New issue

Jump to bottom

Book Store Management System— Use of Hard-coded Credentials in Source Code Leads to Admin Panel Access #2

Open **Upasanabohra** opened this issue on Oct 18 · 0 comments

Upasanabohra commented on Oct 18 Owner

Book Store Management System— Use of Hard-coded Credentials in Source Code Leads to Admin Panel Access

Exploit Author: Upasana Bohra

Vendor Homepage: https://www.sourcecodester.com/php-project

Software Link: https://www.sourcecodester.com/php/15748/book-store-management-system-project-using-php-codeigniter-3-free-source-code.html

Tested on Windows10

LinkedIn Contact: https://www.linkedin.com/in/upasana-bohra-8767b9156/

Hardcoded Credentials:

Hardcoded Passwords, also often referred to as Embedded Credentials, are plain text passwords or other secrets in source code. Password hardcoding refers to the practice of embedding plain text (non-encrypted) passwords and other secrets (SSH Keys, DevOps secrets, etc.) into the source code. Default, hardcoded passwords may be used across many of the same devices, applications, systems, which helps simplify set up at scale, but at the same time, poses a considerable cybersecurity risk.

[Attack Vectors]

An attacker can gain admin panel access using default credentials and do malicious activities

PROOF OF CONCEPT

1 Download source code from https://www.sourcecodester.com/php/15748/book-store-management-system-project-using-php-codeigniter-3-free-source-code.html

2 Now unzip it and go to the Database folder here we can see one SQL file.

3 Now open that file using Notepad and there we can see admin credentials. but the password is encrypted .from pattern I identified that this is MD5 hash. so we can easily decrypt using crackstation.net or any hash cracker tools like Hashcat, John the ripper.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant