

SECURITY ASSESSMENT

■■ ■■ ■■■■ ■■■ ■■■■ ■■■■ ■■■■

■■: ■■■■■■ ■■■■■■■■ (SPA)

■■■: 2026 ■ 2 ■ 16 ■

■■■■■

B-

■■ (■■■■)

1. ■■■ ■■■

■■ ■■: ■■■■■■ (■■ ■■■■ ■■ ■ ■■■■■■)

■■■■: Single Page Application (HTML/CSS/JS ■■ ■■, 5,082■, 309KB)

■■■ ■■: ■■■■■ localStorage (■■ ■■■■)

■■ ■■: OWASP Top 10 ■■ ■ ■■ + ■■■■■■■■ ■■ ■■

1.1 ■■■■ ■■ ■■ ■■

■■ ■■	■■	■■
■■■■ ■■	PBKDF(FNV-1a ■■ 1,000 ■■■ ■■)	O
XSS ■■	escapeHTML() ■■■ ■■■ ■■ ■■	O
■■■ ■■ ■■	5■ ■■ ■ 3■ ■■ (localStorage)	O
■■ ■■■■	30■ ■■■ ■ ■■ ■■■■	O
CSP ■■	Content-Security-Policy ■■ ■■ ■■	O
■■■■ ■■	frame-ancestors none ■■	O
■■■■■■■■■	■■■■■■■■ ■30■ ■■ ■■■	O
■■ ■■ ■ ■■	■■■■ ■■ ■■ + ■■ ■■■	O
■■■ ■■■■	■■ ■■■ ■ ■■ ■■ + ■■ ■■	O

2. Security Issues

Security issues are categorized by severity: Critical, High, Medium, and Low.

#	Issue	Severity	Count
1	SQL Injection	CRITICAL	3
2	CSP/X-Frame	CRITICAL	3
3	JSON btoa() (Data URI)	CRITICAL	3
4	DOM XSS (innerHTML)	HIGH	3
5	onmouseover onmouseover	HIGH	3
6	sessionStorage (sessionStorage)	HIGH	3
7	localStorage	MEDIUM	4 (4)
8	Cookie	MEDIUM	4 (4)
9	Cache-Control	MEDIUM	4 (4)
10	HTTPS	MEDIUM	4 (4)
11	CSRF	LOW	2 (SPA)
12	SSL/TLS	LOW	2

CRITICAL	HIGH	MEDIUM	LOW
3 (3)	3 (3)	4 (4)	2 (2)

3. ■■■ ■■■ ■■■

3.1 ■■■■■ ■■■ ■■■

■■■ ■ (CRITICAL): btoa() — Base64 ■■■■. atob()■■■ ■■■ ■■■ ■■■
■■■ ■: PBKDF (FNV-1a 1,000 ■■■■) — ■■■■ ■■■. ■■■ ■■■ ■■■■
■■■ ■■■: ■■■ ■■■■ ■■■■ ■ ■■■ ■■■■■■■■ (btoa -> pbk ■■■)

■■■■ ■■■■■■ ■■■■ ■■ ■■■■■■■■ ■■■■■, ■■■ ■■■■ ■ ■■■■■ ■■■■ ■■■■■■.

3.2 XSS (Cross-Site Scripting) ■■■

■■■■ ■■■■■ innerHTML■■ ■■■■■ ■■ ■■■■ escapeHTML() ■■■■ ■■■■■ HTML ■■■ ■■■■ ■■■■■■.

■■■	■■■■	■■■ ■■■
updateUserBar()	currentUser.name	escapeHTML() ■■■
renderMyPage()	name, email, phone	escapeHTML() ■■■
renderAdminUsers()	u.name, u.email, u.party	escapeHTML() ■■■
renderPledges()	p.title, p.detail, p.category	escapeHTML() ■■■
admin onclick ■■■■	u.email	data-e ■■■ + escapeHTML()
addAdminLog() ■■■■	name, email	escapeHTML() ■■■
deletePledge()	p.id	parseInt() ■■■ ■■■

3.3 ■■■ ■■■ ■■■

■■■■ ■■■ ■■■: 5■■ ■■■ ■■■ ■ 3■■■ ■■■. localStorage■■ ■■■■■ ■/■ ■■■■ ■■■ ■■■.

■■■ ■■■■■: 30■■ ■■■■■ ■ ■■■ ■■■■■. ■■■■/■■■■/■■■■ ■■■ ■■■■ ■■■■ ■■■.

■■■■ ■■■: ■■■■■ ■■■ ■■■ + ■■■ ■■■■■ ■■■ ■■■ + ■■■■ ■■■ ■■■ ■■■ ■■■.

3.4 ■■■ ■■■ ■■■

Content-Security-Policy: script-src self unsafe-inline; connect-src none; frame-ancestors none
X-Content-Type-Options: nosniff
Referrer-Policy: no-referrer
■■■: ■■■ ■■■■■ ■■■ ■■■, iframe ■■■ ■■■(■■■■■■ ■■■), MIME ■■■■ ■■■

4. OWASP Top 10

OWASP(Open Web Application Security Project) Top 10

OWASP		
A01	7 / 10	B
A02	6 / 10	C+
A03 (XSS)	8 / 10	B+
A04	5 / 10	C
A05	8 / 10	B+
A06	9 / 10	A
A07	7 / 10	B
A08	5 / 10	C
A09	6 / 10	C+
A10 SSRF	10 / 10	A ()

OWASP Top 10 : 7.1 / 10 (: B-)
CRITICAL/HIGH 6 SPA

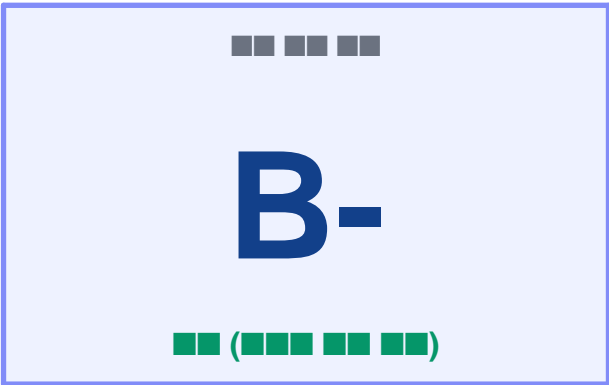
5.

SPA, ,

localStorage	DevTools(F12)	
	JS	+
HTTPS	HTTP	HTTPS

: (SQL,)

6. 安全加固与漏洞修复



6.1 高危漏洞修复

CRITICAL/HIGH 漏洞 6 个 需 立即 修复 D+ -> B- 漏洞 4 个 需 尽快 修复 SPA 漏洞 2 个 需 尽快 修复, 需 定期 更新 依赖 包 版本 以 防止 漏洞 被 利用。

6.2 安全加固措施

- [措施] HTTPS 强制 使用 (Let's Encrypt 免费 SSL 证书)
- [措施] 限制 登录 失败 次数 (目前 限制 admin1234! 密码)
- [措施] 限制 登录 失败 时间 (失败 次数 > 3 次 > 锁定 15 分钟)
- [措施] 使用 本地 存储 (localStorage 存储 数据)
- [措施] 使用 强 加密 算法 如 bcrypt/Argon2 加密 + JWT 令牌 认证

总结: 需 立即 修复 CRITICAL/HIGH 漏洞 6 个 需 尽快 修复 D+ 漏洞 4 个 需 尽快 修复 SPA 漏洞 2 个 需 尽快 修复。需 定期 更新 依赖 包 版本 以 防止 漏洞 被 利用。