

## Instantly share code, notes, and snippets.

sglInnora / [advisory\\_v2board\\_v2.md](#)

Created yesterday

[Code](#) [Revisions](#) 1

V2Board ≤1.7.4 Multiple Vulnerabilities (CVE-2026-37503/37504/37505)

[advisory\\_v2board\\_v2.md](#)**# V2Board ≤ 1.7.4 Multiple Vulnerabilities**

**\*\*Vendor\*\***: V2Board (github.com/v2board/v2board) – unmaintained since 2023  
**\*\*Affected\*\***: ≤ 1.7.4 (all versions; project abandoned)  
**\*\*Reporter\*\***: Feng Ning, Innora Security Research ([feng@innora.ai](mailto:feng@innora.ai))  
**\*\*Disclosure\*\***: 2026-04-30

CVE	Type	CWE	Location
<a href="#">CVE-2026-37503</a>	Stored XSS	CWE-79	theme configuration custom_html
<a href="#">CVE-2026-37504</a>	Sensitive Token Exposure	CWE-598	Server/UniverseContro
<a href="#">CVE-2026-37505</a>	SQL Injection	CWE-89	Admin/UserController ORDER BY

---

**## CVE-2026-37503 – Stored XSS via custom\_html**

Theme configuration renders the `custom_html` field through Blade's unescaped

**\*\*Fix\*\***: switch to `{{ }}` escaped output, or apply `wp_kses`-equivalent filter

---

**## CVE-2026-37504 – server\_token Exposed via GET**

In `app/Http/Controllers/Server/UniverseController.php`, the `server_token` r

**\*\*Fix\*\***: move token acceptance to a request header or POST body. Query parame

---

**## CVE-2026-37505 – SQL Injection via ORDER BY**

`app/Http/Controllers/Admin/UserController.php` builds its `ORDER BY` clause

**\*\*Fix\*\***: validate column names against a hard-coded allowlist; the direction

---

\*Innora Security Research – <https://innora.ai>\*