



# CVE-2020-36062

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2020-36062
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-02-11 16:15:00 UTC
<b>Updated</b>	2023-10-04 17:36:00 UTC
<b>Description</b>	Dairy Farm Shop Management System v1.0 was discovered to contain hardcoded credentials in the source code which allo

## Risk And Classification

**Problem Types:** CWE-798

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Lang
Application	Dairy Farm Shop Management System Project	Dairy Farm Shop Management System	1.0	All	All	All
Application	Phpgurukul	Dairy Farm Shop Management System	1.0	All	All	All

## References

### Reference

- CVE:2020-36062 Dairy Farm Shop Management System — Use of Hard-coded Credentials in Source Code Leads to Admin Panel Access · Is
- Dairy Farm Shop Management System Project, Dairy Farm Shop Management System in Php
- Latest PHP Tutorials | PHP Projects idea | PHP oops Concepts
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**