COMMUNITY CONTENT

Submit #793895: code-projects Online Library Management System in PHP 1.0 Information Disclosure

Title	code-projects Online Library Management System in PHP 1.0 Information Disclosure
Description	The Online Library Management System in PHP v1.0 is vulnerable to Sensitive Information Disclosure due to an exposed SQL database backup file. The application includes a database dump file (library.sql) within a publicly accessible directory under the web root. Because the web server does not restrict access to .sql files, any unauthenticated user can directly access and download the database dump via HTTP. The exposed file can be accessed at: http://localhost/Library/sql/library.sql The database dump contains the full database schema and stored application data. This type of system typically manages sensitive information such as user accounts, student records, issued books, and administrative credentials. Because the file is stored inside a web-accessible directory and lacks access control, attackers can retrieve sensitive data without authentication.
Source	https://github.com/ahmadmarz10-hub/CVEsMarz/blob/main/Sensitive%20Information%20Disclosure%20In%20Online%20Library%20Management%20System%20PHP%20Exposed%20Database%20Backup.md
User	AhmadMarzouk (UID 95993)
Submission	03/31/2026 08:12 PM (10 days ago)
Moderation	04/09/2026 03:04 PM (3 days later)
Status	Accepted
VulDB entry	[code-projects Online Library Management System 1.0 SQL Database Backup File /sql/library.sql information disclosure]
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