Published in System Weakness

Mayur Parmar Follow
Nov 14, 2020 · 2 min read · Listen

CVE-2020–25952

A Tale of SQL Injection Leads to admin panel bypass

Exploit: https://www.exploit-db.com/exploits/49052

CVE:https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-25952

 # Exploit Title: User Registration & Login and User Management System 2.1
Date: 2020–11–14
Exploit Author: Mayur Parmar(th3cyb3rc0p)
Vendor Homepage: https://phpgurukul.com
Software Link: https://phpgurukul.com/user-registration-login-and-user-management-system-with-admin-panel/
Version: 2.1
Tested on Pop OS(Linux)
 # CVE: CVE-2020–25952

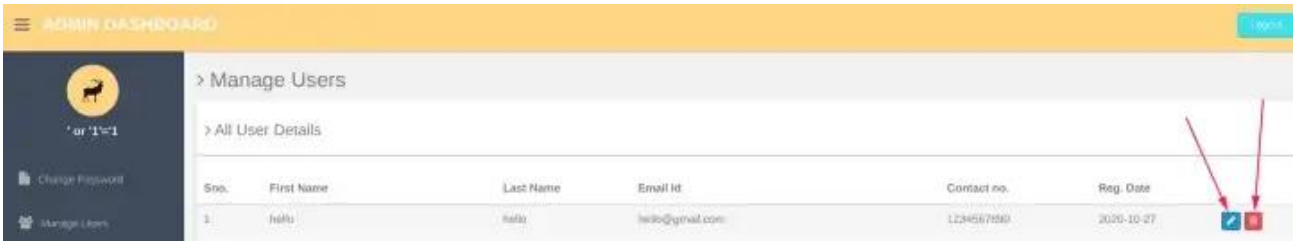
SQL Injection:
SQL injection is a web security vulnerability that allows an attacker to alter the SQL queries made to the database. This can be used to retrieve some sensitive information, like database structure, tables, columns, and their underlying data.

Attack Vector:
An attacker can gain admin panel access using malicious SQL injection queries than they can Update & Delete Userdata.

Steps to reproduce:
1. Open admin login page using the following URL:
-> http://localhost/loginsystem/admin/

2. Now put below Payload in both the fields(User ID & Password)
Payload: ‘ or ‘1’=’1

3. Server accepted our payload and we bypassed the admin panel without any credentials,



Admin Panel

Suggested Mitigation/Remediation Actions:
Parameterized queries should be used to separate the command and data portions of the intended query to the database. These queries prevent an attacker from tampering with the query logic and extending a concatenated database query string. Code reviews should be conducted to identify any additional areas where the application or other applications in the organization are vulnerable to this attack.
Additionally, input validation should be enforced on the server-side in order to ensure that only expected data is sent in queries. Where possible security-specific libraries should be used in order to provide an additional layer of protection.

> *Author at: https://systemweakness.com/*

Author: Mayur Parmar(th3cyb3rc0p)

https://twitter.com/th3cyb3rc0p?lang=en

https://in.linkedin.com/in/th3cyb3rc0p

https://www.instagram.com/th3cyb3rc0p/?hl=en

https://twitter.com/cyberdefecers?lang=en

Cve 2020 25952 Ctf Tryhackme Cyber Defecers Sql Injection