

1. €•, f• • ... XSS (Cross-Site Scripting)

† ‡ ...^%•Š ...<^•Æ•Žf• ••ŽŽ' Š f' " ... •-...•Ž• ‡~Ž™Šf• htmlspecialchars. > „ ...
f'™" œ••• „ -...-%...ÆŽ...' „ -Ž••^•Žf• JavaScript™...••'... ' „ ...^...Ž' " ... •-...•„ ••.
Ž^f%•^ " ^f%•Ž•Žf•: .

2. €•, f• • ... Information Disclosure

Ž^f ...Ÿf<™ " ...™" œ••Žf•™ <••••ŽŽ' Š - config.php -' -...•f„' • Ž• „^•••Ž...
'.....< , •Žf•. Ž...•^...<Ž...' „ f ...Ÿf<™f " ...j f^~œ„' • - error_log(). > „ ... " ^••...-^•, ••„
^•,™^' „f•™...Ž‡fj~^•šff' •^•-^•.

3. €•, f• • ... SQL Injection

†' • SQL--" ^... ' -' " ... Ž•œ„' •••^•- PDO ' f' " ... •-...•Žf•% prepare + execute.
Φ•ŽŽ' • " ... •-...-•„ •" • Ž• " ...' „ -" •œ„' • Ž• " ^•%~œ - -" ^...'. Ž^f%•^: \$stmt =
\$pdo->prepare('SELECT * FROM users WHERE login = ?');

4. €•, f• • ... CSRF (Cross-Site Request Forgery)

† POST-‡...^% ' •...<•- " •Ž „™•Ž CSRF,™ „„...^ ' ' ...Š^•Ž•„' • -' •' ' ff. Ž•^••
- ' " ... Ž•Žf•% -" ^... ' • " ^...f' Š...•f„ •j ... " ^...-•^™•. £•™f%...<^•-...%
" ^••...„-^•, ••„' • ...„ ^•-™• ‡...^% ' ' -Ž•ŸŽ•j... ' • „•.

5. €•, f• • ... Include / Upload

¤~Ž™šff include/require Ž• " ^fŽf%•œ„ " ... •-...-•„ •" •'™f ---...•. €•j^~™•
‡• " ...- „„' ~„' „-~•„, •„... f'™" œ•••„ '-•„' „-~œ, f•^f'™f.