Vulnerability Name	Location (file : line)	Description/fix	
SQL Injection	Model/shelf.php:128	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	
SQL Injection	Model/library.php:90	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	FIXED
SQL Injection	Model/library.php:101	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	FIXED
SQL Injection	Model/library.php:125	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	FIXED
SQL Injection	Model/library.php:126	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	FIXED
SQL Injection	Database/login_val.php:12	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	
SQL Injection	Database/register_user.php:24	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	
SQL Injection	Model/shelf.php:63	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	
SQL Injection	Model/shelf.php:68	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	
SQL Injection	Model/shelf.php:73	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	
SQL Injection	Model/shelf.php:78	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	
SQL Injection	Model/shelf.php:83	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	
SQL Injection	Model/shelf.php:89	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	
SQL Injection	Model/shelf.php:95	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	
SQL Injection	Model/shelf.php:100	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	
SQL Injection	Model/shelf.php:105	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	
SQL Injection	Model/shelf.php:110	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	
SQL Injection	Model/shelf.php:115	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	
SQL Injection	Model/library.php:56	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	FIXED
SQL Injection	Model/library.php:62	Allows undesired sql commands to be passed to the sql command which will then be executed. Input should be escaped before putting in the query.	FIXED
XSS	View/book_details.php:67	Allows any javascript to be sent to the browser where it will be automatically executed, doing potentially harmful things. Output should be escaped before being echoed to the browser	FIXED
XSS	View/book_details.php:78	Allows any javascript to be sent to the browser where it will be automatically executed, doing potentially harmful things. Output should be escaped before being echoed to the browser	FIXED
XSS	View/book_details.php:89	Allows any javascript to be sent to the browser where it will be automatically executed, doing potentially harmful things. Output should be escaped before being echoed to the browser	FIXED

Vulnerability Name	Location (file : line)	Description/fix	
XSS	View/book_details.php:100	Allows any javascript to be sent to the browser where it will be automatically executed, doing potentially harmful things. Output should be escaped before being echoed to the browser	FIXED
XSS	View/book_details.php:110	Allows any javascript to be sent to the browser where it will be automatically executed, doing potentially harmful things. Output should be escaped before being echoed to the browser	
XSS	View/book_details.php:120	Allows any javascript to be sent to the browser where it will be automatically executed, doing potentially harmful things. Output should be escaped before being echoed to the browser	
XSS	View/book_details.php:137	Allows any javascript to be sent to the browser where it will be automatically executed, doing potentially harmful things. Output should be escaped before being echoed to the browser	
Weak Type Comparison	Database/login_val.php:19	Can incorrectly identify two things as being identical because of type coercion when they really aren't, such as 0 and null. Should user === instead of == to prevent this	
Weak Type Comparison	Model/student.php:73	Can incorrectly identify two things as being identical because of type coercion when they really aren't, such as 0 and null. Should user === instead of == to prevent this	