# Security Vulnerability Demonstration

## The Problem with Official datasette-upload-csvs

### What You'll See:

1. **\*\*Secure Upload Button (Green)\*\***: `/upload-secure/database\_name`

- ✅ Only shows the specific database you own

- ✅ Database name is in the URL path (secure)

- ✅ No dropdown with other users' databases

- ✅ Ownership verification before any action

2. **\*\*Insecure Demo Button (Red)\*\***: `/-/upload-csvs`

- ❌ Shows ALL databases in a dropdown

- ❌ User can select ANY database, including ones they don't own

- ❌ No ownership verification per database

- ❌ Major security vulnerability

### Demo Scenario:

Imagine you have these databases:

- `alice\_environmental\_data` (owned by Alice)

- `bob\_pollution\_study` (owned by Bob)

- `carol\_water\_quality` (owned by Carol)

**\*\*With Secure Upload:\*\***

- Alice clicks her secure upload button

- Goes to `/upload-secure/alice\_environmental\_data`

- Can ONLY upload to her database

- Cannot see or access Bob's or Carol's databases

**\*\*With Official Plugin (Insecure):\*\***

- Alice clicks the demo button

- Goes to `/-/upload-csvs`

- Sees a dropdown with ALL THREE databases

- Can select Bob's or Carol's databases

- Can upload malicious data to other users' databases! 🚨

### Why This is Critical:

1. **\*\*Data Integrity\*\***: Users can corrupt other users' data

2. **\*\*Privacy Violation\*\***: Users can see all database names

3. **\*\*Security Breach\*\***: No ownership verification

4. **\*\*Compliance Risk\*\***: Violates data isolation requirements

### Our Solution:

- Database-specific URLs: `/upload-secure/{database\_name}`

- Ownership verification at every step

- No exposure of other users' database names

- Secure, auditable, production-ready

## Demo Instructions for Your Team:

1. **\*\*Login as User A\*\***

2. **\*\*Click the GREEN button\*\*** → See only User A's database

3. **\*\*Click the RED button\*\*** → See ALL databases (security violation!)

4. **\*\*Try to upload to another user's database\*\*** → Should be prevented by our system

This demonstrates why we needed to build a custom solution instead of using the official plugin.