安全体检报告
SECURITY CHECKUP

报告编号 GH-2026-0001
出具日期 2026-11-01
有效期 30 天

结论

覆盖 32 项检查，21 项通过，11 项待处理，其中高危 3 项。建议 7 天内完成高危项修复。

32	21	11	3
本次覆盖检查项	通过	待处理	其中高危

通过率 66% 21/32

01 覆盖范围

域名与证书	7/9	对外暴露面	5/10	账号与鉴权	2/3	数据与传输	2/2
代码与密钥	2/4	依赖与组件	1/2	日志与备份	未覆盖	AI 特有风险	1/2

优先处置项

H-01 **后台管理面板未做鉴权**
任何知道该路径的人都能进入后台，查看并修改全部客户会话记录。

H-02 **数据库备份文件可公开下载**
备份包含全量客户数据与手机号，任何人可直接下载。

H-03 **前端代码硬编码模型 API Key**
任何人打开开发者工具即可取得 key，可直接盗刷额度。

本页可作为安全现状说明，**直接转发给你的客户、招标方或投资人**。 逐项检查记录见第 2 页，风险详情见第 3–4 页。

02 逐项检查结果（32 项）

结果	编号	检查项	检查结论
1 域名与证书			
✓	1.1	证书有效期	剩余 187 天
✓	1.2	强制 HTTPS	http 正确 301 到 https
✗	1.3	**HSTS** M-02	缺少 Strict-Transport-Security
✓	1.4	域名到期	剩余 412 天
✓	1.5	邮件认证 SPF	存在，策略 -all
✗	1.6	**邮件认证 DMARC** M-05	未配置 DMARC 记录
✓	1.7	证书链完整性	中间证书齐全
✓	1.8	TLS 协议版本	仅 1.2 / 1.3
✗	1.9	**子域枚举** M-06	发现 3 个可访问子域，含 test.
2 对外暴露面			
✓	2.1	非必要端口	仅 80 / 443 对外
✗	2.2	**管理后台鉴权** H-01	/admin 直接返回 200
✓	2.3	版本控制泄露	/.git/ 返回 404
✗	2.4	**备份与临时文件** H-02	/backup/2026-10-30.sql 可下载
✓	2.5	调试端点	常见调试路径均不可达
✓	2.6	目录列举	返回 403
✓	2.7	CORS 配置	仅回白名单，未反射任意来源
✗	2.8	**安全响应头** L-02	缺 CSP、X-Frame-Options
✗	2.9	**robots / sitemap** L-05	sitemap 含 /staging 路径
✓	2.10	HTTP 方法	TRACE 已禁用
3 账号与鉴权			
✗	3.1	**会话 Cookie 属性** M-04	会话 Cookie 缺 Secure
✗	3.2	**登录接口限流** M-01	20 次失败无锁定、无验证码
✓	3.3	找回密码流程	重置链接 30 分钟过期，一次性
4 数据与传输			
✓	4.1	数据库公网可达	5432 未对外
✓	4.2	混合内容	页面无 http 资源引用
5 代码与密钥			
✗	5.1	**前端硬编码密钥** H-03	打包产物含 sk- 开头凭证
✗	5.2	**Source Map 暴露** L-03	/static/js/app.js.map 可访问
✓	5.3	依赖锁定文件	package-lock.json 已提交
✓	5.4	公开仓库凭证	组织下 6 个公开仓库，未发现凭证
6 依赖与组件			
✗	6.1	**已知漏洞组件** M-03	3 个依赖命中公开漏洞库
✓	6.2	框架 EOL	主版本仍在支持期
8 AI 特有风险			
✗	8.1	**模型 API Key 暴露** H-03	与 5.1 为同一处 key
✓	8.2	模型代理鉴权	代理要求鉴权，未匿名可用
未覆盖 · 日志与备份（7） 需内部访问权限，属深度评估范围			

03 高危项（3 · 建议 7 天内修复）

H–01 后台管理面板未做鉴权

高危

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

影响	任何知道该路径的人都能进入后台，查看并修改全部客户会话记录。
依据	直接访问返回 200，页面包含客户列表与导出按钮。
修复	接入登录态校验；管理端与用户端分离部署；补充操作日志。
工时	**约 2 小时**

H–02 数据库备份文件可公开下载

高危

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

影响	备份包含全量客户数据与手机号，任何人可直接下载。
依据	不带凭证的 GET 返回 200，Content–Type 为 application/sql。
修复	备份移出 Web 根目录，改用对象存储私有桶；该备份应视为已泄露。
工时	**约 1 小时**

H–03 前端代码硬编码模型 API Key

高危

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

影响	任何人打开开发者工具即可取得 key，可直接盗刷额度。
依据	打包产物中出现 sk– 开头的凭证字符串。
修复	吊销并重新生成；模型调用改走自有后端代理；代理层加鉴权与配额。
工时	**约 3 小时**

04 中危项（6）

编号	风险	位置	建议	工时
M-06	**测试子域对外可访问且无鉴权** 测试环境通常直连生产数据库，且账号密码为默认值。	`https://test.example.com`	测试环境加访问控制（IP 白名单或 Basic Auth），或直接下线。	2h
M-01	**登录接口无速率限制** 可被撞库或暴力破解，且无告警。	`POST /api/login`	加 IP + 账号维度限流；失败 5 次触发验证码。	3h
M-02	**HTTPS 未启用 HSTS** 首次访问可被降级到 HTTP，存在中间人风险。	`app.example.com`	添加 HSTS，max-age 先设 1 天再逐步提高。	0.5h
M-03	**依赖组件存在已知高危漏洞** 所用框架版本存在可远程触发的反序列化漏洞。	`package-lock.json`	升级到修复版本；把依赖扫描加进 CI。	4h
M-04	**会话 Cookie 缺少 Secure 属性** Cookie 可能在明文 HTTP 连接中被截获。	`Set-Cookie: sessionid`	为所有会话 Cookie 添加 Secure 与 SameSite=Lax。	0.5h
M-05	**域名未配置 DMARC** 任何人可以伪造你的域名向你的客户发送钓鱼邮件。	`_dmarc.example.com`	先配置 p=none 收集报告，两周后切到 p=quarantine。	1h

05 低危项（4）

编号	风险	位置	建议	工时
L-02	缺少安全响应头	全站	网关注入统一安全头。	1h
L-03	Source Map 文件可公开访问	`/static/js/app.js.map`	生产构建关闭 sourcemap，或限制其访问。	0.5h
L-05	sitemap 暴露内部路径	`/sitemap.xml`	sitemap 只输出公开页面；内部路径从构建中排除。	0.5h
L-06	错误响应暴露框架版本	`/api/*`	生产环境关闭调试输出，统一错误页。	1h

06 建议节奏

今天

控制当前暴露

- H–01 后台鉴权
- H–02 备份移出 Web 目录

本周内

收敛对外攻击面

- H–03 吊销 key 并改走代理
- M–06 测试子域下线
- M–01 登录限流
- M–05 DMARC

30 天内

补齐基线并形成常态

- M–02 HSTS
- M–03 依赖升级
- M–04 Cookie 属性
- L–02 L–03 L–05 L–06

07 可选：由我们完成修复

¥1800
按本清单打包修复
~~单项合计 ¥2400~~

免费
免费复检一次（7 天内）

按需
单项报价
见附表

以上为按本报告清单打包修复的价格；单项报价见附表。

08 本次体检的边界

- 本次体检仅覆盖授权范围内的资产，不包含内网渗透与社会工程。
- 体检为抽样检查，不能保证发现全部风险。
- 未对发现的凭证做任何验证性使用，也未访问任何业务数据。
- 责任上限不超过本次服务费用。

体检方　Brynden Miki
cto@northwallsec.com

2026–11–01 出具
GH–2026–0001