# Inloggen

Inloggegevens voor medewerkers:

Gebruikersnaam: admin

Password: goedwachtwoord

Algemene bug op de website, uitloggen moet twee keer op worden gedrukt om uit te loggen.

# Dreigingsmodel

A picture containing diagram

Description automatically generated

1: gelre airport website

2: medewerkers inloggen

3: database

4: Aanvaller

5: SQL injection

|  |  |
| --- | --- |
| Risico | SQL-injectie vanuit views met logincomponent. |
| aanvalstechniek | Broncodeinjectie: SQL. |
| kans | Hoog: staat op nummer één van de OWASP Top 10 [(2017-Injection)](https://owasp.org/www-project-top-ten/2017/A1_2017-Injection).  De rede dat de kans zo hoog is is omdat PHP-broncode die het SQL-statement uitvoert hebben minstens de rechten om de hele gebruikerstabel uit te lezen. |
| gevolg | Aanvallers hebben alle login gegevens. Als deze niet gehasht zijn en dus in plain-text opgeslagen in de database. |

De maatregel die hiervoor te volgen zijn is om placeholders in de query te gebruiken. Ook heb ik een functie gebruikt, hieronder te zien. Dat SQL injection niet mogelijk maakt.

Text

Description automatically generated

Deze functie haalt de tags weg, voegt slashes toe, zorgt ervoor dat speciale tekens niet worden ingevoerd en maakt de invoer html leesbaar. Dit wordt zodra de invoer gelijk gedaan

Text

Description automatically generated

Hiermee blijven de gegevens veilig en de invoer blijft onveranderd als de gegevens niks verkeerds doorgeven.

A screenshot of a computer

Description automatically generated with medium confidence

Hierboven worden placeholders gebruikt om SQL injection te verkomen.

Ook als iets leeg blijft moet je een check hiervoor maken.

Graphical user interface, text

Description automatically generated

Zelfs als er iets gebeurt dat ik ben vergeten bij sommige pagina’s staat deze code  
Text

Description automatically generated

PDOException treedt op als er iets in SQL verkeerd gaat. Op de meeste pagina’s maakt dit niet uit maar voor andere wel.