security: block no-permission users + fix IDOR on person API #8616

Merged DawoudIO merged 12 commits into `master` from `fix/revert-person-api-idor` last week

DawoudIO commented last week • edited

Contributor

Summary

Reverts the overly-restrictive PR #8611 and implements the correct IDOR fix with a comprehensive approach to blocking users who have no functional admin permissions.

Problem

1. **IDOR (GHSA-5w59-32c8-933v)**: Any authenticated user could read any person record via `GET /api/person/{id}` — the API had no authorization check
2. **No-permission users**: Users with only `EditSelf=1` (and all other permissions at 0) could log in and see the full admin UI, including all member data, groups, events, and finance menus
3. **PR** security: add auth middleware to person API routes #8611 **was too restrictive**: It required `EditRecords` for all person API access, blocking `EditSelf` users from even their own records

Changes

IDOR Fix

- `src/api/routes/people/people-person.php` — Add inline `canEditPerson()` check on `GET /api/person/{id}`:
  - `EditRecords` users: can view any person
  - `EditSelf` users: can only view own record + family members
  - Others: 403 Forbidden

No-Permission User Block

- `src/ChurchCRM/model/ChurchCRM/User.php` — Add `hasNoAdminPermissions()` method that detects users with no functional permissions (all of AddRecords, EditRecords, DeleteRecords, MenuOptions, ManageGroups, Finance, Notes = 0)
- `src/ChurchCRM/Slim/Middleware/AuthMiddleware.php` — Block in both code paths:
  - **API key auth**: Return 403 JSON
  - **Session auth (MVC pages)**: Redirect to `/external/limited-access`
- `src/Include/PageInit.php` — Block on legacy PHP pages: redirect to `/external/limited-access`

Limited Access Page

- `src/external/routes/system.php` — New route `GET /external/limited-access`
- `src/external/templates/limited-access.php` — Tabler-styled welcome page with:
  - **Verify Family Info** button (generates time-limited token for user's family)
  - **Log Out** button
  - Matches login page styling (no admin chrome)

Test Infrastructure

- `cypress/data/seed.sql` — Add `limited.user` test user (person ID 4, family 2, EditSelf=1 only)
- `cypress/e2e/ui/security/limited-access.spec.js` — 6 tests:
  - Login redirects to `/external/limited-access`
  - Shows Verify + Logout buttons
  - Verify link goes to `/external/verify/{token}`
  - Logout returns to login page
  - Direct dashboard visit redirects to limited-access
  - API call with limited user key returns 403

Security Model

User Type	Web UI	API	Person API GET
Admin	Full access	Full access	Any person
EditRecords	Full access	Full access	Any person
EditSelf + other perms	Full access	Full access	Own record + family
EditSelf only (no other perms)	→ Limited access page	403	403
No permissions at all	→ Limited access page	403	403

Risk Assessment

Users affected: Any user with `usr_EditSelf=1` and all other permission flags at 0. These users will now see a "Welcome" page with family verification instead of the full admin UI. This is intentional — they previously had unauthorized access to all member data.

Test plan

- [ ] Admin user: full access (unchanged)
- [ ] `limited.user` login → sees limited-access page with Verify + Logout
- [ ] `limited.user` clicks Verify → sees family verification for their family only
- [ ] `limited.user` clicks Logout → returns to login
- [ ] `limited.user` tries `/v2/dashboard` → redirected to limited-access
- [ ] `limited.user` API call → 403
- [ ] Run `npx cypress run --spec cypress/e2e/ui/security/limited-access.spec.js`
- [ ] All existing Cypress tests pass (admin users unaffected)

Related

- Reverts: **security: add auth middleware to person API routes** #8611
- Advisory: GHSA-5w59-32c8-933v
- Follow-up: **Redesign EditSelf permission: proper self-service portal** #8617 (EditSelf redesign for self-service portal)

🤖 Generated with Claude Code

`Revert "security: add auth middleware to person API routes (#8611)"` ··· ✕ `852677e`

DawoudIO added this to the **7.2.0** milestone last week

Copilot AI review requested due to automatic review settings last week

DawoudIO requested a review from **a team** as a code owner last week

DawoudIO requested review from **DAcodedBEAT**, **MrClever**, **bigtigerku**, **grayeul** and **respencer** and removed request for **a team** last week

Copilot started reviewing on behalf of **DawoudIO** last week

View session

`security: add canEditPerson() IDOR check to GET /api/person/{id}` ··· ✓ `a71ba1e`

Copilot AI reviewed last week

View reviewed changes

Copilot AI left a comment

Contributor

Pull request overview

Reverts the authorization middleware previously added to `GET /api/person/{personId}`, restoring the route to its prior behavior.

Changes:

- Removes `EditRecordsRoleAuthMiddleware` from the `GET /person/{personId}` handler.
- Updates the inline comment to no longer state an EditRecords requirement.

`src/api/routes/people/people-person.php` Show resolved

DawoudIO mentioned this pull request last week

Redesign EditSelf permission: proper self-service portal #8617

Closed

DawoudIO added the Security label last week

DawoudIO and others added 3 commits last week

`Update README.md` `0ec7095`

`Merge remote-tracking branch 'origin/master' into fix/revert-person-a…` ··· `816bfa8`

`security: block EditSelf-only users + add canEditPerson IDOR check` ··· ✗ `37c0360`

DawoudIO changed the title **Revert: security: add auth middleware to person API routes (#8611) security: fix IDOR on person API + block EditSelf-only users** last week

DawoudIO and others added 3 commits last week

`Merge branch 'master' into fix/revert-person-api-idor` ✓ `dc9d633`

`fix: block no-permission users from both legacy pages AND MVC routes` ··· ✓ `b7a88b5`

`security: add /external/limited-access page for no-permission users` ··· ✗ `18b1efe`

DawoudIO changed the title **security: fix IDOR on person API + block EditSelf-only users security: block no-permission users + fix IDOR on person API** last week

`Merge branch 'master' into fix/revert-person-api-idor` ✗ `6d84f3e`

DawoudIO mentioned this pull request last week

fix: improve family verify page UX — replace broken FAB, add navigation #8620

Merged

8 tasks

DawoudIO requested a review from **Copilot** last week

Copilot started reviewing on behalf of **DawoudIO** last week

View session

DawoudIO mentioned this pull request last week

User limited only to self editing #237

Closed

Copilot AI reviewed last week

View reviewed changes

Copilot AI left a comment

Contributor

Pull request overview

Copilot reviewed 9 out of 9 changed files in this pull request and generated 7 comments.

src/ChurchCRM/model/ChurchCRM/User.php — Show resolved

src/ChurchCRM/model/ChurchCRM/User.php — Show resolved

src/external/routes/system.php — Show resolved

src/external/routes/system.php — Show resolved

src/ChurchCRM/Slim/Middleware/AuthMiddleware.php — Show resolved

locale/README.md — Show resolved

locale/README.md — Show resolved

 `fix: verify link test — assert family name instead of page title` ··· ✕ `3c17025`

claude added 2 commits last week

 `Merge master into fix/revert-person-api-idor` `17acfd0`

 `fix: correct family name assertion and use relative paths in limited-…` ··· ✓ `a80d6b6`

 **DawoudIO** merged commit **28ea7a2** into `master` last week

18 checks passed

View details

 **DawoudIO** deleted the `fix/revert-person-api-idor` branch last week

Reviewers

- **Copilot**
- **respencer**
- **grayeul**
- **DAcodedBEAT**
- **MrClever**
- **bigtigerku**

Assignees

No one assigned

Labels

Security

Projects

None yet

Milestone

7.2.0

Development

Successfully merging this pull request may close these issues.

None yet

3 participants