THIRD PARTY MEMO

Schuldenknooppunt

commissioned by

Stichting Schuldenknooppunt

CONFIDENTIAL

TPM.pdf
Ilona de Bruin, eWPT, eWPTXv2
Version 1.0
2024-12-20

Scope

In opdracht van Stichting Schuldenknooppunt is door Secura B.V. de IT-beveiliging van Schuldenknooppunt onderzocht. Dit onderzoek is gestart op 23 oktober 2024 en is uitgevoerd door Ilona de Bruin, Tom Nijholt en Roy Stultiens. De applicatie is onderzocht binnen de Acceptatie-omgeving aangeboden door Stichting Schuldenknooppunt.

Doel

Dit onderzoek heeft als doel om het beveiligingsniveau van Schuldenknooppunt onafhankelijk vast te stellen, kwetsbaarheden in deze applicatie te identificeren, en mogelijke verbeteringen aan te dragen.

Aanpak

Dit applicatieonderzoek is uitgevoerd aan de hand van de crystal box-methode. Bij het uitvoeren van een onderzoek op basis van deze methode is er vooraf beschikking over inloggegevens, broncode en andere informatie die gebruikt kunnen worden ter ondersteuning van het onderzoek.

Door middel van automatische tests is de beveiliging van de gebruikte applicatiesoftware onderzocht op publiek bekende kwetsbaarheden en configuratiefouten. In een volgende stap is de applicatie handmatig onderzocht, waarbij gebruik is gemaakt van verschillende tools.

Resultaten

Als resultaat van het onderzoek is door Secura een aantal beveiligingsrisico's geïdentificeerd. In totaal zijn er 1 gemiddeld-risico bevinding, 5 laag-risico bevindingen, 11 risico notities en 7 aandachtspunten geïdentificeerd.

Op basis van het uitgevoerde beveiligingsonderzoek zijn er geen afwijkingen gevonden aan het gebruik van open standaarden zoals gedefinieerd door het Forum Standaardisatie en gepubliceerd op de officiële website.[1] Hierbij zijn alleen de standaarden getoetst die binnen de scope van het onderzoek vallen, zoals het gebruik van TLS en HTTPS.

Daarnaast toonde Stichting Schuldenknooppunt een actieve houding omtrent het mitigeren van bevindingen.

Op applicatieniveau is er getest aan de hand van de ASVS. Onderstaande tabel geeft de bevindingen per categorie weer:

[1] https://www.forumstandaardisatie.nl/open-standaarden

ID	Category	✔	✘	OOS	NA
V1	Architecture Design & Threat Modeling	0	0	0	0
V2	Authentication	11	0	0	9
V3	Session Management	10	1	0	1
V4	Access Control	6	0	0	2
V5	Validation Sanitization and Encoding	5	3	0	19
V6	Stored Cryptography	1	0	0	0
V7	Error Handling and Logging	1	0	0	0
V8	Data Protection	3	0	0	1
V9	Communications	2	0	0	0
V10	Malicious Code	0	0	0	3
V11	Business Logic	2	0	0	1
V12	File & Resources	7	1	0	0
V13	API & Web Service	4	1	0	1
V14	Configuration	12	4	0	0

Table 1: Coverage of the OWASP ASVS

Daarnaast is de infrastructuur beoordeeld aan de hand van best practices zoals de CIS Benchmarks. Hierin zijn geen grote bevindingen gedaan die directe acties vereisen.

Het wordt hierbij opgemerkt dat een dergelijk onderzoek slechts een momentopname is. Voortdurend worden er nieuwe aanvalstechnieken ontwikkeld en ontdekt. Daarnaast kan een geringe aanpassing aan de IT-omgeving nieuwe kwetsbaarheden introduceren. Minstens zo belangrijk als het technologische aspect is de rol van processen, procedures en de menselijke factor in informatiebeveiliging. De resultaten van dit onderzoek bieden dan ook geenszins garantie voor de veiligheid van de IT-omgeving en hierin aanwezige of verwerkte data.

Secura B.V.

Datum:	2024-12-20
Naam:	Ilona de Bruin, eWPT, eWPTXv2
Functie:	Security Specialist

Secura B.V.
Vestdijk 59
5611 CA EINDHOVEN
Netherlands

Herikerbergweg 15
1101 CN AMSTERDAM
The Netherlands

T +31 (0)40 23 77 990
W https://www.secura.com