SecurityVERSLAG NERDYGADGETS

**ICTM1n4**

Inhoud

[Inleiding 2](#_Toc59441868)

[Risicoanalyse 3](#_Toc59441869)

[Beschikbaarheid 3](#_Toc59441870)

[Integriteit 3](#_Toc59441871)

[Vertrouwelijkheid 4](#_Toc59441872)

[Ingebouwd veiligheidsniveau 4](#_Toc59441873)

[SQL injectie 4](#_Toc59441874)

[Gevoelige data aflezen 5](#_Toc59441875)

[Rechten op de database 6](#_Toc59441876)

[Passwordpolicy 6](#_Toc59441877)

[Advies over vervolgstappen 7](#_Toc59441878)

[Aflezen/wijzigen van sessies (Sessionhijacking) 7](#_Toc59441879)

[Database is niet meer beschikbaar 8](#_Toc59441880)

[DDOS aanval 9](#_Toc59441881)

[Spam voor mailhost 9](#_Toc59441882)

[Conclusie 10](#_Toc59441883)

# Inleiding

Dit document bevat een verslag van de beveiliging en mogelijke risico’s waar de NerdyGadgets webshop mee te maken kan hebben. Het verslag is opgedeeld in de risicoanalyse met informatie over de mogelijke kwetsbaarheden die de webshop bevat, het al aanwezige veiligheidsniveau met de maatregelen die tegen die kwetsbaarheden zijn genomen, en een advies over verdere vervolgstappen voor het beschermen tegen de kwetsbaarheden. Tot slot bevat dit verslag een conclusie met een samenvatting over wat in het verslag besproken is.

# Risicoanalyse

Dit hoofdstuk van het verslag beschrijft de mogelijke kwetsbaarheden van de NerdyGadgets webshop, deze kwetsbaarheden zijn ingedeeld onder de drie beveiligingsaspecten die zeer belangrijk zijn voor het correct en vertrouwd functioneren van de website. Wanneer één of meerdere van deze beveiligingsaspecten onder druk staat kan dat leiden tot een afname van de reputatie van NerdyGadgets, en als gevolg een afname van de bezoekersaantallen op de webshop. Ook kunnen hier juridische gevolgen aan vasthangen.

## Beschikbaarheid

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kwetsbaarheid** | **Kans** | **Schade** | **Maatregel** | **Restrisico** |
| Database is niet meer beschikbaar | L | H | Meerdere servers, backups | M |
| DDOS aanval | H | H | Blacklists, goede infrastructuur | M |
| Spam voor mailhost | H | M | Afspreken host | M |

De beschikbaarheid van de webshop beschrijft de totale uptime van alle functies van de webshop. Wanneer één of meer functies van de website onbeschikbaar zijn door externe invloed dan spreken we over een verminderde beschikbaarheid. Een aanval of een intern probleem kan slechts één of meer functies van de webshop belemmeren, maar in het ergste geval kunnen bezoekers de website helemaal niet meer bereiken.

## Integriteit

De integriteit van een webshop beschrijft de volledigheid en correctheid van de data die de webshop behandeld en verwerkt. Wanneer data aangepast kan worden door een actor die daar geen rechten voor zou moeten hebben, spreekt men over een verminderde integriteit. Alleen wanneer de data van de webshop volledig aanwezig is in de vorm dat het aanwezig moet zijn, spreken we over volledige integriteit.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kwetsbaarheid** | **Kans** | **Schade** | **Maatregel** | **Restrisico** |
| Verandering van sessie | M | H | SessionManagement | L |
| GET aanpassen | H | H | Geen belangrijke data in de GET zetten | H |
| Rechten Database | M | H | Gepaste gebruikersaccounts | M |
| SQL-injectie | M | H | Prepared statement | L |

## Vertrouwelijkheid

De vertrouwelijkheid van een webshop beschrijft de bescherming van data tegen actors die niet het recht hebben om die data in te zien of te kennen. Wanneer een actor toegang krijgt tot gevoelige data zoals wachtwoorden, e-mails, namen van gebruikers, ook al kan deze actor deze data niet wijzigen, spreekt men over een verminderde vertrouwelijkheid. Het beschermen van de vertrouwelijkheid is belangrijk om de privacy van de klanten en de partners van NerdyGadgets te waarborgen.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kwetsbaarheid** | **Kans** | **Schade** | **Maatregel** | **Restrisico** |
| SQL-injectie | H | H | Prepared statement | L |
| Aflezen van sessies | M | H | SessionManagement | L |
| Wachtwoorden aflezen | M | H | Hashing/passwordpolicy | L |
| Rechten Database | H | H | Gepaste gebruikersaccounts | M |

# Ingebouwd veiligheidsniveau

Dit hoofdstuk bespreekt de veiligheidsmaatregelen die tot nu toe in de webshop aanwezig zijn en hoe deze functioneren. Deze maatregelen hangen af van beschreven kwetsbaarheden in het vorige hoofdstuk. Verdere maatregelen en advies zijn aanwezig in het volgende hoofdstuk.

## SQL-injectie

### Wat het is

Een SQL-injectie is een stuk SQL die uitgevoerd op de server. Deze SQL is aangepast door de ‘hacker’, zodat de server aangepaste resultaten weergeeft die in eerste instantie niet weergegeven mogen worden. Het kan ook zijn dat de ‘hacker’ een stuk code uitvoert die de database zelf in gevaar kan brengen. Dit zou je kunnen doen door de SQL-code af te sluiten met een ‘ (single quote) en vervolgens je eigen SQL-code toe te voegen.

### Risico

Bij een SQL-injectie zijn de grootste risico’s dat er klantgegevens ingezien en/of aangepast worden. Dit is een probleem voor zowel de klant als het bedrijf. Zodra er klantgegevens boven water zijn, kunnen de klanten het bedrijf aanklagen.

Een ander risico is dat er andere gegevens aangepast worden. Denk hierbij aan een kortingscode van 100%. Dit zorgt er dan voor dat iedereen die die code heeft, altijd met 100% korting kan bestelling.

Een laatste risico is dat de ‘hacker’ de complete database verwijderd. Mogelijk is dat de ‘hacker’ voor het verwijderen voor zichzelf een kopie van de database maakt, om deze of aan het bedrijf terug te verkopen, of op de (zwarte) markt aan te bieden.

### Maatregel

SQL-injectie is afgevangen door de ‘msqli\_stmt\_bind\_param’ functie van PHP.   
‘msqli\_stmt\_bind\_param’ is een standaard PHP-functie die invoer op de SQL-functie neutraliseert en voorkomt dat het systeem invoer als SQL-code interpreteert. [[1]](#footnote-1)

Een andere maatregel is om de juiste rechten bij de database users in te stellen. Dit vangt af dat eventuele aangepaste query’s niet uitgevoerd mogen worden op de database. Hiermee voorkom je dat de meeste gegevens worden aangepast en verwijderd.

Door deze maatregel te treffen is SQL-injectie zo goed als onmogelijk geworden. Het kans is daarom laag geworden. Zou er toch een injectie plaats vinden, blijft de schade hoog.

## Gevoelige data aflezen

### Wat het is

Op het moment dat een ‘hacker’ in de database komt, kan diegene alle data uitlezen die hij wilt. In deze data staat sensitieve informatie. Denk hierbij aan wachtwoorden, gebruikersnaam en emailadressen.

Een hash is een beveiligingsmethode die het wachtwoord onleesbaar maakt. Dit kan echter niet teruggedraaid worden. Je kunt checken of je hetzelfde wachtwoord hebt ingevoerd, door de twee hashes met elkaar te vergelijken, of door de hash via een PHP-functie direct met het ingevoerde wachtwoord controleren.

### Risico

Als de gevoelige data uitgelezen kan worden, kan er getest worden met inloggen op andere websites. Zodra de klant op meerdere websites dezelfde combinatie van gebruikersnaam/emailadres en wachtwoord gebruikt, kan de ‘hacker’ hier gebruik van maken.

### Maatregel

De wachtwoorden worden bij ons gehasht in de database gezet. Hiermee voorkom je grotendeels dat de wachtwoorden, zodra de hashes van de wachtwoorden onderschept zijn, te lezen zijn.

De kans dat het wachtwoord gehasht gelezen kan worden, is zo goed als nul. Op het moment dat de hash toch gelezen kan worden, blijft de schade hoog.

## Databaserechten

### Wat het is

Op de database moet worden ingelogd met een SQL-gebruiker. Door verschillende accounts te maken op de database, kun je per account op tabelniveau bepalen wat het account wel en niet mag. De gebruiker ‘root’ is standaard aanwezig, maar bevat uit zichzelf alle mogelijke rechten over de database.

### Risico

Wanneer de root aanwezig is kan er altijd en door iedereen op ingelogd worden. Omdat de root alle mogelijke rechten over een database bevat, is dit een risico. Een gebruiker met toegang tot de root kan bijvoorbeeld de complete database lezen, aanpassen, of totaal verwijderen.

### Maatregel

De database maakt gebruik van verschillende user. Namelijk:

* Klant
* Administrator
* Pi

De user Klant heeft rechten die zich beperken tot het selecteren, invoeren en updaten uit de tabellen die hij nodig heeft uit de database.

De user Administrator heeft rechten die ook de root zou hebben. Echter is deze veiliger, omdat de Administrator een veilig wachtwoord krijgt. Ook wordt de Administrator constant digitaal gemonitord.

De user Pi heeft rechten gebaseerd op dezelfde manier als de rechten van de user Klant. Hij krijgt alleen toegang tot het updaten en invoeren van gegevens in de tabellen die hij nodig heeft

Deze maatregel verminderd de kans aanzienlijk. De gebruikers kunnen niets doen dat buiten hun toegekende rechten valt. De schade blijft hoog, maar hoe ver de schade reikt hangt af van de aanwezigheid van verdere maatregelen.

## Passwordpolicy

### Wat het is

Er worden criteria vastgesteld ten aanzien van het wachtwoord. Dit zorgt ervoor dat er geen hele zwakke wachtwoorden van users ontstaan. Dit helpt ook mee met het hashen van de ingevoerde wachtwoorden. Hoe langer het wachtwoord, hoe langer het duurt om de hash te ontcijferen.

### Risico

Het risico van het geen passwordpolicy hebben, is dat de gebruikers te gemakkelijke wachtwoorden maken. Deze te gemakkelijke wachtwoorden, worden te snel en te gemakkelijk gekraakt.

### Maatregel

Op dit moment wordt er een passwordpolicy gehanteerd. De regels voor een stabiel wachtwoord zijn:

* Het wachtwoord moet minimaal 8 tekens bevatten
* Het wachtwoord moet minimaal 1 hoofdletter en 1 kleine letter.
* Het wachtwoord moet minimaal 1 cijfer bevatten

Door deze maatregel te treffen, verminder je de kans er grotendeels van. De schade blijft hoog.

# Advies over vervolgstappen

Dit hoofdstuk beschrijft advies over verdere veiligheidsmaatregelen die op de NerdyGadgets webshop kunnen worden toegepast. Deze maatregelen kunnen binnen deze sprint niet worden toegepast door een gebrek aan ruimte in de tijdlijn. Enkele van deze maatregelen hangen echter ook af van de aanwezigheid van externe factoren zoals extra servers of databases. De toepassing van deze maatregelen hangt af van de directie van NerdyGadgets.

## Aflezen/wijzigen van sessies (Session-hijacking)

### Wat het is

Session-hijacking is een methode om sessie te onderscheppen, uit te lezen en te wijzigen. Sessies worden vaak gebruikt om data tijdelijk op te slaan. Denk hierbij aan het checken of iemand is ingelogd, of wat er in de winkelwagen staat.

### Risico

Het risico is dat wanneer iemand weet hoe de sessie generatie in elkaar zit, hij tegen de server kan zeggen dat hij ingelogd is, zonder ingelogd te zijn. Ook kan de ‘hacker’ de totaalprijs aanpassen, wat ervoor zorgt dat de ‘hacker’ nooit voor een bestelling hoeft te betalen.

### Advies over maatregelen

Een lijstje van mogelijke maatregelen:

* Een TLS of SSL certificaat
* Een lang nummer of tekst als sessie key
* Het genereren van een nieuwe sessie ID na het succesvolle login

Na deze maatregel uitgevoerd te hebben, verwachten wij dat de kans tussen laag en middel in zit. De schade blijft echter nog steeds hoog.

## Database is niet meer beschikbaar

### Wat het is

De database staat vaak opgeslagen op een server. Deze server kan vanwege allerlei omstandigheden niet meer beschikbaar zijn. Dit kan komen door een, vanuit de server gezien, slechte internetverbinding, maar dit kan ook zijn door dat de server fysiek in brand staat.   
Ook kan het zijn dat een ‘hacker’ de database weggooit. In dit geval wordt er vaak geld gevraagd om de database weer terug te krijgen.

### Risico

Een risico is dat (bepaalde) gegevens niet beschikbaar zijn. Hierdoor kan het bedrijf grote schade oplopen, gebaseerd op de importantie van de data.

Een ander risico is dat de data kwijt geraakt is. Hierdoor kan het bedrijf grote schade oplopen, gebaseerd op de importantie van de data.

### Advies over maatregelen

Eén van de maatregelen die getroffen kunnen worden, is het regelmatig maken van een back-up. Het is wel belangrijk dat de back-up op een afgesloten en offline locatie opgeslagen wordt.

Een tweede server in kunnen schakelen die de eerste server over kan nemen, zodra de hoofdserver niet meer beschikbaar is.

Na deze maatregelen uitgevoerd te hebben, verwachten wij dat de kans gelijk blijft. De schade gaat echter van hoog naar middel.

## DDOS aanval

### Wat het is

Een DDOS-attack is een aanval die veel verzoeken naar de server stuurt. Hierdoor raakt de server overbelast, waardoor er server niet meer goed/volledig werkt.

### Risico

Een consequentie van een DDoS-attack is dat de website niet meer beschikbaar is. Hierdoor kan het bedrijf geen verkoop meer regelen via de website.

### Advies over maatregelen

Een manier om een DDoS-attack tegen te gaan is om automatisch IP-adressen in een blacklist te zetten die teveel verzoeken binnen een bepaald moment uitvoeren.

Een andere maatregel die getroffen kan worden, is het aanschaffen van meerdere servers.  
Wellicht is de aanschaf van meerdere servers niet rendabel in verhouden met de kosten die de schade met zich mee brengen.

Na deze maatregelen uitgevoerd te hebben, verwachten wij dat de kans en schade gelijk blijven.

**Let Op: Een DDoS-attack is zelden volledig tegen te houden.**

## Spam voor mailhost

Op dit moment worden alle mails direct verstuurd. Dit is niet optimaal. Op het moment dat er teveel (vaak boven de 100) mails in een minuut verstuurd worden, kan je host zeggen dat je een spamserver bent.   
Op het moment dat er veel verkeer komt via de mail, is het verstandig om contact op te nemen met je host. Zij kunnen dan jou niet als spamserver noteren, en al je mails door laten gaan.  
Ook kun je verschillende hosts nemen, waardoor het verkeer verdeeld wordt over meerdere servers

### Wat het is

Als er teveel mails door dezelfde mailserver worden verstuurd, kan de host je blokkeren. De host denkt namelijk dat je spam verstuurd.

### Risico

Wanneer de host je blokkeert, staat je server op hun blacklist. In dat geval staat de host niet meer toe dat je enige verdere e-mails verstuurd. Zodra dat het geval is, kan de website geen facturen meer mailen.

### Advies over maatregelen

Een maatregel zou kunnen zijn om zodra je op de blacklist van je host staat, contact op te nemen om je daar af te halen. Hierdoor zou je weer mails kunnen versturen.

Ook zou je verschillende mailhosts kunnen nemen, waardoor je de ballast verdeeld over verschillende hosts.

De schade blijft middel, maar de kans gaat van hoog naar middel.

# Conclusie

Veel kwetsbaarheden van de NerdyGadgets webshop zijn op een basisniveau al beveiligd tegen vele standaard methodes voor het aanvallen van websites en webshops. De webshop is dus relatief resistent tegen simpelere aanvallen, maar blijft kwetsbaar voor aanvallen op een grotere schaal, of aanvallen die gebruik maken van meer ingewikkelde methodes. Het advies is om de al aanwezige veiligheidsmaatregelen te verscherpen en verdere maatregelen toe te voegen aan de hand van dit verslag.

# Bronnenlijst

* 1. https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/#2

1. Zie bron 1 voor meer informatie [↑](#footnote-ref-1)