Saqr صقر

Confidential

Summary for owners

Prepared for

shop.yourcompany.com

Security Assessment

Testing window	Report date	Report ID	Version
4 to 23 November 2026	23 November 2026	SQR-0001-01	1

Document control

About this report

Report	Summary for owners
Prepared for	shop.yourcompany.com
Engagement	Security Assessment
Tasks included	Quick task on shop.yourcompany.com, Full task on shop.yourcompany.com, Quick task on shop.yourcompany.com, Quick task on shop.yourcompany.com, Full task on shop.yourcompany.com (5 tasks)
Prepared by	Security Assessment Team
Report ID	SQR-0001-01
Version and date	Version 1, 23 November 2026
Classification	Confidential
Distribution	The people responsible for shop.yourcompany.com only. Do not forward outside the distribution without the owner's approval.

Contents

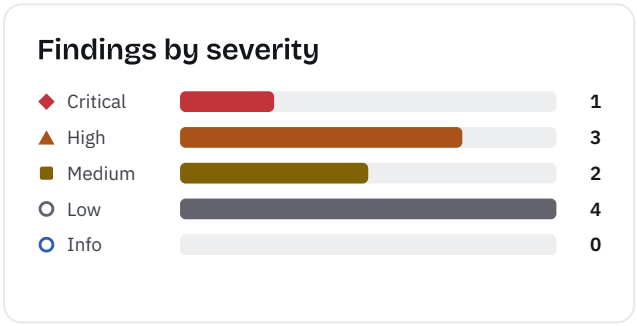
1 Summary 3
2 Top risks and what to do first 4
3 Scope and approach 5
4 Retest status 5
Sign-off and attestation 6

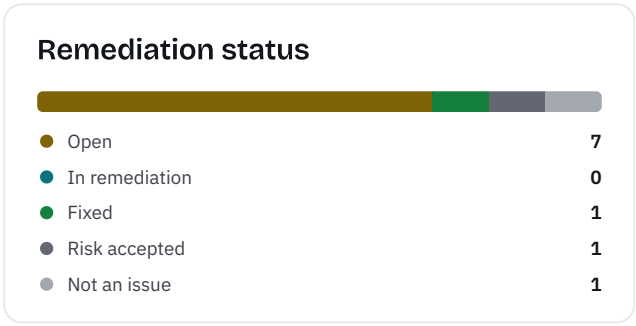
Section 1

Summary

Testing of shop.yourcompany.com (4 to 23 November 2026, 5 tasks) found 10 security findings: 1 critical, 3 high, 2 medium and 4 low. The overall risk is high. The most serious is invoice PDFs can be downloaded without signing in (F-02). 1 finding has already been fixed.

Overall risk	Findings	Critical	High	Medium
▲ High	10	◆ 1	▲ 3	■ 2





What matters most

- Invoice PDFs can be downloaded without signing in (F-02, high).
- Another customer's order can be read by changing the order id (F-03, high).
- Stored script injection in the profile display name (F-04, high).
- Error pages reveal stack traces and file paths (F-05, medium).

Business impact

Some weaknesses could give someone access to data or functions they should not have. They should be fixed in the next release cycle.

Section 2

Top risks and what to do first

The most severe open findings, and the prioritized actions that address every open finding. Each action names the findings it closes.

Ref	Severity	Risk	Business impact
F-02	▲ High	**Invoice PDFs can be downloaded without signing in**	Anyone who guesses or counts through invoice numbers can download every customer's invoice: name, billing address and what was bought.
F-03	▲ High	**Another customer's order can be read by changing the order id**	Any customer can read the orders of all other customers: full name, email address, phone number, shipping address and what they bought.
F-04	▲ High	**Stored script injection in the profile display name**	A customer can save a name that contains script.
F-05	■ Medium	**Error pages reveal stack traces and file paths**	The details make other issues easier to find: table and column names, file layout and exact library versions.
F-06	■ Medium	**No rate limit on the sign-in endpoint**	Passwords can be guessed at scale, and passwords leaked from other sites can be tried against all customer emails.

Prioritized recommendations

#	Action	Addresses	Effort	When
1	**Enforce authorization on every endpoint, denying by default**	F-02	Medium	Within 30 days
2	**Check object ownership on every request that takes an identifier**	F-03	Medium	Within 30 days
3	**Encode output by context and add a strict Content Security Policy**	F-04	Medium	Within 30 days
4	**Remove sensitive data from public responses and require authentication for it**	F-05, F-08, F-09	Low	Within 90 days
5	**Throttle sign-in attempts and add progressive lockout**	F-06	Medium	Within 90 days
6	**Set the standard security headers on every response**	F-07	Low	Next planned release

Effort is an estimate for a typical engineering team: Low is days, Medium is weeks, High needs planning. Timeframes follow the severity of the most serious finding an action addresses.

Section 3

Scope and approach

Target	`shop.yourcompany.com`
Engagement	Security Assessment
Testing window	4 to 23 November 2026

Tasks included

Task	Window	Status
Quick task on shop.yourcompany.com	4 November 2026	Completed
Full task on shop.yourcompany.com	6 November 2026	Completed
Quick task on shop.yourcompany.com	12 November 2026	Completed
Quick task on shop.yourcompany.com	19 November 2026	Completed
Full task on shop.yourcompany.com	From 23 November 2026	Running

Authorised scope

Type	Target	Why it is in scope
Domain	`shop.yourcompany.com`	The target of this report.

Approach

Saqr tested the application the way an outsider on the internet could, then proved each weakness with recorded evidence. The work followed the OWASP Web Security Testing Guide and NIST SP 800-115, with findings classified by CWE and the OWASP Top 10 and scored with CVSS v4.0. Risky actions waited for a person's approval, and every action was written to a tamper-evident audit log.

Section 4

Retest status

0 of 10 findings retested: 0 fixed, 0 still present, 0 inconclusive.

Ref	Finding	Severity	Retest	Date
No finding has been retested yet. Fixed one? Ask Saqr's assistant to retest the finding, or run a new task.				

Sign-off and attestation

Security Assessment Team attests that the testing described in this report was performed within the authorised scope and testing window, that every finding is backed by the evidence recorded during the engagement, and that the report presents the results without omission. Findings reflect the state of the systems during testing.

Prepared by	Reviewed by	Accepted by
Security Assessment Team	Name, role and date	The owner of shop.yourcompany.com