Security

De kwalitatieve securityscan

Inhoud

[Inleiding 2](#_Toc57881083)

[Risicoanalyse 3](#_Toc57881084)

[Beschikbaarheid 3](#_Toc57881085)

[Integriteit 4](#_Toc57881086)

[Vertrouwelijk 5](#_Toc57881087)

[Conclusie 6](#_Toc57881088)

# Inleiding

In dit verslag

# Risicoanalyse

## Beschikbaarheid

|  |  |  |  |
| --- | --- | --- | --- |
| **Kwetsbaarheid** | **Kans** | **Schade** | **Advies** |
| Database is niet meer beschikbaar | L | L | Regelmatige backup, goede server en/of meerde hosts |
| Stroomstoring van server | L | L | Goede server en/of meerde hosts |
| DDOS aanval | M | H | Creeer een blacklist van ip-adressen die te vaak proberen te connecten.  Sommige hosts bieden hier ook services voor |
| Spam voor mailhost | H | H | Eenmalig versturen van het factuur en klantenservice mails |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Integriteit

Correctheid en volledigheid van data die verstuurd wordt

|  |  |  |  |
| --- | --- | --- | --- |
| **Kwetsbaarheid** | **Kans** | **Schade** | **Advies** |
| Verandering van sessie | M | H | Het minimaliseren van het opslaan van data aan de clientside |
| GET aanpassen | H | L | Een POST i.p.v een GET gebruiken |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Vertrouwelijkheid

|  |  |  |  |
| --- | --- | --- | --- |
| **Kwetsbaarheid** | **Kans** | **Schade** | **Advies** |
| SQL injectie | M | H | Invoer steriliseren |
| Aflezen van sessies | M | H | Geen sessie gebruiken |
| Wachtwoorden aflezen | M | H | Gebruik hashes voor wachtwoorden |
|  |  |  |  |

## Ingebouwd veiligheidsniveau

### SQL injectie

### Wachtwoord hashing

### Inloggen

# Conclusie