HackIndex

PENTESTRAPPORT, VOORBEELD

Klantportaal

Groothandel Voorbeeld B.V.

Fictief voorbeeld. De klant, de applicatie en de bevindingen zijn verzonnen. Echte rapporten blijven vertrouwelijk.

OPDRACHT	HI-OP-2026-DEMO
VERSIE	2.0, na de hertest
DATUM	21 april 2026
TESTPERIODE	3 tot en met 7 maart 2026
RUBRICERING	Vertrouwelijk

Documentbeheer

VERSIE	DATUM	WAT ER VERANDERD IS
1.0	12 maart 2026	Rapport na de test
2.0	21 april 2026	Bijgewerkt na de hertest

Contact

PENTESTER	Joshua van der Poll, HackIndex
E-MAIL	info@hackindex.nl
PGP-SLEUTEL	`hackindex.nl/pgp.txt`
CONTACT BIJ DE KLANT	Sanne de Boer, IT-manager

Vertrouwelijkheid

Dit rapport is vertrouwelijk. Het beschrijft zwakke plekken in het klantportaal en is daarmee zelf gevoelig. HackIndex deelt het alleen versleuteld.

Je mag het rapport delen met wie het nodig heeft om de bevindingen op te lossen of te beoordelen: je eigen team, de leverancier die de fixes maakt, je accountant, auditor of toezichthouder.

Een pentest is een momentopname. Dit rapport beschrijft wat HackIndex vond in de versie en de periode op het voorblad, binnen de afgesproken scope.

Samenvatting

VOOR WIE BESLIST

HackIndex heeft van 3 tot en met 7 maart 2026 de webapplicatie en de API van het klantportaal getest, grey box, met 3 rollen. Getest is versie 3.7.2 op de testomgeving.

OORDEEL

De basis is goed, maar medewerkers van de ene klant konden facturen van een andere klant openen. Dat is na de hertest opgelost.

0	1	2	3	2	4
KRITIEK	HOOG	MIDDEL	LAAG	INFORMATIEF	GOED

Wat eerst moet

- Medewerkers van de ene klant kunnen facturen van een andere klant openen, met namen, adressen en bedragen. (01)
- Een sessie blijft geldig na uitloggen. Wie een oude sessie in handen krijgt, kan daarmee verder. (02)
- Het inlogformulier heeft geen limiet op pogingen, zodat wachtwoorden onbeperkt geraden kunnen worden. (03)

Wat goed is

- Rechten tussen de rollen zijn goed afgeschermd: een medewerker komt niet bij beheerfuncties.
- Invoer wordt overal gecontroleerd, ook in de API. Geen injectie gevonden.
- Beheerders loggen in met een tweede stap.

Na de hertest

Na de hertest op 21 april 2026 zijn de hoge en beide middelhoge bevindingen opgelost. De drie lage bevindingen zijn bewust als risico geaccepteerd.

Overzicht van bevindingen

Alle bevindingen, de ernstigste eerst. Het ID gebruik je in mail, tickets en de hertest.

ID	BEVINDING	ERNST	MOEITE	STATUS
HI-OP-2026-DEMO-01	Facturen van andere klanten zijn op te vragen	HOOG	makkelijk	OPGELOST
HI-OP-2026-DEMO-02	Sessie blijft geldig na uitloggen	MIDDEL	makkelijk	OPGELOST
HI-OP-2026-DEMO-03	Geen limiet op inlogpogingen	MIDDEL	makkelijk	OPGELOST
HI-OP-2026-DEMO-04	Foutmelding noemt de versie van het framework	LAAG	makkelijk	RISICO GEACCEPTEERD
HI-OP-2026-DEMO-05	Portaal kan in een andere site worden geladen	LAAG	makkelijk	RISICO GEACCEPTEERD
HI-OP-2026-DEMO-06	Export opent formules in Excel	LAAG	gemiddeld	RISICO GEACCEPTEERD

Scope en aanpak

Wat getest is

ONDERDEEL	ADRES	OMGEVING	VERSIE OF BUILD
Webapplicatie	`https://portaal.groothandel.example`	Test	`3.7.2, commit 4f2a9c1`
API	`https://portaal.groothandel.example/api/v2`	Test	`3.7.2, commit 4f2a9c1`

Hoe

AANPAK	Grey box: met accounts per rol, zonder broncode.
TESTDAGEN	3 tot en met 7 maart 2026, 5 dagen
GETEST VANAF	`203.0.113.24`
STANDAARDEN	OWASP WSTG 4.2, OWASP ASVS 5.0 niveau 2
ERNST	CVSS 4.0 en 3.1, zie de bijlage

Testaccounts

ROL	ACCOUNT	OPMERKING
Medewerker van een klant	`medewerker-a@klant-a.example`	Twee klanten, om tussen klanten te testen
Beheerder van een klant	`beheer-a@klant-a.example`	Beheert de medewerkers van klant A
Beheerder groothandel	`test-beheer@groothandel.example`	Met tweede stap bij inloggen

Afscherming van het doel

BEREIKBAAR VANAF INTERNET	Ja
IP-WHITELIST	Nee
WAF OF FIREWALL	Nee
TEST-IP OP DE WHITELIST	Niet nodig

Wat niet getest is

Wat buiten de test viel, en waarom. Zo is duidelijk waar de grenzen liggen.

- Overbelasting (DoS): uitgesloten in de spelregels.
- Betalingen: verlopen via een externe betaalprovider, geen toestemming om die te testen.
- De koppeling met het ERP-systeem: niet aanwezig in de testomgeving.

Op te ruimen

Tijdens de test zijn deze gegevens aangemaakt. De klant heeft ze verwijderd, HackIndex heeft gecontroleerd dat dat gelukt is.

WAT	WAAR	OPGERUIMD
Vijf testaccounts	`Zie Testaccounts`	Ja, 12 maart 2026
Twee testbestellingen	`/bestellingen, klant A`	Ja, 12 maart 2026

Bevindingen

Gesorteerd op ernst. Elke bevinding heeft dezelfde opbouw: eerst het verhaal in het kort, dan de details om het na te doen en op te lossen.

HI-OP-2026-DEMO-01 Facturen van andere klanten zijn op te vragen

HOOG OPGELOST MOEITE: MAKKELIJK

In het kort

Een ingelogde medewerker kan facturen van andere klanten openen door het factuurnummer in het adres te veranderen. Daarmee liggen namen, adressen en bedragen van alle klanten open.

CVSS 4.0	7.1 CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CVSS 3.1	6.5 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
WAAR	GET /api/v2/facturen/{nummer}
VOORWAARDEN	Ingelogd als medewerker van een klant. Geen andere rechten nodig.
AL AANWEZIG	Inloggen is verplicht, maar de API controleert niet bij welke klant een factuur hoort.
CATEGORIE	OWASP Top 10 2025 A01, CWE-639, ASVS 5.0 V8

Wat er mis is

Het portaal toont in de lijst alleen de eigen facturen. De API die een losse factuur ophaalt, controleert alleen of iemand is ingelogd, niet of de factuur bij de organisatie van die gebruiker hoort. Factuurnummers lopen op, dus ze zijn makkelijk te raden.

Stappen om het na te doen

1. Log in als medewerker van klant A en open een eigen factuur.
2. Verander het factuurnummer in het verzoek in een nummer van klant B.
3. De factuur van klant B wordt getoond.

Bewijs

Een medewerker van klant A haalt factuur 10482 op, die van klant B is.

REQUEST

```
GET /api/v2/facturen/10482 HTTP/2
Host: portaal.groothandel.example
Cookie: session=[afgeschermd, klant A]
```

RESPONSE

```
HTTP/2 200
Content-Type: application/json

{"nummer":10482,"klant":"[klant B]","totaal":"1.250,00"}
```

Impact

Iedere medewerker van iedere klant kan de facturen van alle andere klanten inzien, met namen, adressen, bestellingen en bedragen. Dat kan een datalek zijn dat je moet melden.

Oplossing

KORTE TERMIJN

Haal de factuur op via de organisatie van de ingelogde gebruiker, zodat een factuur van een andere klant niet gevonden wordt.

```
- $factuur = Factuur::findOrFail($nummer);
+ $factuur = $request→user()→organisatie→facturen()→findOrFail($nummer);
```

LANGE TERMIJN

Leg per model vast wie het mag zien, in een policy, en test per route dat een andere klant een 404 krijgt. Zo komt deze fout niet terug bij nieuwe routes.

Controleer de fix

Stap 3 geeft nu een 404.

Referenties

- CWE-639: Authorization Bypass Through User-Controlled Key
- OWASP ASVS 5.0, hoofdstuk V8 Authorization
- OWASP Cheat Sheet: Authorization

Hertest

HERTEST 21 APRIL 2026 OPGELOST

Opgelost in versie 3.8.0. Facturen van andere klanten geven een 404, ook via de export en de pdf-download. Ook geprobeerd met de beheerder van een klant: dezelfde uitkomst.

HI-OP-2026-DEMO-02 Sessie blijft geldig na uitloggen

MIDDEL OPGELOST MOEITE: MAKKELIJK

In het kort

Na uitloggen blijft de sessie op de server geldig. Wie een oude sessie in handen krijgt, bijvoorbeeld op een gedeelde computer, kan daarmee verder werken.

CVSS 4.0	6.3 CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N
CVSS 3.1	4.8 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
WAAR	POST /uitloggen
VOORWAARDEN	Een sessie van een andere gebruiker, bijvoorbeeld van een gedeelde computer.
AL AANWEZIG	Uitloggen verwijdert de cookie in de browser.
CATEGORIE	OWASP Top 10 2025 A07, CWE-613, ASVS 5.0 V7

Wat er mis is

Uitloggen verwijdert alleen de cookie in de browser. De sessie zelf blijft op de server bestaan tot hij na 30 dagen verloopt.

Stappen om het na te doen

1. Log in en bewaar de waarde van de sessiecookie.
2. Log uit.
3. Stuur een verzoek met de bewaarde cookie: je bent nog ingelogd.

Bewijs

Na uitloggen geeft een verzoek met de oude sessie nog steeds de eigen bestellingen terug.

Impact

Een sessie die is uitgelekt of op een gedeelde computer is achtergebleven, blijft tot 30 dagen bruikbaar, ook nadat de gebruiker dacht dat hij veilig was uitgelogd.

Oplossing

KORTE TERMIJN

Trek de sessie bij uitloggen ook op de server in.

LANGE TERMIJN

Verkort de levensduur van sessies tot een werkdag en geef gebruikers een knop om op alle apparaten uit te loggen.

Controleer de fix

Stap 3 stuurt nu door naar de inlogpagina.

Referenties

- CWE-613: Insufficient Session Expiration
- OWASP ASVS 5.0, hoofdstuk V7 Session Management
- OWASP Cheat Sheet: Session Management

Hertest

HERTEST 21 APRIL 2026 OPGELOST

Opgelost in versie 3.8.0. Na uitloggen is de oude sessie ongeldig. Sessies verlopen nu na 8 uur.

HI-OP-2026-DEMO-03 Geen limiet op inlogpogingen

MIDDEL OPGELOST MOEITE: MAKKELIJK

In het kort

Het inlogformulier accepteert onbeperkt pogingen. Een aanvaller kan zo zwakke wachtwoorden van medewerkers raden.

CVSS 4.0	6.3 CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N
CVSS 3.1	4.8 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
WAAR	POST /inloggen
VOORWAARDEN	Geen. Wel een bestaand e-mailadres en een zwak wachtwoord.
AL AANWEZIG	Wachtwoorden moeten minstens 10 tekens zijn.
CATEGORIE	OWASP Top 10 2025 A07, CWE-307, ASVS 5.0 V6

Wat er mis is

Na 200 foute pogingen op één account accepteerde het formulier nog steeds nieuwe pogingen, zonder vertraging of blokkade.

Stappen om het na te doen

1. Stuur 200 inlogpogingen met foute wachtwoorden voor één testaccount.
2. Elke poging krijgt dezelfde foutmelding, zonder vertraging.
3. Inloggen met het juiste wachtwoord lukt daarna gewoon.

Bewijs

200 pogingen in 40 seconden op een testaccount, allemaal beantwoord zonder blokkade.

Impact

Medewerkers met een zwak of uitgelekt wachtwoord zijn over te nemen. Medewerkers hebben geen tweede stap bij inloggen.

Oplossing

KORTE TERMIJN

Beperk het aantal pogingen per account en per IP-adres, bijvoorbeeld 5 per minuut, en vertraag daarna.

LANGE TERMIJN

Bied medewerkers een tweede stap bij inloggen aan, net als beheerders al hebben.

Controleer de fix

Na 5 foute pogingen geeft het formulier een melding dat je even moet wachten.

Referenties

- CWE-307: Improper Restriction of Excessive Authentication Attempts
- OWASP ASVS 5.0, hoofdstuk V6 Authentication
- OWASP Cheat Sheet: Authentication

Hertest

HERTEST 21 APRIL 2026 OPGELOST

Opgelost in versie 3.8.0. Na 5 foute pogingen per minuut volgt een wachttijd, per account en per IP-adres.

HI-OP-2026-DEMO-04 Foutmelding noemt de versie van het framework

LAAG RISICO GEACCEPTEERD MOEITE: MAKKELIJK

In het kort

Bij een fout in de API staat de versie van het framework in de melding. Dat helpt een aanvaller om bekende kwetsbaarheden in die versie te zoeken.

CVSS 4.0	2.3 CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSS 3.1	3.1 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N
WAAR	GET /api/v2/bestellingen?pagina=abc
VOORWAARDEN	Ingelogd als medewerker van een klant.
AL AANWEZIG	Geen.
CATEGORIE	OWASP Top 10 2025 A02, CWE-209, ASVS 5.0 V16

Wat er mis is

Een ongeldige waarde in een parameter geeft een foutpagina met de naam en de versie van het framework.

Stappen om het na te doen

1. Log in als medewerker.
2. Open de lijst met bestellingen met een letter als paginanummer.
3. De foutmelding noemt de versie van het framework.

Bewijs

De foutmelding bevat de naam en het versienummer van het framework.

Impact

Op zichzelf geen schade. Het maakt het wel makkelijker om gericht naar bekende fouten in die versie te zoeken.

Oplossing

`KORTE TERMIJN`

Toon in productie een algemene foutmelding en controleer de invoer van parameters.

`LANGE TERMIJN`

Zet foutdetails standaard uit buiten de ontwikkelomgeving.

Controleer de fix

Stap 3 geeft een algemene melding zonder versie.

Referenties

- CWE-209: Generation of Error Message Containing Sensitive Information
- OWASP ASVS 5.0, hoofdstuk V16 Security Logging and Error Handling

Hertest

`HERTEST 21 APRIL 2026` `RISICO GEACCEPTEERD`

Niet aangepast. De klant heeft het risico geaccepteerd, zie hieronder.

Reactie van de klant

De update naar de nieuwe versie van het framework staat gepland voor het derde kwartaal. Tot die tijd accepteren we dit risico.

HI-OP-2026-DEMO-05 Portaal kan in een andere site worden geladen

`LAAG` `RISICO GEACCEPTEERD` `MOEITE: MAKKELIJK`

In het kort

Het portaal mag in een frame op een andere site staan. Een aanvaller kan een gebruiker zo laten klikken op iets wat hij niet ziet.

`CVSS 4.0`	`2.1 CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N`
`CVSS 3.1`	`3.1 CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N`
`WAAR`	`Alle pagina's, header frame-ancestors ontbreekt`

VOORWAARDEN	Een ingelogde gebruiker die een pagina van de aanvaller bezoekt en daar klikt.
AL AANWEZIG	Belangrijke acties vragen om een bevestiging.
CATEGORIE	OWASP Top 10 2025 A02, CWE-1021, ASVS 5.0 V3

Wat er mis is

Het portaal stuurt geen frame-ancestors in de Content-Security-Policy en geen X-Frame-Options. Elke site mag het portaal in een frame laden.

Stappen om het na te doen

1. Maak een pagina met het portaal in een iframe.
2. Open die pagina terwijl je bent ingelogd.
3. Het portaal wordt getoond en reageert op klikken.

Bewijs

Het portaal laadt ingelogd in een iframe op een testpagina.

Impact

Een aanvaller kan een gebruiker ongemerkt laten klikken. Omdat belangrijke acties een bevestiging vragen, is de schade beperkt.

Oplossing

KORTE TERMIJN

Stuur Content-Security-Policy: frame-ancestors 'none'.

LANGE TERMIJN

Neem de beveiligingsheaders op in de standaardinstellingen van de webserver.

Controleer de fix

De testpagina uit stap 1 toont het portaal niet meer.

Referenties

- CWE-1021: Improper Restriction of Rendered UI Layers
- OWASP ASVS 5.0, hoofdstuk V3 Web Frontend Security

Hertest

HERTEST 21 APRIL 2026 RISICO GEACCEPTEERD

Niet aangepast. De klant heeft het risico geaccepteerd, zie hieronder.

Reactie van de klant

Belangrijke acties vragen al om een bevestiging. De header komt mee in de volgende grote update.

HI-OP-2026-DEMO-06 Export opent formules in Excel

LAAG RISICO GEACCEPTEERD MOEITE: GEMIDDELD

In het kort

Tekst die een klant invult, komt ongewijzigd in de CSV-export. Begint die tekst met een =, dan voert Excel het uit als formule bij wie de export opent.

CVSS 4.0	2.0 CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N
CVSS 3.1	3.7 CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N
WAAR	GET /beheer/export/bestellingen.csv, veld opmerking
VOORWAARDEN	Ingelogd als medewerker van een klant. Een beheerder moet de export openen in Excel en een waarschuwing wegklikken.
AL AANWEZIG	Excel toont een waarschuwing voor het uitvoeren.
CATEGORIE	OWASP Top 10 2025 A05, CWE-1236, ASVS 5.0 V1

Wat er mis is

Het veld opmerking bij een bestelling komt zonder aanpassing in de CSV-export. Waarden die met =, +, - of @ beginnen, worden in Excel als formule gelezen.

Stappen om het na te doen

1. Plaats als klant een bestelling met een opmerking die met = begint.
2. Download als beheerder van de groothandel de export van bestellingen.
3. Open de export in Excel: de opmerking is een formule.

Bewijs

Een onschuldige testformule uit het opmerkingenveld wordt in Excel uitgevoerd.

Impact

Een klant kan een formule laten uitvoeren op de computer van een medewerker van de groothandel, na een waarschuwing van Excel.

Oplossing

KORTE TERMIJN

Zet een apostrof voor waarden die met =, +, - of @ beginnen.

LANGE TERMIJN

Gebruik één exportfunctie voor alle CSV-bestanden die dit standaard doet.

Controleer de fix

De opmerking uit stap 1 staat als tekst in Excel.

Referenties

- CWE-1236: Improper Neutralization of Formula Elements in a CSV File
- OWASP: CSV Injection

Hertest

HERTEST 21 APRIL 2026 **RISICO GEACCEPTEERD**

Niet aangepast. De klant heeft het risico geaccepteerd, zie hieronder.

Reactie van de klant

De export wordt alleen geopend door de eigen financiële afdeling, die de waarschuwing van Excel kent.

Informatief en hardening

Geen kwetsbaarheden, wel verbeteringen die de beveiliging sterker maken. Zonder CVSS-score.

ID	ADVIES	WAAROM	MOEITE
HI-OP-2026-DEMO-I01	Zet een Content-Security-Policy met nonces.	Beperkt de schade als er ooit een XSS is.	Gemiddeld
HI-OP-2026-DEMO-I02	Publiceer een security.txt.	Onderzoekers weten dan waar ze een fout kunnen melden.	Makkelijk

Wat standhield

Wat HackIndex geprobeerd heeft zonder een fout te vinden. Dit laat zien hoe breed er getest is.

ONDERDEEL	WAT GETEST IS	UITKOMST
Rechten tussen rollen	Beheerfuncties en gegevens van de groothandel openen als medewerker of klantbeheerder.	GOED
Invoer	SQL-injectie, XSS en andere injectie in formulieren en de API.	GOED
Bestanden uploaden	Andere bestandstypen, te grote bestanden en paden in bestandsnamen.	GOED
Inloggen beheer	De tweede stap overslaan, opnieuw gebruiken of raden.	GOED

Hertest

Eén hertest binnen 90 dagen na het rapport. De uitkomst staat ook bij elke bevinding.

HERTEST OP	21 april 2026
GETEST OP VERSIE	`3.8.0, commit b81e0d7`
UITKOMST	3 opgelost, 3 risico geaccepteerd

ID	BEVINDING	ERNST	VOOR	NA
HI-OP-2026-DEMO-01	Facturen van andere klanten zijn op te vragen	HOOG	OPEN	OPGELOST
HI-OP-2026-DEMO-02	Sessie blijft geldig na uitloggen	MIDDEL	OPEN	OPGELOST
HI-OP-2026-DEMO-03	Geen limiet op inlogpogingen	MIDDEL	OPEN	OPGELOST
HI-OP-2026-DEMO-04	Foutmelding noemt de versie van het framework	LAAG	OPEN	RISICO GEACCEPTEERD
HI-OP-2026-DEMO-05	Portaal kan in een andere site worden geladen	LAAG	OPEN	RISICO GEACCEPTEERD
HI-OP-2026-DEMO-06	Export opent formules in Excel	LAAG	OPEN	RISICO GEACCEPTEERD

Bijlage: ernst, status en moeite

Ernst

HackIndex bepaalt de ernst met CVSS 4.0 en geeft ook de score in 3.1, zodat je kunt vergelijken. Wijkt de ernst af omdat jouw situatie anders is, dan staat bij de bevinding waarom.

ERNST	CVSS	WANNEER JE HET HOORT	VOORBEELD
KRITIEK	9.0 tot 10.0	Dezelfde dag, per mail en via je noodcontact	Zonder account bij alle klantgegevens
HOOG	7.0 tot 8.9	Binnen één werkdag	Een gewone gebruiker kan zichzelf beheerder maken
MIDDEL	4.0 tot 6.9	In het rapport	Een sessie blijft geldig na uitloggen
LAAG	0.1 tot 3.9	In het rapport	Een foutmelding noemt de versie van je framework
INFORMATIEF	0.0	In het rapport	Een advies om je beveiliging verder te verbeteren
GOED			Getest en standgehouden

Status

STATUS	WAT HET BETEKENT
OPEN	Nog niet opgelost, of nog niet hertest.
OPGELOST	De fout is weg en de oplossing werkt. Ook geprobeerd of hij op een andere manier terugkomt.
DEELS OPGELOST	Het risico is kleiner, maar niet weg. Bij de bevinding staat wat er nog nodig is.
NIET OPGELOST	De fout werkt nog. Bij de bevinding staat waarom de oplossing niet werkte.
RISICO GEACCEPTEERD	Je kiest er bewust voor om dit niet op te lossen. Het blijft zichtbaar in het rapport, met jouw reden.

Moeite om op te lossen

MOEITE	WAT HET BETEKENT
MOEITE: MAKKELIJK	Een instelling of een kleine wijziging op één plek.
MOEITE: GEMIDDELD	Wijzigingen op meer plekken, of een update die je moet testen.
MOEITE: LASTIG	Een onderdeel anders opzetten. Plan het als project.