Corné Noorlander (1054564), Fabio Wolthuis (1093379), Hannah Saunders (1093894) & Merel van der Leeden (1103194)

PO: DIEDERIK MOORLAG,  Project 3/4

Beveiliginsrapport

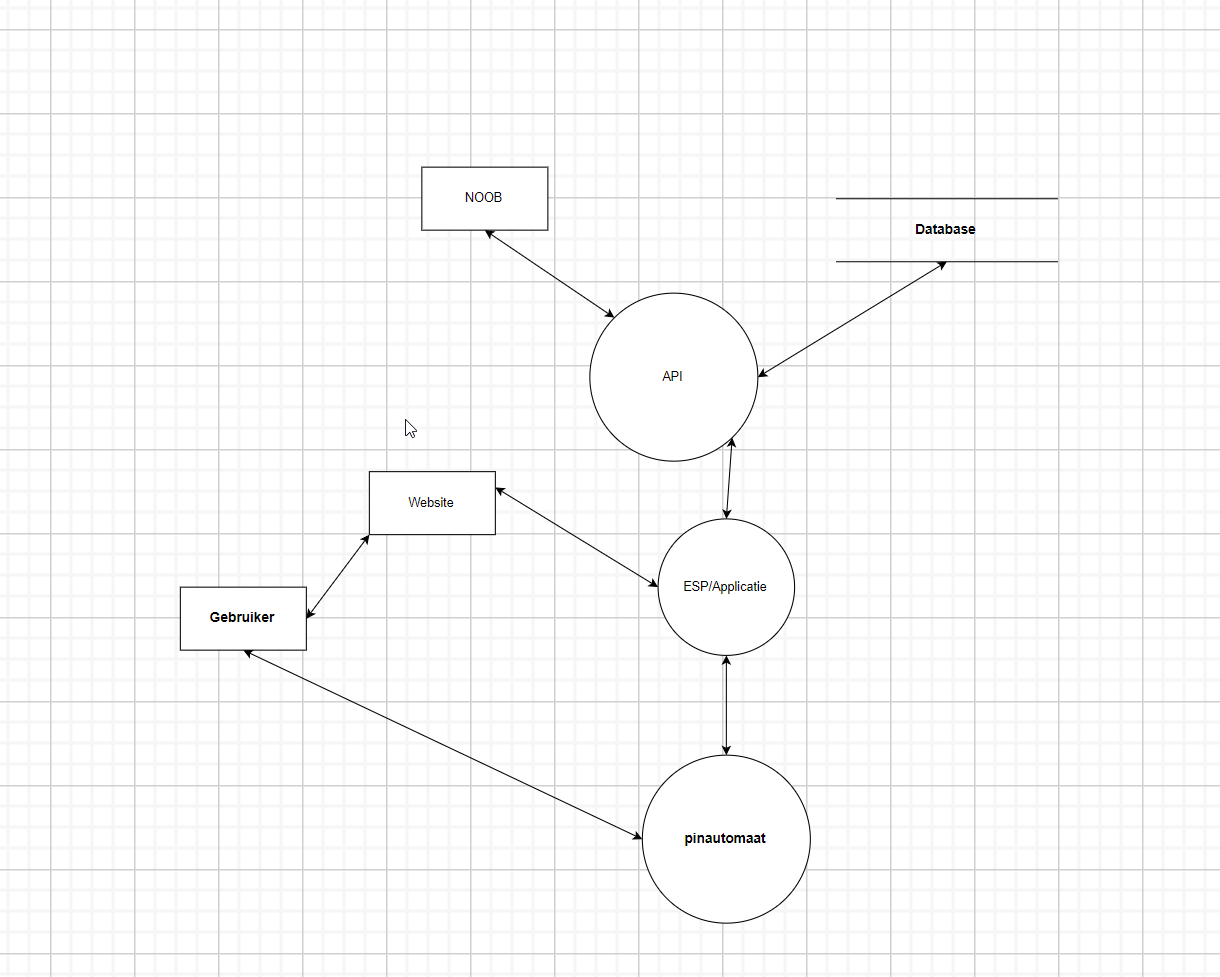
Inhoud

[Inleiding 2](#_Toc198812117)

# Inleiding

Vanuit de bankenvereniging *NOOB* is er gevraagd om een pinautomaat met een banksysteem te ontwerpen en realiseren. Omdat er binnen een banksysteem gevoelige data staat over de klanten, moet zo’n systeem goed beveiligd zijn. In dit verslag wordt er gekeken naar de veiligheidsrisico’s die opkomen bij het maken van een banksysteem met een pinautomaat en hoe deze risico’s verkleint en/of tegengegaan kunnen worden.

# Data Flow Diagram



# Risicoanalyse

## Aanvallen op het systeem

**SQL-injectie**

Op het bansysteem staat onder anderen een database waarop (gevoelige)data staat van de gebruikers. Om hier data uit te krijgen maakt de API gebruik van zogenaamde SQL query’s. Het risico hiermee is dat gebruikers kwaadaardige SQL query’s in zouden kunnen voeren en daarmee aan gevoelige data kunnen komen.[1]

# Oplossingen

## Het systeem

**SQL-injectie**

# Bronvermelding

[1] <https://pentests.nl/pentest-blog/sql-injectie/>

# Changelog

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |