SecurityVERSLAG NERDYGADGETS

# ICTM1n4

Inhoud

[Inleiding 2](#_Toc58756994)

[Risicoanalyse 3](#_Toc58756995)

[Beschikbaarheid 3](#_Toc58756996)

[Integriteit 3](#_Toc58756997)

[Vertrouwelijkheid 3](#_Toc58756998)

[Ingebouwd veiligheidsniveau 4](#_Toc58756999)

[SQL injectie 4](#_Toc58757000)

[Wachtwoord hashing 4](#_Toc58757001)

[Rechten op de database 4](#_Toc58757002)

[Passwordpolicy 4](#_Toc58757003)

[Advies over vervolgstappen 5](#_Toc58757004)

[Aflezen van sessies 5](#_Toc58757005)

[Database is niet meer beschikbaar 5](#_Toc58757006)

[DDOS aanval 5](#_Toc58757007)

[Spam voor mailhost 5](#_Toc58757008)

[Conclusie 6](#_Toc58757009)

# 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 om de webshop verder te kunnen 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** |
| Database is niet meer beschikbaar | L | L |
| Stroomstoring van server | L | L |
| DDOS aanval | M | H |
| Spam voor mailhost | H | H |

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

|  |  |  |
| --- | --- | --- |
| **Kwetsbaarheid** | **Kans** | **Schade** |
| Verandering van sessie | M | H |
| GET aanpassen | H | L |
| Rechten Database | M | H |
| SQL injectie | M | H |

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.

## 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. Als 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** |
| SQL injectie | M | H |
| Aflezen van sessies | M | H |
| Wachtwoorden aflezen | M | H |
| Rechten Database | M | H |

# 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

SQL injectie is afgevangen door de msqli\_stmt\_bind\_param functie van PHP.   
msqli\_stmt\_bind\_param is een standaard php-functie die ervoor zorgt dat alle variabele als parameter in de SQL komen. Zie <https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/#2> voor een verdere uitleg.

## Wachtwoord hashing

Op dit moment worden de wachtwoorden van de accounts met de standaard php hashfunctie gehashed. Deze hash wordt opgeslagen in de database. Hierdoor voorkomen we dat wanneer de wachtwoorden uitgelekt raken, de wachtwoorden vooralsnog onbekend blijven.

## Rechten op de database

Op dit moment word er via de website op de database ingelogd door een gebruiker genaamd: Visitor.   
De pi moet inloggen met de gebruiker Pi.  
Deze hebben specifieke rechten, die beschreven staan in het Technisch Ontwerp.  
Hiermee vang je af dat er dingen op tabelniveau verkeerd afgehandeld/afgekeken worden.

## Passwordpolicy

Op dit moment wordt er een passwordpolicy gehanteerd. Deze zijn:

* Het wachtwoord moet minimaal 8 tekens bevatten
* Het wachtwoord moet minimaal 1 cijfer bevatten
* Gek tekentje?

Dit is ‘waarschijnlijk’ nog niet voldoende. Zie verbeterpunt hierover.

# 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 van sessies

Op dit moment word er veel gewerkt met sessies. Dit is echter niet de meest veilige manier om data over en weer te sturen. Om dit veilig te maken zie: <https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html>

## Database is niet meer beschikbaar

Op dit moment worden er geen standaard backups gemaakt. Ook zijn er geen meerdere databases beschikbaar voor op het moment dat er 1 uitvalt. Het advies is hoerdoor ook om meerdere hosts te hebben, en een regelmatige backup van de database uit te voeren.

## DDOS aanval

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. Een consequentie hiervan is dat de website niet meer beschikbaar is.

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.  
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

# 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.