Derdenverklaring
Beveiligingsonderzoek

MijnDiAd

13 juni 2024

WhiteHats
ethical hackers

Derdenverklaring

Introductie

MijnDiAd heeft WhiteHats ingeschakeld om de webapplicatie Mijn Digitale Administratie ('MijnDiAd') aan periodieke beveiligingsonderzoeken te onderwerpen. Het ultieme doel is het verhogen van de weerbaarheid van opdrachtgever tegen cyberaanvallen ter beperking van de schade die hieruit kan ontstaan. Het project geeft MijnDiAd inzicht in de huidige beveiligingshouding en biedt adviezen over het verbeteren hiervan.

Bij aanvang (april 2020) is de applicatie onderzocht in een time-boxed project. Aansluitend zijn er in de periode van 1 juli 2020 tot juni 2024 dertien vervolgonderzoeken uitgevoerd, waarmee het beeld van de beveiligingshouding geactualiseerd is en alle relevante veranderingen zijn gecontroleerd.

Aanpak

De beveiligingsonderzoeken worden uitgevoerd op basis van WhiteHats' testbatterij die onder meer de procedures van de OWASP Testing Guide v4.2 omvat. Tests zijn uitgevoerd op de acceptatieomgeving. Er zijn geldige applicatieaccounts verstrekt en er is inzage in de broncode verleend.

Kenmerken:

- Totaal aantal bestede uren (april 2020 – juni 2024): 456.
- Geen social engineering- of DDoS-aanvallen uitgevoerd.
- Testomgeving: https://beta9.b.mijndiad.com/.

De onderzoeken worden uitgevoerd door de security experts die over de volgende certificaten beschikken:

- eWPT - Pentesten web applicaties.
- eWPTX - Geavanceerd pentesten web applicaties.

WhiteHats is ISO 27001 (Informatiebeveiliging) en CCV-keurmerk Pentesten (kwaliteit) gecertificeerd.

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 waaronder het verwerken van persoonsgegevens.

Digitally signed by WhiteHats B.V.
Date: 2024.06.13 10:42:35 +02'00'