0-DAY NO CVE HIGH PUBLIC

phpMyAdmin designer settings JSON pmadb SQLi

phpMyAdmin 5.2.3 concatenates json_encode of designer settings into a single-quoted control-user UPDATE. A quote plus hash comments out WHERE username and overwrites another user's row. Labbed. No CVE yet.

NAME phpMyAdmin designer settings JSON pmadb SQLi	TYPE 0-day analysis
CVE n/a	CVE RISK high
DISCLOSURE STATUS public	VENDOR phpMyAdmin
AFFECTED phpMyAdmin 5.2.3 (962857e) with designer pma__designer_settings. 6.x quoteString on ControlUser is the patched shape. 5.2.3 is not.	PUBLISHED 12 Oct 2026
UPDATED 12 Oct 2026	TAGS 0-day, phpmyadmin, sqli, pmadb, designer, cwe-89, authenticated

TL;DR

Lab files and proof-of-concept here.

01 `json_encode` is not `quoteString`

I am @abraxas_null. The proof of concept is on GitHub: **abraxas/phpmyadmin-designer-json-sqli** (loopback client). The lab stack is `lab/` : docker-compose.yml, run.sh, poc.py, init.sql. Authorized lab only. It talks to loopback.

This is **phpMyAdmin 5.2.3** (`962857e`). No CVE yet. CWE-89. 8.1 High (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N`). Remote SQLi. Authenticated cookie login. The sink is the **control user** on `pma__designer_settings` , not the signed-in SQL box.

Designer AJAX `save_setting_value` `json_encode` s the settings blob and concatenates it into a single-quoted UPDATE/INSERT. Username is escaped. The JSON is not. `json_encode` does not escape a single quote. phpMyAdmin 6.x wraps this blob in `quoteString` on ControlUser. 5.2.3 still raw-concats it.

Older designer CVEs (2016-6616, 2019-11768, 2019-18622) were username / database name. This leftover is the JSON `settings_data` column.

02 Why this blob

Same wave as WebAuthn and central columns. The pmadb hunt had two Highs. Central columns is extra / attribute. This one is the designer JSON. 6.x already patched this shape. 5.2.3 did not. That is a leftover, not a new class.

I only wanted Critical or High. "The user already has a SQL box" is the skip for `appdb` . It is not a skip for `phpmyadmin.*` as the control user. `appuser` in this lab has no GRANT on `phpmyadmin` .

03 Pinning RELEASE_5_2_3

Latest 5.2 stable. Tag `RELEASE_5_2_3`. Commit `962857e`. Image `phpmyadmin:5.2.3`. Designer settings table created. Control user granted DML on `phpmyadmin.*`. Seed a victim row `{"keep":"safe"}` so a missing WHERE is visible.

04 The skip list is half the hunt

- PMASA-2025-1 / 2 / 3 already patched in 5.2.2.
- Designer username / db-name CVEs 2016-6616, 2019-11768, 2019-18622. Different column. Do not re-file those.
- CVE-2016-5703 central columns database name. Different feature.
- 6.x `quoteString(..., ControlUser)` on this blob. That is the patched shape. 5.2.3 must still be raw concat or it is not this leftover.
- Designer VQB history stored XSS is a different leftover (table names into HTML). Not this post.

I am not filing designer-off. Feature no-ops. FAIL, not this leftover.

05 Surfaces that returned nothing

Same empty surfaces as the rest of the wave. The interesting negative on this sink is username: it **is** escaped. Inject there and you are labbing the 2016 class, which is closed. Inject in `value`. `json_encode` will put your quote inside the SQL literal.

`RecentFavoriteTable::saveToDb()` already quotes. This function did not copy that.

06 The concat

`libraries/classes/Database/Designer/Common.php` `saveSetting`:

PHP Copy

```php
$orig_data = json_encode($orig_data);
$save_query = 'UPDATE '
    ...
    . " SET settings_data = '" . $orig_data . "'"
    . " WHERE username = '" . $this->dbi->escapeString($username) . "'";
...
    . "', '" . json_encode($save_data) . "');";
$this->dbi->queryAsControlUser($query);
```

`Controllers/Database/DesignerController.php` POST `operation=save_setting_value`. Route `GET|POST /database/designer`. `$_POST['index']` / `$_POST['value']`.

A quote plus `#` in `value` truncates `settings_data` and comments out `WHERE username = 'appuser'`. The UPDATE hits every row. mysqli default is single-statement, so this is not stacked queries. It is a missing WHERE. That is enough.

07 The lab

Loopback `http://127.0.0.1:19220`. Compose project `phpmyadmin-designer-json-sqli`. Cookie login as `appuser`. Clean save stored `{"snap_line":"grid-ok"}` for appuser and left victim at `{"keep":"safe"}`. The same save with `PMA-DESIGNER-JSON-SQLI-WITNESS'#` truncated `settings_data`. Victim row became the truncated witness blob. General log showed the raw quote, not `quoteString`. `sql-error=false`. MySQL accepted the truncated UPDATE.

PLAIN TEXT Copy

```
cd lab && ./run.sh
```

Last line:

PLAIN TEXT Copy

```
SUCCESS phpmyadmin-designer-json-sqli version=5.2.3 how=live raw-concat=yes trunc
```

08 Wrong turns, in the order I made them

Injecting on username. It is escaped. That is the 2016 class, which is closed.

Expecting a `#1064`. The `#` comments out the rest. MySQL accepts the truncated UPDATE. The oracle is row corruption plus the general log, not a syntax error. Central columns was the `#1064` leftover. This one is quieter.

Treating stacked queries as proven. Default `mysqli::query` is single-statement. The missing WHERE is the lab-proven integrity hit.

Calling 6.x this leftover. 6.x `quoteString`s this blob. 5.2.3 does not.

A reverse shell. Theatre. The oracle is a truncated JSON blob on loopback.

09 What an attacker can do

A signed-in phpMyAdmin user who can open Designer can inject SQL as the **control user** on `pma__designer_settings`.

PRIVILEGE	METH
Break the control-user UPDATE/INSERT string (integrity of pmadb SQL)	POS rout

PRIVILEGE	METH
	`ope` with
Truncate own `settings_data` so it is no longer JSON (integrity of own row)	Sam the
Overwrite other users' designer rows without stacked queries (integrity of victim row)	Sam `user`
Extra statements as the control user	Sam link
Reach other pmadb tables (bookmarks, history, `pma__userconfig`)	Only writ

Closed on this lab: unauthenticated access, the signed-in appuser SQL box (appdb only), OS shell, and stacked queries. Feature no-ops if pmadb / designer settings is off.

I am not going to print a stacked payload you can paste at someone else's PMA. If you own the instance, run the proof of concept against loopback.

10 The fix

`quoteString(..., ControlUser)` / `escapeString` on the JSON blob, same as `RecentFavoriteTable::saveToDb()` and phpMyAdmin 6.x on this column. Do not put `json_encode` output inside a single-quoted SQL literal.

Same pin leftovers: phpmyadmin-webauthn, phpmyadmin-pmadb-central-sqli, phpmyadmin-setup-validate, phpmyadmin-csrf-sql.

11 References

- Proof of concept: abraxas/phpmyadmin-designer-json-sqli · phpmyadmin-designer-json-sqli-Abraxas-Labs.py
- Lab: `lab/` · docker-compose.yml · run.sh · poc.py
- @abraxas_null · github.com/abraxas · abraxaslabs.tech · abraxas.null@proton.me
- CWE-89 · 8.1 High
- Tree: phpmyadmin/phpmyadmin RELEASE_5_2_3 (`962857e`) · `Designer/Common.php` `saveSetting`

Abraxas Labs

Independent security research by abraxas.

Analysis of 0-days, n-days, malware, and the

leftovers that still matter.

GitHub **@abraxas_null** **abraxas.null@proton.me** **abraxaslabs.tech**

Home Research Open Source Reading Room About GitHub @abraxas_null Console

Independent research. Private analysis by arrangement. No ads. abraxas.null@proton.me · For defensive awareness and authorized testing only.

© 2026 Abraxas Labs