>ForgeSec

ForgeSec

Demo BV

Pentest rapport

DEMO RAPPORT — Dit is een fictief demonstratierapport met fictieve gegevens.

Geheimhouding

Dit document is de exclusieve eigendom van ForgeSec en Demo BV. Dit document bevat vertrouwelijke gegevens. Dupliceren, heruitgeven of gebruik ervan dient voorafgegaan worden door toestemming van zowel ForgeSec als Demo BV.

Demo BV mag dit document gebruiken voor audits.

Verantwoordelijkheid

Een penetratietest van een webapplicatie wordt beschouwd als een momentopname. De bevindingen en aanbevelingen weerspiegelen de informatie die tijdens de test is verzameld, en houden geen rekening met wijzigingen of aanpassingen buiten die periode.

Tijdgebonden testing laten geen volledige evaluatie van alle beveiligingsmaatregelen toe. ForgeSec heeft de test daarom gericht op het identificeren van de zwakste beveiligingsmaatregelen die een aanvaller zou kunnen misbruiken. ForgeSec raadt aan om dergelijke onderzoeken jaarlijks uit te voeren, door interne of externe partijen, om het blijvende succes van de maatregelen te waarborgen.

Contactinformatie

Naam	Rol	Contact
Jan Janssen	CTO Demo BV	jan@demo-bv.be
Kevin	Tester ForgeSec	kevin@forgesec.be

Beoordelingsoverzicht

Op 10 februari 2026 heeft Demo BV ForgeSec ingeschakeld om de beveiliging van de infrastructuur te evalueren in vergelijking met de huidige best practices in de sector, waaronder een webapplicatiepenetratietest. Alle uitgevoerde testen zijn gebaseerd op de industrienormen.

De fasen van penetratietestactiviteiten omvatten het volgende:

- **Ontdekken** — Scannen en enumeratie uitvoeren om potentiële kwetsbaarheden, zwakke plekken en exploits te identificeren.
- **Aanvallen** — Potentiële kwetsbaarheden bevestigen door middel van exploitatie en aanvullende ontdekking uitvoeren bij nieuwe toegang.
- **Rapportage** — Alle gevonden kwetsbaarheden en exploits documenteren, samen met mislukte pogingen en de sterke en zwakke punten van het bedrijf.

Definitie

Een penetratietest van een webapplicatie is een diepgaande penetratietest. Er wordt getest op potentiële kwetsbaarheden op basis van de beveiligingsrichtlijnen beschreven in de OWASP Top 10.

De activiteiten omvatten onder meer:

- Het in kaart brengen van de website.
- Directory-enumeratie.
- Geautomatiseerde en handmatige injecties.
- Wachtwoordaanvallen.
- Het manipuleren van requests.
- Overige testen afhankelijk van de specifieke inhoud van de site.

CVSS

De onderstaande tabel definieert de verschillende niveaus van impact in de corresponderende CVSS-score. Deze tabel moet worden gebruikt om prioriteiten te stellen om de kwetsbaarheden te mitigeren.

Impact	CVSS V3 score	Definitie
Critical	9.0 — 10.0	Het uitbuiten is eenvoudig en resulteert in het volledige compromitteren van het systeem.
High	7.0 — 8.9	Uitbuiting is moeilijker, maar kan leiden tot verticaal compromitteren.
Moderate	4.0 — 6.9	Kwetsbaarheden bestaan, maar kunnen niet worden uitgebuit. Extra stappen zoals social engineering zijn noodzakelijk.
Low	0.1 — 3.9	Kwetsbaarheden kunnen niet worden uitgebuit, maar ze vergroten de aanvalsvectoren.
Informational	N/A	Louter informatief. Zaken die zijn opgevallen tijdens het testen.

Risico

Het risico wordt berekend aan de hand van 2 factoren: waarschijnlijkheid en impact.

Waarschijnlijkheid
Dit meet de kans dat een zwakheid effectief wordt uitgebuit. De score wordt gegeven op basis van complexiteit, de gebruikte tools, de vaardigheden van de aanvaller en de omgeving van de klant.

Impact
Deze parameter meet welke nadelige effecten de zwakheid heeft op het normale verloop van de werking van de client. Dit is inclusief het waarborgen van de CIA-triad.

Scope

Type	Details
Webapplicatie penetratietest	https://app.demo-bv.be

Uitsluitingen van de scope

Er zijn geen specifieke uitsluitingen gedefinieerd door de klant. ForgeSec verbindt zich ertoe volgende activiteiten niet uit te voeren:

- DDoS
- Social engineering

Daarnaast zal ForgeSec alle testactiviteiten onmiddellijk stopzetten als er vertrouwelijke informatie wordt aangetroffen. De voortzetting van de test zal uitsluitend plaatsvinden na overleg met de klant.

Managementsamenvatting

Penetratietest

ForgeSec evalueerde de security van Demo BV door middel van een webapplicatie penetratietest op 10 februari 2026. De volgende tekst geeft in hoofdlijnen weer welke zaken werden ontdekt. Daarnaast wordt een overzicht gegeven met de zwaktes en sterktes van de website.

ForgeSec heeft geen DDoS-aanval uitgevoerd en geen gebruik gemaakt van social engineering technieken.

De test omvatte zowel manuele als geautomatiseerde tests. Steeds uitgevoerd volgens de standaarden van de industrie om schade aan de infrastructuur te vermijden.

ForgeSec heeft vastgesteld dat de webapplicatie kwetsbaar is voor Broken Access Control, waardoor het mogelijk was om klantengegevens op te halen zonder authenticatie. Na de ontdekking van klantengegevens is ForgeSec gestopt met verdere exploitatie tot dit in detail besproken is met Demo BV.

Aanbevelingen

ForgeSec raadt aan om de toegangscontrole op API-endpoints grondig te herzien, zodat ongeauthenticeerde gebruikers geen klantengegevens kunnen opvragen. Daarnaast is het belangrijk om rate limiting te implementeren op het inlogmechanisme van het administrator-gedeelte van de website. Als laatste wordt aanbevolen om gevoelige informatie zoals server headers en versienummers te verbergen voor eindgebruikers.

Kernsterktes en -zwaktes

Sterktes	Zwaktes
HTTPS correct geconfigureerd	Broken Access Control op API
Moderne security headers aanwezig	Geen rate limiting op login
WAF actief	Klantenbestand zichtbaar zonder auth
Cookie flags correct ingesteld	Server versie-informatie zichtbaar

Samenvatting van de kwetsbaarheden

De volgende tabellen illustreren de gevonden kwetsbaarheden geordend volgens impact gevolgd door aanbevelingen.

Critical	High	Moderate	Low	Informational
1	0	1	2	0

Bevinding	Impact	Aanbeveling
WAPT-001: Broken Access Control / BOLA	Critical	Implementeer autorisatiecontroles op alle API-endpoints. Valideer dat de ingelogde gebruiker toegang heeft tot het opgevraagde object.
WAPT-002: Brute Forcing — Admin Login	Moderate	Implementeer rate limiting en account lockout op het login-mechanisme. Overweeg multi-factor authenticatie.
WAPT-003: Information Disclosure — Server Headers	Low	Verberg server versie-informatie in HTTP-response headers.
WAPT-004: Information Disclosure — Directory Listing	Low	Schakel directory listing uit op de webserver en zorg dat gevoelige paden niet bereikbaar zijn.

Technische samenvatting

WAPT-001: Broken Access Control / BOLA

Omschrijving:	De API-endpoint `/api/v1/customers/{id}` controleert niet of de ingelogde gebruiker geautoriseerd is om de gegevens van de opgegeven klant op te vragen. Door het aanpassen van de ID-parameter in de URL kan een aanvaller de gegevens van willekeurige klanten ophalen, inclusief naam, adres, e-mailadres en telefoonnummer.
Risico:	Waarschijnlijkheid — **HIGH** — Deze aanval is uitgebreid beschreven en is uitvoerbaar door iedere bezoeker van de website. Impact — **HIGH** — Het klantenbestand kan zo volledig achterhaald worden.
PoC:	Navigeer naar `https://app.demo-bv.be/api/v1/customers/1`. Pas vervolgens de ID-parameter aan (bijv. 2, 3, 4, ...) om de gegevens van andere klanten op te halen. Gebruik BurpSuite Intruder om het volledige bereik te enumereren.
Gebruikte tools:	Browser naar keuze. BurpSuite Professional — Intruder
Referentie:	OWASP Top 10:2021 — A01:2021 Broken Access Control
Bewijs:	*[Screenshot: BurpSuite Intruder response met klantengegevens — verwijderd voor demo]*
Mitigatie:	Implementeer autorisatiecontroles op alle API-endpoints. Valideer server-side dat de ingelogde gebruiker daadwerkelijk toegang heeft tot het opgevraagde object. Gebruik een indirect object reference mapping in plaats van directe database-ID's in de URL.

WAPT-002: Brute Forcing — Admin Login

Omschrijving:	Het administrator login-paneel op `/admin/login` heeft geen rate limiting of account lockout-mechanisme. Een aanvaller kan onbeperkt inlogpogingen uitvoeren zonder geblokkeerd te worden, wat brute force aanvallen op wachtwoorden mogelijk maakt.
Risico:	Waarschijnlijkheid — **MODERATE** — Deze aanval is redelijk gemakkelijk met de gebruikelijke tools. Het admin-paneel is publiek bereikbaar. Impact — **HIGH** — Wanneer het administrator-gedeelte wordt gecompromitteerd, kan dit leiden tot onoverzichtelijke schade aan de applicatie en bijbehorende data.
PoC:	Stuur herhaalde POST-requests naar `/admin/login` met verschillende wachtwoorden via BurpSuite Intruder. Na 500+ pogingen binnen 1 minuut werd geen enkele beperking geactiveerd.
Gebruikte tools:	BurpSuite Professional — Intruder
Referentie:	OWASP Top 10:2021 — A07:2021 Identification and Authentication Failures
Bewijs:	*[Screenshot: BurpSuite Intruder resultaten zonder rate limiting — verwijderd voor demo]*
Mitigatie:	Implementeer rate limiting op het login-mechanisme (bijv. maximaal 5 pogingen per minuut per IP-adres). Overweeg account lockout na een vastgesteld aantal mislukte pogingen. Multi-factor authenticatie wordt sterk aanbevolen voor administrator-accounts.

WAPT-003: Information Disclosure — Server Headers

Omschrijving:	Information disclosure gebeurt wanneer de applicatie ongewild achterliggende informatie geeft over de gebruikte technologie. De HTTP-response headers bevatten de exacte versie van de webserver en het gebruikte framework. Dit kan gebruikt worden door aanvallers om hun aanvalsvectoren uit te zetten.
Risico:	Waarschijnlijkheid — **MODERATE** — Bij het onderzoeken van de website kan een aanvaller toevallig op deze informatie stuiten en gebruiken voor gerichte aanvallen. Impact — **LOW** — Afhankelijk van welke software gebruikt wordt, kan dit worden misbruikt, maar er is nooit een zekerheid of de software beveiligingsfouten heeft.
PoC:	Inspecteer de HTTP-response headers bij elke request naar de applicatie. De `Server` en `X-Powered-By` headers bevatten versie-informatie.
Gebruikte tools:	Browser naar keuze — Developer Tools (Network tab)
Referentie:	OWASP Top 10:2021 — A05:2021 Security Misconfiguration
Bewijs:	*[Screenshot: Response headers met versie-informatie — verwijderd voor demo]*
Mitigatie:	Verberg of verwijder de `Server` en `X-Powered-By` headers uit de HTTP-responses. Configureer de webserver om geen versie-informatie prijs te geven.

WAPT-004: Information Disclosure — Directory Listing

Omschrijving:	Information disclosure gebeurt wanneer de applicatie ongewild achterliggende informatie geeft over de gebruikte technologie. Op bepaalde paden is directory listing ingeschakeld, waardoor de inhoud van mappen op de server zichtbaar is voor bezoekers.
Risico:	Waarschijnlijkheid — **LOW** — Een aanvaller moet actief zoeken naar deze paden. De kans is klein maar niet verwaarloosbaar bij gerichte aanvallen. Impact — **LOW** — De zichtbare bestanden bevatten geen directe gevoelige informatie, maar vergroten de aanvalsvectoren door inzicht in de applicatiestructuur.
PoC:	Navigeer naar `https://app.demo-bv.be/assets/` en `https://app.demo-bv.be/uploads/` om de directory listing te zien.
Gebruikte tools:	BurpSuite Professional — Spider/Crawler
Referentie:	OWASP Top 10:2021 — A05:2021 Security Misconfiguration
Bewijs:	*[Screenshot: Directory listing met bestandenlijst — verwijderd voor demo]*
Mitigatie:	Schakel directory listing uit op de webserver. Zorg ervoor dat paden die gevoelige informatie bevatten niet bereikbaar zijn voor de gebruiker. Voeg een standaard `index.html` toe of configureer de webserver om een 403 Forbidden te retourneren.

>ForgeSec

DEMO RAPPORT — Dit is een fictief demonstratierapport.