

Security Vulnerability Report – Stored XSS via CSV Import (Update Existing Records) in ERPNext / Frappe Framework

Severity: High

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

Description

A Stored Cross-Site Scripting (XSS) vulnerability was discovered within the CSV import mechanism of ERPNext when using the “Update Existing Records” option.

An attacker can embed malicious JavaScript code into a CSV field, which is then stored in the database and executed whenever the affected record is viewed by a user within the ERPNext web interface.

This exposure may allow an attacker to compromise user sessions or perform unauthorized actions under the context of a victim's account.

Affected Environment

- Repository: https://github.com/frappe/frappe_docker
- Deployment Method: Default Docker setup
- ERPNext / Frappe Version: last version on 16 - 17 Nov 2025
- Browser Used During Testing: Google chrome Version 142.0.7444.135 (Official Build) (64-bit)

Technical Details

Attack Vector:

A crafted CSV file containing specially formatted HTML/JavaScript is imported into a target Doctype or content in malicious file.

```
<script>alert(document.cookie)</script>
```

Impact:

Successful exploitation results in Stored XSS, which may lead to:

- Execution of arbitrary JavaScript in a victim's browser
- Privilege escalation through session hijacking
- Unauthorized data manipulation
- Potential takeover of administrative accounts
- Compromise of ERPNext workflows and user integrity

Proof of Concept

1. We have logged into the system.

The screenshot shows a web browser window with the URL `192.168.204.130:8080/app/user-profile`. The page is titled "Demo1". On the left, there's a sidebar with "Details" sections for Energy Points (0), Review Points (0), Rank (0), and Monthly Rank (0). Below this are links for "Edit Profile", "User Settings", and "Leaderboard". The main content area has a "Overview" section with a grid calendar for the year 2025. Below it is a "Energy Points" chart showing a single data point at 0 on the y-axis for the date 17-10-2025. At the bottom, there's a "Recent Activity" section stating "No activities to show".

2. We navigated to the application menu to be redirected to ERPNext.

The screenshot shows the ERPNext user profile page for a user named 'Demo1'. The page includes sections for 'Details' (Energy Points, Review Points, Rank, Monthly Rank), an 'Overview' calendar grid, and a 'Recent Activity' section. A context menu is open in the top right corner, listing options like 'My Profile', 'My Settings', 'Session Defaults', 'Reload', 'View Website', 'Apps', 'Toggle Full Width' (which is highlighted with a red arrow), 'Toggle Theme', and 'Log out'. A red box highlights the 'Go to ERPNext' button at the bottom of the main content area.

The screenshot shows the ERPNext app selection screen. It displays a central message 'Select an app to continue' above a logo for 'ERPNext'. Below the logo is a 'Logout' link. The background is light gray, and the overall interface is clean and modern.

3. Then we proceeded to the 'Import Data' menu.

The screenshot shows the ERPNext Home page at the URL 192.168.204.130:8080/app/home. On the left, there's a sidebar under 'PUBLIC' with various links like Home, Accounting, Buying, Selling, Stock, Assets, Manufacturing, Quality, Projects, Support, Users, Website, CRM, Tools, ERPNext Settings, Integrations, ERPNext Integrations, Build, and Hello. The 'Data Import' link is located under the 'Integrations' section. The main content area has sections for 'Your Shortcuts' (Item, Customer, Supplier, Sales Invoice) and 'Reports & Masters' (Accounting, Stock, CRM). Under 'Data Import and Settings', there are links for Import Data, Opening Invoice Creation Tool, Chart of Account Importer, Letter Head, and Email Account. At the bottom right of the main content area are 'Edit' and '+ New' buttons.

4. Add a data import.

The screenshot shows the Data Import list view at the URL 192.168.204.130:8080/app/data-import. The top navigation bar includes a search bar and a '+ Add Data Import' button, which is highlighted with a red arrow. The main interface features a filter bar with dropdowns for Assigned To, Created By, and Tags, along with 'Edit Filters' and 'Save Filter' buttons. A 'Filter Name' input field is also present. The central area displays a message: 'You haven't created a Data Import yet' with a 'Create your first Data Import' button. On the right side, there are 'List View' and 'Grid View' buttons, a 'Last Updated On' filter, and other standard list view controls.

5. Next, select the data type as *Supplier Group* and set the insertion type to *Update Existing Records*, then click *Save*.

New Data Import Not Saved

Document Type * Supplier Group

Import Type * Update Existing Records

Don't Send Emails

Save 2

1

6. We downloaded the example template to review the structure.

Supplier Group Import on 2025-11-1... Pending

Document Type * Supplier Group

Import Type * Update Existing Records

Don't Send Emails

Save

Download Template 1

Import File Attach

OR

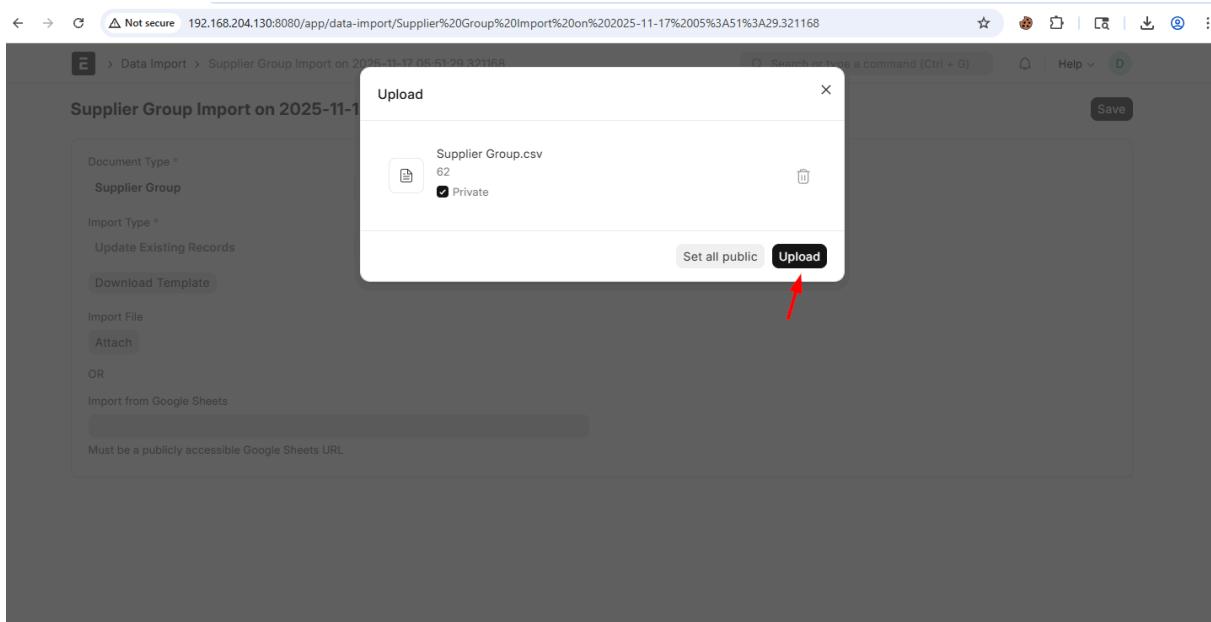
Import from Google Sheets

Must be a publicly accessible Google Sheets URL

7. We attempted to insert a malicious script (XSS) into the CSV file.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Supplier Group Name																
2	<script>alert(document.cookie)</script>																
3																	
4																	
5																	
6																	
7																	
8																	
9																	
10																	
11																	
12																	
13																	
14																	
15																	
16																	
17																	
18																	
19																	
20																	
21																	
22																	
23																	

8. Then we clicked 'Upload' and the file was successfully uploaded.



9. We clicked 'Start Import'.

The screenshot shows a web application interface for 'Supplier Group Import'. At the top, the URL is 192.168.204.130:8080/app/data-import/Supplier%20Group%20Import%20on%202025-11-17%2005%3A51%3A29.321168. The page title is 'Supplier Group Import on 2025-11-1...' with a status of 'Pending'. A red arrow points to the 'Start Import' button in the top right corner. In the 'Import File' section, there is a file input field containing the URL '/private/files/Supplier Groupd1c6f8.csv'. Below this, there is a 'Preview' section with a table mapping 'Sr. No' to 'Supplier Group Name'. The table has one row with value '2'.

10. The website executed the malicious script.

