COMMUNITY CONTENT

Home › Submit › 782202

Submit #782202: halex CourseSEL 1.1.0 SQL Injection

Title	halex CourseSEL 1.1.0 SQL Injection
Description	A SQL Injection vulnerability exists in the CourseSEL system (a ThinkPHP 3.2 based application) due to the lack of parameterization and improper input sanitization in the Apps/Index/Controller/IndexController.class.php file. The check_sel method directly concatenates the user-supplied HTTP GET parameter seid into the SQL query string using the framework's where() method. An authenticated attacker with standard student privileges can exploit this vulnerability to trigger an Error-based SQL Injection, allowing them to bypass authorization, extract sensitive database schemas, and dump administrative credentials.
Source	⚠ https://github.com/zy606/Vulnerability-Report/tree/main/CourseSEL-SQLi
User	Zyyyy (UID 96412)
Submission	03/18/2026 09:52 AM (18 days ago)
Moderation	04/04/2026 08:42 AM (17 days later)
Status	Accepted
VulDB entry	355290 [halex CourseSEL up to 1.1.0 HTTP GET Parameter IndexController.class.php check_sel seid sql injection]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling