

# Security Vulnerability Report – HTML Link Injection in ERPNext PDF Files

**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

ERPNext does not sanitize or remove certain HTML tags—specifically `<a>` hyperlinks—in fields that are intended for plain text. Although JavaScript is blocked (preventing XSS), the HTML is still preserved in the generated PDF document.

As a result, an attacker can inject malicious clickable links into an ERP-generated PDF. Since PDF files generated by the ERP system are generally considered trustworthy, users are highly likely to click these links, potentially enabling phishing attacks or malware delivery. This issue occurs in the 'Add Quality Goal' function.

## Affected Environment

- Repository: [https://github.com/frappe/frappe\\_docker](https://github.com/frappe/frappe_docker)
- Deployment Method: Default Docker setup
- ERPNext / Frappe Version: last version on 16 - 17 Nov 2025

```
        "versions": {  
            "erpnext": "15.88.1",  
            "frappe": "15.88.2"  
        },
```

- 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.

The attacker requires **only the ability to create or edit a document** in ERPNext (e.g., lower-privilege user, employee, or compromised account).

The attack flow is as follows:

1. The attacker inputs **HTML containing a malicious `<a href>` link** into a text field that does not sanitize HTML.
2. ERPNext **saves and stores the HTML** without removing or escaping it.
3. A legitimate user (e.g., manager, accountant, customer-facing staff) opens the record and exports it via **Print → PDF**.
4. The generated PDF includes a **clickable malicious link**.
5. The user or external recipient clicks the link, believing it to be part of an official ERP document.
6. The attacker redirects them to:
  - a phishing page
  - a credential-stealing website
  - a malware download
  - any external malicious resource

```
<a href="https://bcr1e3y9x4q4hlqu7qdzakc63cu0noc.oastify.com">See Informations</a>
```

### **Impact:**

- Phishing attacks through ERP-issued PDF documents
- Redirecting users to credential-harvesting pages
- Malware distribution
- Social engineering attacks targeting internal staff or external customers
- Ability to embed deceptive messages such as "Click here to verify payment"

### **Recommendation**

- Escape or sanitize HTML before generating PDF output
- Block `<a>`, `<img>`, `<iframe>` and other HTML tags in non-Rich Text fields
- Enable server-side HTML stripping on fields not intended to contain markup
- Ensure wkhtmltopdf receives only sanitized, non-executable content

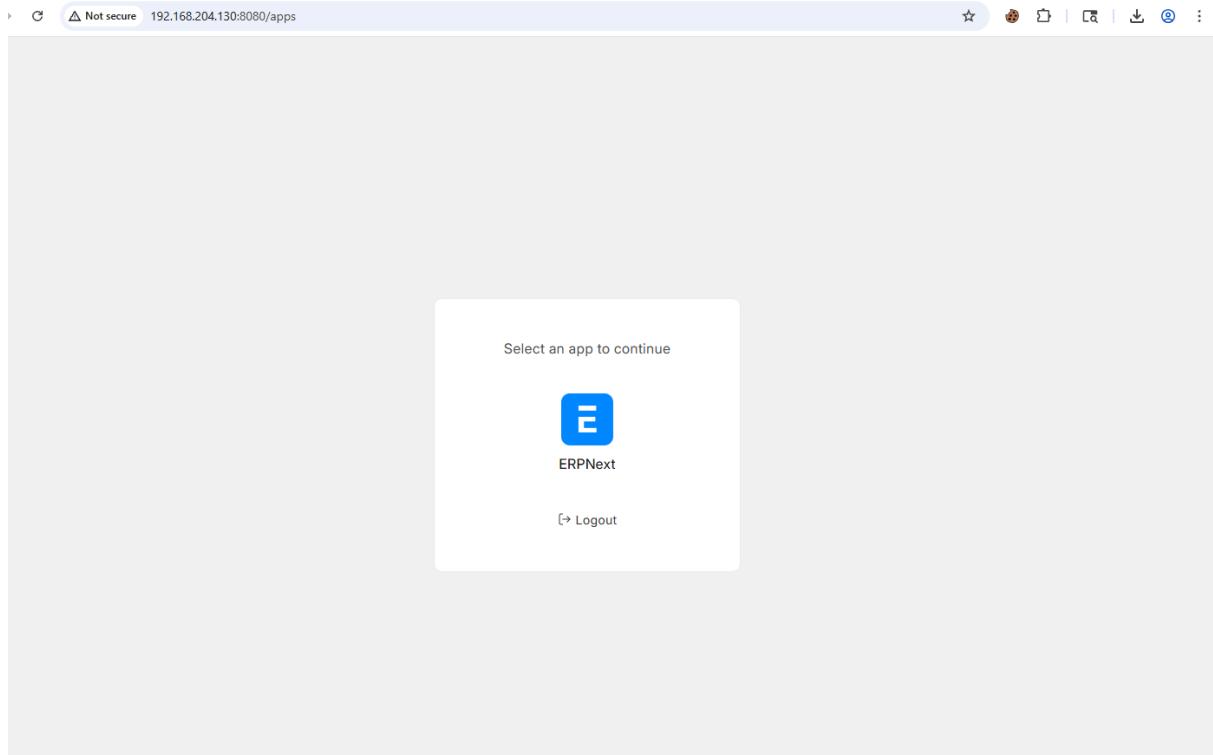
### **Proof of Concept**

1. We have logged into the system.

The screenshot shows the ERPNext user profile page at the URL `192.168.204.130:8080/app/user-profile`. The page has a header with a search bar and a 'Change User' button. On the left, there's a sidebar with a user icon and the name 'Demo1'. Below it are sections for 'Details' (Energy Points, Review Points, Rank, Monthly Rank) and links to 'Edit Profile', 'User Settings', and 'Leaderboard'. The main content area has tabs for 'Overview' and 'Energy Points'. The 'Overview' tab shows a grid calendar for the year 2025. The 'Energy Points' tab displays a line chart from October 17, 2025, to November 17, 2025. A 'Recent Activity' section below shows 'No activities to show'.

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

This screenshot is identical to the first one, but a context menu is open over the calendar grid in the 'Overview' section. The menu items include 'My Profile', 'My Settings', 'Session Defaults', 'Reload', 'View Website', 'Apps' (which is highlighted with a red arrow), 'Toggle Full Width', 'Toggle Theme', and 'Log out'. A red box highlights the 'Go to ERPNext' button at the bottom right of the calendar grid.



### 3. Then we proceeded to the 'Quality Goal' menu.

A screenshot of the ERPNext application interface. The URL is 192.168.204.130:8080/app/quality. The left sidebar shows a tree structure with categories like PUBLIC, Home, Accounting, Buying, Selling, Stock, Assets, Manufacturing, Quality (which is expanded), Projects, Support, Users, Website, CRM, Tools, ERPNext Settings, Integrations, ERPNext Integrations, Build, and Hello. A red arrow points to the "Quality" icon in the sidebar. The main content area is titled "Quality". It contains sections for "Your Shortcuts" (with links to Quality Goal, Quality Procedure, Quality Inspection, Quality Review, Quality Action, Non Conformance, and a link to "0 Open"), "Reports &amp; Masters" (with links to Quality Goal, Quality Procedure, and Tree of Procedures), "Goal and Procedure" (with links to Quality Goal, Quality Procedure, and Tree of Procedures), "Feedback" (with links to Quality Feedback and Quality Feedback Template), "Meeting" (with a link to Quality Meeting), and "Review and Action" (with links to Non Conformance, Quality Review, and Quality Action). A red arrow also points to the "Quality Goal" link under the "Goal and Procedure" section. The bottom right of the main content area has "Edit" and "+ New" buttons.

### 4. We attempted to add a Quality Goal.

The screenshot shows a list view of 'Quality Goal'. There are two entries:

ID	Monitoring Frequency	Procedure
&{document.vulnerable=true};	None	9 m · 0 ·
Demo	None	51 m · 2 ·

At the top right, there is a button labeled '+ Add Quality Goal'.

5. We attempted to insert an HTML `<a>` tag into the Objective and Target fields, and then saved the record.

The screenshot shows the 'New Quality Goal' form. The 'Goal' field is set to 'Demo02'. The 'Monitoring Frequency' is set to 'None'. In the 'Objectives' section, there is one row:

No.	Objective *	Target	UOM
1	<a>	<a href="https://bcrl3y9x4q4hlua7adzake63cu0ncc..."	UOM

The 'Save' button has a red circle with the number '3' over it.

6. We discovered that the website renders HTML tags.

The screenshot shows the 'Demo02' Quality Goal edit screen. The 'Objectives' section contains a table with one row. The first column has a checkbox, the second column is 'No.', the third is 'Objective \*', and the fourth is 'Target'. The row contains:  1 [See Informations](#) See Informations. A red box highlights the 'See Informations' link, and a red arrow points to it from below.

## Using another screen, we simulated a different user.

1. After logging in as a different user, we accessed the Quality Goal section.

The screenshot shows the Quality Goal list screen. The table has columns: ID, Monitoring Frequency, Procedure, and Last Updated On. The rows are: Demo02 (Monitoring Frequency: None, Procedure: None, Last Updated On: 2 m), &{document.vulnerable=true;}, and Demo (Monitoring Frequency: None, Procedure: None, Last Updated On: 13 m). The 'Demo02' row is highlighted with a red box.

2. Then, we clicked 'Print PDF' and observed that the PDF file rendered the HTML tags. We then attempted to click the link.

The screenshot shows a web browser window with the URL [192.168.204.130:8080/app/print/Quality%20Goal/Demo02](http://192.168.204.130:8080/app/print/Quality%20Goal/Demo02). The page title is "Demo02". On the left, there are three input fields: "Print Format", "Language" (set to "en"), and "Letter Head". The main content area is titled "Quality Goal" and displays a table with one row. The table has columns for "Sr", "Objective", and "Target". The first row contains the value "1" in the "Sr" column, "See Informations" in the "Objective" column, and "See Informations" in the "Target" column. A red arrow points to the "Objective" column.

Sr	Objective	Target
1	See Informations	See Informations

3. We found that it sent a request to a malicious website.

The screenshot shows the same web browser window as the previous one, but the URL has changed to [192.168.204.130:8080/app/print/Quality%20Goal/Demo02](http://192.168.204.130:8080/app/print/Quality%20Goal/Demo02). The "Help" button in the top right corner is highlighted with a red box. The main content area is titled "Quality Goal" and displays a table with one row. The table has columns for "Sr", "Objective", and "Target". The first row contains the value "1" in the "Sr" column, a URL "iuucyrmrlsj95xs9oy1pduezjjlgz" in the "Objective" column, and "See Informations" in the "Target" column. A red box highlights the URL in the "Objective" column.

Sr	Objective	Target
1	iuucyrmrlsj95xs9oy1pduezjjlgz	See Informations

## Collaborator:

#	Time	Type	Payload	Source IP address	Comment
6	2568 Nov-16 21:24:28.829 UTC	HTTP	3dhtfvzlywnwidvzr50247vdm1cp1	184.105.102.124	
7	2568 Nov-16 21:24:59.829 UTC	HTTP	3dhtfvzlywnwidvzr50247vdm1cp1	184.105.102.124	
8	2568 Nov-17 09:01:17.572 UTC	DNS	0gylegymulnshp3bknqwnhj3g75y/n	40.2.108.100	
9	2568 Nov-17 09:01:17.633 UTC	DNS	0gylegymulnshp3bknqwnhj3g75y/n	40.2.108.100	
10	2568 Nov-17 09:01:18.491 UTC	HTTP	0gylegymulnshp3bknqwnhj3g75y/n	184.105.102.124	
11	2568 Nov-17 09:41:32.339 UTC	DNS	bcr1e3y9k4q4hluiqu7qdakc63cu0noc	103.242.251.103	
12	2568 Nov-17 09:41:32.443 UTC	DNS	bcr1e3y9k4q4hluiqu7qdakc63cu0noc	40.2.108.100	
13	2568 Nov-17 09:41:33.376 UTC	HTTP	bcr1e3y9k4q4hluiqu7qdakc63cu0noc	184.105.102.124	
14	2568 Nov-17 09:41:48.841 UTC	HTTP	bcr1e3y9k4q4hluiqu7qdakc63cu0noc	184.105.102.124	
15	2568 Nov-17 09:41:49.758 UTC	HTTP	bcr1e3y9k4q4hluiqu7qdakc63cu0noc	184.105.102.124	
16	2568 Nov-17 09:41:49.758 UTC	HTTP	bcr1e3y9k4q4hluiqu7qdakc63cu0noc	184.105.102.124	