COMMUNITY CONTENT

Home › Submit › 786307

Submit #786307: code-projects Online Application System For Admission In PHP 1.0 Information Disclosure

Title code-projects Online Application System For Admission In PHP 1.0 Information Disclosure

Description The Online Application System for Admission in PHP v1.0 is affected by a Sensitive Information Disclosure vulnerability due to an exposed SQL database backup file.

The application stores a database dump file (oas.sql) inside a publicly accessible directory within the web root. Because the web server does not restrict access to .sql files, any remote user can directly access and download the database dump without authentication.

The exposed file can be accessed via:

http://localhost/OnlineApplicationSystem_PHP/enrollment/database/oas.sql

Since the SQL file contains the complete database structure and stored application data, an attacker can retrieve sensitive information including user records, credentials, application data, and database schema.

This vulnerability arises from improper server configuration and insecure storage of backup files inside web-accessible directories.

Source https://github.com/ahmadmarz10-hub/CVEsMarz/blob/main/Sensitive%20Information%20Disclosure%20in%20Online%20Application%20System%20for%20Admission%20PHP%20Exposed%20Database%20Backup.md

User AhmadMarzouk (UID 95993)

Submission 03/23/2026 06:08 PM (14 days ago)

Moderation 04/05/2026 10:46 PM (13 days later)

Status Approved

VulDB entry [code-projects Online Application System for Admission 1.0 oas.sql sensitive information]

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