0-DAY NO CVE HIGH PUBLIC

phpMyAdmin 5.2.3, /config/set clears 2FA

phpMyAdmin 5.2.3 POST /config/set writes any allowlisted preference, including 2fa, with no validation. Settings Two-factor still calls TwoFactor::check(true). /config/set does not. Next password login is password-only. Labbed. No CVE yet.

NAME phpMyAdmin 5.2.3, /config/set clears 2FA	TYPE 0-day analysis
CVE n/a	CVE RISK high
DISCLOSURE STATUS public	VENDOR phpMyAdmin
AFFECTED phpMyAdmin 5.2.3 tag RELEASE_5_2_3 (962857e). Cookie login. CSRF token required. Completes XSS or CSRF to a durable 2FA strip. Does not skip the MySQL password.	PUBLISHED 12 Oct 2026
UPDATED 12 Oct 2026	TAGS 0-day, phpmyadmin, 2fa, privilege-leftover, cwe-620, authenticated

TL;DR

Lab files and proof-of-concept **here**.

01 Settings asked for the factor. /config/set did not

I am @abraxas_null. The proof of concept is on GitHub: **abraxas/phpmyadmin-config-set-2fa** (loopback client). The lab stack is `lab/`: Dockerfile, docker-compose.yml, config.inc.php, init.sql, run.sh, poc.py. Authorized lab only. It talks to loopback.

This is **phpMyAdmin 5.2.3** (`962857e4f63d42e38f11ff4d63f5e722018add76`). No CVE yet. CWE-620. 8.1 High (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N`). Remote privilege leftover. Cookie login. CSRF token required.

Settings → Two-factor will not drop the factor until `TwoFactor::check(true)` returns true. `POST /config/set` writes any allowlisted preference, including `2fa`. `UserPreferences::persistOption` is documented "No validation is done!" `json_decode('null')` is PHP null. The default for that path is also null, so the key is unset. The next password login has no TOTP, WebAuthn, or Simple prompt. Durable strip, not a one-request skip.

I did not need leftover #1 (CustomServer signature). I did not skip the MySQL password.

02 Why phpMyAdmin

I had already published the CustomServer WebAuthn leftover on this pin. That bug is "the second factor never checks the signature." This one is "a preference writer will delete the second factor without presenting it." They are not the same class. One is a skip of WebAuthn crypto after the password. One is a durable removal of whatever backend is stored in pmadb.

phpMyAdmin stores 2FA in `pma__userconfig` as a JSON object under key `2fa`. The Settings UI knows that object is authentication. The AJAX preference endpoint does not.

03 Pinning RELEASE_5_2_3

Latest 5.2.x GA. Tag `RELEASE_5_2_3`. Commit `962857e4f63d42e38f11ff4d63f5e722018add76`. The lab builds from that tag on `php:8.2-apache` so `$cfg['DBG']['simple2fa']` can enroll the Simple backend without a hardware key. TOTP and WebAuthn live in the same `2fa` preference key. The leftover is the writer, not the lab-only flag.

04 The skip list is half the hunt

- **PMASA-2025-1/2/3.** Already in 5.2.2.
- **CustomServer WebAuthn.** Already public. Signature never checked. Different handler, different factor, different leftover.
- Settings → Two-factor `2fa_remove` is the path that still demands the factor. That is the negative control, not the bug.

Closed on this leftover: unauthenticated access, skipping the MySQL password, OS RCE, reading other users' pmadb rows.

Other 5.2.3 leftovers from the same review sit in their own packs. XSS and CSRF that can POST a page token complete this strip. Those are separate reports.

05 Surfaces that returned nothing

I looked at `/config/get` first. It reads. Then `/preferences/two-factor`. It checks. Then the JS helper in `functions.js` that posts `index.php?route=/config/set` for theme and appearance prefs. `2fa` is on the same allowlist as those prefs. The comment on `persistOption` is honest. The allowlist is not.

A second session hitting `2fa_confirm` after enroll was the proof Settings still works. POST `2fa_remove` without the factor stayed on the confirm UI and left `backend=simple` in pmadb. That is the product doing what the product said. `/config/set` is the leftover.

06 The leftover

`SetConfigController.php`:

PHP Copy

```php
$result = $this->config->setUserValue(null, $key, json_decode($value));
```

`UserPreferences.php` `apply()` allowlists `2fa` so the key is not dropped as an unknown pref. `persistOption('2fa', null, $default)` unsets `config_data['2fa']`.

`TwoFactorController` will not `configure('')` until `TwoFactor::check(true)` returns true. Two writers. One of them asked.

07 Wrong turns in the order they happened

I treated Settings `2fa_remove` as the hole. It still demands the factor. pmadb still had `backend=simple` after that POST.

I almost claimed unauthenticated access. Cookie login and a CSRF token are required. XSS or CSRF that can POST the page token is a chain, not this lab.

I almost claimed a skip of the MySQL password. The next login is password-only. It is still a password login.

I treated this as leftover #1. CustomServer never verifies a WebAuthn assertion. This path deletes the stored factor. Different files.

Theatre: a reverse shell.

08 The lab

Pin `RELEASE_5_2_3` copied or cloned into `lab/src/` for the image. mysql:8.0. Host bind **127.0.0.1:19280**. Compose project `phpmyadmin-config-set-2fa`. Cookie auth, pmadb `pma__userconfig`. `$cfg['DBG']['simple2fa']=true` only so Settings can enroll Simple.

Settings enrolled Simple 2FA. A second browser hit the `2fa_confirm` page. POST `2fa_remove` without the factor stayed on the confirm UI and left `backend=simple` in pmadb. POST `/config/set` `key=2fa` `value=null` returned `success:true`, pmadb became `[]`, and the next login landed in the normal UI.

PLAIN TEXT Copy

```
python3 phpmyadmin-config-set-2fa-Abraxas-Labs.py
# or: cd lab && ./run.sh
```

Last line:

PLAIN TEXT Copy

```
SUCCESS phpmyadmin-config-set-2fa enroll=simple ui-remove-blocked=yes config-set-
```

09 What an attacker can do

Strip 2FA from a phpMyAdmin account without presenting TOTP, WebAuthn, or the Simple confirm field. The next password login is password-only. Full PMA as that MySQL user (SQL, users, export).

PRIVILEGE	METHOD / PATH
Persist `2fa` to null and drop the second factor from pmadb	Authenticated `POST index.php?route=/config/set` `key=2fa` `value=null` plus a valid `token`
Log in with password only after that write	New cookie session, same MySQL user
Keep the current session while 2FA disappears for later logins	Same handler; `persistOption` writes the store, not the live `two_factor_check` flag
Chain from stored XSS or CSRF that can POST with the page token	Same-review leftovers, not this lab
Remove 2FA through Settings	`POST /preferences/two-factor` `2fa_remove=1`

PRIVILEGE	METHOD / PATH

Closed on this leftover: unauthenticated access, skipping the MySQL password, OS RCE, reading other users' pmadb rows.

10 The fix

Deny `2fa` (and other auth keys) on `/config/set`. Require `TwoFactor::check(true)` before any 2FA mutation. Keep the Settings path as the only writer.

11 Contact

Abraxas Labs - abraxaslabs.tech - github.com/abraxas - @abraxas_null - abraxas.null@proton.me

A x

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**

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

© 2026 Abraxas Labs