What Could Go Wrong?

Security Details In Your Code	Cross-Site Scripting Attacks (XSS)	Cross-Site Request Forgery (CSRF)	Cross-Origin Resource Sharing (CORS)
Your JavaScript code can be read by ANYONE	Attack pattern where malicious JS code gets injected + executed	Attack pattern that depends on injected content (e.g. image)	Not an attack pattern but a security concept
Security-relevant details can be read	Injected code can do ANYTHING your code could do as well	Requests to malicious servers are made with user's cookies	Requests are only allowed from same origin (domain)
Attackers may be able to abuse exposed data	Very dangerous: Full behind-the-scenes control for attacker	Actions can be executed without the user knowing	Controlled via server-side response headers and browser
Example: Database access credentials exposed in code	Example: Unchecked user-generated content	Example: Malicious image URL, XSS	Example: JavaScript Modules