HackDefense

Testrapport

penetratietest Coronamelder

versie 1.0 - definitief

Danny de Weille
d.deweille@hackdefense.nl

Mark Koek
m.koek@hackdefense.nl

15 juli 2020

HackDefense BV

Postbus 3025
2301 DA Leiden

(071) 204 0101

`https://hackdefense.nl/`

Project

Projectnaam	penetratietest Coronamelder
Opdrachtgever	Ministerie van VWS
Rapport voor	Ministerie van VWS
Projectnummer	PR20043
Offertenummer	O20431

Documentgeschiedenis

Versie	*Datum*	*Auteur*	*Omschrijving*
0.1	14-Jul-2020	Mark Koek	eerste concept
1.0	15-Jul-2020	Mark Koek	definitief na review door opdrachtgever

Managementsamenvatting

Het Ministerie van VWS heeft HackDefense gevraagd om een penetratietest uit te voeren van `coronamelder.nl`, en om eventueel maatregelen ter verbetering van de beveiliging te adviseren.

We zijn positief over de beveiliging van deze site, en zien geen bezwaren tegen ingebruikname in de huidige vorm. We geven in dit rapport enkele kleine suggesties, waaraan geen of slechts een minimaal risico verbonden is.

In dit rapport vindt u de details van ons onderzoek en onze bevindingen, en geven we technische aanbevelingen.

Inhoudsopgave

Hoofdstuk 1

Uw vraag

1.1 Achtergrond

Het Ministerie wil met spoed een website online brengen die informatie geeft over de – nog in ontwikkeling zijnde – CoronaMelder-app. Op deze site moet een pentest worden uitgevoerd voor de geplande ingebruikname op woensdag 15 juli a.s.

1.2 Scope

Onderzocht zijn:

- de ”live” website in preproductie op `coronamelder.nl`, tijdelijk opengesteld voor onze IP-adressen;
- de code van de site, openbaar beschikbaar via `https://github.com/minvws/nl-covid19-notification-app-website`
- de site, lokaal draaiend in een Docker-container, gedownload van `https://hub.docker.com/r/starefossen/github-pages`.

1.2.1 Aanvalsperspectief

De beveiliging is getest vanuit het perspectief van de internet-gebruiker. Testaccounts of beheertoegang waren niet noodzakelijk.

1.2.2 Testvorm

De gehanteerde testvorm is *white box*. Alle informatie over de site staat op Github. Een volledige *code review* was echter geen onderdeel van het onderzoek.

Social engineering of *Denial-of-Service attacks* (DoS of DDoS) zijn niet aan de orde en op geen enkele wijze uitgevoerd.

1.2.3 Tijdstippen en locaties tests

Tests zijn uitgevoerd op 10, 13 en 14 juli 2020 vanuit ons kantoor in Leiden.

1.2.4 Adresinformatie

Alle tests via het internet zijn uitgevoerd vanaf de volgende adressen:

Naam	*IPv4-adres*	*IPv6-adres*
`pentest23.hackdefense.com`	`95.168.173.23`	`2001:1af8:5000:a00c:1::23`
`pentest31.hackdefense.com`	`95.168.173.31`	`2001:1af8:5000:a00c:1::31`

Eventuele door u waargenomen inbraakpogingen afkomstig van andere adressen waren geen onderdeel van de test.

1.3 Onderzoeksvraag

De in dit onderzoek te beantwoorden onderzoeksvragen luiden als volgt:

Kunnen – binnen de beschikbare tijd – kwetsbaarheden in de beveiliging van de site worden geïdentificeerd?

Dit alles voor zover mogelijk binnen de voor de test beschikbare tijd.

Beveiligingsissues die niet direct tot ongeautoriseerde toegang of mogelijke verstoring van het systeem leiden maar die wel zouden kunnen helpen bij een aanval, m.a.w. waarvan de oplossing tot een robuustere beveiliging leiden, zijn uiteraard ook gerapporteerd.

1.4 Overige randvoorwaarden

- Het onderzoek is uitgevoerd door OSCP-gecertificeerde pentesters.
- Het onderzoek was beperkt tot 1,5 mensdagen, inclusief rapportage.
- Voor het onderzoek is de *Web Application Firewall* van Akamai niet uitgeschakeld, waardoor het denkbaar (doch onwaarschijnlijk) is dat kwetsbaarheden daardoor afgeschermd zijn.

Hoofdstuk 2

Onze bevindingen

2.1 Aanpak

Om de onderzoeksvragen te beantwoorden zijn we als volgt te werk gegaan.

2.1.1 Algemeen

In het algemeen geldt voor de onderzoeken en tests van HackDefense dat uitvoer van tooling voor ons niet leidend is. Tooling is een hulpmiddel, het is het gereedschap van de vakman. Conclusies worden getrokken door de vakmensen zelf, voor wie een goed begrip van de werking van het te testen object het belangrijkste element van een beveiligingstoets is.

De uitvoer van de tooling is daarom altijd handmatig geverifieerd. Ook zijn tests die niet geautomatiseerd uitvoerbaar zijn met de hand uitgevoerd. Daarbij telt onze 25 jaar kennis en ervaring in computer- en netwerkbeveiliging en ons begrip van de context van de applicatie.

2.1.2 Webapplicatietest

Allereerst is er een poortscan en een vulnerability scan uitgevoerd van de URL's en IP-adressen in scope. Daarbij is gebruik gemaakt van *NMap*, *Nessus*, *Nikto*, *DirB/Dirbuster* en de *Active Scan*-component van *BurpSuite Pro*.

Tegelijkertijd hebben we ons met handmatige tests een beeld gevormd van de werking van de webapplicatie. Onze basistool daarbij is de *intercepting proxy* van *BurpSuite Pro*.

De resultaten van de scanner zijn handmatig geverifieerd. Daarbij zijn ook ondersteunende scan-modules van BurpSuite Pro gebruikt voor de handmatige test (waarbij bijvoorbeeld voor de tester inzichtelijk wordt gemaakt waar gebruikersinvoer terugkomt in de uitvoer), zodat we handmatig ook hebben kunnen testen op kwetsbaarheden die de scanner mogelijk niet heeft gedetecteerd c.q. niet heeft kunnen detecteren.

2.2 Analyse

2.2.1 Algemeen

Het gaat bij dit onderzoek om een zeer eenvoudige website (een zogenaamde *one pager*) waarbij geen gebruikersinvoer mogelijk is. Het aanvalsoppervlak is daardoor beperkt.

We hebben in `coronamelder.nl` dan ook geen beveiligingsproblemen aangetroffen die in websites en -applicaties veel voorkomen, zoals bijvoorbeeld *Cross-Site Scripting* of *SQL Injection*.

Omdat er geen sprake is van een login, of verschillende functionaliteiten voor verschillende rollen, zijn er ook geen issues in het sessiemanagement geconstateerd.

Voorts stellen we vast dat aan standaard-zaken zoals HTTP-headers die in het algemeen voor de beveiliging aanbevelenswaardig zijn veel aandacht is besteed. Ook de cryptografische bescherming van de verbinding tussen browser en server (met SSL/TLS) is op de juiste wijze ingesteld.

Ook valt op dat er niet, zoals bij het gros van de websites die wij onderzoeken, data gelekt wordt naar grote internetbedrijven ten behoeve van bezoekersregistratie of -analyse. Dit wordt door een voorziening van de Rijksoverheid zelf gedaan.

Al met al is onze analyse van deze site dus positief. De beveiliging is van ver bovengemiddeld niveau.

2.2.2 Mogelijk vervolgonderzoek

De limitatie in tijd (”time box”) van deze opdracht was voldoende om een goede test te kunnen uitvoeren. Elke beveiligingstest heeft ruimte voor meer onderzoek, maar in dit geval zijn we van mening dat een goede analyse van de applicatie heeft kunnen plaatsvinden en dat het onwaarschijnlijk is dat meer onderzoekstijd meer zinvolle informatie zou hebben opgeleverd.

Hoofdstuk 3

Conclusies en aanbevelingen

3.1 Conclusies

Dit project had ten doel de volgende onderzoeksvragen te beantwoorden:

Kunnen – binnen de beschikbare tijd – kwetsbaarheden in de beveiliging van de site worden geïdentificeerd?

We concluderen dat we geen bevindingen hebben gedaan die we een kwetsbaarheid in de beveiliging kunnen noemen. In de bijlage vindt u alleen drie kleine suggesties c.q. aandachtspunten die een laag of nihil risico vormen.

3.2 Aanbevelingen

We zien geen bezwaar in de ingebruikname van de site in de huidige vorm.

Voor meer details, en voor de aanbevelingen ten aanzien van de bevindingen met een laag of nihil risico verwijzen we de geïnteresseerde lezer naar de specifieke bevindingen in Bijlage A.[1]

[1] We geven zo concreet mogelijke aanbevelingen om u zo goed mogelijk op weg te helpen met het oplossen van specifieke risico's. We kunnen echter nooit uitsluiten dat een door ons gedane aanbeveling technisch niet exact werkt in uw omgeving. Verifieer altijd (door een hertest of eigen tests) of het gerapporteerde issue is opgelost na doorvoering van onze technische aanbeveling.

Bijlage A

Technische bevindingen

In deze bijlage vindt u onze specifieke bevindingen ten aanzien van het onderzoeksobject. Hierop zijn de algemene conclusies en aanbevelingen van HackDefense gebaseerd. Elke bevinding gaat gepaard met een risico-inschatting en een concreet technisch advies.

Risico-inschattingen zijn ingedeeld op basis van de volgende algemene werkwijze[1]:

- **Zeer Hoog** – Er bestaat een direct risico op verlies van systeem- of data-integriteit. We raden aan om direct actie te ondernemen om dit issue te verhelpen.
- **Hoog** – Het risico van een inbraak of lek is significant maar niet acuut; een hacker zou in het algemeen nog één element nodig hebben om tot een volledige inbraak te komen. We adviseren om zo snel mogelijk actie te ondernemen.
- **Midden** – Er is sprake van een risico, maar er is geen direct inbraakgevaar. Desondanks is sprake van een belangrijke verbetering van de beveiliging en we adviseren een relevante wijziging door te voeren bij de eerstvolgende gelegenheid voor onderhoud.
- **Laag** – Een kans om de algemene robuustheid en beveiligingsniveau van het onderzoeksobject te verbeteren. Hierbij adviseren we om een oplossing voor het issue mee te nemen in een volgende release of ander majeur onderhoudsmoment.
- **Info** – Er is geen direct beveilingsrisico, maar we willen onze constatering wel graag met u delen. Ook kan er sprake van zijn dat een bepaalde nieuwe beveiligingsoptie niet wordt ingezet op het onderzoeksobject, en willen we u de suggestie doen om deze optie in te zetten.

We baseren onze inschatting op de meest recente versie van het *Common Vulnerability Scoring System* (CVSS) zoals dat te vinden is op `https://first.org/cvss/`.

Daarbij geldt de volgende inschaling:

[1] Ondanks het hierboven beschreven systeem en onze best mogelijke inschatting is het vaststellen van zakelijke risico's formeel geen onderdeel van ons onderzoek. We bevelen dan ook aan om uw eigen risico-inschatting te maken voordat u prioriteiten bepaalt voor het oplossen van de door ons gedane bevindingen.

CVSS-score	*CVSS-categorie*	*Onze categorie*
9,0 t/m 10,0	Critical	**Zeer Hoog**
7,0 t/m 8,9	High	**Hoog**
4,0 t/m 6,9	Medium	**Midden**
0,1 t/m 3,9	Low	**Laag**
0,0	None	**Info**

U vindt hieronder onze bevindingen in detail. Om het intern distribueren van individuele bevindingen mogelijk te maken start elke bevinding op een aparte pagina.

A.1 Type server te achterhalen via foutpagina

De site verbergt op alle pagina's welke server-software er gebruikt wordt, maar via bepaalde foutpagina's is dit toch te zien.

Risico

3,7 – Laag
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/CR:L/MC:L

Voor een aanvaller kan dit nuttige informatie zijn. Omdat het versienummer niet zichtbaar is schalen we het risico laag in.

Betreft de systemen

`coronamelder.nl`

Waarneming

Als een foutconditie optreedt, bijvoorbeeld door `/../` op te vragen, dan geeft de server de volgende HTTP-respons:

```
HTTP/1.1 400 Bad Request
Content-Type: text/html
Content-Length: 150
Date: Mon, 13 Jul 2020 13:28:58 GMT
Connection: close
Strict-Transport-Security: max-age=15768000 ; preload


<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

Aanbeveling

Pas de foutpagina aan zodanig dat niet wordt aangegeven dat NGINX wordt gebruikt.

A.2 Suggesties voor de Content-Security-Policy

De site heeft een goede *Content Security Policy*, maar enkele nieuwe features zouden hem nog verder kunnen verbeteren.

Risico

0,0 – Info
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Er is geen risico, we doen een suggestie voor de toekomst.

Betreft de systemen

`coronamelder.nl`

Waarneming

De site geeft de volgende Content Security Policy:

```
default-src 'self' statistiek.rijksoverheid.nl;
img-src 'self' statistiek.rijksoverheid.nl data:;
style-src 'self'; script-src 'self' statistiek.rijksoverheid.nl;
font-src 'self' statistiek.rijksoverheid.nl data:;
object-src 'none';
```

Dit is al veel sterker dan de meeste sites, maar er zijn twee nieuwere features van deze header die wellicht een zinvolle aanvulling zijn.

Aanbeveling

Voeg de volgende settings toe:

- Om het omzeilen van de host-beperking tot `statistiek.rijksoverheid.nl` tegen te gaan kan het nuttig zijn om `strict-dynamic` toe te voegen in combinatie met nonces of hashes die de specifieke scripts identificeren.
- Om zogeheten *DOM based XSS*-aanvallen te voorkomen is het mogelijk om via de Content Security Policy aan te geven dat scripts niet direct data vanuit de gebruiker mogen toepassen op gevaarlijke plaatsen in de DOM. Dit kan door `require-trusted-types-for 'script'` aan de policy toe te voegen.[2]

[2] voor meer informatie over "trusted types", zie bijvoorbeeld `https://web.dev/trusted-types/`

A.3 Meerdere Cache-Control headers

De server geeft twee headers met dezelfde naam (`Cache-Control`) terug.

Risico

0,0 – Info
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Er is geen risico, we doen een suggestie ten aanzien van mogelijke caching issues.

Betreft de systemen

`coronamelder.nl`

Waarneming

De server geeft op een normaal verzoek de volgende HTTP-headers terug:

```
HTTP/1.1 200 OK
Content-Type: text/html
Cache-Control: max-age=300
Content-Security-Policy: default-src 'self' statistiek.rijksoverheid.nl;
img-src 'self' statistiek.rijksoverheid.nl data:; style-src 'self';
script-src 'self' statistiek.rijksoverheid.nl; font-src 'self'
statistiek.rijksoverheid.nl data:; object-src 'none';
Referrer-Policy: origin
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Cache-Control: public, no-transform
Content-Length: 57879
Connection: close
Vary: Accept-Encoding
Strict-Transport-Security: max-age=15768000 ; preload
```

Hoewel dit volgens de toepasselijke RFC's is toegestaan gaat niet alle client software (browsers maar ook proxies) hier correct mee om. Sommige accepteren alle waarden maar er is ook software die alleen de eerste accepteert, of alleen de laatste. Daarmee wordt het gedrag onvoorspelbaar.

Dit heeft geen beveiligingsgevolgen, maar wilden we u toch niet onthouden omdat het in de toekomst misschien tot bugs zou kunnen leiden.

Aanbeveling

Voeg beide headers samen tot:

```
Cache-Control: max-age=300, public, no-transform
```