

# Thomas More application

## Penetration Test Report

Siebe Gios - IT-student

## Confidentieel

De informatie in dit rapport is confidentieel. Het mag niet openbaar worden gemaakt of gekopieerd zonder uitdrukkelijke schriftelijke toestemming van Thomas More



## Inhoud

<b>1. Overzicht .....</b>	<b>2</b>
<b>2. Beheer overzicht .....</b>	<b>3</b>
<b>2.1. Context.....</b>	<b>3</b>
<b>2.2. Observaties.....</b>	<b>3</b>
<b>2.2.1. Positieve Observaties.....</b>	<b>3</b>
<b>2.2.2. Negatieve Observaties .....</b>	<b>4</b>
<b>2.3. Conclusie .....</b>	<b>4</b>
<b>3. Lijst van bevindingen .....</b>	<b>5</b>
<b>4. Bijlage A: TESTCASES .....</b>	<b>2</b>
<b>5. Bijlage B: Ernst classificatie .....</b>	<b>4</b>
<b>5.1. Kritiek.....</b>	<b>4</b>
<b>5.2. Hoog 2</b>	
<b>5.3. Medium .....</b>	<b>3</b>
<b>5.4. Laag 4</b>	
<b>5.5. Informatief .....</b>	<b>5</b>
<b>6. Vertrouwelijkheid en aansprakelijkheid .....</b>	<b>6</b>

# 1. Overzicht

## Tijd scope

*Initiele opdracht (2023-09-10- 2023-12-17):*

- **Uitgevoerd door Siebe Gios**

## Materiaal scope

- **Test webapplicatie in ASP.net**

## Document versie

Versie	Datum	Auteur	Commentaar
<b>v1.0</b>	<b>17-Dec-2023</b>	<b>Siebe Gios</b>	<b>Eerste overdracht aan klant</b>

*Tabel 1.1*

## 2. Beheer overzicht

Voor alle ontdekte kwetsbaarheden zijn de volgende risicoclassificaties toegekend:

KRITIEK	HOOG	MEDIUM	LAAG	INFO
1 finding	1 finding	No findings	No findings	No findings

Tabel 2.1: Aantallen zoeken op ernst.

### 2.1. Context

Ik verkreeg een applicatie van Thomas More in de les Application Security. Op deze applicatie heb ik een uitgebreid pentesting project uitgevoerd. Ik paste alle leerstof die we gezien hebben en vindt enkele zaken die toch eens moeten bekeken worden.

Thomas More heeft me gevraagd een web applicatie pentesting project uit te werken tussen 9 september en 17 december.

Het doel van het project was om beveiligingsproblemen te vinden in de applicatie van Thomas More.

Dit rapport biedt Thomas More een overzicht van alle geïdentificeerde kwetsbaarheden en definieert maatregelen om de beveiliging van de applicatiecomponenten te optimaliseren.

### 2.2. Observaties

#### 2.2.1. Positieve Observaties

Tijdens het uitgevoerde pentesting-project vielen enkele positieve aspecten op. Allereerst is de applicatie op veel vlakken goed beveiligd. Het oogt redelijk mooi, maar er is nog wel werk aan de winkel op vlak van security. Bovendien werd een uitgebreide pentest gedaan, waarbij verschillende aanvalsvectoren uitvoerig werden uitgevoerd, waaronder SQL-injecties, command injection, directory traversal, information disclosure, authenticatie en access control, debugger overflows, XSS, en SSRF.

## 2.2.2. Negatieve Observaties

Echter, naast enkel positieve observaties zijn ook kritieke kwetsbaarheden ontdekt. Een zorgwekkende path traversal-mogelijkheid op de /admin-route stelt onbevoegden in staat alle gebruikersaccounts inclusief hun wachtwoorden te benaderen. Bovendien wijst de identificatie van een zwak wachtwoordbeleid op een verhoogd risico op ongeautoriseerde toegang. Het ontbreken van een goede toegangscontrole op de /admin-route vergroot dit risico verder, evenals de aanwezigheid van een XSS-kwetsbaarheid in het contactformulier, wat kan leiden tot het uitvoeren van schadelijke scripts in de context van andere gebruikers.

## 2.3. Conclusie

In conclusie, ondanks de aanwezige beveiligingen en testinspanningen, vereisen de vastgestelde kwetsbaarheden onmiddellijke aandacht. Het risico dat voortkomt uit de path traversal op /admin, het zwakke wachtwoordbeleid, het gebrek aan toegangscontrole op /admin en de aanwezige XSS in het contactformulier benadrukken de noodzaak van onmiddellijke corrigerende maatregelen. Om de algehele beveiliging te waarborgen, wordt aanbevolen deze kwesties snel te adresseren en een proactieve benadering te behouden om toekomstige beveiligingsrisico's te minimaliseren. Het implementeren van robuuste beveiligingsmaatregelen is cruciaal om de integriteit en vertrouwelijkheid van gegevens te handhaven.

### 3. Lijst van bevindingen

Onderstaande tabel geeft een overzicht van alle bevindingen.

Titel	Status	Ernst	Pagina
Path traversal	✗ Onopgelost	Kritiek	6
Zwakke password policy	✗ Onopgelost	Hoog	9
Geen access control	✗ Onopgelost	Medium	11
Cross-site scripting/ XSS	✗ Onopgelost	Hoog	13

Tabel 3.1: Bevindingen gerangschikt op ernst en status.

## Path traversal

Kritiek

### Beschrijving

De recent ontdekte kwetsbaarheid binnen de applicatie, gerelateerd aan path traversal, is van ernstige aard en heeft aanzienlijke implicaties voor de beveiliging van het systeem. Deze specifieke zwakte maakt het mogelijk voor kwaadwillenden om zonder enige belemmering toegang te verkrijgen tot alle gebruikersaccounts, inclusief hun wachtwoorden en rollen, simpelweg door '/admin' aan de URL toe te voegen.

De procedure van het toevoegen van '/admin' aan de URL fungeert als een onbedoelde poort naar de administratieve functies van de website, waarbij de aanvaller zichzelf adminrechten verleent. Deze ongeautoriseerde toegang tot gevoelige informatie creëert een uiterst gevaarlijke situatie waarin de integriteit van het gehele gebruikersbestand en de beheerdersfuncties in gevaar worden gebracht.

De kern van deze kwetsbaarheid ligt in het gebrek aan afdoende controle op gebruikersinvoer binnen de website. Door dit tekort kunnen kwaadwillende actoren URLs manipuleren en onbedoelde paden binnen de applicatie verkennen, waarbij ze beveiligde delen van het systeem kunnen bereiken die normaal gesproken buiten hun bereik zouden moeten liggen.

Het risico wordt versterkt door het feit dat deze actie niet gepaard gaat met enige vorm van authenticatie of autorisatiecontrole. Als gevolg hiervan kunnen kwaadwillenden zonder enige beperking gevoelige gegevens extraheren, zoals gebruikersnamen, wachtwoorden en de bijbehorende rollen. Het ontbreken van deze fundamentele beveiligingsmechanismen betekent dat een aanvaller ongeoorloofd kan rondsnuffelen in beveiligde gebieden van de applicatie en cruciale informatie kan buitmaken.

Het identificeren en onmiddellijk aanpakken van deze kwetsbaarheid is van het grootste belang om de integriteit van het systeem te waarborgen en potentiële schadelijke activiteiten van kwaadwillende actoren te voorkomen. Correctieve maatregelen, zoals het implementeren van inputvalidatie en het afdwingen van strikte autorisatiecontroles, zijn noodzakelijk om deze kwetsbaarheid te verhelpen en toekomstige beveiligingsrisico's te minimaliseren.

### Risico

De geïdentificeerde path traversal-kwetsbaarheid in de applicatie vormt een aanzienlijk risico voor de veiligheid en integriteit van het systeem. De mogelijkheid voor aanvallers om '/admin' aan de URL toe te voegen, opent de deur naar diverse potentiële bedreigingen en heeft aanzienlijke gevolgen:

1. **Ongeautoriseerde toegang tot gebruikersgegevens:** Door de kwetsbaarheid kunnen aanvallers vertrouwelijke gebruikersgegevens opvragen, waaronder persoonlijke informatie, contactgegevens en andere gevoelige details die in het gebruikersprofiel zijn opgeslagen. Deze informatie kan worden misbruikt voor identiteitsdiefstal, phishing-aanvallen of andere kwaadwillige activiteiten.
2. **Wachtwoordinformatie blootgesteld:** De mogelijkheid om wachtwoorden te verkrijgen via deze kwetsbaarheid betekent dat aanvallers onbeperkte toegang kunnen krijgen tot gebruikersaccounts. Dit heeft niet alleen gevolgen voor de getroffen gebruikers op de applicatie, maar het kan ook resulteren in het overnemen van andere accounts als gebruikers hergebruik maken van wachtwoorden.
3. **Misbruik van administratieve functies:** Aangezien de kwetsbaarheid adminrechten verleent, kunnen aanvallers ongeautoriseerde toegang krijgen tot de administratieve functies van de website. Dit opent mogelijkheden voor het wijzigen van systeeminstellingen, het toevoegen



van kwaadaardige gebruikers, het manipuleren van gegevens en andere acties die de integriteit van het systeem in gevaar brengen.

4. **Datalek en compliance risico:** Het ongeautoriseerd verkrijgen van gevoelige informatie als gevolg van deze kwetsbaarheid kan leiden tot een datalek, wat ernstige juridische en compliance-gevolgen met zich meebrengt. Organisaties kunnen aansprakelijk worden gesteld voor schendingen van gegevensbeschermingswetten en kunnen boetes en reputatieschade oplopen.
5. **Verlies van vertrouwen:** Het ontdekken van dergelijke kwetsbaarheden kan het vertrouwen van gebruikers in het platform aantasten. Een geslaagde aanval kan leiden tot een verlies van geloofwaardigheid en loyaliteit van zowel gebruikers als zakelijke partners.

In combinatie vormen deze risico's een ernstige bedreiging voor de algehele beveiliging en functionaliteit van de applicatie. Het is van cruciaal belang om onmiddellijk corrigerende maatregelen te nemen om deze kwetsbaarheid te verhelpen en potentiële schade te voorkomen.

### **Aanbevelingen**

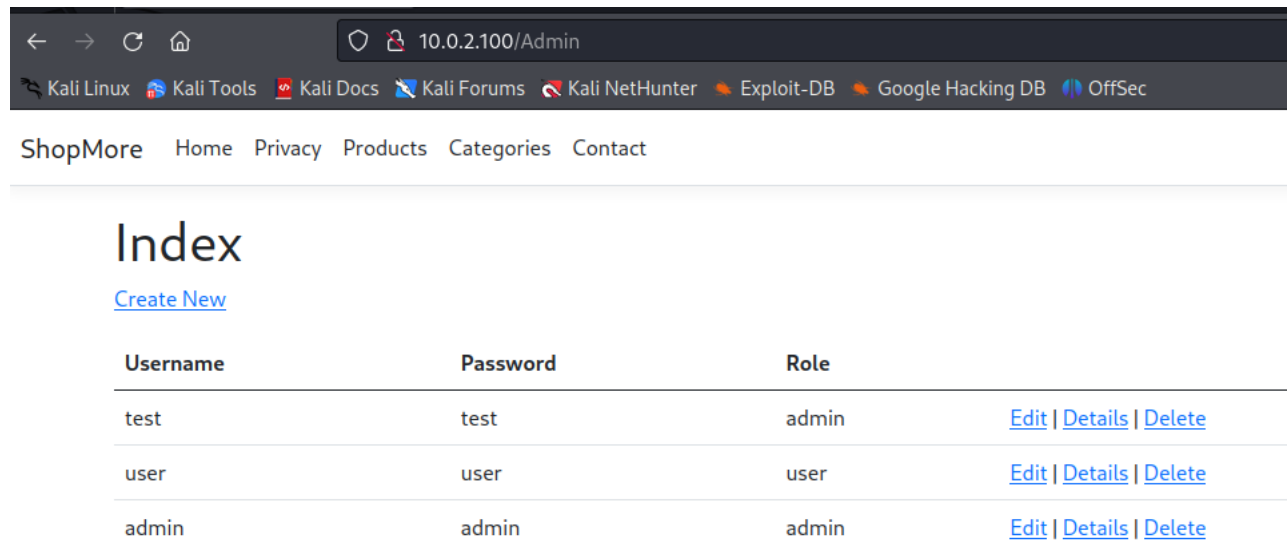
Om dit risico te mitigeren, wordt sterk aanbevolen om onmiddellijk de nodige maatregelen te nemen:

1. **Directe bevestiging en herstel:** Blokkeer onmiddellijk de '/admin'-toegang via de URL en implementeer een robuuste inputvalidatie om path traversal-aanvallen te voorkomen.
2. **Gebruikersrechtenbeheer:** Herzien en versterk het gebruikersrechtenbeheer om ervoor te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot beheerdersfuncties en gevoelige informatie.
3. **Intrusie detectie en monitoring:** Implementeer systemen voor intrusiedetectie en -monitoring om verdachte activiteiten te identificeren en snel te reageren op potentiële aanvallen.
4. **Periodieke security audits:** Voer regelmatig beveiligingsaudits uit om kwetsbaarheden te identificeren en te verhelpen, en zorg ervoor dat de website voldoet aan beveiligingsstandaarden.

Door deze maatregelen te nemen, kan de kwetsbaarheid worden verholpen en kan de integriteit en veiligheid van de applicatie worden gewaarborgd.

## Bewijs

Het bewijs voor deze kwetsbaarheid is gedemonstreerd door het toevoegen van '/admin' aan de URL van de website, wat directe toegang verschaft tot alle gebruikersaccounts, inclusief hun wachtwoorden en rollen.



ShopMore Home Privacy Products Categories Contact

# Index

[Create New](#)

Username	Password	Role	
test	test	admin	<a href="#">Edit</a>   <a href="#">Details</a>   <a href="#">Delete</a>
user	user	user	<a href="#">Edit</a>   <a href="#">Details</a>   <a href="#">Delete</a>
admin	admin	admin	<a href="#">Edit</a>   <a href="#">Details</a>   <a href="#">Delete</a>

## Zwakke password policy

Hoog

### Beschrijving

In de recent ontdekte kwetsbaarheid binnen de applicatie, met betrekking tot zwakke wachtwoordbeleidsmaatregelen, wordt de veiligheid en integriteit van het systeem ernstig bedreigd. Deze specifieke zwakte stelt kwaadwillende actoren in staat om ongeautoriseerde toegang te verkrijgen tot gebruikersaccounts door het gebruik van zwakke wachtwoorden en gebrek aan veiligheidsmaatregelen.

De aanvaller kan eenvoudig gebruikmaken van zwakke wachtwoorden om toegang te verkrijgen tot accounts en potentieel schadelijke acties uit te voeren, zoals het wijzigen van gegevens, uitvoeren van transacties of andere ongeautoriseerde activiteiten.

Deze kwetsbaarheid wordt verder versterkt door het ontbreken van een effectief wachtwoordbeleid binnen de website, waardoor kwaadwillende actoren vrij spel hebben om accounts te compromitteren en mogelijke schade aan te richten.

### Risico

De geïdentificeerde zwakke wachtwoordbeleidskwetsbaarheid in de applicatie vormt een aanzienlijk risico voor de veiligheid en integriteit van het systeem. De mogelijkheid voor aanvallers om toegang te krijgen tot accounts met zwakke wachtwoorden heeft aanzienlijke gevolgen: Ongeautoriseerde acties namens gebruikers: Kwaadaardige scripts kunnen worden gebruikt om acties namens de gebruiker uit te voeren zonder hun medeweten. Dit omvat het uitvoeren van transacties, het wijzigen van gegevens of het uitvoeren van acties op platforms waar de gebruiker is ingelogd.

1. Ongeautoriseerde toegang tot accounts: Kwaadwillende actoren kunnen eenvoudig toegang krijgen tot gebruikersaccounts door het gebruik van zwakke wachtwoorden, waardoor ze ongeautoriseerde activiteiten kunnen uitvoeren.
2. Risico op gegevensdiefstal: Aanvallers kunnen gevoelige informatie zoals persoonlijke gegevens of andere vertrouwelijke informatie stelen door zwakke wachtwoorden te exploiteren.
3. Identiteitsdiefstal: Zwakke wachtwoorden vergroten het risico op identiteitsdiefstal, waarbij aanvallers zich kunnen voordoen als legitieme gebruikers.

### Aanbevelingen

Om dit risico te mitigeren, wordt sterk aanbevolen om onmiddellijk de nodige maatregelen te nemen:

1. Sterk wachtwoordbeleid: Implementeer een sterk wachtwoordbeleid dat het gebruik van zwakke wachtwoorden voorkomt en gebruikers aanmoedigt sterke, unieke wachtwoorden te gebruiken.
2. Twee-factor-authenticatie (2FA): Activeer twee-factor-authenticatie om een extra beveiligingslaag toe te voegen aan gebruikersaccounts.
3. Periodieke wachtwoordwijziging: Moedig regelmatige wachtwoordwijzigingen aan om de beveiliging van accounts te versterken.
4. Wachtwoordhashing: Sla wachtwoorden veilig op door gebruik te maken van sterke hash-algoritmen.

5. **Gebruikersbewustzijn:** Informeer gebruikers over het belang van sterke wachtwoorden en de gevaren van zwakke wachtwoordpraktijken.

Het onmiddellijk aanpakken van deze password-kwetsbaarheid is cruciaal om de integriteit en veiligheid van de applicatie te waarborgen en potentiële schade te voorkomen.

### Bewijs

Het bewijs voor deze kwetsbaarheid is gedemonstreerd door het tonen van de huidige wachtwoorden van de gebruikers.

## Index

[Create New](#)

Username	Password	Role	
test	test	admin	<a href="#">Edit</a>   <a href="#">Details</a>   <a href="#">Delete</a>
user	user	user	<a href="#">Edit</a>   <a href="#">Details</a>   <a href="#">Delete</a>
admin	admin	admin	<a href="#">Edit</a>   <a href="#">Details</a>   <a href="#">Delete</a>

## Geen access control

Medium

### Beschrijving

De geïdentificeerde kwetsbaarheid in de applicatie betreft het ontbreken van een goede toegangscontrole, waardoor ongeautoriseerde gebruikers eenvoudig toegang kunnen krijgen tot gevoelige informatie. Specifiek kunnen kwaadwillende actoren zonder enige beperking naar de '/admin'-pagina navigeren, waar ze vrijelijk toegang hebben tot de lijst van accounts, inclusief hun bijbehorende wachtwoorden.

### Risico

De afwezigheid van access control in de applicatie vormt een aanzienlijk risico voor de vertrouwelijkheid en integriteit van gebruikersgegevens. De potentiële gevolgen zijn onder meer:

1. Ongeautoriseerde toegang tot gebruikersaccounts: Aanvallers kunnen zonder belemmeringen toegang krijgen tot de admin-pagina en alle gebruikersaccounts, inclusief de bijbehorende wachtwoorden, inzien.
2. Potentiële misbruik van gebruikersgegevens: Met toegang tot wachtwoorden kunnen kwaadwillende actoren de accounts van gebruikers compromitteren, wat kan leiden tot ongeautoriseerde acties namens de gebruikers.
3. Mogelijke schade aan de integriteit van gebruikersgegevens: De kwetsbaarheid kan resulteren in ongeoorloofde wijzigingen in accountinstellingen, met mogelijke negatieve gevolgen voor de gebruikers.

### Aanbevelingen

Om dit risico te adresseren, worden de volgende maatregelen ten eerste aanbevolen:

1. Implementeer sterke access control: Stel strikte toegangscontrolemechanismen in om ervoor te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot gevoelige delen van de applicatie, zoals de admin-pagina.
2. Autoriseer alleen noodzakelijke functionaliteiten: Beperk de rechten van gebruikers tot alleen die functies die essentieel zijn voor hun taken, om het risico van ongeoorloofde toegang te minimaliseren.
3. Voer regelmatige security audits uit: Periodieke beveiligingsaudits helpen bij het identificeren en adresseren van kwetsbaarheden, waaronder problemen met access control.
4. Implementeer sterke authenticatie: Versterk authenticatiemechanismen om ongeautoriseerde toegang verder te beperken, bijvoorbeeld door middel van tweefactorauthenticatie.
5. Hanteer het 'Principle of Least Privilege': Geef gebruikers en processen alleen de minimale toegangsrechten die noodzakelijk zijn om hun taken uit te voeren.

Het onmiddellijk aanpakken van deze password-kwetsbaarheid is cruciaal om de integriteit en veiligheid van de applicatie te waarborgen en potentiële schade te voorkomen.

### Bewijs

Het bewijs voor het ontbreken van access control is aangetoond door de eenvoudige mogelijkheid voor een aanvaller om zonder beperkingen naar de '/admin'-pagina te navigeren en toegang te verkrijgen tot accounts met hun wachtwoorden, zonder ingelogd te zijn.

# Index

[Create New](#)

Username	Password	Role	
test	test	admin	<a href="#">Edit</a>   <a href="#">Details</a>   <a href="#">Delete</a>
user	user	user	<a href="#">Edit</a>   <a href="#">Details</a>   <a href="#">Delete</a>
admin	admin	admin	<a href="#">Edit</a>   <a href="#">Details</a>   <a href="#">Delete</a>

## Cross-site scripting / XSS

Hoog

### Beschrijving

In de recent ontdekte kwetsbaarheid binnen de applicatie, met betrekking tot Cross-site Scripting (XSS), wordt de veiligheid en integriteit van het systeem ernstig bedreigd. Deze specifieke zwakte stelt kwaadwillende actoren in staat om schadelijke scripts in te voegen via het contactformulier van de website. Door het gebrek aan afdoende controle op gebruikersinvoer kunnen deze scripts vervolgens worden uitgevoerd in de browsers van andere gebruikers die de geïnfecteerde pagina bezoeken.

De aanvaller kan eenvoudig kwaadaardige code, zoals JavaScript, invoegen in velden van het contactformulier. Wanneer andere gebruikers deze pagina openen, wordt de ingevoegde code uitgevoerd in de context van hun browser, wat kan leiden tot diverse aanvallen, zoals het stelen van sessiegegevens, het wijzigen van gebruikersinstellingen, of het omleiden naar schadelijke websites.

Deze kwetsbaarheid is verder versterkt door het ontbreken van een goed inputvalidatiebeleid binnen de website, waardoor kwaadwillende actoren vrijelijk schadelijke scripts kunnen injecteren en zo de beveiligingsmaatregelen omzeilen.

### Risico

De geïdentificeerde XSS-kwetsbaarheid in de applicatie vormt een aanzienlijk risico voor de veiligheid en integriteit van het systeem. De mogelijkheid voor aanvallers om Javascript uit te voeren in het contact forum, opent de deur naar diverse potentiële bedreigingen en heeft aanzienlijke gevolgen:

1. Ongeautoriseerde acties namens gebruikers: Kwaadaardige scripts kunnen worden gebruikt om acties namens de gebruiker uit te voeren zonder hun medeweten. Dit omvat het uitvoeren van transacties, het wijzigen van gegevens of het uitvoeren van acties op platforms waar de gebruiker is ingelogd.
2. Diefstal van gebruikersgegevens: Aanvallers kunnen gebruikmaken van de XSS-kwetsbaarheid om gevoelige informatie zoals sessiecookies of andere gebruikersgegevens te stelen, waardoor ze mogelijk toegang krijgen tot accounts van slachtoffers.
3. Phishing en sociale ingenieurskunst: Door het injecteren van valse login-formulieren of waarschuwingmeldingen kunnen aanvallers proberen gebruikers te misleiden en hun inloggegevens te ontfutselen.
4. Schadelijke redirections: XSS maakt het mogelijk om gebruikers door te sturen naar schadelijke websites, waardoor ze mogelijk slachtoffer worden van verdere aanvallen of malware-infecties.

### Aanbevelingen

Om dit risico te mitigeren, wordt sterk aanbevolen om onmiddellijk de nodige maatregelen te nemen:

1. Inputvalidatie en sanitization: Implementeer strikte inputvalidatie en sanering van gebruikersinvoer, vooral in velden van het contactformulier. Dit voorkomt dat kwaadaardige scripts worden uitgevoerd.
2. Content Security Policy (CSP): Implementeer een Content Security Policy om de uitvoering van externe scripts te beperken en verdachte bronnen te blokkeren.
3. Security headers: Configureer HTTP-beveiligingsheaders, zoals X-XSS-Protection, om extra

bescherming tegen XSS-aanvallen te bieden.

4. **Regelmatige security audits:** Voer regelmatig audits uit om mogelijke kwetsbaarheden te identificeren en te verhelpen, en zorg ervoor dat de website voldoet aan de nieuwste beveiligingsstandaarden.

Het onmiddellijk aanpakken van deze XSS-kwetsbaarheid is cruciaal om de integriteit en veiligheid van de applicatie te waarborgen en potentiële schade te voorkomen.

### Bewijs

Het bewijs voor deze kwetsbaarheid is gedemonstreerd door het invoegen van Javascript in het contact forum, wat simpel het domein van je applicatie print.

The screenshot shows a web application interface for a 'Contact form'. At the top, it says 'Please enter your name' above a text input field. The input field contains the payload: `<script>alert(document.domain)</script>`. Below the input field is a 'Message' section, also containing the same payload. A blue 'Submit' button is located at the bottom left. A dark grey alert box is displayed in the center of the screen, showing the IP address '10.0.2.100' with a globe icon and an 'OK' button. At the bottom of the form, a message states 'Your message was successfully send!' followed by labels for 'Name:' and 'Message:'.





## 4. Bijlage A: TESTCASES

Voor deze penetratietest zijn onderstaande testgevallen allemaal beoordeeld. Voor testgevallen die van toepassing zijn op de huidige scope geeft de kolom Status aan wie verantwoordelijk was voor de uitvoering.

Titel	Beschrijving	Status
Testen voor SQL injecties	Proberen om andere data uit de database te krijgen.	Getest door Siebe Gios
Testen voor login credentials.	Proberen inloggen in iemands account.	Getest door Siebe Gios
Testen voor command injection	Proberen systeem commando's uit te voeren.	Getest door Siebe Gios
Testen voor directory traversal	Proberen om naar bepaalde paden te gaan en verborgen data te tonen.	Getest door Siebe Gios
Testen voor information disclosure	Kijken of er data open staat die niet mag open staan.	Getest door Siebe Gios
Testen voor authenticatie en access control	Proberen om naar bepaalde paden te gaan en verborgen data te tonen, zonder me te authenticeren.	Getest door Siebe Gios
Testen voor debugger overflows	Proberen om gebruik te maken van de debugger overflows.	Getest door Siebe Gios

<b>Testen voor XSS</b>	<b>Proberen om Javascript code uit te voeren op de website.</b>	<b>Getest door Siebe Gios</b>
<b>Testen voor SSRF</b>	<b>Proberen server requests te laten maken op onbedoelde locatie.</b>	<b>Getest door Siebe Gios</b>

## 5. Bijlage B: Ernst classificatie

Ik maak gebruik van versie 3.1 van het Common Vulnerability Scoring System (CVSS) als een eerste scoresysteem voor de ernst van de pentestbevindingen. Het helpt ons de ernst van kwetsbaarheden te standaardiseren en onze klanten te helpen prioriteit te geven aan herstelinspanningen. We erkennen echter dat een CVSS-score op zichzelf geen directe indicator is van de impact van een kwetsbaarheid op de zakelijke context. Daarom doen we voor elke bevinding handmatig evalueer de CVSS-ranglijst opnieuw en pas deze indien nodig aan zodat deze past bij de context van de huidige penetratietest. Hierdoor kunnen we een nauwkeurigere en relevantere beoordeling geven van de risico's die samenhangen met de kwetsbaarheden die we identificeren.

Voor alle niet-informatieve bevindingen geven we de CVSS-vector aan het begin van de beschrijving. Wanneer er meerdere aanvalsvectoren mogelijk zijn, houden we rekening met de zwaarste.

Meer informatie over CVSS in volgende hyperlinks:

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

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

### 5.1. Kritiek

#### Karakteristieken

- **Geen uitgebreide kennis vereist; het is gemakkelijk om de kwetsbaarheid te activeren.**
- **Tools en scripts die de kwetsbaarheid activeren zijn openbaar beschikbaar.**
- **Het beveiligingslek kan worden geactiveerd zonder handmatige interactie van de gebruiker.**
- **De kwetsbaarheid kan worden geactiveerd door een anonieme actor.**
- **De klant noemde de materialisatie van deze kwetsbaarheid als een “Doomsday Scenario”.**

Tenzij anders overeengekomen, worden bevindingen van deze categorie onmiddellijk gecommuniceerd naar de contactpersonen vermeld in het scopeformulier.



## 5.2. Hoog

### Karakteristieken

- **Geen uitgebreide kennis vereist; het is gemakkelijk om de kwetsbaarheid te activeren.**
- **Tools en scripts die de kwetsbaarheid activeren zijn openbaar beschikbaar.**
- **Het beveiligingslek kan worden geactiveerd zonder handmatige interactie van de gebruiker.**

## 5.3. Medium

### Karakteristieken

- **Alleen mogelijk als aan meerdere eisen wordt voldaan.**
- **Het is minder waarschijnlijk dat dit voorkomt vanwege de behoefte aan specifieke vaardigheden.**
- **Er is weinig of geen impact op het bedrijf.**
- **Kan niet worden geautomatiseerd.**

## 5.4. Laag

### Karakteristieken

- **De kwetsbaarheid is moeilijk te misbruiken (er is bijvoorbeeld een tegenstander voor nodig die aanzienlijke hoeveelheden netwerkverkeer versleuteld met dezelfde sleutel onderschept).**
- **Het is minder waarschijnlijk dat dit voorkomt vanwege de behoefte aan gespecialiseerde vaardigheden.**
- **Er is weinig of geen impact op het bedrijf.**
- **Kan alleen gebruikt worden in combinatie met andere kwetsbaarheden.**
- **Kan niet worden geautomatiseerd.**



## 5.5. Informatief

### Karakteristieken

**Bevindingen in deze categorie kunnen twee verschillende aard hebben.**

- 1. Ze brengen een puur theoretische kwetsbaarheid met zich mee**
- 2. Op het moment van testen en tijdens de testperiode waren we niet in staat voldoende informatie te verzamelen om de impact van deze bevinding te beoordelen. In dit geval zou een informatieve bevinding een effectieve CVSS-beoordeling kunnen hebben van ergens tussen 0 en 10.**

**We raden aan om alle bevindingen in deze categorie te evalueren om te bepalen of ze opnieuw moeten worden geëvalueerd.**

**Als de bevinding een puur theoretische kwetsbaarheid met zich meebrengt, is er geen sprake van**

- Geen realistische impact op de vertrouwelijkheid, integriteit of beschikbaarheid**
- OF**
- een waarschijnlijkheid van (bijna) nul dat dit zal gebeuren**

## 6. Vertrouwelijkheid en aansprakelijkheid

Dit document bevat informatie die vertrouwelijk is voor de klant, Thomas More en eventueel derde partijen die officieel betrokken zijn bij de projecten waarover dit document rapporteert. De informatie in dit document is Het is uitdrukkelijk verboden deze aan andere partijen bekend te maken, tenzij hiervoor schriftelijke toestemming van Thomas More is verkregen. Het document wordt strikt vertrouwelijk aan de ontvanger verstrekt en mag uitsluitend voor interne doeleinden worden gebruikt doeleinden van de ontvanger. Het verkopen, kopiëren, reproduceren en/of verspreiden van dit rapport op welke andere manier dan ook aan derden, geheel of gedeeltelijk, in welke kwestie of vorm dan ook, is verboden zonder voorafgaande schriftelijke toestemming van Torean.

Thomas More heeft er alles aan gedaan om ervoor te zorgen dat de informatie in dit rapport accuraat is. De informatie kan echter gebaseerd zijn op gegevens van derden en/of hun softwareproducten en als zodanig is Thomas More niet aansprakelijk voor eventuele problemen die kunnen optreden als gevolg van eventuele onjuistheden in dit document. Bovendien spoort het tijdgebonden karakter van een penetratietest onze onderzoekers aan om zoveel mogelijk te vinden in de tijd die ze hebben. Dit leidt er onvermijdelijk toe dat een penetratietest niet uitputtend is met betrekking tot alle mogelijke problemen die zich in het te testen IT-systeem kunnen voordoen.