TECHNICAL SECURITY REPORT

Detailed Vulnerability Analysis
Target: https://lovable.dev/ | Generated: 2025-12-18T14:26:41.938Z

VULNERABILITY DETAILS

CRITICAL: SQL Injection Vulnerability

CVE: CVE-2021-44228
The application is vulnerable to SQL injection attacks through user input fields.

MEDIUM: SMB Signing Not Required

CVE: CVE-2020-0796
SMB server does not require message signing, vulnerable to relay attacks.

MEDIUM: SSL/TLS Configuration Weakness

Server supports weak cipher suites that could be exploited.

INFO: Information Disclosure via Server Banner

Server reveals detailed version information in response headers.

HIGH: FTP Anonymous Login Enabled

FTP server allows anonymous login which could expose sensitive data.

EXPLOITATION EVIDENCE

' Not Exploited: SQL Injection Payload Injection

' EXPLOITED: SMB Relay Attack

```
Successfully relayed authentication to target
```

' Not Exploited: SSL/TLS Downgrade Attack

' Not Exploited: Generic Exploit Attempt

' EXPLOITED: FTP Anonymous Access Exploitation

```
Uploaded test file to verify write access
```

REMEDIATION CODE SNIPPETS

SQL Injection Vulnerability

Language: text | Effort: 2-4 hours

```
Use parameterized queries or prepared statements. Implement input validation and sanitization.
```

Implementation:

FTP Anonymous Login Enabled

Language: text | Effort: 2-4 hours

```
Disable anonymous FTP access. Require authentication for all users.
```

Implementation:

SMB Signing Not Required

Language: text | Effort: 2-4 hours

```
# Remediation steps for: SMB Signing Not Required
1. Review the vulnerability details
2. Apply vendor patches if available
3. Implement compensating controls
4. Verify fix through re-testing
```

Implementation: Follow vendor recommendations and security best practices for this vulnerability type.

SSL/TLS Configuration Weakness

Language: nginx | Effort: 1-2 hours

```
ssl_protocols TLSv1.2 TLSv1.3;
ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256;
ssl_prefer_server_ciphers off;
```

Implementation: Update SSL/TLS configuration to use only modern protocols and cipher suites.

Information Disclosure via Server Banner

Language: text | Effort: 2-4 hours

```
# Remediation steps for: Information Disclosure via Server Banner
1. Review the vulnerability details
2. Apply vendor patches if available
3. Implement compensating controls
4. Verify fix through re-testing
```

Implementation: Follow vendor recommendations and security best practices for this vulnerability type.