere de private key. Berichten die met een publieke sleutels zijn vergrendeld kunnen alleen worden ontgrendeld met de private sleutel samen met de publieke sleutel. Asymmetrische encryptie wordt vaak verwerkt in SSL-certificaten op het internet. Voordeel van het gebruik van een asymmetrische encryptie is dat uitwisseling van de benodigde sleutels plaats kan vinden via een onveilig kanaal. Nadeel van asymmetrische encryptie is dat de sleutellengtes heel groot zijn (bijv. 4096 bytes), waardoor coderen en decoderen veel rekenkracht voor nodig is.

Hashing[21][22]
Voor hashing gebruikt men algoritmen die data door elkaar schudt. In tegenstelling tot symmetrische en asymmetrische encryptie is het proces niet omkeerbaar. Wat onleesbaar is gemaakt, blijft onleesbaar. De enige mogelijkheid om dit terug te keren naar de bron is om de originele data opnieuw te laten hashen met hetzelfde algoritme. Komen de eerste en tweede uitkomst dezelfde? Betekent het dat je wel met dezelfde data te maken hebt. Hashing wordt in het algemeen gebruikt om wachtwoorden te beschermen.

AES encryptie[23][26]
AES staat voor Advanced Encryption standard. Het is een symmetrische encryptie algoritme en een van de meest veiligste encryptie. De overheid van de verenigde staten gebruikt AES encryptie voor hun geheime data. AES encryptie encrypt in blokken, de blokken zijn 128 bits, 192 bits enz. AES kan tot 256 bits encrypten, waarbij 128 bits het meest efficiëntste is. Kan grote data encrypten. Bovendien is AES encryptie ook open source[28].

3DES encryptie[26]
3DES encryptie staat voor Triple Data Encryption Standard. Het is een symmetrische encryptie, en het doet precies waarvoor de naam staat. Drie keren encrypten met 3 verschillende sleutels van 56 bits. Omdat 3DES encryptie 3 keer wordt uitgevoerd is het niet het meest efficiënte encryptie methode die er bestaat. Ook is het makkelijk om te decrypten, omdat 3DES een kleinere blok lengte gebruikt.

Twofish[26]
Twofish heeft een blok grootte van 128bits tot 256 bits. Het werkt bijna net als AES, maar de ronde die het erover doet is niet gevarieert net als bij AES. Er is altijd 16 ronden.
Het voordeel van Twofish is, is dat het een gratis gebruikt mag worden zonder enige problemen.

RSA[26][27]
RSA is genaamd naar Rivest,Shamir en Adleman. Deze 3 mensen hebben RSA ontworpen.
RSA is een asymmetrische encryptie, dat 2 sleutels gebruikt. Een publieke en een private key.
Je hebt beide sleutels nodig om een bericht of data te encrypten en te decrypten. De algoritme maakt gebruik van het product van 2 grote priem getallen. Meeste RSA sleutels zijn de 1024 bits en 2048 sleutels. Omdat de sleutels zo groot zijn, duurt het wel een tijdje om te encrypten en te decrypten. Voordeel hiervan is dat het moeilijk is om te ontcijferen voor hackers, zij weten namelijk ook niet welke priemgetallen er gebruikt wordt. Niet geschikt voor grote data.

Encryptie	Snel	Veilig (secure)	Gratis
AES	X	X	X
3DES			X
Twofish	X		X
RSA		X	X

Kwaliteitseisen (Security)

- Data encrypted door sturen
- Onnodige poorten sluiten
- Code controleren en onnodige eruit slopen
- Database beveiligen
- Liefst API gebruiken en geen directe verbinding
- Encryptie gebruiken dat

Advies Security

Het is beter om geen directe verbinding te maken met de database en liefst de database ook goed beveiligen. Idem met data versturen. Het encryptie dat aangeraden wordt is AES aangezien die veilig, snel en open source is. Ook is beter om simpele SQL injection te voorkomen door te whitelisten en blacklisten wat wel en niet ingevoerd mag worden. Het zou ook slim zijn om de pasjes niet kopieerbaar te maken door EMV-chip pasjes te gebruiken, maar natuurlijk niet verplicht voor school project, omdat het geld kost.

1.3 Vertrouwen

Het is belangrijk om de gebruikers te overtuigen dat onze product goed en veilig is.
Hoe zorgen we ervoor dat de klanten ons vertrouwen? Eerste kennismaking met onze product is heel belangrijk, want dit blijft bij klanten hangen. Maak een goede logo, een nette GUI, Veilige GUI en Database. De klanten overtuigen dat onze product gemaakt zijn door professionelen enz. Wij moeten als bank de klant ook overtuigen dat geen data van hun gaan lekken, daarom moet ons hele bank goed beveiligd ingericht worden.

De foto's die gebruikt worden voor onze bank is natuurlijk niet een goed idee.

Kwaliteitseisen

- Goede logo
- Nette werkende GUI
- Klanten overtuigen dat ons product uitstekend is
- Klanten overtuigen dat ons product beveiligd is

1.4 Tevredenheid

Voor een bank is het belangrijk dat de gebruikers tevreden zijn met onze diensten. Vandaar hebben we kwaliteitseisen nodig zijn. Feedback van docenten en gebruikers vragen en die mee te nemen naar volgende sprint om te verbeteren.

Kwaliteitseisen:

- Niet verkeerde biljetten of te weinig biljetten uitspugen
- Geldautomaat moet correct werken
- Het creëren van een veilige en vertrouwde omgeving
- Maak er geen complex, moeizaam proces van (Vriendelijk voor gebruikers)
- Uitspugen van geld mag niet te lang duren

Risico log

fx 16-05-2018

	A	B	C	D	E	F	G	H	I
1	#	Risico Beschrijving	Kans	Impact	Risico	Maatregel	Status	Status Omschrijving	Datum
2	R1	Stroeve communicatie begin project, laat bijeengekomen voor plan individuele bijdrage groepsdeel	4	3	12	Beter communiceren over bijeenkomsten plannen	:)	Probleem opgelost door betere afspraken te maken over communicatie	09-05-2018
3	R2	Afwezigheid projectlid	2	2	4	Goede communicatie met betrekking tot afspraken en werk overnemen	:)	Geen probleem bij de groep, communicatie verliep goed	16-05-2018
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									

Sheet1

Github naam: HjimR
Link: https://github.com/HjimR/Project4Individueel

Kans: schaal 1 (klein) t/m 5 (zeer groot)
Impact: schaal 1 (zeer lage) t/m 5 (zeer hoge)
Risico: = kans * impact
:): [status] :) opgelost, :| bezig; :(niet opgelost; N nieuw

Issue tracking log

Groepsnaam: Saatbank

#	Datum	Issue	Verantwoordelijk	😶	Datum	Beschrijving
J1	**16-05-18**	**Nog niet helemaal een idee**	**Jimmy**	😐	**18-05-18**	**Idee binnen**
					19-05-18	**Bezig met ontwerp**

Tot nu toe niet veel issues (wat goed is)

Bronnenlijst

[1] https://www.youtube.com/watch?v=OXXKE4sN-4Y
[2] https://en.wikipedia.org/wiki/Aluminium
[3] http://www.infomine.com/investment/metal-prices/aluminum/
[4] https://en.wikipedia.org/wiki/Iron
[5] http://www.infomine.com/investment/metal-prices/iron-ore-fines/
[6] https://en.wikipedia.org/wiki/Stainless_steel
[7] https://agmetalminer.com/metal-prices/stainless-steel/
[8] https://en.wikipedia.org/wiki/Lego_Mindstorms_NXT
[9]https://www.anaheimautomation.com/manuals/forms/Stepper%20Stepper%20Motors%2020120301%20-%20Stepper%20Motors%20versus%20Servo%20Motors.pdf
[10]http://www.alertboot.com/blog/blogs/endpoint_security/archive/2009/02/03/usb-port-security-control-software-how-it-works-and-why-you-need-it.aspx
[11] https://securebox.comodo.com/whitelist-vs-blacklist/
[12] https://www.mulesoft.com/resources/api/what-is-an-api
[13] https://en.wikipedia.org/wiki/Transport_Layer_Security
[14]https://en.wikipedia.org/wiki/Skimming_(fraud)
[15] https://www.thebalance.com/how-credit-card-skimming-works-960773
[16] https://www.politie.nl/themas/skimming.html
[17]https://www.w3schools.com/sql/sql_injection.asp
[18] https://en.wikipedia.org/wiki/SQL_injection
[19] https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
[20]https://nl.wikipedia.org/wiki/Encryptie
[21]https://www.clarox.nl/bestanden-versleutelen
[22]https://nl.wikipedia.org/wiki/Encryptie#Symmetrisch
[23]https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[24]https://en.wikipedia.org/wiki/SHA-1
[25] https://www.chasepaymentech.com/faq_emv_chip_card_technology.html
[26] http://www.toptenreviews.com/software/articles/secure-encryption-methods/
[27] https://en.wikipedia.org/wiki/RSA_(cryptosystem)
[28] https://www.aescrypt.com/

Bijlage

NXT brick

geld dispenser met lego mindstorm

Github link: https://github.com/HjimR/Project4Individueel