GROVIATECH SOLUTIONS LIMITED
Trustworthy.Transparent.Talented

Security review

Example Co. customer portal and public website

This is a sample. Every name, finding and date in this document is invented. Our real reports are covered by signed NDAs and are never shared, so this one shows how a report is written and laid out, nothing more.

PREPARED FOR	Example Co. (a made-up company)
PREPARED BY	Groviatech Solutions Limited
TESTING WINDOW	Invented: one week in March
TYPE OF WORK	Manual website and web application security review
CONFIDENTIALITY	The real version of this report would be shared only with the contacts named in the agreement

Summary in plain English

We reviewed Example Co.’s public website and customer portal the way an attacker would, by hand, using test accounts you gave us. The site is in reasonable shape. The pages are served over HTTPS, card payments are handled by a payment provider so card numbers never reach your server, and the admin area does require a sign-in.

We found one serious problem and four smaller ones. The serious one is that anyone can try an unlimited number of passwords against the admin sign-in. Fixing it takes a day or less. Fixing everything in this report is around two days of work for a developer.

1	2	1	1
High	Medium	Low	Info

Fix these first

1. Limit password attempts on the admin sign-in and require a second step for admin accounts (F-01).

2. Stop sending customer email addresses to the browser on the reviews page (F-02).

3. Add the missing cookie settings and security headers (F-03, F-04). Both are small changes.

How we rate each finding

We rate a finding by how easily it could be used against you and how much damage it could do, not by how technical it sounds.

HIGH	Could give an attacker access to accounts or data soon, with little effort. Fix first.
MEDIUM	Real exposure, but it needs more effort or a second weakness to be used. Fix soon.
LOW	Weakens your defenses without being a way in by itself. Fix when convenient.
INFO	Worth knowing. No action is strictly needed.

Findings

Each finding says what we saw, why it matters, and what to do about it, in that order.

F-01 HIGH /admin/login

The admin sign-in accepts unlimited password guesses

WHAT WE FOUND

We sent 500 wrong passwords in about a minute. The site answered every one normally. Nothing slowed us down and the account was never locked.

WHY IT MATTERS

Anyone can run a list of common passwords against your admin account until one works. Admin access means access to every customer record.

HOW TO FIX IT

Limit sign-in attempts, for example lock or slow the account after 5 failures in 15 minutes. Require a second step, such as an authenticator app, for every admin account.

Reference: OWASP Top 10 (2021) A07: Identification and Authentication Failures

F-02 MEDIUM /reviews

Customer email addresses are sent to every visitor

WHAT WE FOUND

Each review on this page carries the reviewer’s full email address in the data the page loads, although the page only displays a first name.

WHY IT MATTERS

Anyone can read the page source and collect real customer email addresses for spam or phishing.

HOW TO FIX IT

Stop sending the email field to the browser. Send only what the page actually shows.

Reference: OWASP API Security Top 10 (2023) API3: Broken Object Property Level Authorization

F-03 MEDIUM

All signed-in pages

The sign-in cookie is missing protective settings

WHAT WE FOUND

The cookie that keeps a customer signed in is sent without the Secure and SameSite settings.

WHY IT MATTERS

Without Secure, the cookie can travel over an unencrypted connection. Without SameSite, other websites can more easily trigger actions on a signed-in customer’s behalf.

HOW TO FIX IT

Set Secure, HttpOnly and SameSite=Lax on the session cookie.

Reference: OWASP Top 10 (2021) A05: Security Misconfiguration

F-04 LOW

All pages

Four standard security headers are missing

WHAT WE FOUND

Responses do not include Content-Security-Policy, X-Content-Type-Options, Referrer-Policy or Permissions-Policy.

WHY IT MATTERS

These headers tell the browser to be more careful with your pages. Without them, a mistake elsewhere is easier to exploit.

HOW TO FIX IT

Add the headers in your hosting or server settings. Most take a single line each.

Reference: OWASP Top 10 (2021) A05: Security Misconfiguration

F-05 INFO

All pages

The server announces its software version

WHAT WE FOUND

Response headers name the web server software and its version number.

WHY IT MATTERS

This is not a weakness by itself, but it tells an attacker which known issues to try first.

HOW TO FIX IT

Hide the version string in the server settings.

Reference: OWASP Top 10 (2021) A05: Security Misconfiguration

What we tested, and what we did not

Tested. The public website, the customer portal (with two test accounts you provided) and the admin sign-in page. We tested by hand against the OWASP Top 10 and the OWASP Application Security Verification Standard, and used tools only to speed up checks we then confirmed manually.

Not tested. Attacks that overload the site, tricking your staff, physical access, and the systems run by your payment provider and other outside services.

A security test shows what we found at the time we tested. It cannot prove that no weaknesses remain.

Retest

On penetration tests, we retest your fixes for free. This table shows what that looks like. The results here are invented.

Finding	Result	Note
F-01	Fixed	Account now locks after 5 failed attempts. Authenticator app required.
F-02	Fixed	Email field removed from the page data.
F-03	Fixed	Secure, HttpOnly and SameSite=Lax now set.
F-04	Fixed	All four headers present.
F-05	Open	Left as is. Accepted by Example Co.

Want one of these for your own site?

Book a free audit at groviatech.vercel.app/contact and we will tell you which kind of review fits, or that you do not need one.