

SECURITY ASSESSMENT



■ ■ ■: 2026 ■ 2 ■ 16 ■



1. [REDACTED]

[REDACTED]: [REDACTED] ([REDACTED] [REDACTED] [REDACTED] [REDACTED])

[REDACTED]: Single Page Application (HTML/CSS/JS [REDACTED], 5,082 [REDACTED], 309KB)

[REDACTED]: [REDACTED] localStorage ([REDACTED] [REDACTED])

[REDACTED]: OWASP Top 10 [REDACTED] [REDACTED] + [REDACTED] [REDACTED]

1.1 [REDACTED] [REDACTED] [REDACTED]

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

2. [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED]. [REDACTED] [REDACTED] [REDACTED] [REDACTED].

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

CRITICAL	HIGH	MEDIUM	LOW
3 [REDACTED] ([REDACTED])	3 [REDACTED] ([REDACTED])	4 [REDACTED] ([REDACTED])	2 [REDACTED] ([REDACTED])

3. [REDACTED]

3.1 [REDACTED]

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

[REDACTED], [REDACTED] [REDACTED].

3.2 XSS (Cross-Site Scripting) [REDACTED]

[REDACTED] innerHTML [REDACTED] escapeHTML() [REDACTED] HTML [REDACTED].

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

3.3 [REDACTED]

[REDACTED]: 5 [REDACTED] 3 [REDACTED]. localStorage [REDACTED] / [REDACTED].

[REDACTED]: 30 [REDACTED] [REDACTED]. [REDACTED] / [REDACTED] / [REDACTED].

[REDACTED]: [REDACTED] + [REDACTED] + [REDACTED].

3.4 [REDACTED]

Content-Security-Policy: script-src self unsafe-inline; connect-src none; frame-ancestors none

X-Content-Type-Options: nosniff

Referrer-Policy: no-referrer

[REDACTED]: [REDACTED], iframe [REDACTED]([REDACTED]), MIME [REDACTED]

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 [REDACTED] 6 [REDACTED] SPA [REDACTED]

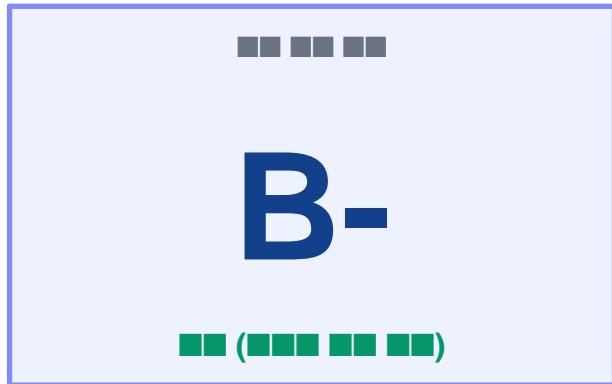
5.

SPA

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

SQL: `SELECT * FROM table WHERE column = value;`. SQL (SQL, SELECT, WHERE)

6. [REDACTED]



6.1 [REDACTED]

CRITICAL/HIGH [REDACTED] 6 [REDACTED] [REDACTED] D+ -> B- [REDACTED] [REDACTED]. [REDACTED] [REDACTED] 4 [REDACTED] [REDACTED] SPA [REDACTED]
[REDACTED], [REDACTED] [REDACTED] [REDACTED].

6.2 [REDACTED]

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

[REDACTED]: [REDACTED] CRITICAL/HIGH [REDACTED] [REDACTED], HTTPS [REDACTED] + [REDACTED] [REDACTED] [REDACTED] [REDACTED].
[REDACTED]. [REDACTED] [REDACTED] [REDACTED] [REDACTED], [REDACTED] [REDACTED] [REDACTED] [REDACTED].