Onderzoek 2FA

Fontys | Tilburg

Xander van veen, Kayle Boersen

2022

[Wachtwoord doorsturen 2](#_Toc116900256)

[Oplossing inloggen via link 3](#_Toc116900257)

[Oplossing 2-staps authenticatie 3](#_Toc116900258)

[Conclusie 3](#_Toc116900259)

# Wachtwoord doorsturen

Na de bespreking met Will, Sander en David zijn er een paar punten omhoog gekomen.  
  
We gaven Will een paar opties voor login. Zo zou een user kunnen in loggen met behulp van een email en wachtwoord of alleen een email.  
Als je voor de optie koos om alleen email te gebruiken, zou je in je mailbox een email krijgen met een login link.  
  
**Oplossing wachtwoord via mail**

Door dit te bespreken kwam Will met het idee om als mensen hun wachtwoord vergeten zijn, in plaats van een link krijgen om een nieuw wachtwoord te creëren, om een mail te sturen met hun wachtwoord erin.  
Er zijn een paar problemen als we praten over het terugsturen van een gebruikers wachtwoord.

* Dit zou dus betekenen dat we de wachtwoorden niet moeten encrypteren zodat we het wachtwoord terug kunnen vinden. Als er ooit een database lek is, zou dit dus betekenen dat iedereen zijn of haar email en wachtwoord openliggen. Als de gebruiker dan een wachtwoord hebben dat ze ook gebruiken voor hun email kunnen ze snel alles verliezen.

Als we de wachtwoorden duur zouden sturen voordat ze encrypte worden lopen we tegen een ander probleem aan.

* Als we de gebruiker hun wachtwoord sturen betekent dit dat dit wachtwoord dus op een locatie opgeslagen wordt zoals hun e-mail. Als iemand ooit deze mail ziet of per ongelijk doorgestuurd krijgen zal dit wachtwoord dus openliggen.
* Een “Man in the middle” aanval ([MITM](https://en.wikipedia.org/wiki/Man-in-the-middle_attack)). Hiermee bedoelen we dat er een persoon zit tussen de jou computer en de website. Zo zou dit persoon dan een bericht kunnen inzien met jouw wachtwoord erin.
* Als we het zo doen dat het wachtwoord na registreren meteen door sturen naar het email adres, betekent dit dat iemand die alleen je email heeft, anoniem berichten kan sturen via de website.

Bron:

<https://www.passcamp.com/blog/dangers-of-storing-and-sharing-passwords-in-plaintext/>

<https://www.securecodewarrior.com/blog/coders-conquer-security-infrastructure-as-codesensitive-data-storage-plaintext-storage-of-passwords>

# Oplossing inloggen via link

De laatste tijd komt er een trend omhoog van het inloggen via een link in de mail, dit wordt ook wel “Auth0” genoemd. Hierbij wordt er niet meer om een wachtwoord gevraagd en is de vorm van authenticatie het feit dat de gebruiker het email adres beheerd. Meer en meer websites beginnen deze vorm van registreren/inloggen te gebruiken zoals Slack, Medium en Google. Hiervoor zijn goede redenen te vinden:

Voordelen

* Gebruiksvriendelijker, de gebruiker hoeft geen wachtwoord meer te onthouden voor de website specifiek en het proces wordt versimpeld.
* Heel het registreer proces wordt geschrapt waardoor de gebruiker makkelijker en sneller de website kan gebruiken.
* Het risico van een database lek zal nooit wachtwoorden bevatten sinds deze niet opgeslagen worden.
* De optie voor wachtwoord vergeten weglaten sinds dit overbodig is.

Nadelen

* De gebruiker zal op hetzelfde apparaat de mail moeten openen, jongere groepen openen sneller de mail op hun telefoon terwijl ze proberen in te loggen op bijvoorbeeld een computer.

# Oplossing 2-staps authenticatie

Als tweede optie is er de reguliere vorm van 2-staps authenticatie. Hierbij registreert de gebruiker met wachtwoord en email waarna er een email verstuurd wordt naar de gebruiker. In die mail staat een code of link waarmee de gebruiker bewijst dat het email adres van hem/haar is. Hieraan zitten ook weer voor- en nadelen:

Voordelen

* Wel bekende vorm van authenticatie.

Nadelen

* Het moeten onthouden van een wachtwoord voor de website die mogelijk te vergeten is waardoor het proces start van ‘wachtwoord vergeten’.
* Kost langer om te registreren.

Bron:

[Log in without Passwords: Introducing Auth0 Passwordless](https://auth0.com/blog/auth0-passwordless-email-authentication-and-sms-login-without-passwords/)

# Conclusie

De meest veilige en gebruiksvriendelijke vorm van het authentiseren van een gebruiker is via een inloglink in de mail zonder wachtwoord. Dit voorkomt alle risico’s van wachtwoorden in mails of databases.