

[New issue](#)[Jump to bottom](#)

CVE:2020-36062 Dairy Farm Shop Management System — Use of Hard-coded Credentials in Source Code Leads to Admin Panel Access #3

[Open](#)

VivekPanday12 opened this issue on Jan 23 · 0 comments

VivekPanday12 commented on Jan 23

[Owner](#)

Exploit Title: Dairy Farm Shop Management System — Use of Hard-coded Credentials in Source Code Leads to Admin Panel Access

Date: 2020-12-25**Exploit Author: VIVEK PANDAY****Vendor Homepage: <https://phpgurukul.com/>****Software Link: <https://phpgurukul.com/dairy-farm-shop-management-system-using-php-and-mysql/>****Version: 1.0****Tested on: Windows 10****LinkedIn Contact: <https://www.linkedin.com/in/vivek-panday-796768149/>**

CVE:2020-36062

[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://phpgurukul.com/dairy-farm-shop-management-system-using-php-and-mysql/>

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.

Mitigation:Always use a strong encryption algorithm like SHA-256 with SALT.Never use default credentials always change during installation time

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

