COMMUNITY CONTENT

Home › Submit › 782291

Submit #782291: https://www.campcodes.com/ Online Learning Management System V1.0 Unrestricted Upload

Title	https://www.campcodes.com/ Online Learning Management System V1.0 Unrestricted Upload
Description	The Online Learning Management System (OLMS) suffers from a critical vulnerability categorized as Unrestricted Upload of File with Dangerous Type (CWE-434). This flaw exists within the lesson attachment upload functionality handled by Crud_model.php. The application fails to enforce a secure whitelist for file extensions. Instead, it renames uploaded files using an MD5 hash but blindly appends the original, user-supplied extension (e.g., .php). Furthermore, the dynamically generated filename and its exact storage path are explicitly disclosed in the HTML source code of the frontend view (lessons.php). As a result, an attacker can upload a malicious PHP web shell, easily retrieve its hidden path from the frontend, and execute arbitrary system commands, leading to complete Remote Code Execution (RCE) and server compromise.
Source	⚠ https://github.com/whatyourname12345/CVE/tree/main/OLMS
User	chenkh (UID 96588)
Submission	03/18/2026 03:35 PM (18 days ago)
Moderation	04/04/2026 03:20 PM (17 days later)
Status	Accepted
VulDB entry	355310 [Campcodes Complete Online Learning Management System 1.0 Crud_model.php add_lesson unrestricted upload]
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