Security

Inhoud

[Inleiding 2](#_Toc58590804)

[Risicoanalyse 3](#_Toc58590805)

[Beschikbaarheid 3](#_Toc58590806)

[Integriteit 3](#_Toc58590807)

[Vertrouwelijkheid 3](#_Toc58590808)

[Ingebouwd veiligheidsniveau 4](#_Toc58590809)

[SQL injectie 4](#_Toc58590810)

[Wachtwoord hashing 4](#_Toc58590811)

[Rechten op de database 4](#_Toc58590812)

[Passwordpolicy 4](#_Toc58590813)

[Advies over vervolgstappen 5](#_Toc58590814)

[Stel officieel passwordpolicy op 5](#_Toc58590815)

[Aflezen van sessies 5](#_Toc58590816)

[Database is niet meer beschikbaar 5](#_Toc58590817)

[DDOS aanval 5](#_Toc58590818)

[Spam voor mailhost 5](#_Toc58590819)

[Conclusie 6](#_Toc58590820)

# Inleiding

DEZE

# Risicoanalyse

DEZE

## Beschikbaarheid

DEZE

|  |  |  |
| --- | --- | --- |
| **Kwetsbaarheid** | **Kans** | **Schade** |
| Database is niet meer beschikbaar | L | L |
| Stroomstoring van server | L | L |
| DDOS aanval | M | H |
| Spam voor mailhost | H | H |

## Integriteit

Correctheid en volledigheid van data die verstuurd wordt

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

## Vertrouwelijkheid

DEZE

|  |  |  |
| --- | --- | --- |
| **Kwetsbaarheid** | **Kans** | **Schade** |
| SQL injectie | M | H |
| Aflezen van sessies | M | H |
| Wachtwoorden aflezen | M | H |
| Rechten Database | M | H |

## Ingebouwd veiligheidsniveau

### 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

DEZE

### Stel officieel passwordpolicy op

De passwordpolicy is op dit moment nog niet van de standaard van NerdyGadgets. Hier moet een richtlijn over worden opgevraagd, en vervolgens moet die worden geïmplementeerd.

### 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 nooit 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

DEZE