|  |
| --- |
| ICTM1N2 |
| Concept Securityscan |
| Windesheim |

|  |
| --- |
| Kevin Scherpenzeel, Siem Evertsen, Yannick Santing, Sem van Der Meulen  15-12-2019 |

**Risicoanalyse**

Het grootse gevaar bij dit project is het verliezen van klantgegevens of dat de site wordt gehackt als dit misgaat komen er niet alleen directe problemen maar zou het ook het vertrouwen en beschikbaarheid in het bedrijf WWI kapot kunnen maken. Om dit te voorkomen moeten we extra maatregelen treffen. Ook moeten we kijken of het opslaan van klantgegevens een goed idee is.

Ook moeten we kijken dat er geen virussen op de site komen, want virussen kunnen credit cart gegevens van klanten openbaar komen te staan. Hiervoor moet een dure antivirussoftware geïnstalleerd worden. Ook al kost dit veel geld is het toch de moeite waard om dit erop te zetten, want anders beschadigen de virussen de klantgegevens en de website. Door deze problemen daalt de vertrouwelijkheid ook weer van de website en zullen dus minder mensen dingen gaan bestellen.

Er is ook de risico dat hackers door SQL-injecties de website kapot kunnen maken. Op deze manier kunnen hackers gratis producten bestellen of de database van onze website kapot maken door SQL-query’s in het inlogsysteem te of de zoekbalk te gebruiken. Een voorbeeldje hiervan is DROP TABLE users. Door fouten in de database wordt de beschikbaarheid van de website ook minder, omdat de database dan niet werkt. Dan is er dus ook een downtime wat de beschikbaarheid verminderd. Als deze query wordt uitgevoerd word de hele tabel users in de database verwijderd. Hiervoor kunnen meerdere maatregels voor worden getroffen. Ten eerste moet voordat de website online gaat er een grondige test periode komen zodat er zo min mogelijk fouten in het systeem zitten. Ten tweede moet er regelmatig iemand zijn die de orders nakijkt zodat er niet alsnog misbruik wordt gemaakt van eventuele fouten in het systeem.

**Beschrijving ingebouwd veiligheidsniveau**

Voor de webshop zijn er veel verschillende maatregelingen genomen om alles veilig te houden.   
Zo is er extra code toegevoegd die sql injecties tegen gaan, want als ze met een sql injectie in de database kunnen komen kunnen ze overal bij, zoals klantgegevens, orders, prijzen etc. Er wordt mysqli gebruikt om injecties tegen te gaan, door mysqli kunnen er geen sql query’s in het inlog scherm of de zoekbalk worden ingevuld. Daarnaast worden wachtwoorden van gebruikers versleutelt met md5. Door md5 zijn de wachtwoorden niet meer zichtbaar in de database, dus als iemand wel je database hackt kan diegene niet bij accounts van klanten.   
$password = md5($password\_1); Dit stukje code zorgt ervoor dat de wachtwoorden in de database worden gehashed.  Door deze maatregels kunnen woord de beschikbaarheid van de website hoger, de vertrouwelijkheid wordt hoger en de betrouwbaarheid stijgt. Verder moet er ook nog een stukje privacy in voor komen, dit doen we door bijvoorbeeld wachtwoorden weer te geven met \*\*\*\*, zodat anderen je wachtwoord niet kunnen bekijken bij het inloggen of registreren.

**Advies**

Wachtwoorden kunnen nog niet worden veranderd en het advies om dit aan te pakken is door middel van een mail te sturen naar het mail account van de gebruiker. In deze mail staat dan een code waarmee de gebruiken kan verifiëren dat hij de gebruiker is. Wanneer de code is ingevuld dan kan hij het wachtwoord veranderen.

Ook wordt er geadviseerd om javascript injections tegen te gaan. Hier is nog niet naar gekeken.