Insecure Parameter Handling: Unauthorized Modification of Immutable 'nick' Field

Moderate **NeoRazorX** published **GHSA-pp79-hqv6-vmc3** last week

Package

php **neorazorx/facturascripts** (Composer)

Affected versions	Patched versions
<= 2025.92	None

Description

Summary

The application fails to validate the `nick` parameter during a `POST` request to the `EditUser` controller. Although the UI prevents editing this field, a user can bypass this restriction using a proxy to rename any account (including the Administrator). This leads to Broken Access Control and potential Audit Log Corruption.

Details

The vulnerability exists in the user update logic. When a `POST` request is sent to `/EditUser`, the backend processes the `nick` form-data parameter without checking if it matches the original value or if the user has the privilege to change a unique identifier that is intended to be immutable.

PoC

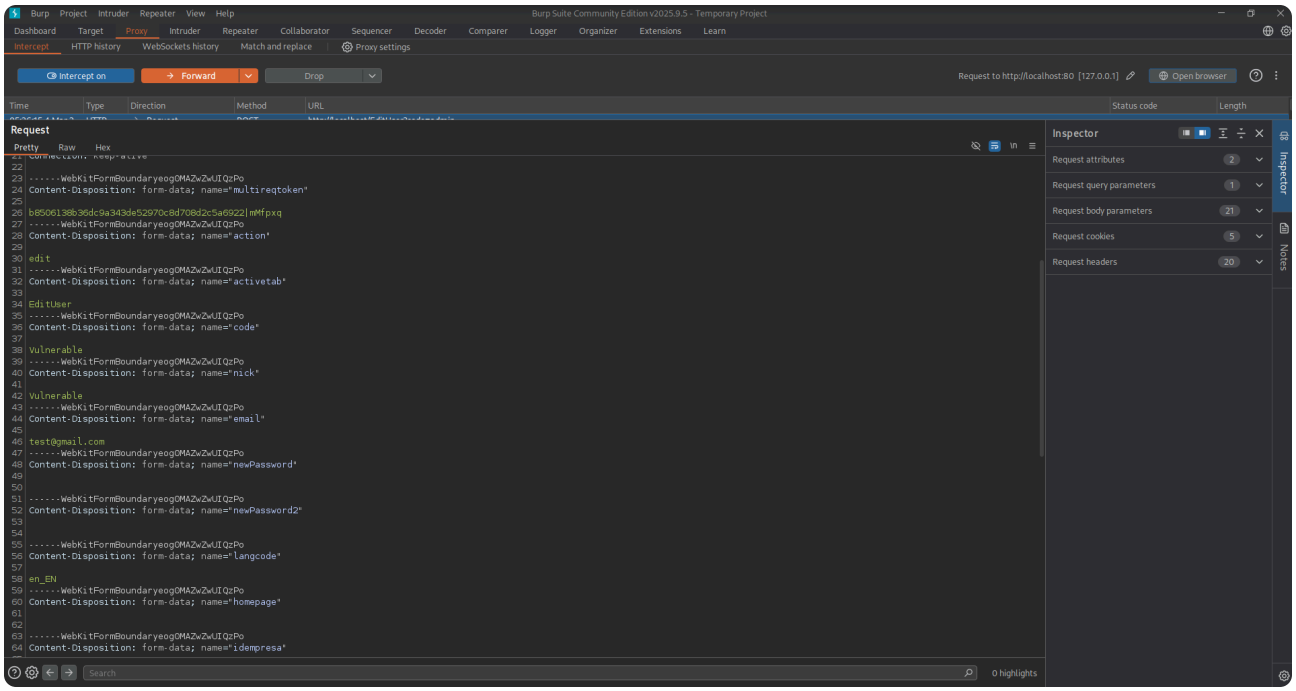
1. Log in to the dashboard as any user (e.g. admin user).

2. Go to your Profile by clicking your username/avatar in the top right.

3. Open Burp Suite and ensure Intercept is ON.

5. Click the Save button in the UI.

6. In Burp Suite, locate `nick` in the body:



7. Change the value admin to Vulnerable (or any other string).

8. Click Forward in Burp Suite.

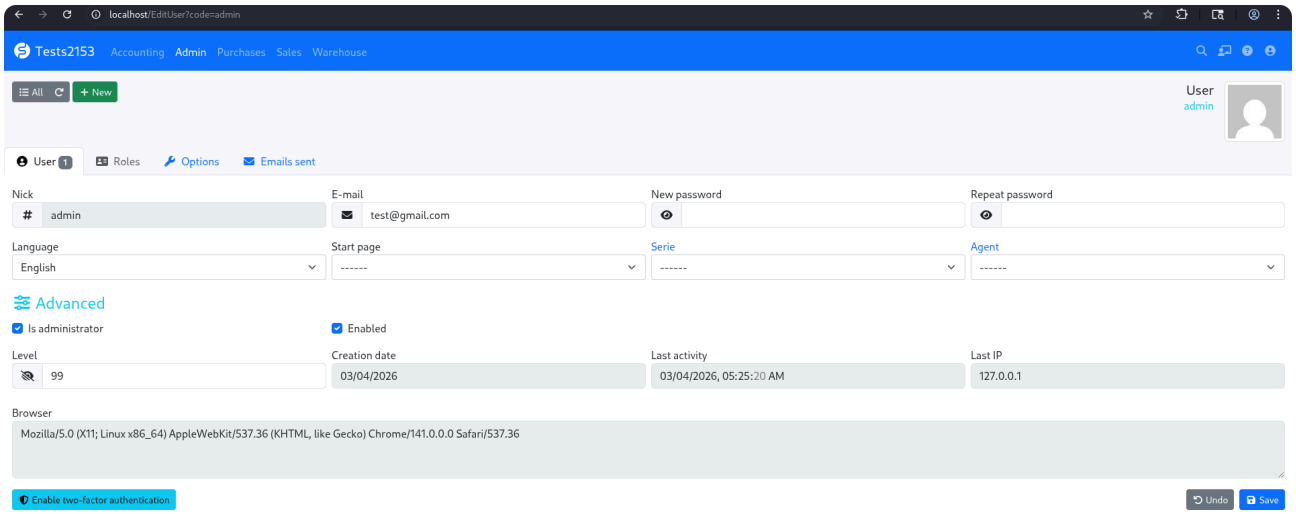
The application will log the user out. You can now log back in using the username Vulnerable and the original password.

Impact

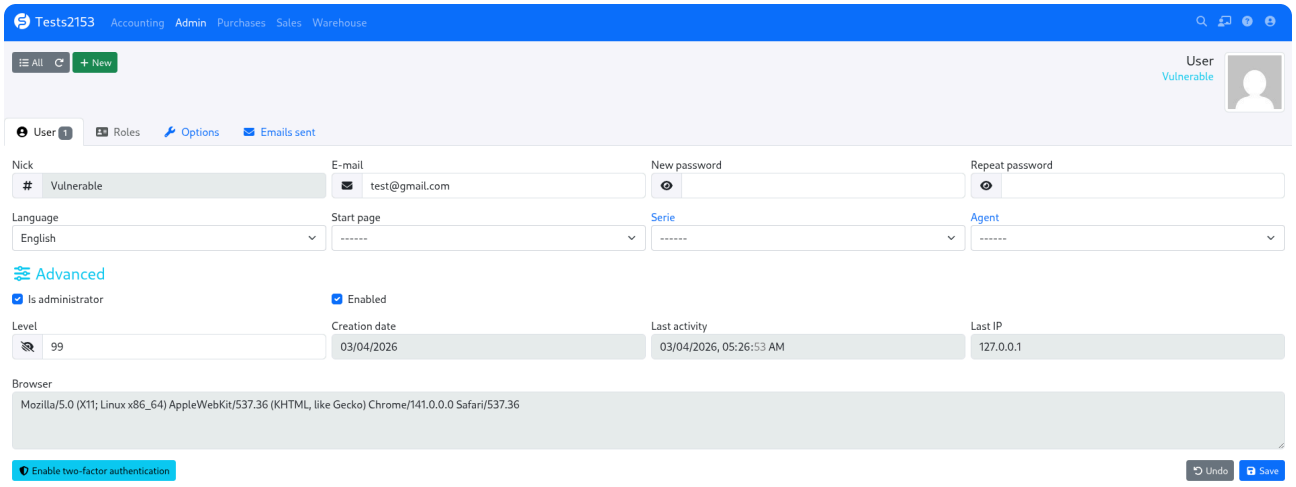
An attacker can effectively sabotage the system's audit trail, performing malicious actions and then renaming their account to evade detection or frame other users. This breakdown in accountability facilitates identity impersonation and risks data corruption, as internal references to the original username become orphaned, undermining the overall integrity of the multi-user environment.

Result

Before



After



Severity

Moderate 4.3 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None

Scope	Unchanged
Confidentiality	None
Integrity	Low
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

CVE ID

CVE-2026-32699

Weaknesses

▶ CWE-284

Credits

TurkiOS Reporter