HackIndex

PENETRATION TEST REPORT, SAMPLE

Customer portal

Example Wholesale Ltd

A made-up example. The client, the application and the findings are invented. Real reports stay confidential.

ENGAGEMENT	HI-OP-2026-DEMO
VERSION	2.0, after the retest
DATE	21 April 2026
TEST PERIOD	3 to 7 March 2026
CLASSIFICATION	Confidential

Document control

VERSION	DATE	WHAT CHANGED
1.0	12 March 2026	Report after the test
2.0	21 April 2026	Updated after the retest

Contact

PENTESTER	Joshua van der Poll, HackIndex
EMAIL	info@hackindex.nl
PGP KEY	`hackindex.nl/pgp.txt`
CLIENT CONTACT	Sanne de Boer, IT manager

Confidentiality

This report is confidential. It describes weak spots in the customer portal and is sensitive in its own right. HackIndex only shares it encrypted.

You may share the report with anyone who needs it to fix or assess the findings: your own team, the supplier who makes the fixes, your accountant, auditor or regulator.

A penetration test is a snapshot. This report describes what HackIndex found in the version and the period on the cover, within the agreed scope.

Summary

FOR DECISION MAKERS

From 3 to 7 March 2026, HackIndex tested the web application and API of the customer portal, grey box, with 3 roles. The version tested is 3.7.2 on the test environment.

VERDICT

The foundation is solid, but staff of one customer could open invoices of another customer. That is fixed after the retest.

0	1	2	3	2	4
CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL	GOOD

What comes first

- Staff of one customer can open invoices of another customer, with names, addresses and amounts. (01)
- A session stays valid after logging out. Anyone who gets hold of an old session can keep using it. (02)
- The login form has no limit on attempts, so passwords can be guessed without limit. (03)

What is good

- Permissions between roles are separated properly: staff cannot reach admin functions.
- Input is checked everywhere, in the API as well. No injection found.
- Administrators log in with a second step.

After the retest

After the retest on 21 April 2026, the high and both medium findings are fixed. The three low findings are knowingly accepted as a risk.

Findings overview

All findings, most severe first. Use the ID in email, tickets and the retest.

ID	FINDING	SEVERITY	EFFORT	STATUS
HI-OP-2026-DEMO-01	Invoices of other customers can be requested	HIGH	easy	FIXED
HI-OP-2026-DEMO-02	Session stays valid after logging out	MEDIUM	easy	FIXED
HI-OP-2026-DEMO-03	No limit on login attempts	MEDIUM	easy	FIXED
HI-OP-2026-DEMO-04	Error message shows the framework version	LOW	easy	RISK ACCEPTED
HI-OP-2026-DEMO-05	Portal can be loaded inside another site	LOW	easy	RISK ACCEPTED
HI-OP-2026-DEMO-06	Export runs formulas in Excel	LOW	moderate	RISK ACCEPTED

Scope and approach

What was tested

COMPONENT	ADDRESS	ENVIRONMENT	VERSION OR BUILD
Web application	`https://portal.wholesale.example`	Test	`3.7.2, commit 4f2a9c1`
API	`https://portal.wholesale.example/api/v2`	Test	`3.7.2, commit 4f2a9c1`

How

APPROACH	Grey box: with accounts per role, without source code.
TEST DAYS	3 to 7 March 2026, 5 days
TESTED FROM	`203.0.113.24`
STANDARDS	OWASP WSTG 4.2, OWASP ASVS 5.0 level 2
SEVERITY	CVSS 4.0 and 3.1, see the appendix

Test accounts

ROLE	ACCOUNT	NOTE
Customer staff	`staff-a@customer-a.example`	Two customers, to test between customers
Customer administrator	`admin-a@customer-a.example`	Manages the staff of customer A
Wholesaler administrator	`test-admin@wholesale.example`	With a second login step

Target protection

REACHABLE FROM THE INTERNET	Yes
IP ALLOWLIST	No
WAF OR FIREWALL	No
TEST IP ON THE ALLOWLIST	Not needed

What was not tested

What was outside the test, and why. This makes clear where the limits are.

- Overload (DoS): excluded in the rules of engagement.

- Payments: handled by an external payment provider, no permission to test them.
- The link with the ERP system: not present in the test environment.

To clean up

These items were created during the test. The client removed them, and HackIndex checked that it worked.

WHAT	WHERE	CLEANED UP
Five test accounts	See Test accounts	Yes, 12 March 2026
Two test orders	/orders, customer A	Yes, 12 March 2026

Findings

Sorted by severity. Every finding has the same structure: first the short story, then the details to reproduce and fix it.

HI-OP-2026-DEMO-01 Invoices of other customers can be requested

HIGH FIXED EFFORT: EASY

In short

A logged-in staff member can open invoices of other customers by changing the invoice number in the address. This exposes names, addresses and amounts of all customers.

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
WHERE	GET /api/v2/invoices/{number}
PREREQUISITES	Logged in as staff of a customer. No other rights needed.
ALREADY IN PLACE	Login is required, but the API does not check which customer an invoice belongs to.
CATEGORY	OWASP Top 10 2025 A01, CWE-639, ASVS 5.0 V8

What is wrong

The portal only lists your own invoices. The API that fetches a single invoice only checks that someone is logged in, not that the invoice belongs to that user's organisation. Invoice numbers are sequential, so they are easy to guess.

Steps to reproduce

1. Log in as staff of customer A and open one of your own invoices.
2. Change the invoice number in the request to one of customer B.
3. The invoice of customer B is shown.

Evidence

Staff of customer A fetch invoice 10482, which belongs to customer B.

REQUEST

```
GET /api/v2/invoices/10482 HTTP/2
Host: portal.wholesale.example
Cookie: session=[redacted, customer A]
```

RESPONSE

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

{"number":10482,"customer":"[customer B]","total":"1,250.00"}
```

Impact

Any staff member of any customer can view the invoices of all other customers, with names, addresses, orders and amounts. This may be a data breach you have to report.

Fix

SHORT TERM

Fetch the invoice through the organisation of the logged-in user, so an invoice of another customer is not found.

```
- $invoice = Invoice::findOrFail($number);
+ $invoice = $request->user()->organisation->invoices()->findOrFail($number);
```

LONG TERM

Define per model who may see it, in a policy, and test per route that another customer gets a 404. This keeps the flaw from coming back with new routes.

Verify the fix

Step 3 now returns a 404.

References

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

Retest

RETEST 21 APRIL 2026 FIXED

Fixed in version 3.8.0. Invoices of other customers return a 404, also through the export and the PDF download. Also tried with a customer administrator: the same outcome.

HI-OP-2026-DEMO-02 Session stays valid after logging out

MEDIUM FIXED EFFORT: EASY

In short

After logging out, the session stays valid on the server. Anyone who gets hold of an old session, for example on a shared computer, can keep working with it.

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
WHERE	POST /logout
PREREQUISITES	A session of another user, for example from a shared computer.
ALREADY IN PLACE	Logging out removes the cookie in the browser.
CATEGORY	OWASP Top 10 2025 A07, CWE-613, ASVS 5.0 V7

What is wrong

Logging out only removes the cookie in the browser. The session itself stays on the server until it expires after 30 days.

Steps to reproduce

1. Log in and save the value of the session cookie.
2. Log out.
3. Send a request with the saved cookie: you are still logged in.

Evidence

After logging out, a request with the old session still returns your own orders.

Impact

A session that leaked or was left behind on a shared computer stays usable for up to 30 days, even after the user thought they had logged out safely.

Fix

SHORT TERM

Revoke the session on the server as well when logging out.

LONG TERM

Shorten the session lifetime to one working day and give users a button to log out on all devices.

Verify the fix

Step 3 now redirects to the login page.

References

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

Retest

RETEST 21 APRIL 2026 FIXED

Fixed in version 3.8.0. After logging out, the old session is invalid. Sessions now expire after 8 hours.

HI-OP-2026-DEMO-03 No limit on login attempts

MEDIUM FIXED EFFORT: EASY

In short

The login form accepts unlimited attempts. An attacker can guess weak passwords of staff this way.

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
WHERE	POST /login
PREREQUISITES	None. It does need an existing email address and a weak password.
ALREADY IN PLACE	Passwords must be at least 10 characters.
CATEGORY	OWASP Top 10 2025 A07, CWE-307, ASVS 5.0 V6

What is wrong

After 200 failed attempts on one account, the form still accepted new attempts, without delay or lockout.

Steps to reproduce

1. Send 200 login attempts with wrong passwords for one test account.
2. Every attempt gets the same error message, without delay.
3. Logging in with the right password still works afterwards.

Evidence

200 attempts in 40 seconds on a test account, all answered without lockout.

Impact

Staff with a weak or leaked password can be taken over. Staff have no second login step.

Fix

SHORT TERM

Limit attempts per account and per IP address, for example 5 per minute, and slow down after that.

LONG TERM

Offer staff a second login step, as administrators already have.

Verify the fix

After 5 failed attempts, the form asks you to wait a moment.

References

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

Retest

RETEST 21 APRIL 2026 FIXED

Fixed in version 3.8.0. After 5 failed attempts per minute there is a waiting time, per account and per IP address.

HI-OP-2026-DEMO-04 Error message shows the framework version

LOW RISK ACCEPTED EFFORT: EASY

In short

An error in the API shows the framework version in the message. That helps an attacker look for known vulnerabilities in that version.

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
WHERE	GET /api/v2/orders?page=abc
PREREQUISITES	Logged in as staff of a customer.
ALREADY IN PLACE	None.
CATEGORY	OWASP Top 10 2025 A02, CWE-209, ASVS 5.0 V16

What is wrong

An invalid value in a parameter returns an error page with the name and version of the framework.

Steps to reproduce

1. Log in as staff.
2. Open the list of orders with a letter as the page number.
3. The error message shows the framework version.

Evidence

The error message contains the name and version number of the framework.

Impact

No harm on its own. It does make it easier to look for known flaws in that version.

Fix

`SHORT TERM`

Show a generic error message in production and validate parameter input.

`LONG TERM`

Turn error details off by default outside the development environment.

Verify the fix

Step 3 returns a generic message without a version.

References

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

Retest

`RETEST 21 APRIL 2026` `RISK ACCEPTED`

Not changed. The client accepted the risk, see below.

Client response

The update to the new framework version is planned for the third quarter. Until then we accept this risk.

HI-OP-2026-DEMO-05 Portal can be loaded inside another site

`LOW` `RISK ACCEPTED` `EFFORT: EASY`

In short

The portal may be shown in a frame on another site. An attacker can use this to make a user click on something they cannot see.

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
WHERE	All pages, frame-ancestors header missing
PREREQUISITES	A logged-in user who visits a page of the attacker and clicks there.
ALREADY IN PLACE	Important actions ask for confirmation.
CATEGORY	OWASP Top 10 2025 A02, CWE-1021, ASVS 5.0 V3

What is wrong

The portal sends no frame-ancestors in the Content-Security-Policy and no X-Frame-Options. Any site may load the portal in a frame.

Steps to reproduce

1. Create a page with the portal in an iframe.
2. Open that page while logged in.
3. The portal is shown and responds to clicks.

Evidence

The portal loads, logged in, inside an iframe on a test page.

Impact

An attacker can make a user click without noticing. Because important actions ask for confirmation, the damage is limited.

Fix

`SHORT TERM`

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

`LONG TERM`

Include the security headers in the default web server configuration.

Verify the fix

The test page from step 1 no longer shows the portal.

References

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

Retest

`RETEST 21 APRIL 2026` `RISK ACCEPTED`

Not changed. The client accepted the risk, see below.

Client response

Important actions already ask for confirmation. The header comes with the next major update.

HI-OP-2026-DEMO-06 Export runs formulas in Excel

`LOW` `RISK ACCEPTED` `EFFORT: MODERATE`

In short

Text a customer enters ends up unchanged in the CSV export. If that text starts with =, Excel runs it as a formula for whoever opens the export.

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
WHERE	GET /admin/export/orders.csv, field note
PREREQUISITES	Logged in as staff of a customer. An administrator must open the export in Excel and dismiss a warning.
ALREADY IN PLACE	Excel shows a warning before running it.
CATEGORY	OWASP Top 10 2025 A05, CWE-1236, ASVS 5.0 V1

What is wrong

The note field of an order goes into the CSV export unchanged. Values that start with =, +, - or @ are read as a formula by Excel.

Steps to reproduce

1. As a customer, place an order with a note that starts with =.
2. As a wholesaler administrator, download the orders export.
3. Open the export in Excel: the note is a formula.

Evidence

A harmless test formula from the note field runs in Excel.

Impact

A customer can have a formula run on the computer of a wholesaler employee, after a warning from Excel.

Fix

SHORT TERM

Put an apostrophe before values that start with =, +, - or @.

LONG TERM

Use one export function for all CSV files that does this by default.

Verify the fix

The note from step 1 shows as text in Excel.

References

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

Retest

RETEST 21 APRIL 2026 RISK ACCEPTED

Not changed. The client accepted the risk, see below.

Client response

The export is only opened by our own finance team, who know the Excel warning.

Informational and hardening

Not vulnerabilities, but improvements that make your security stronger. Without a CVSS score.

ID	ADVICE	WHY	EFFORT
HI-OP-2026-DEMO-I01	Set a Content-Security-Policy with nonces.	Limits the damage if there is ever an XSS.	Moderate
HI-OP-2026-DEMO-I02	Publish a security.txt.	Researchers then know where to report a flaw.	Easy

What held up

What HackIndex tried without finding a flaw. This shows how broadly was tested.

COMPONENT	WHAT WAS TESTED	OUTCOME
Permissions between roles	Opening admin functions and wholesaler data as staff or customer administrator.	GOOD
Input	SQL injection, XSS and other injection in forms and the API.	GOOD
File uploads	Other file types, oversized files and paths in file names.	GOOD
Admin login	Skipping, reusing or guessing the second step.	GOOD

Retest

One retest within 90 days of the report. The outcome is also shown with each finding.

RETEST ON	21 April 2026
VERSION TESTED	`3.8.0, commit b81e0d7`
OUTCOME	3 fixed, 3 risk accepted

ID	FINDING	SEVERITY	BEFORE	AFTER
HI-OP-2026-DEMO-01	Invoices of other customers can be requested	HIGH	OPEN	FIXED
HI-OP-2026-DEMO-02	Session stays valid after logging out	MEDIUM	OPEN	FIXED
HI-OP-2026-DEMO-03	No limit on login attempts	MEDIUM	OPEN	FIXED
HI-OP-2026-DEMO-04	Error message shows the framework version	LOW	OPEN	RISK ACCEPTED
HI-OP-2026-DEMO-05	Portal can be loaded inside another site	LOW	OPEN	RISK ACCEPTED
HI-OP-2026-DEMO-06	Export runs formulas in Excel	LOW	OPEN	RISK ACCEPTED

Appendix: severity, status and effort

Severity

HackIndex sets the severity with CVSS 4.0 and also gives the score in 3.1, so you can compare. If the severity differs because your situation is different, the finding says why.

SEVERITY	CVSS	WHEN YOU HEAR ABOUT IT	EXAMPLE
CRITICAL	9.0 to 10.0	The same day, by email and through your emergency contact	All customer data without an account
HIGH	7.0 to 8.9	Within one working day	A regular user can make themselves an administrator
MEDIUM	4.0 to 6.9	In the report	A session stays valid after logging out
LOW	0.1 to 3.9	In the report	An error message shows the version of your framework
INFORMATIONAL	0.0	In the report	Advice to improve your security further
GOOD			Tested and held up

Status

STATUS	WHAT IT MEANS
OPEN	Not fixed yet, or not retested yet.
FIXED	The flaw is gone and the fix works. Also checked whether it comes back another way.
PARTLY FIXED	The risk is smaller, but not gone. The finding says what is still needed.
NOT FIXED	The flaw still works. The finding explains why the fix did not work.
RISK ACCEPTED	You choose not to fix this. It stays visible in the report, with your reason.

Effort to fix

EFFORT	WHAT IT MEANS
EFFORT: EASY	A setting or a small change in one place.
EFFORT: MODERATE	Changes in several places, or an update you need to test.
EFFORT: HARD	Redesigning a component. Plan it as a project.