Pentesting

Verslag

Application Security

2 APP/AI 01

Academiejaar 2023-2024

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

Contents

1 OVERVIEW

1.1 Klant

Thomas More Geel

- Alexander Hensels
- Michaël Cloots

1.2 Tijdsbereik

Testing van 05/10/20 – 17/12/2023

- Uitgevoerd door Lintermans Thijs
- Review door Lintermans Thijs

1.3 Materiaal toepassingsgebied

- ASP .net webapplicatie
    - 10.0.2.100/

1.4 Document versie

Versie	Datum	Auteur	Commentaar
v1.0	17 december 2023	Lintermans Thijs	Eerste inlevering aan klant

2 EXECUTIVE SUMMARY

2.1 Risico Classificering

Voor alle gevonden kwetsbaarheden is er een risico classificering gedaan.

Kritisch	Hoog	Middelmatig	Laag	Info
1 kwetsbaarheid	1 kwetsbaarheid	Niets gevonden	Niets gevonden	1 zaak

2.2 Context

De penetratietest voor Thomas More Geel werd uitgevoerd om de veiligheid van de nieuwe webapplicatie te testen. Het voornaamste doel was het op zoek gaan en identificeren van kwetsbaarheden die een bedreiging kunnen zijn voor de veiligheid van de applicatie en mogelijks ook de organisatie.

Dit verslag geeft een overzicht van alle kwetsbaarheden en hun mogelijke bedreiging. Ook enkele aanbevelingen voor het oplossen van deze kwetsbaarheden.

2.3 Observaties

2.3.1 Positieve observaties

Na het uitvoeren van grondige testen, zijn er zeker positieve zaken verder gekomen uit de applicatie. Zo is de webapplicatie goed beveiligd tegen de meer opvallende en zeer schadelijke kwetsbaarheden. Dus de initiële configuratie van de webapplicatie is zeer goed gemaakt.

2.3.2 Negatieve observaties

Alhoewel er positieve aspecten zijn aan de webapplicatie, zijn er ook enkele negatieve observaties gedaan.

Bij het opstarten van de applicatie en het bekijken van de verschillende tabbladen, is direct zichtbaar dat acces control een zwak punt is. Zonder in te loggen of extra rechten te hebben, is er de mogelijkheid om zaken, zoals producten en categorieën, aan te passen. Dit lijkt misschien niet zo een erge kwetsbaarheid, maar dit kan zeer vervelend zijn als gebruikers zaken verwijderen. Ook kan men denken waar komt slechte acces control nog voor en zo nog meer schade aanrichten. Zo zijn we tijdens het testen ook terecht gekomen op de admin pagina. Ook omdat er slechte acces control is.

Op deze admin pagina kunnen de wachtwoorden bekeken worden, deze staan in plain tekst. Dit is iets wat voor vele gebruikers veel schade kan aanrichten. Ook kan men wachtwoorden verwijderen of aanpassen. Bij het bekijken van de wachtwoorden viel het ook op dat de wachtwoorden zeer gemakkelijk zijn. Dit duidt dan op een slechte password policy.

2.4 Conclusie

Na het uitvoeren van de uitgebreide testen, kan er geconcludeerd worden dat de webapplicatie op bepaalde vlakken zeer goed beveiligd is. Dat gezegd hebbende, kunnen de kwetsbaarheden die gevonden zijn een zeer groot risico vormen. Ze vereisen daarom dan ook onmiddellijke aandacht, aangezien dit schadelijk kan zijn voor niet enkel de applicatie, maar ook op de reputatie van het bedrijf.

3 LIJST VAN BEVINDINGEN

Hier vindt u een overzicht van alle bevindingen.

Titel	Status	Ernst	Pagina
Slechte acces control	Onopgelost	Kritisch	7
Wachtwoorden opgeslagen in Plain Text.	Onopgelost	Hoog	12
Slechte password policy	Onopgelost	Info	13

3.1 Acces Control

Kritisch

3.1.1 Omschrijving

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:H/VA:N/SC:L/SI:H/SA:N

Tijdens het testen van de webapplicatie is er vastgesteld dat er onvoldoende acces control wordt gedaan. Acces control of toegangscontrole is een cruciaal deel van de beveiliging. Het is het toepassen van beperkingen op wie of wat gemachtigd is om tot bepaalde zaken toegang te krijgen of uit te voeren.

Bij verder onderzoek en testen zijn er 2 problemen vastgesteld op basis van acces control.

Het eerste probleem is dat niet-ingelogde gebruikers of gebruikers met beperkte rechten verschillende zaken konden aanpassen. Hier spreken we dan van een slechte Role-Based Access Control.

Op de webapplicatie zijn er de tabbladen “Products” en “Categories”. Bij het openen van deze tabbladen is er een mogelijkheid om producten of categorieën aan te passen, te verwijderen en ook nieuwe aan te maken. Ook kan men de details zien van de categorieën. Dit duidt op een gebrek aan juiste toegangscontrole op basis van gebruikersrollen.

Het tweede probleem gaat over vertical privilege escalation. Dit wil zeggen dat een gebruiker extra functionaliteiten kan krijgen die ervoor zorgen dat hij toegang kan krijgen tot bronnen of acties kan uitvoeren die buiten het oorspronkelijk toegewezen autorisatieniveau vallen van deze gebruiker.

Op de webapplicatie kan een gebruiker toegang krijgen tot de admin pagina. Dit kan allemaal worden gedaan door na de IP of hostnaam van de website “/admin” te zetten. Na het uitvoeren van deze link, krijgt de gebruiker toegang.

3.1.2 Risico

Slechte toegangscontrole kan leiden tot aanzienlijke risico’s op vlak van veiligheid. Enkele risico’s voor deze webapplicatie zijn:

- Bij het toegang krijgen tot de admin-pagina, kan een gebruiker veel schade aanrichten. De gebruiker kan de gebruikersnaam, het wachtwoord en de rol van alle gebruikers zien. Ook kan hij/zij gebruikersgegevens aanpassen en gebruikers verwijderen.

- De toegang tot de admin-pagina kan ook leiden tot een data breach, waar al deze gevoelige gegevens worden geëxfiltreerd. Deze kunnen dan geleaked worden, wat kan leiden tot financiële en reputatie problemen.

- Het aanpassen van producten of categorieën, kan leiden tot ontevredenheid bij klanten. Ook kan het leiden tot financiële en reputatie problemen.

    - Prijzen van producten kunnen aangepast worden.
    - Producten en categorieën kunnen verwijderd worden, waardoor er geen verkoop mogelijk is.

3.1.3 Aanbevelingen

Voor deze kwetsbaarheid raden we enkele zaken aan.

Eerst raden we aan om het principe van “Least privileges” toe te passen. Dit betekent dat een gebruiker de minimumrechten wordt toegewezen die nodig zijn om te kunnen doen wat er moet gebeuren.

Ook raden we aan om de permissions op elke verzoek na te gaan. Ongeacht welk verzoek moet er eerst bekeken worden of de gebruiker dit verzoek mag maken.

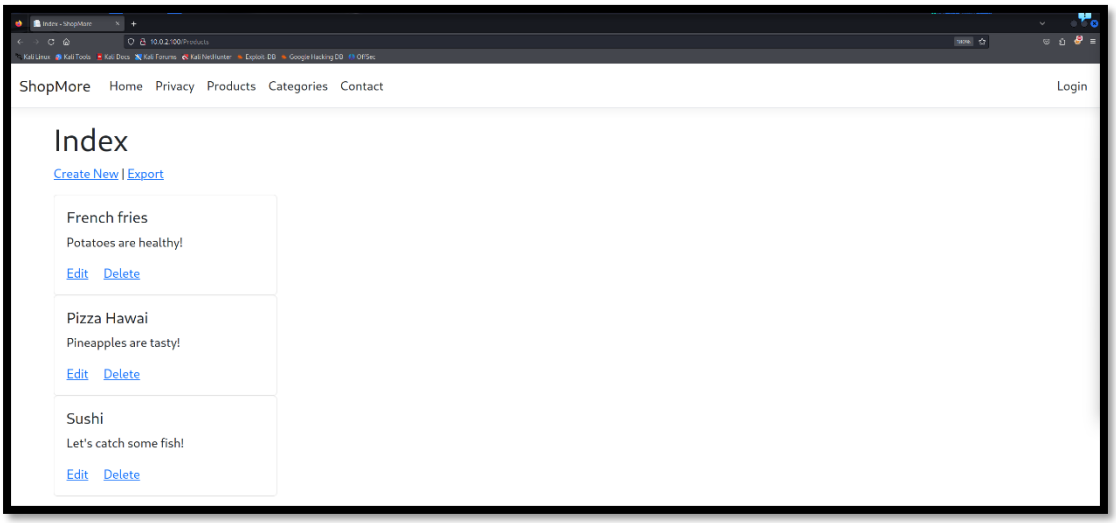
Referentie:https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html

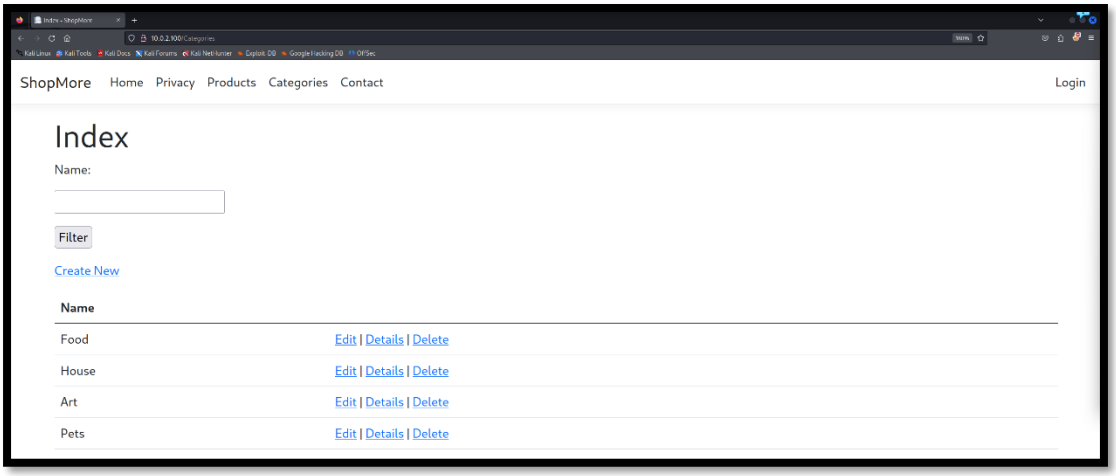
3.1.4 Bewijs

Bij het openen van de tabbladen “Products” en “Categories” kan je zaken aanpassen zonder ingelogd te zijn. Ook als ik ben ingelogd als gewone gebruiker heb ik deze mogelijkheid nog.

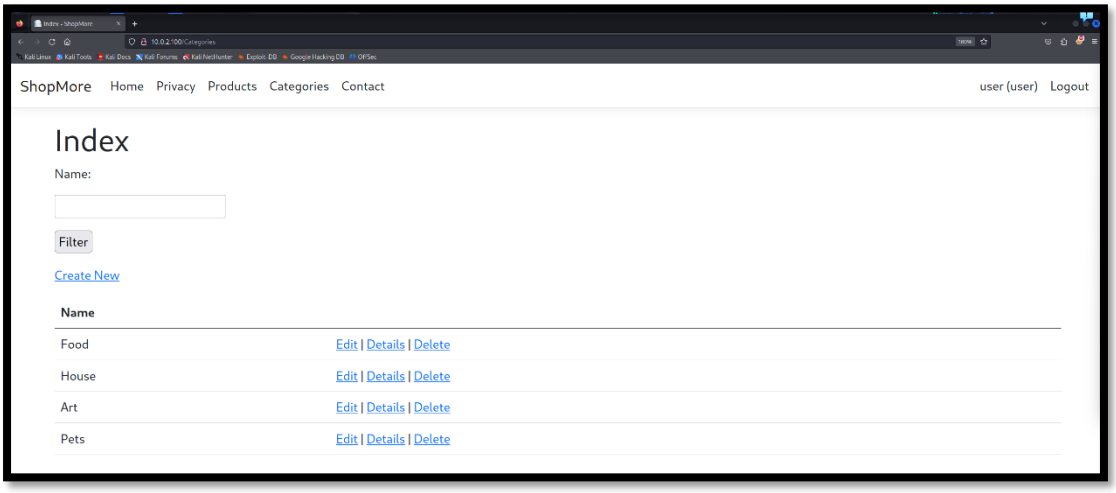
3.1.4.1 Niet ingelogd

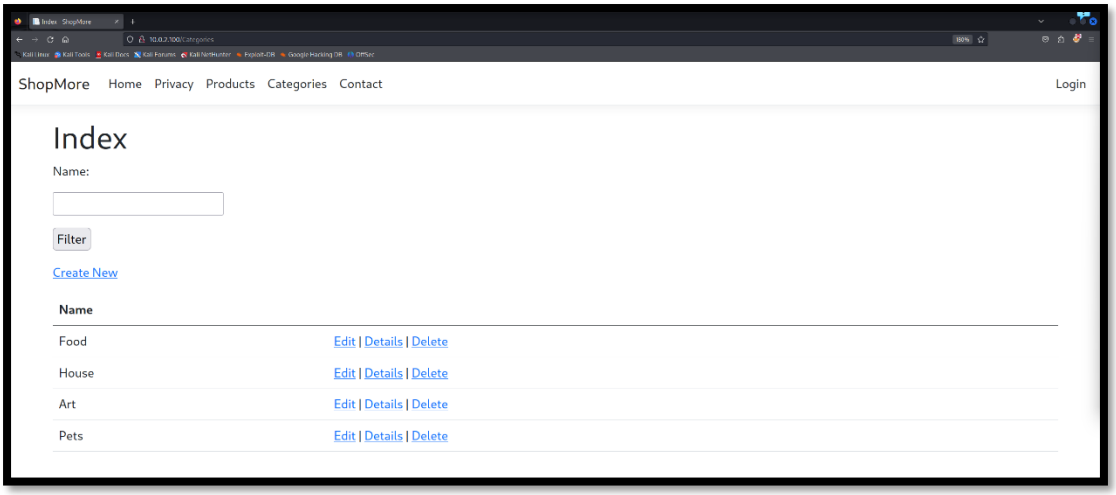
3.1.4.2



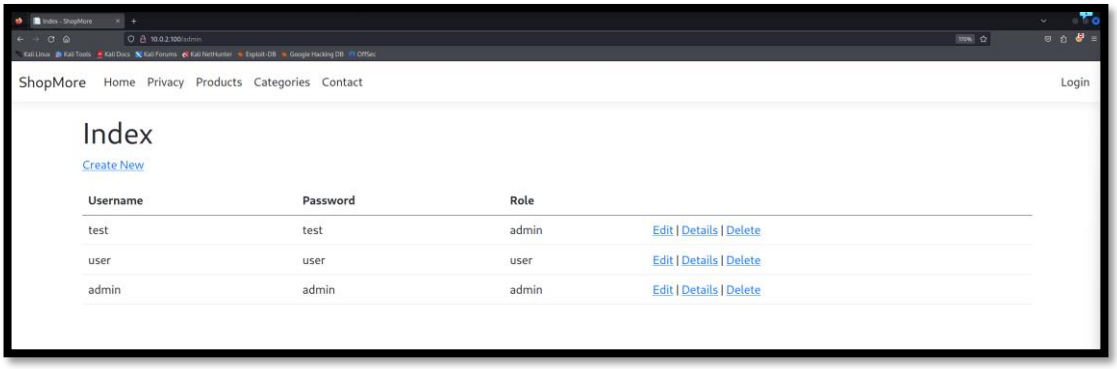


3.1.4.3 Ingelogd





Door “/admin” achter de IP te zetten krijgt men toegang tot de admin-pagina.



3.2 Wachtwoorden opgeslagen in Plain Tekst

Hoog

3.2.1 Omschrijving

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:H/VA:N/SC:L/SI:H/SA:N

Bij het bekijken van de wachtwoorden op de admin-pagina viel het op dat de wachtwoorden in plain tekst waren geschreven. Als je dan op de admin-pagina komt, kan iedereen de wachtwoorden lezen van alle gebruikers.

3.2.2 Risico

Het tonen van wachtwoorden in plain tekst kan ernstige risico's met zich meenemen:

- Schending van de privacy van de gebruiker.
- Kans op het tonen van deze wachtwoorden in logs of andere manieren. Zo kan iedereen deze wachtwoorden bekijken.
- Als deze gegevens worden geleaked, kan iedereen die deze gegevens heeft op de accounts van deze gebruikers.
- Bij het ondervinden van dit, kan dit leiden tot reputatieschade van de organisatie.

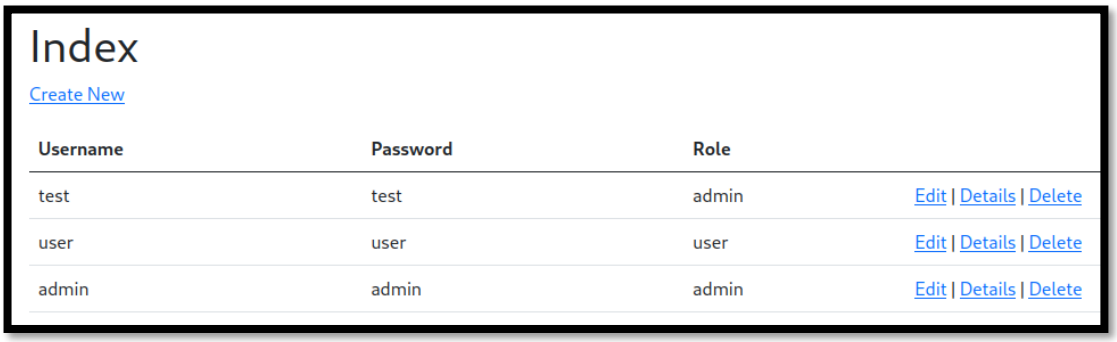
3.2.3 Aanbevelingen

Over het algemeen wordt aanbevolen om gebruik te maken van hashing algoritmen. Dit zal ervoor zorgen dat het wachtwoord wordt omgezet naar een collectie van nummers. Daarnaast is het ook belangrijk om gebruikt te maken van een "salt". Dit zal een willekeurig aantal gegevens toevoegen aan het wachtwoord voordat dit gehasht wordt. Op deze manier is het nog moeilijker om de wachtwoorden te kraken.

Referentie: https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

3.2.4 Bewijs

Hier kunnen we zien dat we de wachtwoorden zo kunnen lezen.



3.3 Password Policy

Info

3.3.1 Omschrijving

Bij het bekijken van de wachtwoorden op de admin pagina, viel het op dat de wachtwoorden zeer zwak zijn. Een zwak wachtwoord kan een aanzienlijk risico vormen voor de gebruikers, maar ook de mensen met meer rechten op de webapplicatie.

Zwakke wachtwoorden op een webapplicatie kan maar één iets betekenen, er is een slechte tot geen password policy.

3.3.2 Risico

Zwakke wachtwoorden kunnen veel, zeer schadelijke risico's met zich meebrengen.

- Organisaties kunnen aansprakelijk gesteld worden door inbreuken op een account van een gebruiker als gevolg van een zwak wachtwoord. Dit heeft dan mogelijke juridische en financiële gevolgen

- Aanvallers kunnen gemakkelijk toegang krijgen tot het account van een gebruiker. Hier kunnen dan frauduleuze activiteiten uit verder komen.

- Aanvallers kunnen toegang krijgen tot een account van een persoon met meer rechten. Dit kan leiden tot onomkeerbare schade.

- Bij het vaak voorkomen van inbreuken op accounts van gebruikers, kan er reputatie- en vertrouwensschade zijn.

3.3.3 Aanbevelingen

Om deze risico's tegen te gaan, wordt er sterk aangeraden om een betere regels te maken voor wachtwoorden.

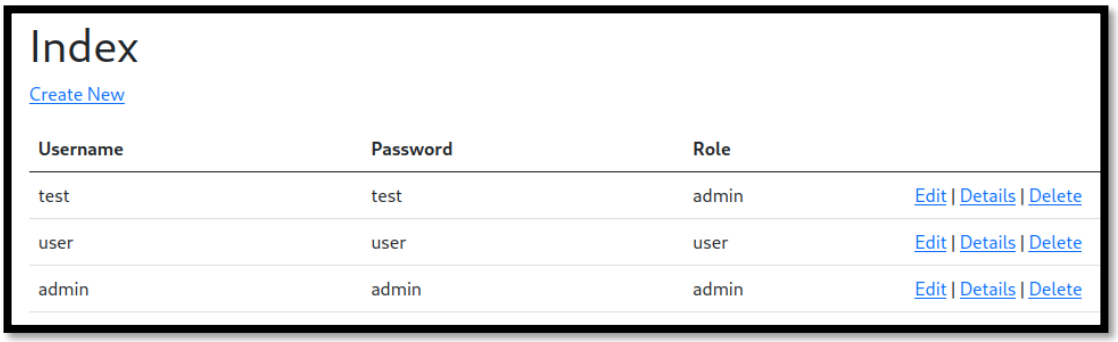
- Vereis dat gebruikers hun wachtwoorden voldoen aan een bepaalde lengte. Een aanbevolen lengte is 12 tekens.

- Vereis dat gebruikers verschillende tekens in hun wachtwoord gebruiken. Zorg ervoor dat er zeker hoofdletters, kleine letters, symbolen en cijfers in zitten.

Referentie: https://www.odit.be/5-gouden-regels-waaraan-je-password-policy-moet-voldoen/

3.3.4 Bewijs

Op de admin-pagina is er te zien dat de wachtwoorden heel gemakkelijk zijn.



Index

Create New

Username	Password	Role	
test	test	admin	Edit | Details | Delete
user	user	user	Edit | Details | Delete
admin	admin	admin	Edit | Details | Delete

4 BIJLAGE A: TESTGEVALLEN

In onderstaande tabel ziet u welke testgevallen er tijdens deze pentest behandelt zijn.

Titel	Omschrijving	Status
SQL Injection	Query's die een applicatie maakt naar zijn database aanpassen of zelf sturen.	Getest door Thijs Lintermans
Command injection	Laat anvallers toe om operating commando's uit te voeren op de server.	Getest door Thijs Lintermans
Acces Control	Bekijkt wie of wat toestemming heeft om bepaalde acties uit te voeren	Getest door Thijs Lintermans
Cross-Site Scripting (XSS)	Aanvaller die kwaadaardige scripts injecteert op de webpagina.	Getest door Thijs Lintermans
Information disclosure	Het onbewust tonen van gevoelige gegevens.	Getest door Thijs Lintermans
Directory Traversal	Het proberen toegang krijgen tot bestanden of mappen die buiten rootdirectory van applicatie ligt. Dit wordt gedaan door slechte bestandspaden samen te stellen.	Getest door Thijs Lintermans

5 BIJLAGE B: METHODOLOGY

5.1 Klantgesprek

Tijdens dit gesprek is er een eerste kennismaking met de klant. Tijdens dit gesprek worden de regels en beperkingen van de test vastgelegd. Ook wordt er het toepassingsgebied beslist.

5.2 Informatieverzameling

Hier gaat de pentester de applicatie bekijken. Hij/zij gebruikt de applicatie en maakt zich hier meer met bekend. Ook wordt er gekeken en nagedacht over mogelijke opties waar er kwetsbaarheden kunnen zitten.

5.3 Testing

Tijdens deze fase gebeurt al het testen. Hier gaat de pentester alle mogelijke kwetsbaarheden bekijken en de applicatie testen.

5.4 Rapporteren

Alle kwetsbaarheden die gevonden zijn tijdens de pentest worden in deze fase gedocumenteerd.

5.5 Review

Nadat het rapport is aangemaakt en aangevuld met alle kwetsbaarheden, wordt deze nog eens nagekeken door een collega pentester.

5.6 Inleveren

Als alles uitgevoerd is wordt het eindproduct ingeleverd bij de klant.

6 BIJLAGE C: ERNSTCLASSIFICATIE

Voor kwetsbaarheden die we vinden, gebruiken we versie 4.0 van het Common Vulnerability Scoring System (CVSS) om een score te geven. Het helpt ons om de kwetsbaarheid een score te geven waarvan de klanten kunnen zien welke kwetsbaarheden prioriteit hebben.

Voor alle non-informatieve kwetsbaarheden, plaatsen we de CVSS-score in het begin van de omschrijving.

Voor meer informatie over CVSS kan je volgende websites bekijken:

https://www.first.org/cvss/

https://www.first.org/cvss/user-guide#2-1-CVSS-Measures-Severity-not-Risk

6.1 Kritisch

Karakteristieken

- Hoog potentieel voor exploitatie.
- Grote impact op het systeem.
- Hoge kans op succesvolle exploitatie
- Mogelijks vatbaar voor automatische exploitatie tools.

6.2 Hoog

Karakteristieken

- Kunnen aanzienlijke impact hebben.
- Niet veel kennis voor nodig.
- Mogelijks vatbaar voor automatische exploitatie tools

6.3 Medium

Karakteristieken

- Matige impact.
- Meer kennis voor nodig.
- Enkel mogelijk bij voldoen aan verschillende vereisten.
- Is niet vatbaar voor automatische exploitatie tools.

6.4 Laag

Karakteristieken

- Beperkte impact
- Vereist uitgebreide technische vaardigheden.
- Is niet vatbaar voor automatische exploitatie tools.
- Zeer moeilijke te exploiteren.

6.5 Info

Karakteristieken

Kwetsbaarheden in deze categorie zijn puur informatief. Deze kunnen nog steeds een impact hebben op de organisatie, maar zijn kwetsbaarheden die niet kunnen getest worden.

7 VERTROUWELIJKHEID & AANSPRAKELIJKHEID

Dit document bevat vertrouwelijke informatie voor de klant, Thomas More Geel, en mogelijk derde partijen die officieel betrokken zijn bij het project(en) waarover dit document rapporteert. Het is uitdrukkelijk verboden om informatie uit dit document aan andere partijen bekend te maken, tenzij schriftelijke toestemming van Thomas More Geel is verkregen. Het document wordt vertrouwelijk aan de ontvanger verstrekt en mag uitsluitend worden gebruikt voor interne zakelijke doeleinden. Verkoop, kopiëren, reproductie en/of distributie van dit rapport aan enige derde partij, geheel of gedeeltelijk, op welke manier dan ook, is verboden zonder voorafgaande schriftelijke toestemming van Lintermans Thijs.

Lintermans Thijs heeft alle mogelijke inspanningen geleverd om ervoor te zorgen dat de informatie in dit rapport juist is. Echter, de informatie kan gebaseerd zijn op gegevens verstrekt door derde partijen en/of hun softwareproducten, en als zodanig is Lintermans Thijs niet aansprakelijk voor eventuele problemen die kunnen ontstaan als gevolg van onnauwkeurigheden in dit document.