



Onderzoek security

Jay van Helden
Kelly van der Hoek
Jochem Wienk
Juni 2021

VERSIEBEHEER

VERSIES

VERSIE	DATUM	AUTEUR	WIJZIGINGEN	STATUS
1.0	8-02-2021	Jay van Helden	Opzet template	
1.1	8-03-2021	Jochem, Kelly, Jay	H1 t/m H4	

VERSPREIDING

VERSIE	DATUM	INGELEVERD BIJ
	3-6-2021	Fred Veldmeijer

INHOUDSOPGAVE

1. Inleiding	3
2. Onderzoeksstrategieën.....	4
3. Bieb.....	5
Welke tools zijn er om de security te kunnen waarborgen?	5
3.1 Network security monitoring tools	5
3.2 Encryption tools.....	6
3.3 Web vulnerability scanning tools	6
3.4 Penetration testing	7
3.5 Network defense wireless tools.....	7
3.6 Network intrusion & detection.....	8
3.7 Continuous Integration.....	8
3.8 Security Design Patterns.....	8
3.9 JWT	9
3.10 Two Factor Authentication	9
4. Veldwerk	10
4.1 Interviewvragen met docent:.....	10
4.2 Interviewvragen met Pharmapartners:	11
5. Werkplaats	12
5.1 inlog scherm	12
5.1.1 2FA.....	12
5.2 JWT	13
6. Showroom.....	14
7 Conclusie.....	15
8 Advies	17

1. Inleiding

Wij werken met onze subgroep aan 2 onderzoeksvragen. Met het DOT framework proberen we deze vragen te beantwoorden. In dit document wordt de vraag beantwoord: Hoe kan de security gewaarborgd worden? Dit document proberen we door het semester heen iteratief aan te vullen. Aan het eind van het semester hebben we een conclusie op de vraag "Welke security tools zijn geschikt voor de Medicom agenda applicatie?"

2. Onderzoeksstrategieën

In dit document worden verschillende onderzoeksstrategieën toegepast om erachter te komen hoe de security kan worden gewaarborgd. In hoofdstuk 3 wordt er een bieb onderzoek gedaan. Daarna in hoofdstuk 4 wordt er een veldwerk interviews gehouden. In hoofdstuk 5 worden de geïmplementeerde onderdelen getoond. In hoofdstuk 6 wordt de tool gedemonstreerd aan de klant en docenten doormiddel van een showroom. Dan in hoofdstuk 7 wordt er een conclusie gemaakt en tenslotte in hoofdstuk 8 wordt er een advies gegeven.

3. Bieb

In dit hoofdstuk worden verschillende tools onderzocht die kunnen bijdrage aan de security van een applicatie.

Welke tools zijn er om de security te kunnen waarborgen?

Om te onderzoeken hoe de security kan worden gewaarborgd wordt er gekeken naar bestaande tools die hierbij kunnen helpen. Er bestaan veel security tools zo zijn er o.a.:

- Network security monitoring tools
- Encryption tools
- Web Vulnerability scanning tools
- Penetration testing tools
- Network defense wireles tools
- Network intrusion and detection tools
- Continuous integration
- Security Design Patterns
- OWASP
- JWT
- Two Factor Authentication

Om meer inzicht in deze soorten tools te krijgen wordt er bij alle soorten tools gekeken worden naar voorbeelden van deze soort tools en waar ze voor gebruikt worden.

3.1 Network security monitoring tools

Network security monitoring tools controleren en volgen netwerkactiviteiten op problemen die worden veroorzaakt door defecte apparaten of overbelaste bronnen. Verder analyseert het een groot aantal complexe factoren om beheerders te waarschuwen voor bekende kwaadaardige activiteiten in een poging een bedreiging te stoppen.

- Argus (OpenArgus, sd) ¹
- P0f (Zalewski, sd) ²
- Nagios (Nagios, sd) ³
- Splunk (Splunk, sd) ⁴
- OSSEC (Ossec, sd) ⁵

¹ OpenArgus. (sd). *openargus - Home*. Opgehaald van openargus.org: <https://openargus.org/>

² Zalewski, M. (sd). *p0f v3*. Opgehaald van lcamtuf.coredump.cx: <https://lcamtuf.coredump.cx/p0f3/>

³ Nagios. (sd). *Nagios - The Industry Standard In IT Infrastructure Monitoring*. Opgehaald van www.nagios.org: <https://www.nagios.org/>

⁴ Splunk. (sd). *The Data-to-Everything Platform Built for the Cloud | Splunk*. Opgehaald van www.splunk.com: <https://www.splunk.com/>

⁵ Ossec. (sd). *OSSEC - World's Most Widely Used Host Intrusion Detection System - HIDS*. Opgehaald van www.ossec.net: <https://www.ossec.net/>

3.2 Encryption tools

Encryptie is het proces waarbij een bericht zodanig wordt veranderd dat de inhoud ervan wordt verborgen en niet kan worden gelezen zonder de juiste decoderingssleutel. Dit is een fundamentele beveiligingstool die vertrouwelijkheid met codering implementeert.

- Tor (Tor Project, sd) ⁶
- KeePass (KeePass, sd) ⁷

3.3 Web Vulnerability scanning tools

Web Vulnerability tools zijn geautomatiseerde tools waarmee organisaties kunnen controleren of hun netwerken, systemen en applicaties zwakke plekken in de beveiliging hebben waardoor ze aan aanvallen kunnen worden blootgesteld.

- Burp Suite (PortSwigger, sd) ⁸
- Nikto (Sullo & Lodge, sd)
- Paros (SourceForge, sd)
- Nmap (Nmap, sd)
- Nessus (Tenable, sd)
- Nexpose (Rapid7, sd)

⁶ Tor Project. (sd). *Tor Project | Anonymity Online*. Opgehaald van www.torproject.org: <https://www.torproject.org/>

⁷ KeePass. (sd). *KeePass Password Safe*. Opgehaald van keepass.info: <https://keepass.info/>

⁸ PortSwigger. (sd). *Burp Suite - Application Security Testing Software - PortSwigger*. Opgehaald van [portswigger.net](https://portswigger.net/burp): <https://portswigger.net/burp>

Sullo, C., & Lodge, D. (sd). *Nikto2 | CIRT.net*. Opgehaald van cirt.net: <https://cirt.net/Nikto2>

SourceForge. (sd). *Paros download | SourceForge.net*. Opgehaald van [sourceforge.net](https://sourceforge.net/projects/paros/): <https://sourceforge.net/projects/paros/>

Nmap. (sd). *Nmap: the Network Mapper - Free Security Scanner*. Opgehaald van nmap.org: <https://nmap.org/>

Tenable. (sd). *#1 Vulnerability Assessment Solution | Nessus Professional™*. Opgehaald van [www.tenable.com](https://www.tenable.com/products/nessus/nessus-professional): <https://www.tenable.com/products/nessus/nessus-professional>

Rapid7. (sd). *Nexpose: Vulnerability Scanner & Software | Rapid7*. Opgehaald van [www.rapid7.com](https://www.rapid7.com/products/nexpose/): <https://www.rapid7.com/products/nexpose/>

3.4 Penetration testing

Penetratie testen is het proberen binnen te dringen van een computersysteem of applicatie om op deze manier te achterhalen waar zwakheden liggen waar dan aangevallen kan worden. (Rosencrance, sd)

Er zijn twee bekende programma's die dit automatisch kunnen doen ⁹:

- Metasploit (Metasploit, sd)
- Kali Linux (Kali, sd)

3.5 Network defense wireless tools

Deze verdedigingen tegen verstoring oftewel 'denial of service'. Enkele voorbeelden van netwerkverdediging zijn firewalls, gedemilitariseerde zones (DMZ's), virtuele privénetwerken (VPN's), inbraakdetectiesystemen (IDS's) en kwetsbaarheidsscanners. ¹⁰

- Aircrack (AirCrack, sd)
- Netstumbler (NetStumbler, sd)
- KisMAC (KisMAC, sd)

⁹ Metasploit. (sd). *Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit*. Opgehaald van www.metasploit.com: <https://www.metasploit.com/>

Kali. (sd). *Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution*. Opgehaald van www.kali.org: <https://www.kali.org/>

Rosencrance, L. (sd). *What is pen test (penetration testing)? - Definition from WhatIs.com*. Opgehaald van [searchsecurity.techtarget.com](https://searchsecurity.techtarget.com/definition/penetration-testing#:~:text=Penetration%20testing%2C%20also%20called%20pen,software%20applications%20or%20performed%20manually): <https://searchsecurity.techtarget.com/definition/penetration-testing#:~:text=Penetration%20testing%2C%20also%20called%20pen,software%20applications%20or%20performed%20manually>

¹⁰ AirCrack. (sd). *Aircrack-ng*. Opgehaald van www.aircrack-ng.org: <https://www.aircrack-ng.org/>

NetStumbler. (sd). *Downloads | NetStumbler*. Opgehaald van www.netstumbler.com: <http://www.netstumbler.com/downloads/>

KisMAC. (sd). *Free WiFi scanner and security software for Mac - KisMAC*. Opgehaald van kismac-ng.org: <https://kismac-ng.org/>

3.6 Network intrusion & detection

Dit zorgt voor het opmerken van verschillende activiteiten die als gevaarlijk gezien kunnen worden. Deze worden dan vermeld en kunnen opgehaald en bekeken worden door een administrator of beheerder van het netwerk. ¹¹

- Snort (Snort, sd)
- Forcepoint (Forcepoint, sd)
- GFI LanGuard (GFI Software, sd)
- Acunetix (Acunetix, sd)

3.7 Continuous Integration

Door beveiligingstests een onderdeel te maken van continuous integration, worden beveiligingsnormen in het software afgedwongen.

3.8 Security Design Patterns

Door security design pattern toe te passen zorg je ervoor dat vertrouwelijke informatie wordt afgeschermd en alleen gezien mag worden door geautoriseerde personen.

¹¹ Snort. (sd). *Snort - Network Intrusion Detection & Prevention System*. Opgehaald van www.snort.org: <https://www.snort.org/>

Forcepoint. (sd). *Next Generation Firewall - NGFW | Forcepoint*. Opgehaald van www.forcepoint.com: <https://www.forcepoint.com/product/ngfw-next-generation-firewall>

GFI Software. (sd). *Network Security, Network Monitor and Network scanner with Vulnerability Scanning, Patch Management and Application Security | GFI LanGuard performs vulnerability assessments to discover threats early*. Opgehaald van www.gfi.com: <https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard>

Acunetix. (sd). *Acunetix | Web Application Security Scanner*. Opgehaald van www.acunetix.com: <https://www.acunetix.com/>

3.9 JWT

JWT staat voor json web token en is een open standaard voor het veilig versturen van informatie tussen 2 partijen in een json object. Deze informatie kan worden vertrouwd omdat het digitaal is ondertekend. JWT wordt gebruikt voor autorisatie en informatie-uitwisseling.

Als de JWT goed wordt toegepast is er een access token en een refresh token. De access token heeft een korte geldigheidsduur (Bijv. 5 minuten) en de refresh een langere geldigheidsduur. (Bijv. 8 uur)

Beide tokens worden in de frontend apart opgeslagen. Bijv. de refresh token wordt in de local storage opgeslagen en de access token in de cookies.

Wanneer er een API-call gemaakt moet worden naar een backend dan wordt de access token meegestuurd. Als deze niet meer geldig is dan wordt de refresh token gestuurd om een nieuwe access token aan te vragen.

3.10 Two Factor Authentication

Er zijn meerdere manieren om in te loggen waar je gebruik maakt van:

Iets dat u weet: een wachtwoord, pincode, postcode of antwoord op een vraag (meisjesnaam moeder, naam huisdier, enzovoort)

Iets wat je hebt: een telefoon, creditcard, bankpas

Iets wat je bent: een biometrische zoals een vingerafdruk, netvlies, gezicht of stem

Door gebruik te maken van two factor authentication dan moeten gebruikers een wachtwoord invullen (iets dat je weet) en een code dat gegenereerd wordt door (in dit geval) de Google/Microsoft authenticator app. (iets dat je hebt)

2 factor authenticatie is een authenticatie methode waarbij je 2 stappen moet uitvoeren om succesvol te authentifieren. De eerste stap is vaak het invoeren van een gebruikersnaam en wachtwoord. De 2e stap is ruimer, denk aan bijvoorbeeld sms-verificatie.

<https://wettransfer.com/downloads/043f71d920d690c2258f5fb1ba404e8620210429082843/66ad40e06359c92350be62ef031f5d2f20210429082911/d7ef78>

4. Veldwerk

In dit hoofdstuk wordt er onderzocht welke tools er worden gebruikt op het gebied van security. Hiervoor zal er een interview worden gehouden met iemand die ervaring heeft op dit gebied. Eerst zal er een interview gehouden worden met docenten om kennis op te doen van de beschikbare tools om de security te waarborgen.

Vervolgens wordt er met Pharmapartners een interview gehouden om erachter te komen welke tools zij al gebruiken en welke zij nog niet gebruiken.

Op basis van het biebonderzoek en de interviews gaan we kijken van welke tools er een POC gemaakt zal worden.

4.1 Interviewvragen met docent: Bij welke ICT-bedrijven heb je gewerkt?

Bij Atos, Eurocom, zij maakten software voor in de zorg. Gericht voor ouderen.

En ik heb software gemaakt voor E-bikes voor het bedrijf RIH.

Welke tools werden er door deze bedrijven gebruikt om de security te waarborgen?

Bij Eurocom gebruikten ze certificaten. Elk apparaat dat was gekoppeld aan het netwerk had een certificaat. En deze certificaat werden gebruikt om een versleuteling te creëren.

Ook werd er gebruik gemaakt van Entity Framework omdat volgens het OWASP lijst SQL injection nog steeds op nummer één staat en door middel van een ORM kun je dit gemakkelijk voorkomen. Ook password hashing is erg belangrijk omdat hackers die toch toegang hebben kunnen krijgen tot de database niks kunnen doen met de gehashte wachtwoorden.

Er wordt ook gebruik gemaakt van HTTPS.

Welke tools/manieren ken je nog meer die de security waarborgen?

- Door het OWASP lijst af te gaan kun je al veel aanvallen tegenhouden.
- Wat wij als proftaak nog kunnen toepassen is JWT met refresh tokens. Op dit moment hebben wij in het project wel JWT toegepast maar niet de refresh tokens.
- Een ORM zoals JPA of Entity Framework.
- Authenticatie en Autorisatie afhandelen op de gateway. Op de microservices moeten dan nog wel je JWT gecontroleerd worden.
- Secure databases en obfuscation.
- In de gateway authorization en authentication implementeren.
- Certificaten, RBAC role based access control en wachtwoorden hashen.

4.2 Interviewvragen met Pharmapartners:

Welke security tools gebruiken jullie op dit moment binnen het agenda systeem/Medicom? Waarom worden deze gebruikt?

- Ze maken gebruik van security patterns, certificaten, security, OWASP, Multifactor authentication, Gehashte wachtwoorden.
- Ze maken nog geen gebruik van veilige verbinding met https.
- Elke huisarts heeft een eigen database: Multitenancy.
- Ze hebben een JavaFX container binnen de client. Hierdoor kan niet iemand zomaar de code inspecteren.
- Pharmapartners probeert up to date te blijven met versioning van software.
- Met Jenkins wordt na elke build de code gecontroleerd met SonarQube en de unittesten worden uitgevoerd.
- Eigen database per huisarts Multitenancy?

Zijn er security tools die jullie wel hebben onderzocht maar niet gebruiken en welke redenen hadden jullie om deze niet te gebruiken?

Wireshark om dingen inzichtelijk te maken.

Aan welke eisen moet een security tool voldoen om gebruikt te worden?

Ze zijn er vrij in. Wel moet er rekening gehouden worden met welke informatie gedeeld en opgeslagen wordt met een leverancier.

Welke info wordt opgeslagen – is het herleidbaar naar een persoon (mag niet vanuit wetgeving)

Wat zijn de gevolgen als de Medicom applicatie niet goed beveiligd is?

Privacygevoelige info komt op straat. Zoals NAW-gegevens.

Gegevens van de zorg zijn veel geld waard voor hackers

Zijn er nog punten waar wij op moeten letten?

Design patterns zijn het belangrijkste om veilige code te schrijven. Transacties en fallbacks indien er iets niet goed gaat. En de security & privacy by design zijn punten waar goed op gelet moeten worden.

5. Werkplaats

In dit hoofdstuk worden security tools uitgewerkt door middel van een proof of concept (POC). Er is in dit onderzoek ervoor gekozen om niet alle onderdelen te implementeren. Dit is gedaan omdat er rekening gehouden moest worden met de beschikbare tijd. We hebben gekozen voor Two factor Authentication als authenticatie en JWT voor autorisatie.

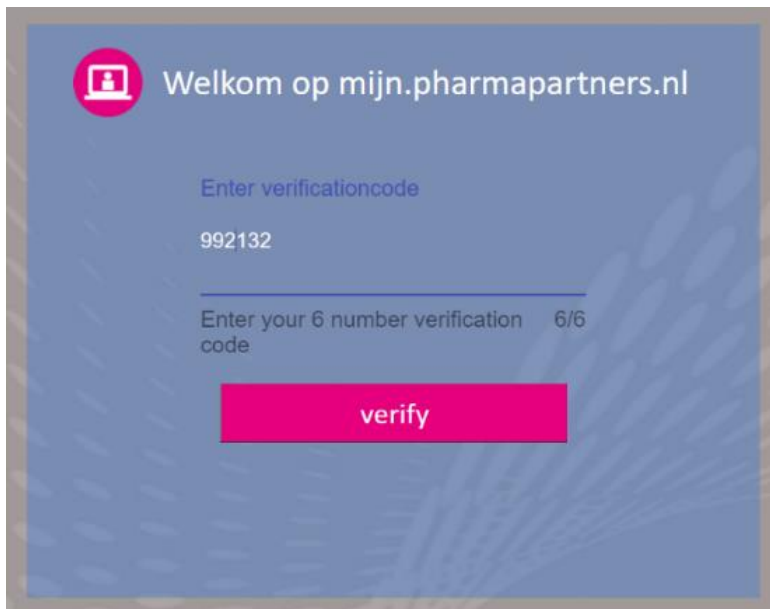
5.1 inlog scherm

Bij het inloggen wordt er gebruik gemaakt van een gebruikersnaam en wachtwoord.



5.1.1 2FA

Na het inloggen met gebruikersnaam en wachtwoord moet er een zes cijferige code ingevoerd worden. Dit haalt de gebruiker op van de Google/Microsoft authenticator op.



Code Google Authenticator:

students@fhict (agenda@example.com)

992 132

5.2 JWT

Hieronder wordt de JWT uitgelegd.

Een JWT-token:

```
Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJkb2t0ZXIiLCJleHAiOiE2MTk3MjI0MzAsIm1hdCI6MTYxOTY4NjQzMmH0.BCae4pGM1rzK-0680mDVTpRcASj1Zshjo6zEkVMXQnrUztFH3AM1ychHyQzSe7yFPL1y80015oEBjWYacr1t1g
```

Door gebruik te maken van een `JwtRequestFilter` in de backend wordt elke request dat naar de backend gaat gecontroleerd op JWT-tokens. Deze tokens worden dan gevalideerd of ze wel geldig zijn.

```
@Component
public class JwtRequestFilter extends OncePerRequestFilter {
```

Als de tokens niet geldig zijn dan volgt er een error. Er wordt dan geen informatie opgehaald vanuit de backend.

Volgens het biebonderzoek moet er ook gebruik gemaakt worden van refresh tokens. Maar dit hebben wij niet kunnen implementeren omdat dit te veel werk zou zijn voor de korte tijd dat wij hebben om aan het project te werken. Ook was volgens het interview met Kevin duidelijk dat we meer moeten focussen op design patterns. Het bedrijf maakt al gebruik van JWT-tokens.

6. Showroom

Na het maken van de POC's worden deze getoond aan de opdrachtgeven en docenten. Hiervoor zullen we feedback ontvangen en deze feedback zullen we toepassen.

Tijdens de sprint demo hebben we de two factor authentication getoond aan de opdrachtgever. Ze waren hier wel erg tevreden mee. Zelf gebruiken zij de windows authenticator app en tijdens de demo hebben wij de google authenticator app getoond.

We hebben ze laten zien dat we gebruik maken van jwt tokens. Ook aangegeven dat het niet gelukt is om refresh tokens toe te passen maar we hebben ze aangegeven dat dit wel good practice is.

7 Conclusie

Op basis van het biebonderzoek, veldwerk, werkplaats en showroom komt er een conclusie op de vraag: "Welke security tools zijn geschikt voor de Medicom agenda applicatie?"

JWT

Het advies is om gebruik te maken van access tokens en refresh tokens. Dit voegt een extra laag aan beveiliging omdat hackers twee verschillende tokens moeten onderscheppen. Als ze de access token hebben dan is de geldigheidsduur maar erg kort.

Bij het controleren van de JWT-token in de backend moet er altijd gecontroleerd worden op de signature. Als dit niet het geval is dan kan een kwaadwillige de JWT-token aanpassen.

Two factor authentication

Aangezien Pharmapartners met veel vertrouwelijke informatie werkt, is het aangeraden om two factor authentication altijd aan te zetten voor alle gebruikers.

Network security monitoring tools

Medicom kan dit gebruiken voor het analyseren en monitoren van ingaande en uitgaande traffic om zo cyber bedreigingen te herkennen.

Encryption tools

Medicom kan encryption tools gebruiken om de persoonsgegevens te beveiligen die in de patiënten doseer staan.

Web vulnerability scanning tools

Aangezien Medicom met persoonlijke gegevens werkt is het belangrijk om goed in de gaten te hebben hoe en waar de zwakke plekken in de applicatie zitten zodat deze kunnen worden verbeterd. Daar kunnen web vulnerability scanning tools een grote bijdrage aan geven

Penetration testing tools

Penetratietesten zijn handig om zwakke plekken te ontdekken in je applicatie. Hierdoor kan er voorkomen worden dat de applicatie wordt gehackt.

Network intrusion and detection tools

Door network intrusion and detection software te gebruiken kan Medicom Cyber-attacks detecteren.

Continuous integration

Door beveiligingstests een onderdeel te maken van continuous integration, worden beveiligingsnormen in de software afgedwongen. Hierdoor zal Medicom altijd aan de beveiligingsnormen voldoen.

Security Design Patterns

Er zijn veel verschillende design patterns, Voor Medicom adviseren wij om gebruik te maken van Authenticator, authorization en roles om ervoor te zorgen dat de geautoriseerde personen bij de vertrouwelijke informatie mogen komen. Single access point, door middel van een API, Input validation om ervoor te zorgen dat de input geldig is.

OWASP

OWASP geeft aan welke risico's meer prioriteit hebben dan andere risico's. Door het toepassen van OWASP worden de meeste voorkomende risico's verholpen waardoor de applicatie veiliger wordt.

8 Advies

Antwoord op de vraag: "Welke security tools zijn geschikt voor de Medicom agenda applicatie?"

Voor de Medicom agenda applicatie zijn alle onderzochte tool geschikt, echter is het tijdrovend om alles toe te gaan passen. Daarom adviseren wij om de OWASP, JWT en securitydesign patterns toe te passen. Wij adviseren JWT-tokens omdat het schaalbaarder is dan sessies en cookies. Dit komt omdat JWT-tokens client side opgeslagen worden en sessie en cookies server side. Daarnaast is er gekozen voor OWASP om de meest gebruikte beveiliging risico's te voorkomen. Wij adviseren ook securitydesign patterns toe te passen om de code kwaliteit en veiligheid te bewaren. Deze onderdelen zijn gekozen om de security punten binnen de applicatie te kunnen waarborgen.