Mitigation

SQL Injection:

The SQL Injection is possible due to unsanitized user input in SQL queries.

Mitigation – Using prepared statements in SQL queries.

Cross-Site Scripting:

The XSS attack is possible due to lack of input/output validation, and input being displayed without encoding.

Mitigation – Input validation and Content Security Policy (CSP) should be incorporated.

Cross Site Request Forgery:

Browser automatically sends cookies without request verification.

Mitigation – Using CSRF tokens can protect from the attack.

File Inclusion Attack:

User-controlled file paths and lack of validation.

Mitigation – Sanitize inputs and disable remote includes.

Attack	**Mitigation**
SQL Injection	Prepared Statements – SQL queries
Cross-Site Scripting	Input validation & CSP
Cross Site Request Forgery	CSRF Tokens
File Inclusion	Disable remote includes