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. ■■■ ■■ ■■

■■■ ■■■■ ■■■■ ■■■ ■■■■■. ■■ ■■ ■■■ ■■ ■■■ ■■ ■■■■■.

#	■■■	■■	■■
1	■■■ ■■■■ ■■ ■■	CRITICAL	■■ ■■
2	CSP/X-Frame ■■ ■■■	CRITICAL	■■ ■■
3	■■■■ btoa() ■■■ (■■ ■■)	CRITICAL	■■ ■■
4	■■ ■■■ XSS (innerHTML ■■■)	HIGH	■■ ■■
5	■■■ ■■■ onclick ■■■	HIGH	■■ ■■
6	■■■ ■■ ■■ ■■ (sessionStorage)	HIGH	■■ ■■
7	localStorage ■■■ ■■ ■■	MEDIUM	■■ (■■■)
8	■■■■■■ ■■ ■■	MEDIUM	■■ (■■■)
9	■■ ■■■■ ■■ ■■■	MEDIUM	■■ (■■■)
10	HTTPS ■■■	MEDIUM	■■ (■■ ■)
11	CSRF ■■ ■■■	LOW	■■ (SPA)
12	■■■ ■■ ■■ ■■	LOW	■■

CRITICAL	HIGH	MEDIUM	LOW
3■ (■■ ■■)	3■ (■■ ■■)	4■ (■■■ ■■)	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 ■■■ ■■■ ■■■ ■■■■■.

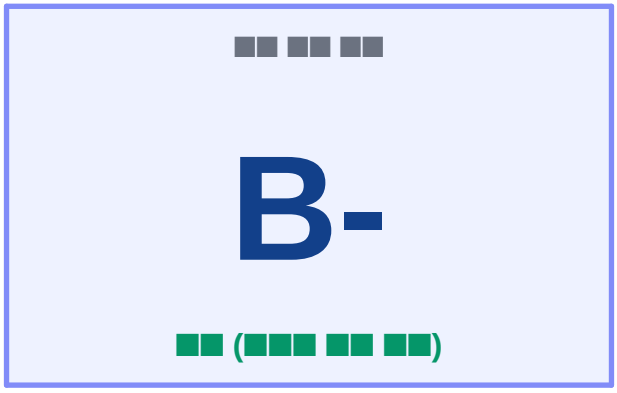
5. ■■ ■■ ■ ■■■ ■■

■■ ■■■ ■■ ■■ ■■■■■■ SPA ■■■ ■■■ ■■■, ■■ ■■■■ ■■■■ ■■■ ■■■ ■■■■■■.

■■ ■■	■■	■■ ■■
localStorage ■■ ■■	DevTools(F12)■ ■■ ■■■ ■■ ■■	■■■■ ■■ ■■, ■■■ ■■■
■■■■■■ ■■	■■ ■■■ ■■■■■ ■■	■■ ■■, ■■ ■■■■ ■■
■■ ■■ ■■■	JS ■■■■ ■■■ ■■ ■■	■■ ■■ + ■■■ ■■■■ ■■
HTTPS ■■■	■■ ■■■ ■■ HTTP ■■	■■ ■ HTTPS ■■ ■■ ■■

■■: ■ ■■■■ ■■ ■■■■ ■■■ ■■■■■■ ■■■■ ■■ ■■■ ■■■■ ■■■■. ■■■ ■■■■ ■■ ■■(SQL ■■■, ■■ ■■ ■)■ ■■■■■ ■■■■■■. ■■ ■■■ ■■ ■■■ ■■■■■ ■■■■■ ■■■■ ■■ ■■■■■ ■■ ■■■ ■■■■■.

6. ■■ ■■ ■ ■■■■



6.1 ■■ ■■ ■■

CRITICAL/HIGH ■■■ 6■ ■■ ■■ ■■■■ D+ -> B- ■■■■ ■■■■■■■. ■■ ■■ 4■■ ■■ ■■ SPA ■■■ ■■■ ■■■■, ■■ ■■■■■■ ■■■■ ■■ ■■■ ■■■■■■■.

6.2 ■■ ■■ ■■

- [■■] HTTPS ■■■■ ■■ (Let's Encrypt ■ ■■ SSL ■■■ ■■)
- [■■] ■■■ ■■■■ ■■ ■■ (■■ ■■■■ admin1234! ■■ ■■)
- [■■] ■■■ ■■■■ ■■■ ■■ (■■■ ■■■ > ■■ > ■■■ ■■)
- [■■] ■■ ■■■ ■■ ■■ (localStorage ■■ ■■)
- [■■] ■■ ■■ ■■■■ ■■ ■ bcrypt/Argon2 ■■ + JWT ■■ ■■ ■■

■■: ■ ■■■■ CRITICAL/HIGH ■■ ■■■ ■■ ■■■■■■, HTTPS ■■ + ■■■ ■■■■ ■■ ■■ ■■ ■■ ■■■■■. ■■ ■■■ ■■■ ■■ ■■■■ ■■■ ■■■■■, ■■■ ■■ ■■ ■■ ■■■ ■■■■■.

■ ■■■■ 2026■ 2■ 16■ ■■ ■■ ■■ ■■■■, ■■ ■■■ ■■ ■■■■. ■■■ ■■■■ ■■■ ■■■■, ■■■■ ■■■■ ■■■■■.