Security Checkup Report

SECURITY CHECKUP

Report no. GH-2026-0001
Issued 2026-11-01
Valid for 30 days

CONCLUSION

32 checks performed, 21 passed, 11 open, of which 3 are high severity. Remediation of the high-severity items is recommended within 7 days.

32	21	11	3
checks covered	Passed	Open	High severity

Pass rate 66% 21/32

01 Coverage

Domain & certificates	7/9	External exposure	5/10	Accounts & authentication	2/3	Data & transport	2/2
Code & secrets	2/4	Dependencies	1/2	Logging & backups	Not covered	AI-specific risks	1/2

Priority findings

H-01 **Admin panel reachable without authentication**
Anyone who knows the path can open the admin panel and read or modify every customer conversation record.

H-02 **Database backup publicly downloadable**
The backup contains the full customer dataset including phone numbers, and anyone can download it.

H-03 **Model API key hardcoded in frontend code**
Anyone can open developer tools and take the key, then spend the account balance.

> This page can serve as a statement of current security posture and be **forwarded directly to customers, tender boards or investors**. Item-by-item records are on page 2; finding details on pages 3–4.

02 Item-by-item results (32 checks)

	ID	CHECK	RESULT
1 Domain & certificates			
✓	1.1	Certificate validity	187 days remaining
✓	1.2	HTTPS enforcement	http redirects with 301 to https
✗	1.3	**HSTS** M-02	Strict-Transport-Security missing
✓	1.4	Domain expiry	412 days remaining
✓	1.5	Email authentication: SPF	present, policy -all
✗	1.6	**Email authentication: DMARC** M-05	no DMARC record
✓	1.7	Certificate chain	intermediate certificates present
✓	1.8	TLS versions	1.2 / 1.3 only
✗	1.9	**Subdomain enumeration** M-06	3 reachable subdomains, including test.
2 External exposure			
✓	2.1	Unnecessary ports	only 80 / 443 exposed
✗	2.2	**Admin panel authentication** H-01	/admin returns 200
✓	2.3	Version control exposure	/.git/ returns 404
✗	2.4	**Backups and temporary files** H-02	/backup/2026-10-30.sql is downloadable
✓	2.5	Debug endpoints	none of the common debug paths reachable
✓	2.6	Directory listing	returns 403
✓	2.7	CORS configuration	allowlist only, no origin reflection
✗	2.8	**Security headers** L-02	CSP and X-Frame-Options missing
✗	2.9	**robots / sitemap** L-05	sitemap includes /staging
✓	2.10	HTTP methods	TRACE disabled
3 Accounts & authentication			
✗	3.1	**Session cookie attributes** M-04	session cookie missing Secure
✗	3.2	**Login rate limiting** M-01	20 failed attempts, no lockout or captcha
✓	3.3	Password reset flow	reset link expires in 30 minutes, single use
4 Data & transport			
✓	4.1	Database reachable from the internet	5432 not exposed
✓	4.2	Mixed content	no http resources referenced
5 Code & secrets			
✗	5.1	**Hardcoded keys in frontend** H-03	bundle contains an sk- credential
✗	5.2	**Source map exposure** L-03	/static/js/app.js.map is reachable
✓	5.3	Dependency lockfile	package-lock.json committed
✓	5.4	Credentials in public repositories	6 public repositories, none contained credentials
6 Dependencies			
✗	6.1	**Components with known vulnerabilities** M-03	3 dependencies match public vulnerability data
✓	6.2	Framework end of life	major version still supported
8 AI-specific risks			
✗	8.1	**Model API key exposure** H-03	same key as 5.1
✓	8.2	Model proxy authentication	proxy requires authentication, not anonymously usable
Not covered · Logging & backups (7) — requires internal access, outside the scope of an external assessment			

03 High-severity items (3 · remediate within 7 days)

H-01 Admin panel reachable without authentication

High

`https://app.example.com/admin`

Impact	Anyone who knows the path can open the admin panel and read or modify every customer conversation record.
Evidence	A direct request returns 200; the page lists customers and includes an export button.
Fix	Require an authenticated session; serve admin and customer surfaces separately; add an audit log.
Hours	**approx. 2 hours**

H-02 Database backup publicly downloadable

High

`https://app.example.com/backup/2026-10-30.sql`

Impact	The backup contains the full customer dataset including phone numbers, and anyone can download it.
Evidence	An unauthenticated GET returns 200 with Content-Type application/sql.
Fix	Move backups outside the web root into a private bucket; treat this backup as already disclosed.
Hours	**approx. 1 hours**

H-03 Model API key hardcoded in frontend code

High

`https://app.example.com/static/js/app.js`

Impact	Anyone can open developer tools and take the key, then spend the account balance.
Evidence	A credential string beginning with sk- appears in the production bundle.
Fix	Revoke and reissue the key; route model calls through your own backend proxy; add authentication and quota at the proxy.
Hours	**approx. 3 hours**

04 Medium-severity items (6)

ID	FINDING	LOCATION	RECOMMENDATION	HOURS
M-06	**Test subdomain publicly reachable and unauthenticated** Test environments usually connect to production data and keep default credentials.	`https://test.example.com`	Put access control in front of the test environment (IP allowlist or Basic Auth), or take it offline.	2h
M-01	**No rate limiting on the login endpoint** Credential stuffing or brute force is possible, with no alerting.	`POST /api/login`	Rate limit by IP and by account; require a captcha after five failures.	3h
M-02	**HSTS not enabled** The first request can be downgraded to HTTP, exposing users to interception.	`app.example.com`	Add HSTS; start with max-age of one day and raise it gradually.	0.5h
M-03	**Dependencies with known high-severity vulnerabilities** The framework version in use has a remotely triggerable deserialisation flaw.	`package-lock.json`	Upgrade to a fixed version; add dependency scanning to CI.	4h
M-04	**Session cookie missing the Secure attribute** The cookie can be captured over a plaintext HTTP connection.	`Set-Cookie: sessionid`	Add Secure and SameSite=Lax to every session cookie.	0.5h
M-05	**DMARC not configured** Anyone can send phishing email to your customers using your domain.	`_dmarc.example.com`	Publish p=none to collect reports, then switch to p=quarantine after two weeks.	1h

05 Low-severity items (4)

ID	FINDING	LOCATION	RECOMMENDATION	HOURS
L-02	Security headers missing	`site-wide`	Inject a common set of security headers at the gateway.	1h
L-03	Source maps publicly accessible	`/static/js/app.js.map`	Disable sourcemaps in production builds, or restrict access to them.	0.5h
L-05	Sitemap exposes internal paths	`/sitemap.xml`	Emit only public pages in the sitemap; exclude internal paths at build time.	0.5h
L-06	Error responses expose the framework version	`/api/*`	Disable debug output in production and return a single error page.	1h

06 Suggested timeline

Today

Contain current exposure

- H–01 Admin auth
- H–02 Move backup

This week

Reduce the external attack surface

- H–03 Rotate key, use proxy
- M–06 Retire test subdomain
- M–01 Login rate limiting
- M–05 DMARC

Within 30 days

Establish baselines as routine practice

- M–02 HSTS
- M–03 Dependency upgrades
- M–04 Cookie attributes
- L–02 L–03 L–05 L–06

07 Optional: remediation by us

$250
Remediation of the items in this report
~~Items total $340~~

Included
One recheck, included (within 7 days)

On request
Per–item quote
see schedule

The figure above covers remediation of every item in this report. A per–item quote is in the schedule.

08 Scope and limitations

- This assessment covers only the assets within the authorised scope. It does not include internal network penetration testing or social engineering.
- The assessment is a sample. It cannot guarantee that every risk has been found.
- No discovered credential was used to validate access, and no business data was accessed.
- Liability is limited to the fee paid for this engagement.

Assessed by Brynden Miki
cto@northwallsec.com

2026–11–01 Issued
GH–2026–0001