Door groep 3;versie 1.0.0

Security Rapport

Van NerdyGadgets

# Inleiding

Tegenwoordig worden er veel cyberaanvallen gepleegd op websites en webshops, waardoor bijvoorbeeld waardevolle gegevens van klanten en wachtwoorden worden gehackt en misbruikt. Als gevolg hiervan wil NerdyGadgets een grondig onderzoek uitvoeren naar de beveiligingsmaatregelen die wij hebben genomen voor onze webshop. Het doel hiervan is om potentiële problemen te identificeren voordat kwaadwillige hackers dat doen. Daarom stellen wij ons de vraag: hoe veilig is webshop NerdyGadgets voor de klant en het bedrijf.

Om die hoofdvraag te beantwoorden, hebben wij diverse bronnen gebruikt. Een bron die we vaak hebben gebruikt, is de theorie van Inleiding Security. Andere bronnen die we hebben gebruikt zijn onder andere Kinsta, Tweakers en Wikipedia. Echter zijn er paar randvoorwaarden voor de bronnen, namelijk dat bepaalde websites niet met helemaal betrouwbaar zijn, waardoor we de maatregelen voor de risico’s niet 100% kunnen gaan werken op de risico’s.

Dit rapportage is het resultaat van een onderzoek naar de veiligheid van onze webshop NerdyGadgets. Het doel van dit rapport is om inzicht te krijgen om potentiële risico’s te identificeren en suggesties te doen om de veiligheid te verbeteren van de website. Daarom start het rapport met een paar risico’s die de website in gevaar zouden kunnen brengen. Hierbij bedenken we bijpassende maatregelen om de risico’s te vermijden. Vervolgens komt een beschrijving van een ingebouwd beveiligingsniveau. Tot slot volgt een advies voor vervolgstappen.

Inhoudsopgave

[Inleiding 1](#_Toc152096293)

[Risicoanalyse 3](#_Toc152096294)

[Beschrijving ingebouwd veiligheidsniveau 4](#_Toc152096295)

[Advies over vervolgstappen 5](#_Toc152096296)

[Conclusie 6](#_Toc152096297)

# Risicoanalyse

Geschreven door: Alexander Dijkhuizen en Wiljan Verhoeven

Een risicoanalyse kan verschillende mogelijke risico’s voor een webshop identificeren, waarbij de focus ligt op de beschikbaarheid, integriteit en vertrouwelijkheid.

De mate waarin de gebruikers en het bedrijfsinformatiesysteem toegang hebben tot de informatie die ze nodig hebben, wordt ook wel beschikbaarheid genoemd. Integriteit is de mate waarin de informatie up-to-date is en geen fouten bevat. Vertrouwelijkheid is de mate waarin informatie alleen toegankelijk is voor een bepaalde groep die daar rechten toe heeft.

Hier zijn voorbeelden die voor mogelijke risico’s:

1. Een risico kan zijn ongeautoriseerde toegang tot klantgegevens of bestelgegevens. Hierbij zijn de vertrouwelijkheid en integriteit in gevaar. Als ongeautoriseerde gebruikers toegang krijgen tot klantgegevens, kan dit leiden tot een schending van de vertrouwelijkheid van deze gegevens. Ook kan onvoldoende authenticatie leiden tot ongeautoriseerde wijzigingen in bestelgegevens, waardoor de integriteit in gevaar komt. Mogelijke maatregelen zijn om sterke authenticatieprotocollen, het laten bewijzen dat de persoon echt is wie hij of zij zegt dat-ie is, te implementeren, zoals een twee-factor-authenticatie. Ook kan een zorg voor een uitgebreid autorisatiesysteem dat toegangsrechten op basis van gebruikersrollen beperken een goede maatregel zijn voor deze risico. Als laatst is het regelmatig uitvoeren van audits, het bijhouden wat er precies gebeurt, om de effectiviteit van het systeem te controleren een goede maatregel.
2. Een risico kan zijn manipulatie van de database en diefstal van gevoelige informatie. Hierbij zijn in integriteit en vertrouwelijkheid in gevaar. SQL-injectieaanvallen richten zich vaak op databasemanipulatie, waardoor de integriteit van opgeslagen gegevens wordt bedreigd. Een aanvaller kan de vertrouwelijkheid schenden als hij of zij code-injectie, het misbruiken van een computerfout waarbij een programma onjuiste gegevens verwerkt, kan gebruiken om bijvoorbeeld gevoelige gegevens door te verkopen. Mogelijke maatregelen kan zijn het beperken van databasegebruikersrechten om de impact van een succesvolle aanval te minimaliseren. Ook om SQL-injectie te voorkomen, is het ‘hashen’ van wachtwoorden, een specifieke set tekens of een sleutel die kan worden verander in een andere waarde, om meer gevoelige gegevens te beschermen.
3. Een risico kan zijn gestolen gegevens tijdens de gegevensoverdracht tussen de gebruiker en de webserver. Het feit dat HTTP (Hypertext Transfer Protocol) geen versleuteling biedt, maakt het verzenden van gegevens in platte tekst mogelijk voor hackers met slechte bedoelingen. Als er een onveilige verbinding is, kan een aanvaller de verzonden gegevens stelen en gevoelige gegevens zoals inloggegevens, persoonlijke gegevens of betalingsgegevens zien. Dit kan de vertrouwelijkheid van gegevens die worden verzonden gaan schenden. Een mogelijke maatregel kan zijn het gebruik maken van HTTPS (Hypertext Transfer Protocol Secure), wat zorgt voor versleutelde communicatie tussen de webserver en de browser van de gebruiker.
4. Een risico kan zijn het verlies van gegevens als gevolg van onvoorziene gebeurtenissen. Hierbij komt de beschikbaarheid van gegevens in gevaar. Het gebrek aan regelmatige back-ups kan leiden tot gegevensverlies en verstoring van de beschikbaarheid veroorzaken. Mogelijke maatregelen kan zijn regelmatig back-ups maken van alle belangrijke gegevens. Ook het bewaren van back-ups apart van het primaire systeem, zoals op een USB of op een externe locatie is een goede maatregel voor deze risico.
5. Een Distributed of service (DDoS)-aanval kan de beschikbaarheid van de webshop verstoren door de servers te overbelasten. Dit kan leiden tot langdurige downtime en verlies van klanten. Ook gaan terugkerende klanten hierdoor minder vertrouwen hebben in de webshop. Maatregelen kunnen bestaan uit het implementeren van DDoS-bescherming diensten en het schaalbaar maken van de infrastructuur om de impact van de aanvallen te verminderen.
6. Het kan zijn dat er ongeautoriseerde toegang komt tot financiële gegevens bij kwetsbare beveiliging van het betalingssysteem. Hierdoor zouden en ongeautoriseerde mensen bij de financiële gegevens van andere komen en deze gebruiken voor hun eigen doeleinde. Het implementeren van secure socket layer (SSL)-certificaten en volgen van PCI DSS (Payment Card Industry Data Security Standard) zijn manieren om dit risico te verminderen.
7. Onvoldoende sessie beveiliging kan leiden tot sessie-hijacking, waarbij iemand de controle overneemt van een actieve sessie, hierdoor kan een hacker de gegevens die zijn opgeslagen in de cookie gebruiken om in te loggen op andere accounts. Sterke sessie beheer praktijken zoals het gebruik van unieke sessie id’s en regelmatig sessietokens vernieuwen zijn nodig om dit risico tegen te gaan.
8. Wanneer een webshop afhankelijk is van een derde partij zoals een plug-in kan er een beveiligingslek ontstaan. Als de derde partij geen juiste beveiligingsmaatregelen heeft kunnen hackers via de derde partij in de data van de webshop komen. Maatregelen tegen dit risico zijn het regelmatig checken van de beveiligingsmaatregelen checken van de derde partij en updates en patches zo snel mogelijk toepassen.

De risico’s worden nog een keer in een tabel weergegeven in een vorm van kwalitatieve risicoanalyse en kan een waarde krijgen van laag (L), gemiddeld (G) of hoog (H):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Kwetsbaarheid** | **Kans** | **Toelichting kans** | **Schade** | **Toelichting schade** | **Maatregelen** |
| Onvoldoende authenticatie | L | Het kost veel moeite om in de database te komen. | H | De hacker heeft de informatie van personen die op de database staan. | Sterke authenticatieprotocollen, zoals een twee-factor-authenticatie;  Een uitgebreid autorisatiesysteem;  Regelmatig uitvoeren van audits |
| SQL-injectie-aanval | H | Het is niet lastig om een database aan te kunnen passen via een tekstvak. | H | De gebruiker kan de database aanpassen en gegevens bemachtigen. | Het beperken van databasegebruikersrechten om de impact van een succesvolle aanval te minimaliseren;  Ook om SQL-injectie te voorkomen, is het ‘hashen’ van wachtwoorden |
| Gestolen gegevens tijdens de gegevensoverdracht | H | Hackers gaan vaak naar de overdracht van de informatie, omdat het de zwaktes is van beveiliging. | H | De hacker krijg niet alleen informatie van wat er verstuurd wordt, maar ook van wie en naar wie. | Het gebruik maken van HTTPS |
| Het verlies van gegevens als gevolg van onvoorziene gebeurtenissen | L | Het is onvoorspelbaar dat bijvoorbeeld een overstroming of stroomuitval gebeurd, maar de kans is er wel | H | Zonder maatregel is de kans groot dat je alle gegevens van de database verliest. | Regelmatig back-ups maken van alle belangrijke gegeven;  Het bewaren van back-ups apart van het primaire systeem, zoals op een USB of op een externe locatie |
| Distributed of service (DDoS)-aanval | L | Er zijn weinig motieven van de hacker om een DDoS-aanval te plegen. Ook is er echt veel internetverkeer nodig, voordat de server wordt overbelast. | G | De website is offline is een tijdje offline, waardoor je klanten mogelijk verliest en geld. | Implementeren van DDoS-bescherming diensten;  Het schaalbaar maken van de infrastructuur om de impact van de aanvallen te verminderen |
| Ongeautoriseerde toegang | G | Hackers moeten toegang hebben tot accounts en iedere keer proberen tot e-mail en wachtwoord gelijk zijn. | H | Ongeautoriseerd persoon kan toegang krijgen tot admin-account dat wellicht taken kan uitvoeren dat hij niet mag. | Het implementeren van secure socket layer-certificaten;  Volgen van PCI DSS |
| Onvoldoende sessie beveiliging | L | Hiervoor moet de hacker controle nemen van het apparaat van een persoon. | H | Hij kan hiermee het account overnemen van de persoon en hiermee accountgegevens stelen of aanpassen. | Sterke sessie beheer praktijken zoals het gebruik van unieke sessie id’s en regelmatig sessietokens vernieuwen |
| Afhankelijk van een derde partij | L | De derde partij moet achterlopen op beveiligingsstandaarden en moet de hacker op de hoogte zijn van de derde partij’s achterlopende beveiligingsstandaarden. | H | Via deze derde partij kan de hacker de database aanpassen. | Regelmatig checken van de beveiligingsmaatregelen checken van de derde partij en updates en patches zo snel mogelijk toepassen. |

# Beschrijving ingebouwd veiligheidsniveau

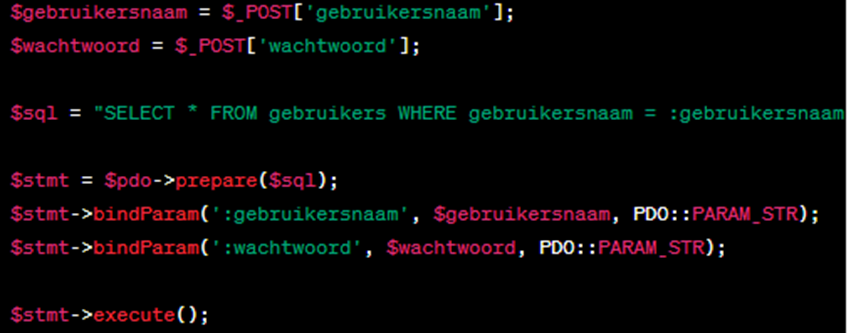
Geschreven door Danyaal Burney & Hieu Phan

In dit gedeelte gaan we dieper in op de maatregelen die we hebben genomen om de beveiliging van onze webshop te waarborgen, zoals eerder vastgesteld in de risicoanalyse. We willen duidelijk maken hoe we specifieke beveiligingseisen hebben omgezet naar concrete oplossingen op onze website. We bespreken hoe we de vertrouwelijkheid van gevoelige informatie behouden, hoe we aanvallen op de integriteit voorkomen en hoe we cruciale aspecten zoals autorisatie, authenticatie en identificatie hebben verwerkt. Om deze aanpak tastbaarder te maken, laten we enkele korte stukjes code zien die illustreren hoe deze beveiligingsmaatregelen zijn geïntegreerd in de structuur van de website. Deze codefragmenten dienen niet alleen als praktisch voorbeeld van onze implementatie, maar ook als handige referentie voor het ontwikkelteam en andere betrokkenen bij het onderhoud en de verdere ontwikkeling van de webshop.

## 2.1 SQL Injectie

Om te voorkomen dat SQL injectie-aanvallen kunnen plaatsvinden, hebben we verschillende preventieve maatregelen genomen. Hierbij maken we gebruik van correcte programmeercodes en controleren we de invoer van de gebruiker zorgvuldig om te waarborgen dat deze voldoet aan de gestelde voorwaarden. Om te voorkomen dat SQL-injectieaanvallen plaatsvinden, implementeren we aanvullende beveiligingsmaatregelen. Een kritisch aspect van onze beveiligingsstrategie omvat het zorgvuldig coderen van onze programma's. We voeren grondige controles uit op alle gebruikersinvoer om te verifiëren of deze voldoet aan vooraf bepaalde voorwaarden. Dit proces van inputvalidatie is van cruciaal belang om het risico op schadelijke invoer, die SQL-query's zou kunnen manipuleren, te verminderen.

Hier is een voorbeeld hoe dit met een code kan worden geïmplementeerd:



## 2.2 Wachtwoord Hashing

In ons streven om de gegevens van onze gebruikers op de webshop te beschermen, hebben we extra stappen genomen die echt van betekenis zijn. Een van deze belangrijke maatregelen is het zogenaamde 'hashen' van wachtwoorden. In feite betekent dit simpelweg dat we een soort unieke code genereren op basis van het ingevoerde wachtwoord. Het bijzondere hieraan is dat het een eenrichtingsproces is. Met andere woorden, zelfs als er ongeautoriseerde toegang is tot onze databases, kunnen de gehashte wachtwoorden niet zomaar worden omgezet naar leesbare tekst.

Deze aanpak voegt een extra laag van bescherming toe aan de persoonlijke gegevens van onze gebruikers. Dus, zelfs in het onwaarschijnlijke geval van een datalek, kunnen indringers niet direct toegang krijgen tot bruikbare wachtwoorden. Dit beschermt de vertrouwelijkheid van de informatie die onze gebruikers invoeren, wat vanzelfsprekend van groot belang is voor hun online veiligheid.

Waarom doen we dit? Niet alleen als reactie op mogelijke risico's, maar ook als proactieve maatregel om de integriteit van onze webshop te waarborgen. Door wachtwoorden te hashen, verhogen we niet alleen aanzienlijk de beveiliging van onze online omgeving, maar laten we ook zien dat we serieus bezig zijn met het beschermen van de privacy van onze gebruikers. Deze maatregel maakt integraal deel uit van ons bredere streven om een veilige digitale ruimte te bieden aan iedereen die onze webshop bezoekt.

# Advies over vervolgstappen

Geschreven door: Shahzaib Saleem

In dit hoofdstuk nemen we een diepere duik in de veiligheid van de webshop en bieden we praktische adviezen om ervoor te zorgen dat jouw online winkel een veilige en betrouwbare omgeving blijft. We begrijpen dat de wereld van online beveiliging complex kan lijken, maar maak je geen zorgen, we gaan stap voor stap door de belangrijkste punten.

Met het internet dat altijd in beweging is, zijn er nieuwe gevaren die kunnen opduiken. Of het nu gaat om hackers die proberen je webshop offline te halen, mensen die proberen in te breken met brute kracht, of stiekeme scripts die je webpagina's willen verpesten, we willen ervoor zorgen dat je webshop hier tegen bestand is.

**DDoS aanval**

* Een DDoS-aanval, oftewel Distributed Denial-of-Service, is als een digitale storm die jouw website tijdelijk ontoegankelijk maakt. Hoe gebeurt dit precies? Nou, stel je voor dat er een enorme hoeveelheid verkeer naar jouw server wordt gestuurd. Het lijkt een beetje op een snelweg die plotseling overspoeld wordt met auto's, waardoor alles vast komt te zitten.

*Waarom is dit een probleem?*

* Als dit gebeurt, kunnen mensen je website niet meer bezoeken. Het is alsof de deuren van je online winkel even op slot zitten. En dat is natuurlijk het laatste wat je wilt als ondernemer.

*Wat kunnen we hieraan doen?*

* Gelukkig zijn er manieren om jezelf te beschermen tegen deze digitale overstroming. Moderne firewalls, als de poortwachters van het internet, hebben slimme trucjes om een DDoS-aanval te herkennen. Ze kunnen als een soort superheld de aanval stoppen voordat deze schade aanricht.   
    
  Maar dat is niet alles. Je kunt ook overwegen om een soort digitaal schild in te schakelen - een anti-DDoS-service. Dit is als het inhuren van een beveiligingsdienst voor je website. Ze houden constant een oogje in het zeil en kunnen verdacht verkeer herkennen. Stel je voor dat ze ongewenste gasten aan de deur zien staan en deze vriendelijk, maar resoluut, wegsturen.

*Technische kant*

* Nu, als je meer van de technische kant houdt, zijn er tal van ingewikkelde maatregelen die je kunt nemen. Je kunt bijvoorbeeld specifieke regels instellen om verdacht verkeer te blokkeren. Het is als het beveiligen van je huis met geavanceerde sloten en alarmen, maar dan voor je website.

Kortom, er zijn verschillende manieren om jezelf te beschermen tegen een DDoS-aanval. Of het nu gaat om slimme firewalls of een externe beveiligingsdienst, deze digitale schilden zorgen ervoor dat jouw online winkel blijft draaien, zelfs als er een digitale storm opsteekt.

**Brute-Force**

* Een Brute-Force aanval op een login scherm is als een digitale inbraakpoging waarbij hackers proberen binnen te glippen door verschillende combinaties van wachtwoorden lukraak uit te proberen. Het is alsof ze keer op keer proberen verschillende sleutels in het slot van je voordeur te steken, hopend dat er eentje past.

*Waarom is dit een probleem?*

* Als deze aanvallen succesvol zijn, kunnen hackers toegang krijgen tot je website alsof ze een geheime deur hebben gevonden. En eenmaal binnen kunnen ze chaos veroorzaken, zoals het veranderen van je website of het misbruiken van gevoelige gegevens. Dat is natuurlijk iets wat je koste wat het wilt voorkomen.

*Wat kunnen we hieraan doen?*

* Nu, hier komt het goede nieuws: we kunnen ons ertegen beschermen. Hoewel we Brute-Force aanvallen niet helemaal kunnen voorkomen, kunnen we ze wel verzwakken en minimaliseren.
* Stel je voor dat je de voordeur van je huis beveiligt met een slimme camera en een alarmsysteem. Als iemand herhaaldelijk probeert binnen te komen, wordt dat meteen opgemerkt. Op dezelfde manier kunnen we het login-scherm uitrusten met beschermingsmaatregelen.

*Technische kant*

* Op technisch vlak kunnen we slimme beveiligingsregels instellen. Bijvoorbeeld, we kunnen het systeem zo instellen dat het tijdelijk wordt vergrendeld na een aantal mislukte pogingen. Het is als het automatisch sluiten van de deur als iemand te vaak de verkeerde sleutel gebruikt. Uiteindelijk zullen de aanvallers ontmoedigd raken en stoppen.

Kortom, Brute-Force aanvallen zijn als een digitale inbraakpoging, maar met de juiste beveiligingsmaatregelen kunnen we ervoor zorgen dat het lijkt alsof er een ondoordringbaar schild rondom je website staat. Zo blijft de digitale voordeur veilig vergrendeld, zelfs als hackers allerlei sleutels proberen.

# Conclusie

Hoe veilig is webshop NerdyGadgets voor de klant en het bedrijf? In dit rapport probeerden we deze vraag te beantwoorden.

In hoofdstuk 1 hebben we kunnen concluderen welke mogelijke risico’s er zijn die de webshop kunnen bedreigen op vlaktes van betrouwbaarheid, integriteit en vertrouwelijkheid. We hebben gezien welke risico een hoge, lage of een gemiddelde kans en schaden hebben en hoe we deze dan oplossen. Daarom kunnen we zeggen dat de risico’s met vooral de hoogste schade, een hogere prioriteit hebben om het te implementeren, zodat de kans lager wordt.

In hoofdstuk 2 hebben we laten zien welke risico’s we al hebben genomen. Daar hebben we gezegd dat we al risico’s hebben genomen tegen SQL-injecties en het gebruik maken van wachtwoord hashing. Dit bevordert het vertrouwen van de klant in onze website, waardoor het bedrijf geen klanten verliest en blijft groeien in succes.

In hoofdstuk 3 namen we een diepere duik in de in de veiligheid van de webshop en bieden we praktische adviezen om ervoor te zorgen dat jouw online winkel een veilige en betrouwbare omgeving blijft. We hebben gekeken naar DDoS-aanvallen en Brute-Force-aanvallen en ons zelf verdiept waarom dit een probleem is, wat we hier tegen aan kunnen doen en op technische kanten we dit kunnen verbeteren.

We kunnen hiermee concluderen dat de veiligheid van de webshop in een goede richting gaat, zoals al implementeren van SQL-injecties en wachtwoord hashing. Echter kunnen we ook zeggen dat er veel aan de veiligheid nog moet worden gedaan, zoals een sterkere authenticatie.

Hoewel er meer dreigingen op kunnen komen en meer risico’s ontstaan, blijft de webshop groeien in verbeteringen en voeren we zoveel mogelijk beveiligingsmaatregelingen in om de klant tevreden te houden en het bedrijf succesvol in werking. De klant zelf kan ook maatregelen nemen, zoals een antivirussysteem aanschaffen. Alleen samen kunnen we de veiligheid van NerdyGadgets bevorderen.

# Literatuurlijst

Daityari, S. (2023, 12 oktober). SQL injectie: Een gedetailleerde handleiding voor WordPress gebruikers. Kinsta. Geraadpleegd op 28 november 2023, van https://kinsta.com/nl/blog/sql-injecties/

Schellevis, J. (2012, 19 maart). SQL-injectie en XSS: de beste verdediging. Tweakers. Geraadpleegd op 28 november 2023, van https://tweakers.net/reviews/2531/all/sql-injectie-en-xss-de-beste-verdediging.html

Wikipedia-bijdragers. (2023, 8 september). Distributed denial-of-service. Wikipedia. Geraadpleegd op 28 november 2023, van https://nl.wikipedia.org/wiki/Distributed\_denial-of-service

Windesheim. (2023). Inleiding Security - Rise. leren.windesheim.nl. Geraadpleegd op 28 november 2023, van https://leren.windesheim.nl/d2l/le/lessons/67817/topics/805644