Table of Contents

Legal

Confidentiality

This document contains sensitive and confidential information, it should not be shared with any other 3rd parties without written permission.

GDPR

This document may contain personal data subject to the General Data Protection Regulation (GDPR). Handle any personal data in accordance with applicable data protection laws.

Disclaimers

The information provided in this document is for general informational purposes only and should not be construed as professional advice. The author(s) disclaim any liability for damages arising from the use of this information.

Change

The author(s) reserve the right to modify these terms. Review this document periodically for updates.

Contact

For inquiries, contact 087524805

Change Log

Date	Version	Comments
1/1/2021	0.1	Initial Report
10/1/2021	0.2	Recon Stage

2 Technical Details

2.1 SQL Injection CRITICAL ID: 1

We discovered that using specially crafted requests a malicious actor can communicate with the database and query it to retrieve stored data including data stored in the users tables.

URL	https://food.cstad.shop
Parameter	id
References	https://owasp.org/www-community/attacks/SQL_Injection
Request	POST rest/user/login HTTP/1.1 Host: domain.shop Accept: application/json, text/plain, */*
Response	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Vary: Accept-Encoding