efekaanakkar / **Apartment-Visitors-Management-System-CVEs** Public

Code Issues Pull requests Actions Projects Security and quality

1 Branch 0 Tags Go to file Go to file Code

efekaanakkar Document SQL injection proof of concept in README

a468497 · yesterday

CVE-2026-39109	Update README.md	yesterday
CVE-2026-39110	Redact sensitive informatio…	yesterday
CVE-2026-39111	Document SQL injection pr…	yesterday
CVE-2026-39112	Enhance README with sec…	2 days ago
images	Rename CVE-2026-39112_…	2 days ago
LICENSE	Initial commit	2 days ago
README.md	Revise README structure …	2 days ago

README MIT license

🛡️ Apartment Visitors Management System CVEs

📌 Overview

This repository documents multiple security vulnerabilities discovered in **Apartment Visitors Management System v1.1**.
The issues include SQL Injection and Stored Cross-Site Scripting (XSS), each assigned a CVE identifier.

🚨 CVE List

CVE-2026-39109

- **Vulnerability Type:** SQL Injection
- **Affected Component:** Login Page (`index.php`)
- **Attack Vector:** `username` parameter
- **Impact:** Unauthorized database access / data disclosure

CVE-2026-39110

- **Vulnerability Type:** SQL Injection
- **Affected Component:** Forgot Password (`forgot-password.php`)
- **Attack Vector:** `contactno` parameter
- **Impact:** Sensitive data extraction

CVE-2026-39111

- **Vulnerability Type:** SQL Injection
- **Affected Component:** Forgot Password (`forgot-password.php`)
- **Attack Vector:** `email` parameter
- **Impact:** Database information disclosure

CVE-2026-39112

- **Vulnerability Type:** Stored Cross-Site Scripting (XSS)
- **Affected Component:** Visitor Form (`visitors-form.php`)
- **Attack Vector:** `visname` parameter
- **Impact:** Execution of arbitrary JavaScript in authenticated user sessions

---

🧠 Summary

The vulnerabilities are caused by improper input validation and unsafe handling of user-supplied data, leading to:

- SQL Injection in authentication and password recovery modules
- Stored XSS in visitor management functionality

⚙️ Affected Version

- Apartment Visitors Management System v1.1

🔬 Proof of Concept

Each CVE directory contains:

- Request samples
- Payloads
- Validation steps (Burp Suite / SQLmap)

🛠️ Tools Used

- Burp Suite
- SQLmap
- Manual testing

🛡️ Mitigation

- Use prepared statements (parameterized queries)
- Validate and sanitize all inputs
- Apply output encoding for user-controlled data
- Follow OWASP secure coding practices

🔗 References

- https://phpgurukul.com/apartment-visitors-management-system-using-php-and-mysql/

👤 Discoverer

Efe Kaan Akkar

⚠️ Disclaimer

This repository is for educational and security research purposes only.
All testing was conducted in a controlled environment.

Releases

No releases published

Packages

No packages published

Contributors 1

efekaanakkar