Van: [redacted]@tweedegolf.com>
Verzonden: donderdag 14 mei 2020 11:11
Aan: [redacted]@nijmegen.nl>
Onderwerp: Re: het werkt

Hoi [redacted],

Ik denk dat het goed is om even een videocall te doen over de status. Dat is wat makkelijker overleggen. Heb je daar vandaag tijd voor?

Groetjes,

[redacted]

On Thu, May 14, 2020 at 9:14 AM [redacted] <[redacted]@nijmegen.nl> wrote:

Dag [redacted],

- De 26e is ok
- We kunnen die vertaling ook als issue opschrijven in juni meenemen, als dat efficienter is
- Wat is de status van dit issue: https://tgrep.nl/gemeente-nijmegen/veilig-bellen/-/issues/54 ? Is die geimplementeerd? (kan het nog niet terugvinden waar ik dan de url zou moeten meegeven)
- Mbt de secret: ik kijk wel even of de auditor er iets van zegt.

Groeten,

[redacted]

Van: [redacted] <[redacted]@tweedegolf.com>
Verzonden: woensdag 13 mei 2020 18:53
Aan: [redacted] <[redacted]@nijmegen.nl>
Onderwerp: Re: het werkt

Hoi [redacted],

De publieke repository is hier te vinden: https://github.com/tweedegolf/veilig-bellen. We hebben daarin nog niet opgenomen hoe het werkt met de buttons, maar ik kan wel even een referentie naar frontend-public/src/example.html opnemen. Dat lijkt me het duidelijkst.

Ik heb het urenoverzicht bijgewerkt. We hebben op dit moment nog 17 uur over. Daarvan hebben we 16 uur gereserveerd, dus nog 1 uurtje over. Ik dat het doen van die vertalingen wel lukt, maar het maakt de code wel wat minder 'schoon' als we dat niet met een mooi vertaalframeworkje doen. Ik wil het nog eventjes overleggen dus.

Wat betreft de secrets: de lengte van de secret en het aantal verschillende tekens (a-z, A-Z, 0-9) maakt dat er (26 * 26 * 10) ^ 19 ~ 5.8 * 10 ^72 mogelijke secrets zijn. De veiligheid is op dit enorme getal gebaseerd. Er is gewoon een enorme hoeveelheid rekenkracht en een een enorme hoeveelheid tijd nodig om dit te brute-forcen. Daarnaast zijn dit dezelfde secrets die gebruikt worden om de credentials van de IRMA server op te halen. Die is dus even moeilijk te brute forcen. Ik maak me hier niet zo veel zorgen over. Mocht je toch nog niet gerust zijn, dan zou je eventueel een rate limit in kunnen stellen in nginx.

Oja, wat betreft de projectretro: voel je ervoor om die 26 mei om 9:30 te houden? Lijkt me dat we binnen een uur makkelijk klaar zijn.

Groetjes

[redacted]

On Wed, May 13, 2020 at 2:30 PM [redacted] <[redacted]@nijmegen.nl> wrote:

Dag [redacted],

Mooi. In de readme duidelijk opnemen wat er geïncludede moet worden om de button te laten werken op een willekeurige pagina zou ook fijn zijn. Scheelt mij weer uitzo

Zijn de uren eind van de dag ook bijgewerkt? Dan kan ik intern ook even doorgeven hoe het daarmee staat en wat we nog ‘over’ hebben.

Zit in de laatste versie (die wij nog niet hebben draaien) ook de mogelijkheid om te linken naar een externe site met BSN als parameter?

En zien jullie nog kans om alle labeltjes in het agent portaal in het NL te doen? (dus telefoonnummer ipv phonenumber bijvoorbeeld).

En nog een vraag:

ik zag dat de agent pagina zelf (client side) contact opneemt met de backend (https://backend.dev.irma-bellen.nl/disclose?secret=OgNljcIT1uDtKUdPJDa5)

Hoe voorkom je zo dat iemand gaat proberen de backend te brute-forcen door er maar secrets op af te vuren? Die backend is voor de hele wereld benaderbaar.

Secrets leven natuurlijk maar een beperkte tijd in die backend, maar toch. Of is jullie inschatting dat het niet mogelijk is om dit te misbruiken?

We zouden aan de AWS kant wat aanvullende maatregelen kunnen nemen (filteren op ip en requests per ip, of referer)

Groeten,

[redacted]

Van: [redacted] <[redacted]@tweedegolf.com>
Verzonden: woensdag 13 mei 2020 13:48
Aan: [redacted] <[redacted]@nijmegen.nl>
Onderwerp: Re: het werkt

Ha [redacted],

Mooi zo! Tof om te zien dat het werkt. Wij leggen nog even de laatste hand aan de Readme voor de publieke repo. Aan het eind van de dag stuur ik je hierover nog even een update.

Groetjes,

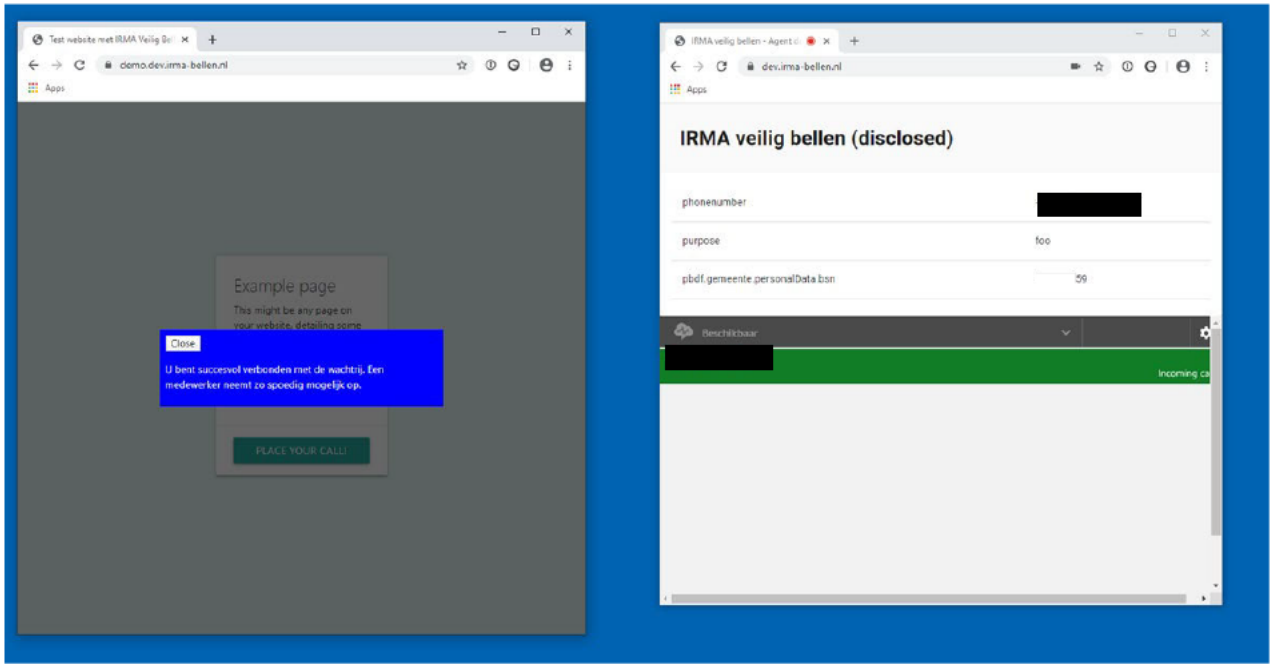
[redacted]

On Wed, May 13, 2020 at 9:50 AM [redacted] <[redacted]r@nijmegen.nl> wrote:

Ha,

Vanochtend nog 2 probleempjes verholpen ([redacted] had een verkeerde url van de backend, het agent portaal een net niet helemaal goede url van de backend) en nu kan ik bellen, zie ik attributen en de knop laat de status zien.

Volgende week met [redacted] de laatste versie erop zetten.
En ik zal ook eens even zorgen dat we in DEV demo attributen gaan uitvragen ;-) (daarom zie je nu alleen de laatste twee cijfers van mijn echte BSN ;-))



Groeten,

[redacted]