# AutoRules Report

Generated: 04/10/2025, 18:40:34 | Model: openai/gpt-oss-120b | Workers: 10 | Duration: 21s | Tokens: 19,688 | Cost: $0.0079

| 148 | 145 | 3 | 1 |
|---|---|---|---|
| Total Files | Passed | Failed | Rules |

## Rule Summaries

| Rule | Status | Files Checked |
|---|---|---|
| ▼ **Never send the users password to the server** | FAILED | 145/148 passed |

### Rule: “Never send the user’s password to the server”

#### Scope

- **Project type:** Zero-knowledge OAuth/OIDC – the user’s password and derived private keys must never be transmitted to the back-end, except when a private key is wrapped/enveloped with a key that the server does not know.

#### Overall Outcome

| Status | Number of Files |
|---|---|
| PASSED | 145 |
| FAILED | 3 |
| TOTAL | 148 |

All but three source files satisfy the rule according to the automated check.

---

## Files that FAILED

| File | Why it failed (summary) |
|---|---|
| `src/http/proxy.ts` | Acts as a thin proxy that pipes **all** incoming HTTP and WebSocket traffic directly to the Vite dev server ( `request.pipe(proxyRequest)` ). It does **no inspection, validation, or transformation** of request bodies or headers. Consequently, any password or private-key material sent by a client will be forwarded unchanged to the downstream server, violating the “never send password” rule. |
| `src/http/routers/adminRouter.ts` | Exposes a number of admin endpoints that accept raw password data (e.g., `POST /admin/password/change/start` , `POST /admin/users/:id/password/reset` , etc.). The router simply forwards the request to the controller without any client-side encryption, OPAQUE processing, or wrapping of private keys. Hence the router can allow clear-text passwords (or unwrapped private keys) to be sent to the server. |
| `src/http/routers/userRouter.ts` | Similar to the admin router, this router defines routes for password-change and password-verification flows ( `POST /password/change/start` , `.../finish` , `.../verify/start` , `.../verify/finish` ). The request bodies are passed straight to controller functions with **no evidence** that the password is transformed (e.g., encrypted, zero-knowledge |

| Rule | Status | Files Checked |
|---|---|---|

| File | Why it failed (summary) |
|---|---|
| | proof, PAKE). This means the user's password is likely being transmitted to the server in clear text, breaching the zero-knowledge requirement. |

*No other files were flagged as sending passwords or private keys to the server.*

---

## Files that PASSED

- **145 files** including utilities ( `jwk.ts` , `pkce.ts` , `crypto.ts` , `csrf.ts` , ...), models, services, controllers, and most routers.
- The pass verdict indicates that these files **do not contain code that directly forwards raw passwords or unwrapped private-key material** to the server, or they implement proper wrapping/enveloping where required.
- Notably, all **controller implementations** (e.g., `wrappedEncPrivGet.ts` , `opaqueRegisterStart.ts` , `opaqueLoginFinish.ts` , etc.) were marked as passing, suggesting they handle data in a zero-knowledge-compatible manner (e.g., using OPAQUE or wrapped keys). The failures are limited to the **router/proxy layers**, which act as pass-through mechanisms.

---

## Key Facts

1. **Only three files breach the rule** – a proxy that blindly forwards traffic and two routers that expose password-handling endpoints without client-side protection.
2. **No evidence** was found in the scanned files of **private-key material being sent unwrapped** to the server. The failures focus solely on password transmission.
3. The vast majority of the codebase (145 files) complies with the zero-knowledge requirement, indicating that the core logic (OPAQUE flows, wrapped key handling, etc.) respects the rule.
4. The identified problematic files are part of the **transport layer** (proxy & routing) rather than the business-logic layer, which may explain why they were missed by the higher-level controllers.

---

### Bottom Line

- **Compliance:** 97.97 % (145/148) of the codebase adheres to the "never send the user's password to the server" rule.
- **Violations:** 2.03 % (3/148) of the codebase contains components that could forward raw passwords (or unwrapped private keys) to the server, specifically the generic proxy and two routers.

These are the only areas where the rule is not satisfied; all other modules pass the automated check.

## File Details

| File | Status | Rules Checked |
|---|---|---|
| ▶ src/utils/jwk.ts | PASSED | 1 rule |
| ▶ src/utils/pagination.ts | PASSED | 1 rule |
| ▶ src/errors.ts | PASSED | 1 rule |
| ▶ src/utils/pkce.ts | PASSED | 1 rule |
| ▶ src/utils/totp.ts | PASSED | 1 rule |
| ▶ src/utils/security.ts | PASSED | 1 rule |
| ▶ src/createServer.ts | PASSED | 1 rule |
| ▶ src/utils/jwk.test.ts | PASSED | 1 rule |

| File | Status | Rules Checked |
|---|---|---|
| src/types.ts | PASSED | 1 rule |
| src/utils/csrf.ts | PASSED | 1 rule |
| src/utils/crypto.ts | PASSED | 1 rule |
| src/services/zkDelivery.test.ts | PASSED | 1 rule |
| src/main.ts | PASSED | 1 rule |
| src/services/settings.ts | PASSED | 1 rule |
| src/utils/csrf.test.ts | PASSED | 1 rule |
| src/utils/http.ts | PASSED | 1 rule |
| src/services/zkDelivery.ts | PASSED | 1 rule |
| src/utils/auditWrapper.ts | PASSED | 1 rule |
| src/services/opaqueState.ts | PASSED | 1 rule |
| src/services/sessions.ts | PASSED | 1 rule |
| src/services/branding.ts | PASSED | 1 rule |
| src/models/wrappedRootKeys.ts | PASSED | 1 rule |
| src/models/usersDirectory.ts | PASSED | 1 rule |
| src/services/opaque.ts | PASSED | 1 rule |
| src/services/audit.ts | PASSED | 1 rule |
| src/services/jwks.ts | PASSED | 1 rule |
| src/models/userPermissions.ts | PASSED | 1 rule |
| src/models/userEncryptionKeys.ts | PASSED | 1 rule |
| src/services/kek.ts | PASSED | 1 rule |
| src/models/registration.ts | PASSED | 1 rule |
| src/models/users.ts | PASSED | 1 rule |
| src/models/settings.ts | PASSED | 1 rule |
| src/models/groupsList.ts | PASSED | 1 rule |

| File | Status | Rules Checked |
|---|---|---|
| src/models/jwks.ts | PASSED | 1 rule |
| src/models/permissions.ts | PASSED | 1 rule |
| src/models/install.ts | PASSED | 1 rule |
| src/models/clients.ts | PASSED | 1 rule |
| src/models/authCodes.ts | PASSED | 1 rule |
| src/models/passwords.ts | PASSED | 1 rule |
| src/models/otp.ts | PASSED | 1 rule |
| src/models/authorize.ts | PASSED | 1 rule |
| src/models/adminUsers.ts | PASSED | 1 rule |
| src/models/access.ts | PASSED | 1 rule |
| src/models/auditLogs.ts | PASSED | 1 rule |
| src/models/groups.ts | PASSED | 1 rule |
| src/models/adminPasswords.ts | PASSED | 1 rule |
| src/http/openapi-helpers.ts | PASSED | 1 rule |
| src/lib/secureLogger.ts | PASSED | 1 rule |
| src/middleware/rateLimit.ts | PASSED | 1 rule |
| src/db/pglite.ts | PASSED | 1 rule |
| src/db/schema.ts | PASSED | 1 rule |
| src/http/openapi.ts | PASSED | 1 rule |
| src/config/loadConfig.ts | PASSED | 1 rule |
| src/db/drizzle.ts | PASSED | 1 rule |
| src/context/createContext.ts | PASSED | 1 rule |
| src/http/createServer.ts | PASSED | 1 rule |
| src/config/saveConfig.ts | PASSED | 1 rule |
| src/db/migrate.ts | PASSED | 1 rule |

| File | Status | Rules Checked |
|---|---|---|
| src/http/routers/installRouter.ts | PASSED | 1 rule |
| src/http/proxy.ts | FAILED | 1 rule |
| src/controllers/user/wrappedEncPrivGet.ts | PASSED | 1 rule |
| src/controllers/user/wrappedEncPrivPut.ts | PASSED | 1 rule |
| src/controllers/user/wrappedDrkPut.ts | PASSED | 1 rule |
| src/lib/opaque/opaque-ts-wrapper.ts | PASSED | 1 rule |
| src/http/routers/adminRouter.ts | FAILED | 1 rule |
| src/controllers/user/wrappedDrk.ts | PASSED | 1 rule |
| src/http/routers/userRouter.ts | FAILED | 1 rule |
| src/controllers/user/wellKnownJwks.ts | PASSED | 1 rule |
| src/controllers/user/refreshToken.ts | PASSED | 1 rule |
| src/controllers/user/session.ts | PASSED | 1 rule |
| src/controllers/user/wellKnownOpenid.ts | PASSED | 1 rule |
| src/controllers/user/usersDirectory.ts | PASSED | 1 rule |
| src/controllers/user/token.ts | PASSED | 1 rule |
| src/controllers/user/passwordChangeVerifyStart.ts | PASSED | 1 rule |
| src/controllers/user/otpStatus.ts | PASSED | 1 rule |
| src/controllers/user/passwordChangeStart.ts | PASSED | 1 rule |
| src/controllers/user/passwordChangeFinish.ts | PASSED | 1 rule |
| src/controllers/user/otpSetupInit.ts | PASSED | 1 rule |
| src/controllers/user/otpVerify.ts | PASSED | 1 rule |
| src/controllers/user/otpSetupVerify.ts | PASSED | 1 rule |
| src/controllers/user/passwordChangeVerifyFinish.ts | PASSED | 1 rule |
| src/controllers/user/opaqueRegisterStart.ts | PASSED | 1 rule |
| src/controllers/user/opaqueRegisterFinish.ts | PASSED | 1 rule |

| File | Status | Rules Checked |
|---|---|---|
| src/controllers/user/encPublicGet.ts | PASSED | 1 rule |
| src/controllers/user/opaqueLoginFinish.ts | PASSED | 1 rule |
| src/controllers/user/encPublicPut.ts | PASSED | 1 rule |
| src/controllers/user/getUserApps.ts | PASSED | 1 rule |
| src/controllers/user/opaqueLoginStart.ts | PASSED | 1 rule |
| src/controllers/user/opaqueLoginFinish.test.ts | PASSED | 1 rule |
| src/controllers/user/logout.ts | PASSED | 1 rule |
| src/controllers/user/authorizeFinalize.ts | PASSED | 1 rule |
| src/controllers/user/authorize.ts | PASSED | 1 rule |
| src/controllers/user/otpReauth.ts | PASSED | 1 rule |
| src/controllers/admin/users.ts | PASSED | 1 rule |
| src/controllers/admin/userPermissions.ts | PASSED | 1 rule |
| src/controllers/install/opaqueRegisterFinish.ts | PASSED | 1 rule |
| src/controllers/install/postInstallComplete.ts | PASSED | 1 rule |
| src/controllers/install/getInstall.ts | PASSED | 1 rule |
| src/controllers/install/opaqueRegisterStart.ts | PASSED | 1 rule |
| src/controllers/admin/userOtpUnlock.ts | PASSED | 1 rule |
| src/controllers/admin/userUpdate.ts | PASSED | 1 rule |
| src/controllers/admin/userPasswordSetStart.ts | PASSED | 1 rule |
| src/controllers/admin/userPasswordSetFinish.ts | PASSED | 1 rule |
| src/controllers/admin/userOtp.ts | PASSED | 1 rule |
| src/controllers/admin/userGroupsUpdate.ts | PASSED | 1 rule |
| src/controllers/admin/userGroups.ts | PASSED | 1 rule |
| src/controllers/admin/userPasswordReset.ts | PASSED | 1 rule |
| src/controllers/admin/userOtpDelete.ts | PASSED | 1 rule |

| File | Status | Rules Checked |
|---|---|---|
| src/controllers/admin/settingsUpdate.ts | PASSED | 1 rule |
| src/controllers/admin/userPermissionsUpdate.ts | PASSED | 1 rule |
| src/controllers/admin/userDelete.ts | PASSED | 1 rule |
| src/controllers/admin/userCreate.ts | PASSED | 1 rule |
| src/controllers/admin/settings.ts | PASSED | 1 rule |
| src/controllers/admin/session.ts | PASSED | 1 rule |
| src/controllers/admin/permissionCreate.ts | PASSED | 1 rule |
| src/controllers/admin/passwordChangeStart.ts | PASSED | 1 rule |
| src/controllers/admin/otp.ts | PASSED | 1 rule |
| src/controllers/admin/permissions.ts | PASSED | 1 rule |
| src/controllers/admin/permissionDelete.ts | PASSED | 1 rule |
| src/controllers/admin/refreshToken.ts | PASSED | 1 rule |
| src/controllers/admin/passwordChangeFinish.ts | PASSED | 1 rule |
| src/controllers/admin/opaqueLoginStart.ts | PASSED | 1 rule |
| src/controllers/admin/opaqueLoginFinish.ts | PASSED | 1 rule |
| src/controllers/admin/groupUsers.ts | PASSED | 1 rule |
| src/controllers/admin/jwks.ts | PASSED | 1 rule |
| src/controllers/admin/logout.ts | PASSED | 1 rule |
| src/controllers/admin/jwksRotate.ts | PASSED | 1 rule |
| src/controllers/admin/groupUsersUpdate.ts | PASSED | 1 rule |
| src/controllers/admin/groups.ts | PASSED | 1 rule |
| src/controllers/admin/groupDelete.ts | PASSED | 1 rule |
| src/controllers/admin/opaqueLoginFinish.test.ts | PASSED | 1 rule |
| src/controllers/admin/groupUpdate.ts | PASSED | 1 rule |
| src/controllers/admin/clientDelete.ts | PASSED | 1 rule |

| File | Status | Rules Checked |
|---|---|---|
| src/controllers/admin/clientCreate.ts | PASSED | 1 rule |
| src/controllers/admin/groupCreate.ts | PASSED | 1 rule |
| src/controllers/admin/clients.ts | PASSED | 1 rule |
| src/controllers/admin/auditLogs.ts | PASSED | 1 rule |
| src/controllers/admin/clientUpdate.ts | PASSED | 1 rule |
| src/controllers/admin/auditLogExport.ts | PASSED | 1 rule |
| src/controllers/admin/auditLogDetail.ts | PASSED | 1 rule |
| src/controllers/admin/adminUsers.ts | PASSED | 1 rule |
| src/controllers/admin/adminUserUpdate.ts | PASSED | 1 rule |
| src/controllers/admin/adminUserDelete.ts | PASSED | 1 rule |
| src/controllers/admin/adminUserPasswordReset.ts | PASSED | 1 rule |
| src/controllers/admin/adminUserPasswordSetFinish.ts | PASSED | 1 rule |
| src/controllers/admin/adminOtp.ts | PASSED | 1 rule |
| src/controllers/admin/adminUserCreate.ts | PASSED | 1 rule |
| src/controllers/admin/adminUserPasswordSetStart.ts | PASSED | 1 rule |