Rapport

- De wordpress login is gevoelig voor brute force attacks omdat ik geen ip's opsla.
- Gevolgen: Mensen kunnen de site bruteforcen om zo toegang te krijgen tot het admin panel.
- Oplossing: Ip opslaan en kijken hoe vaak bijv. per minuut vanaf het ip een login request komt.

Pentest

Ik heb mijn honeypot laten testen door pentest-tools.com. Hun conclusie was dat de Overall risk Medium was. Dit kwam omdat ik de password autocomplete niet had uitgezet, een insecure cookie had en er ontbraken een paar security headers:

- X-Frame-Options
- X-XSS-Protection
- Strict-Transport-Security
- X-Content-Type-Options

Honeypot

In mijn honeypot heb ik een log systeem ingebouwd waardoor je kan zien welk ip met welke login inlogd. Hiermee zou je bijvoorbeeld ook een brute force aanval mee kunnen voorkomen.

Owasp top 10

A3 – De website is beveiligd in het zoekveld tegen XSS attacks
A6 - Voor het wachtwoord-veld staat autocomplete aan.
A8 - Met CSRF kan je tokens achterhalen.