Derdenverklaring

MijnDiAd

20 januari 2022
Vertrouwelijk

WhiteHats
ethical hackers

Derdenverklaring

Introductie

MijnDiAd heeft WhiteHats opdracht gegeven om de webapplicatie *Mijn Digitale Administratie* ('MijnDiAd') aan periodieke beveiligingsonderzoeken te onderwerpen.

Bij aanvang (april 2020) is de applicatie onderzocht in een time-boxed project. Aansluitend zijn er in de periode van 1 juli 2020 tot januari 2022 vijf vervolgonderzoeken uitgevoerd, waarmee het beeld van de beveiligingshouding geactualiseerd is en alle relevante veranderingen zijn gecontroleerd.

Scope

De beveiligingsonderzoeken worden uitgevoerd op basis van WhiteHats' testbatterij die onder meer de procedures van de OWASP Testing Guide v4 omvat. Tests zijn uitgevoerd op de acceptatieomgeving. Er zijn geldige applicatieaccounts verstrekt en er is inzage in de broncode verleend.

- Aantal bestede uren eerste onderzoek (april 2020): 99.
- Aantal bestede uren vervolgonderzoeken (juli 2020 – januari 2022): 105.
- Geen social engineering- of DDoS-aanvallen uitgevoerd.
- Testomgeving: https://beta9.mijndiad.nl

Resultaat

MijnDiAd is een omvangrijke, moderne PHP-applicatie. De backend van de applicatie is ontwikkeld met het Laravel-framework. De op Vue-gebaseerde frontend communiceert via een API met de backend. De applicatiearchitectuur voorziet in het scheiden van gegevens van verschillende klanten door het gebruik van aparte databases.

Alle bevindingen met betrekking op de meest recente versie van de webapplicatie hebben prioriteit 'laag', 'minimaal' of 'ok'. De oplossing heeft daarmee een solide beveiligingshouding en is naar oordeel van WhiteHats geschikt voor het beoogde doel en het verwerken van persoonsgegevens.

WhiteHats B.V.

Digitaal ondertekend door
WhiteHats B.V.
Datum: 2022.01.20 11:08:51 +01'00'