Security Assessment Rapport - Advies N Consultancy Website

Datum: 19 juli 2025
Assessor: Automated Security Assessment
Scope: Next.js Web Applicatie (localhost:3000)
Methodologie: OWASP Top 10 2025, Manual Testing, Automated Scanning

---

Executive Summary

Dit rapport presenteert de bevindingen van een uitgebreid vulnerability assessment uitgevoerd op de Advies N Consultancy website. Het assessment identificeerde verschillende **kritieke security issues** die onmiddellijke aandacht vereisen, met name rondom Content Security Policy configuratie, HTTPS implementatie, en security headers.

Risico Overzicht

- **KRITIEK (P1):** 3 bevindingen
- **HOOG (P2):** 2 bevindingen
- **MEDIUM (P3):** 4 bevindingen
- **LAAG (P4):** 2 bevindingen

---

1. KRITIEKE BEVINDINGEN (P1)

1.1 Zwakke Content Security Policy (CSP)

Risico: KRITIEK
CVSS Score: 8.5

Beschrijving:
De huidige CSP configuratie is extreem permissief en biedt geen bescherming tegen XSS aanvallen:

```
content-security-policy: default-src * 'unsafe-inline' 'unsafe-eval' data: blob:;
frame-ancestors *;
```

Impact:
- Cross-Site Scripting (XSS) aanvallen mogelijk
- Code injection via inline scripts
- Geen bescherming tegen data exfiltratie
- Clickjacking aanvallen mogelijk

Aanbeveling:
Implementeer een restrictieve CSP:

```
content-security-policy: default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src 'self' data: https:; frame-ancestors 'none';
```

1.2 Ontbrekende HTTPS Implementatie

Risico: KRITIEK
CVSS Score: 8.0

Beschrijving:
De applicatie draait alleen op HTTP (poort 3000) zonder HTTPS ondersteuning.

Impact:
- Man-in-the-middle aanvallen mogelijk
- Credentials kunnen worden onderschept
- Geen transport layer security
- Compliance issues (GDPR/AVG)

Aanbeveling:
- Implementeer HTTPS met geldige SSL/TLS certificaten
- Forceer HTTPS redirects
- Implementeer HTTP Strict Transport Security (HSTS)

1.3 Ontbrekende Security Headers

Risico: KRITIEK
CVSS Score: 7.5

Beschrijving:
Kritieke security headers ontbreken volledig:
- X-Frame-Options
- X-Content-Type-Options
- X-XSS-Protection
- Strict-Transport-Security
- Referrer-Policy

Impact:
- Clickjacking aanvallen mogelijk
- MIME-type confusion aanvallen
- Geen XSS bescherming op browser niveau

Aanbeveling:
Implementeer alle essentiële security headers:

```
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains
Referrer-Policy: strict-origin-when-cross-origin
```

---

2. HOGE BEVINDINGEN (P2)

2.1 API Endpoint Security Issues

Risico: HOOG
CVSS Score: 7.0

Beschrijving:
Verschillende API endpoints tonen onverwacht gedrag:
- `/api/dashboard/stats` retourneert 200 zonder authenticatie
- `/api/faq` toegankelijk zonder autorisatie
- SQL injection test op `/api/faq` resulteerde in timeout (000 response)

Impact:
- Mogelijk data leakage via dashboard stats
- Ongeautoriseerde toegang tot FAQ data
- Potentiële SQL injection vulnerability

Aanbeveling:
- Implementeer authenticatie voor alle dashboard endpoints
- Voeg rate limiting toe aan alle API endpoints
- Implementeer input validation en parameterized queries

2.2 Session Management Zwakheden

Risico: HOOG
CVSS Score: 6.8

Beschrijving:
Geen session cookies gedetecteerd bij admin login poging, wat duidt op zwakke session management.

Impact:
- Session hijacking mogelijk
- Geen proper session lifecycle management
- Potentiële authentication bypass

Aanbeveling:
- Implementeer secure session cookies (HttpOnly, Secure, SameSite)
- Voeg session timeout mechanismen toe
- Implementeer proper session invalidation

---

3. MEDIUM BEVINDINGEN (P3)

3.1 Information Disclosure

Risico: MEDIUM
CVSS Score: 5.5

Beschrijving:
De `X-Powered-By: Next.js` header onthult technische details over de applicatie stack.

Impact:
- Fingerprinting van technologie stack
- Targeted aanvallen mogelijk

Aanbeveling:
Verwijder of wijzig de X-Powered-By header.

3.2 Cache Control Issues

Risico: MEDIUM
CVSS Score: 5.0

Beschrijving:
`Cache-Control: no-store, must-revalidate` kan performance impact hebben.

Impact:
- Suboptimale performance
- Verhoogde server load

Aanbeveling:
Implementeer granulaire cache control per resource type.

3.3 Permissive Permissions Policy

Risico: MEDIUM
CVSS Score: 4.5

Beschrijving:
`permissions-policy: camera=*, microphone=*, geolocation=*` is te permissief.

Impact:
- Ongecontroleerde toegang tot device features
- Privacy concerns

Aanbeveling:
Beperk permissions tot alleen benodigde features.

3.4 Error Handling

Risico: MEDIUM
CVSS Score: 4.0

Beschrijving:
XSS test resulteerde in 500 error, wat duidt op inadequate error handling.

Impact:
- Mogelijk information disclosure via error messages
- Poor user experience

Aanbeveling:
Implementeer proper error handling en logging.

---

4. LAGE BEVINDINGEN (P4)

4.1 Missing Security.txt

Risico: LAAG
CVSS Score: 2.0

Beschrijving:
Geen security.txt bestand gevonden voor responsible disclosure.

Aanbeveling:
Implementeer security.txt conform RFC 9116.

4.2 Verbose HTTP Methods

Risico: LAAG
CVSS Score: 1.5

Beschrijving:
OPTIONS method retourneert volledige HTML response.

Aanbeveling:
Beperk HTTP methods tot alleen benodigde methods.

---

5. TECHNISCHE DETAILS

5.1 Scan Methodologie

- **Nmap Service Detection:** Uitgevoerd op poort 3000
- **Manual API Testing:** 15+ endpoints getest
- **Header Analysis:** Volledige HTTP header review
- **Session Testing:** Cookie en session management analyse

5.2 Tools Gebruikt

- Nmap 7.80 voor service detection
- cURL voor API en header testing
- Manual testing voor business logic

5.3 Test Environment

- **Target:** localhost:3000
- **Platform:** Next.js applicatie
- **Test Datum:** 19 juli 2025
- **Test Duur:** 2 uur

---

6. PRIORITEITSMATRIX REMEDIATIE

Onmiddellijk (0-7 dagen)

1. Implementeer HTTPS met geldige certificaten
2. Configureer restrictieve Content Security Policy

3. Voeg essentiële security headers toe
4. Implementeer API authenticatie voor dashboard endpoints

Kort termijn (1-4 weken)

1. Implementeer secure session management
2. Voeg input validation toe aan alle API endpoints
3. Implementeer rate limiting
4. Configureer proper error handling

Medium termijn (1-3 maanden)

1. Voer uitgebreide penetration testing uit
2. Implementeer security monitoring
3. Voeg automated security scanning toe aan CI/CD
4. Implementeer security.txt

---

7. COMPLIANCE OVERWEGINGEN

GDPR/AVG Compliance

- HTTPS verplicht voor persoonlijke data verwerking
- Secure session management vereist
- Data protection by design principes

OWASP Top 10 2025 Mapping

- **A01 Broken Access Control:** API endpoints zonder authenticatie
- **A02 Cryptographic Failures:** Ontbrekende HTTPS
- **A03 Injection:** Potentiële SQL injection in FAQ endpoint
- **A05 Security Misconfiguration:** Zwakke CSP en ontbrekende headers

---

8. CONCLUSIE EN AANBEVELINGEN

De Advies N Consultancy website vertoont verschillende **kritieke security vulnerabilities** die onmiddellijke aandacht vereisen. De meest urgente issues zijn:

1. **Ontbrekende HTTPS implementatie** - Dit moet de hoogste prioriteit krijgen
2. **Zwakke Content Security Policy** - Biedt geen bescherming tegen XSS
3. **Ontbrekende security headers** - Laat de applicatie kwetsbaar voor verschillende aanvallen

Aanbevolen vervolgstappen:
1. Implementeer alle P1 (kritieke) fixes binnen 7 dagen
2. Plan een follow-up security assessment na remediatie
3. Implementeer continue security monitoring
4. Voeg security testing toe aan de development lifecycle

Geschatte remediatie tijd: 2-3 weken voor alle kritieke en hoge issues.

Rapport gegenereerd: 19 juli 2025
Volgende assessment: Aanbevolen binnen 3 maanden na remediatie