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

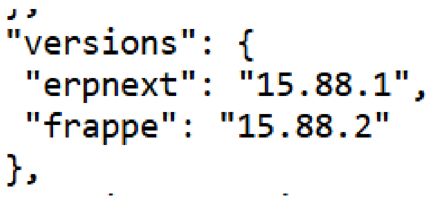
Description

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
- 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://bcr1e3y9x4q4hluqu7qdzakc63cu0noc.oastify.com">See Informations</a>
```

Impact:

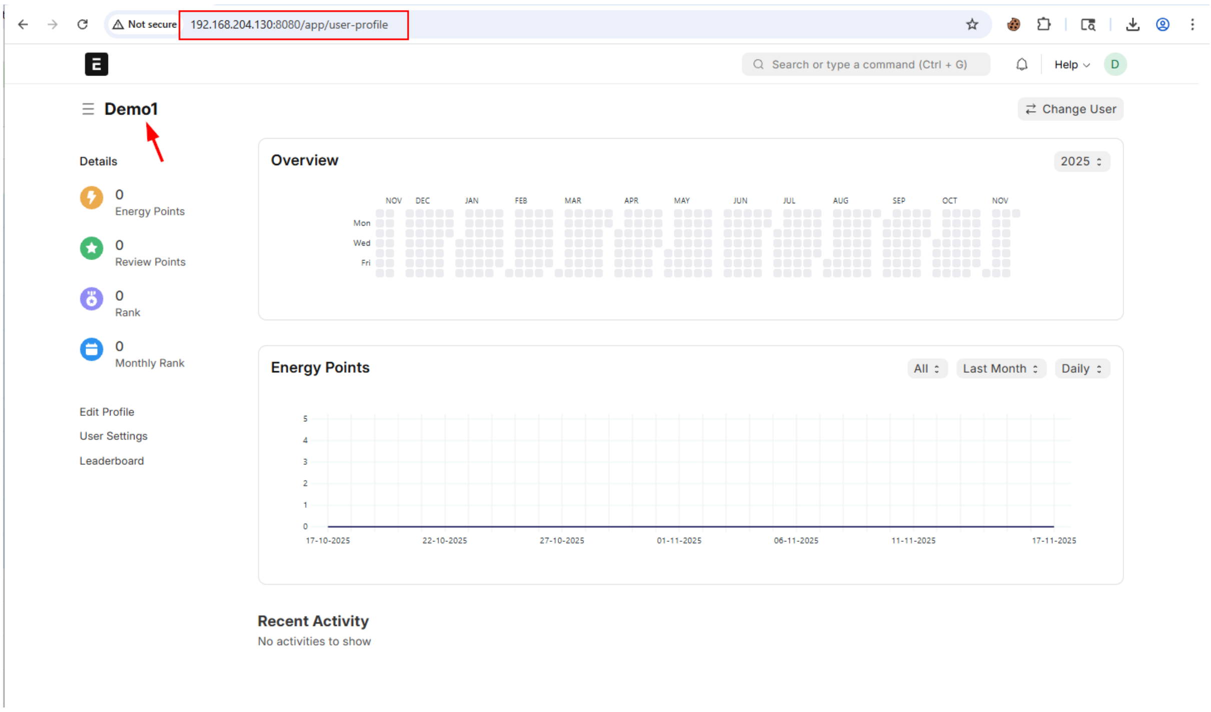
- Phishing attacks through ERP-issued PDF documents
- Redirecting users to credential-harvesting pages
- Malware distribution
- Social engineering attacks targeting internal staff or external customers
- Ability to embed deceptive messages such as “Click here to verify payment”

Recommendation

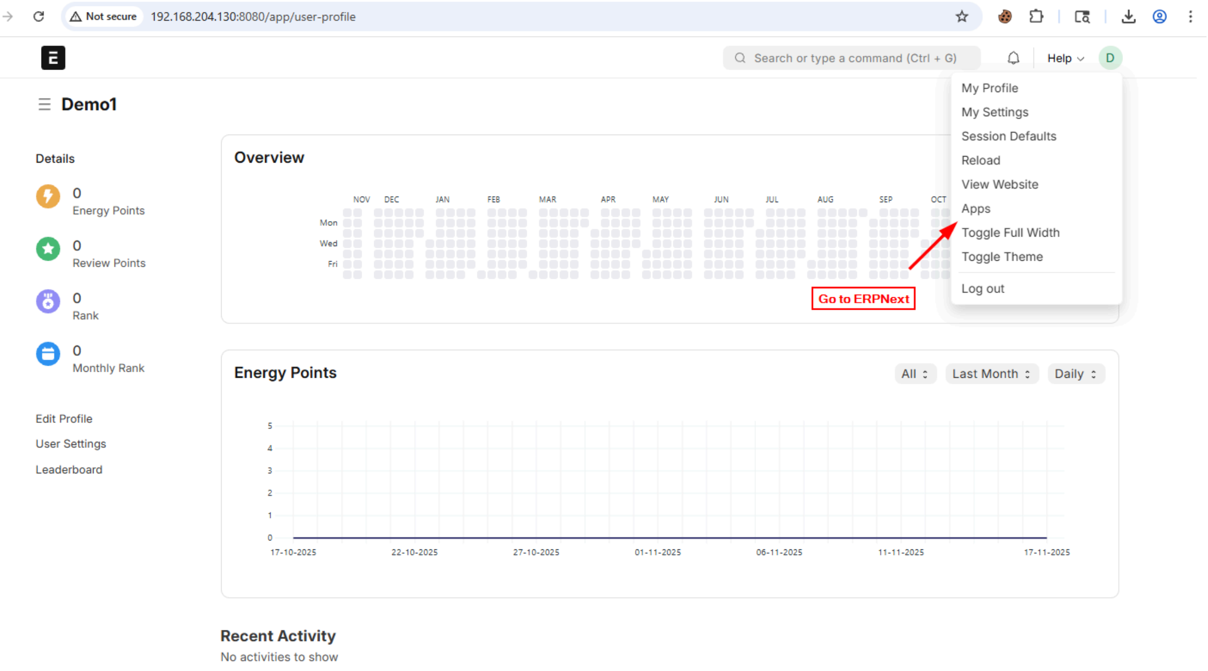
- Escape or sanitize HTML before generating PDF output
- Block `<a>`, `<img>`, `<iframe>` and other HTML tags in non–Rich Text fields
- Enable server-side HTML stripping on fields not intended to contain markup
- Ensure wkhtmltopdf receives only sanitized, non-executable content

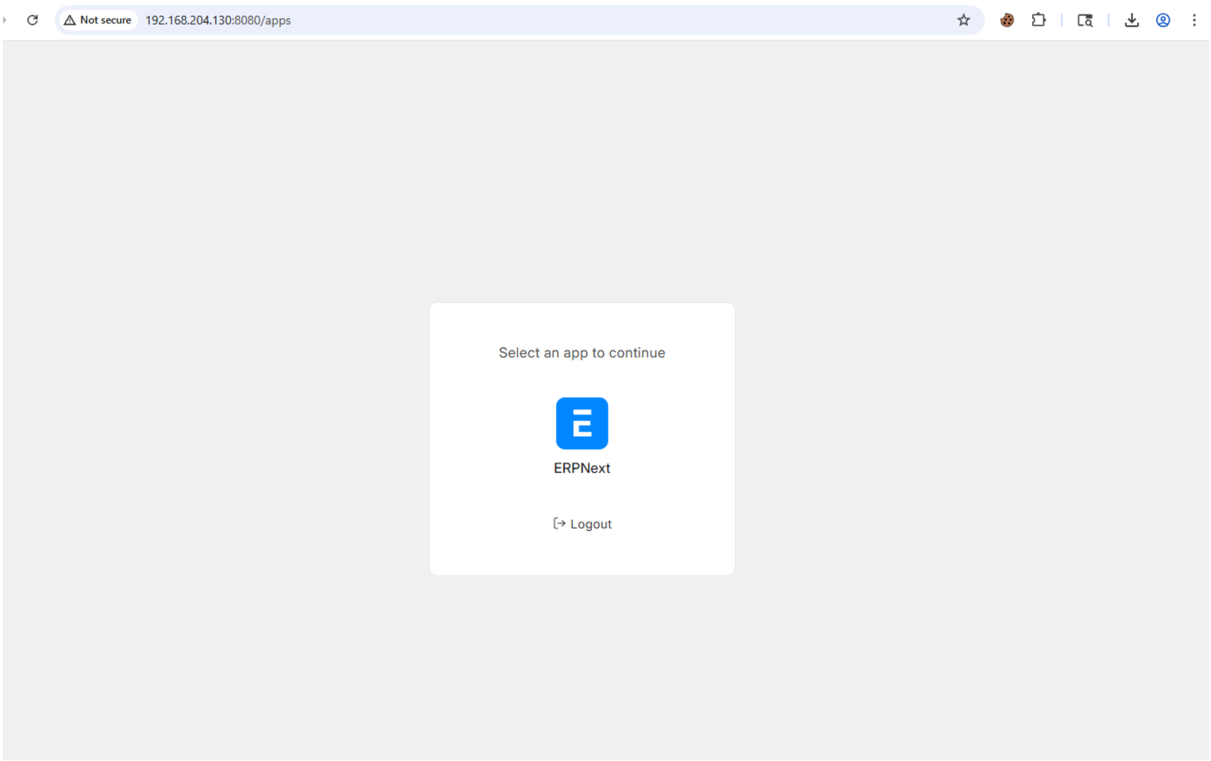
Proof of Concept

1. We have logged into the system.

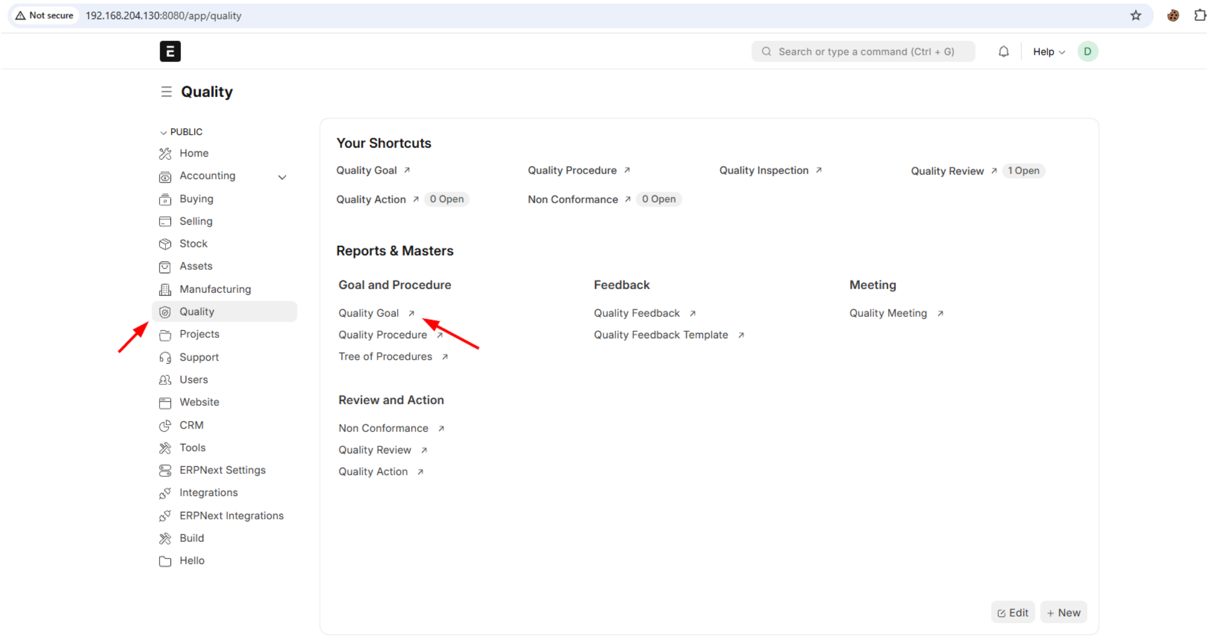


2. We navigated to the application menu to be redirected to ERPNext.

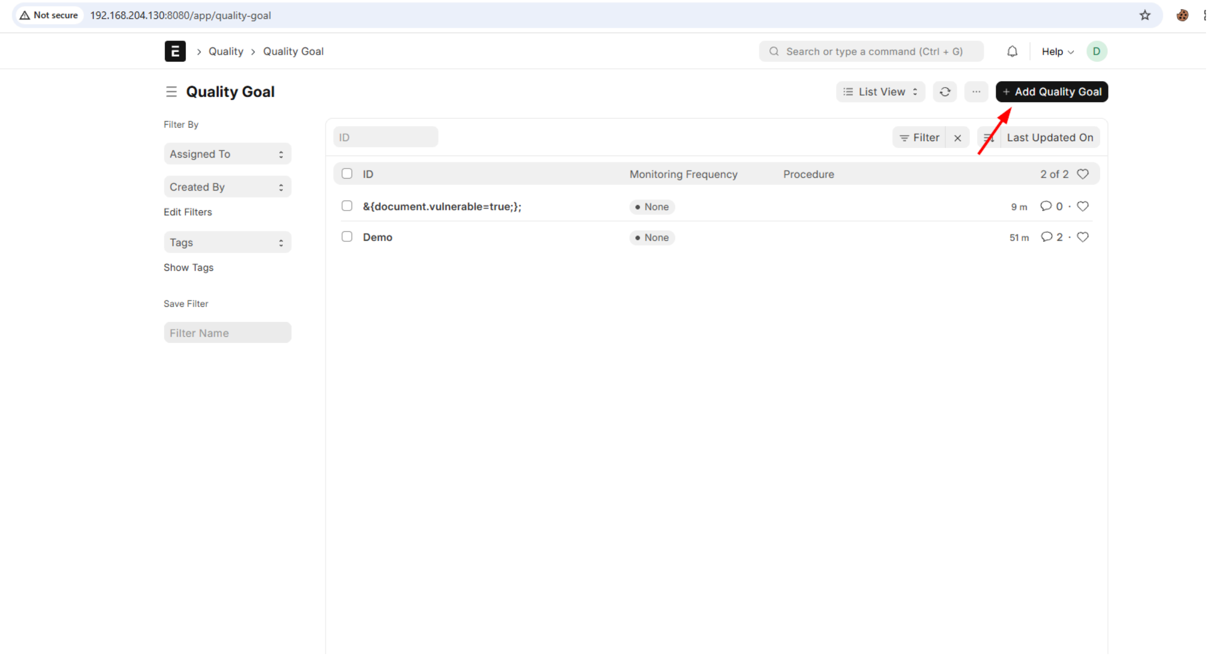




3. Then we proceeded to the ‘Quality Goal’ menu.



4. We attempted to add a Quality Goal.



Not secure 192.168.204.130:8080/app/quality-goal

Quality > Quality Goal

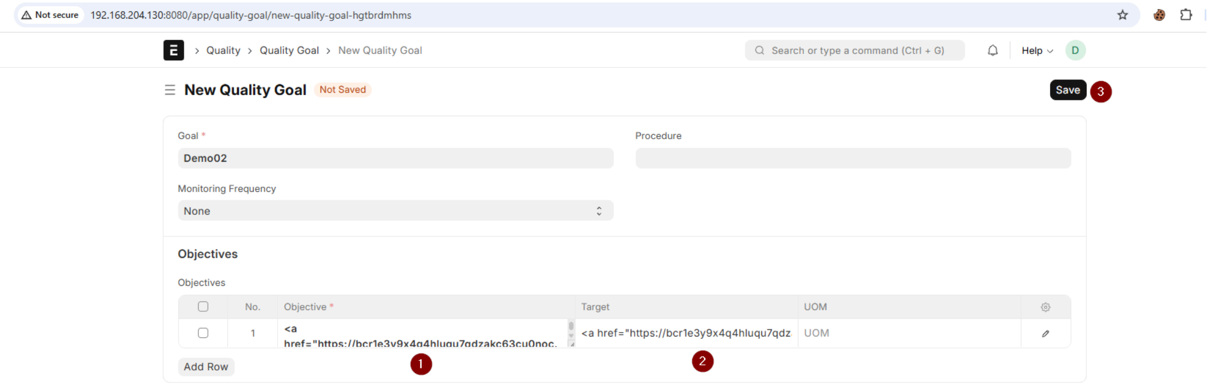
Search or type a command (Ctrl + G)

Quality Goal

Filter By

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

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



Not secure 192.168.204.130:8080/app/quality-goal/new-quality-goal-hgtbrdmhms

Quality > Quality Goal > New Quality Goal

Search or type a command (Ctrl + G)

New Quality Goal Not Saved

Goal *: Demo02

Procedure:

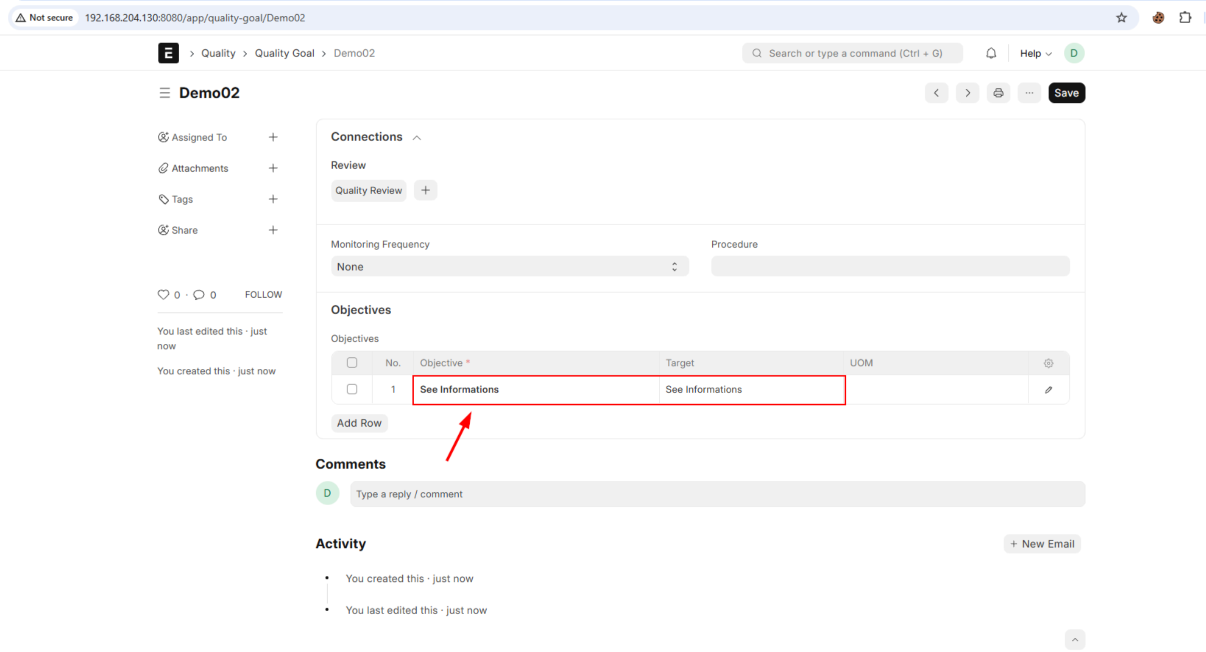
Monitoring Frequency: None

Objectives

Objectives

☐	No.	Objective *	Target	UOM
☐	1	<a href="https://bcr1e3y9x4q4hluqu7qdzakc63cu0noc.	<a href="https://bcr1e3y9x4q4hluqu7qdz	UOM

6. We discovered that the website renders HTML tags.


Not secure 192.168.204.130:8080/app/quality-goal/Demo02

Quality > Quality Goal > Demo02

Search or type a command (Ctrl + G)

Help D

Demo02

Save

Assigned To +

Attachments +

Tags +

Share +

0 · 0 FOLLOW

You last edited this · just now

You created this · just now

Connections

Review

Quality Review +

Monitoring Frequency: None

Procedure

Objectives

Objectives

	No.	Objective *	Target	UOM
□	1	See Informations	See Informations	

Add Row

Comments

D Type a reply / comment

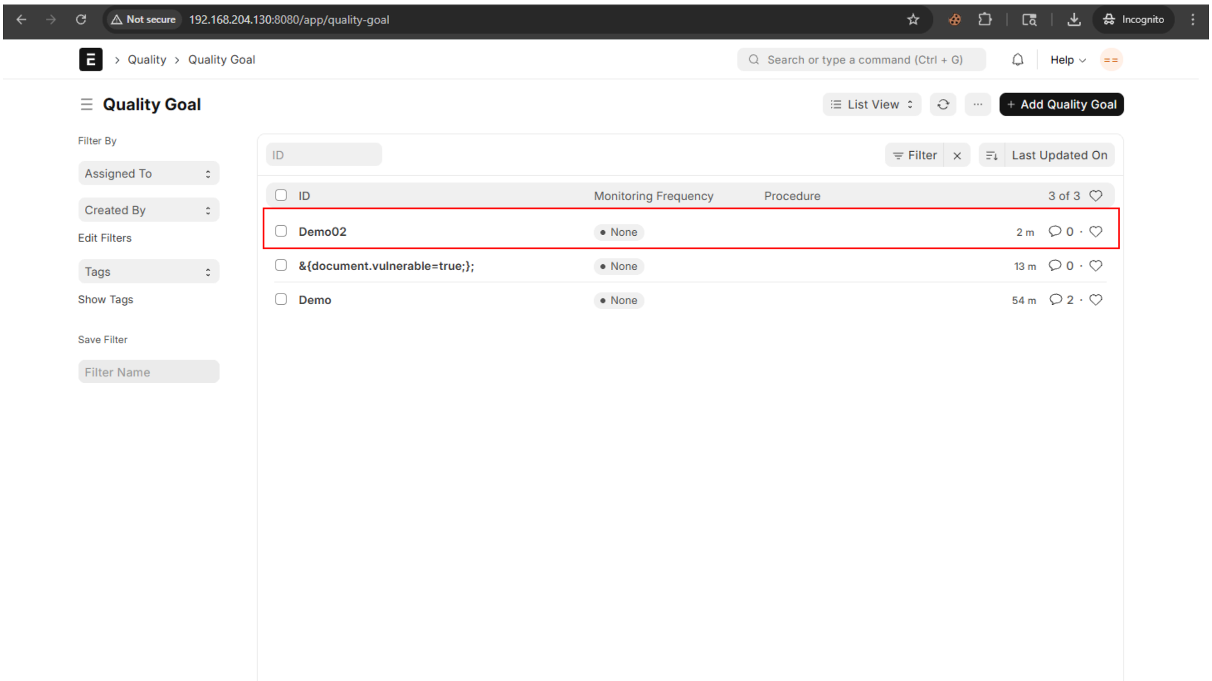
Activity

+ New Email

- You created this · just now
- You last edited this · just now

Using another screen, we simulated a different user.

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


Not secure 192.168.204.130:8080/app/quality-goal

Incognito

Quality > Quality Goal

Search or type a command (Ctrl + G)

Help

Quality Goal

List View

+ Add Quality Goal

Filter By

Assigned To

Created By

Edit Filters

Tags

Show Tags

Save Filter

Filter Name

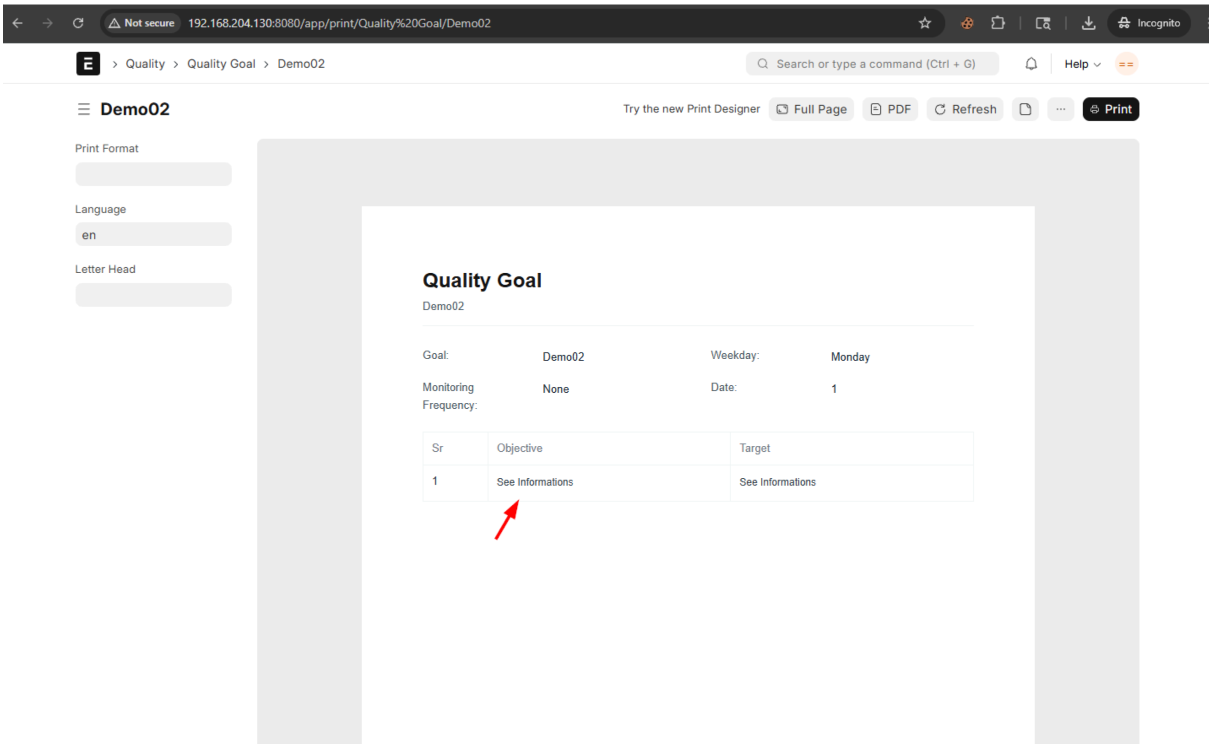
ID

Filter

Last Updated On

	ID	Monitoring Frequency	Procedure	3 of 3
□	Demo02	● None		2 m 0 ·
□	&{document.vulnerable=true;};	● None		13 m 0 ·
□	Demo	● None		54 m 2 ·

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


Not secure
192.168.204.130:8080/app/print/Quality%20Goal/Demo02
Incognito
Quality > Quality Goal > Demo02
Search or type a command (Ctrl + G)
Help
Try the new Print Designer
Full Page
PDF
Refresh
Print

Demo02

Print Format

Language: en

Letter Head

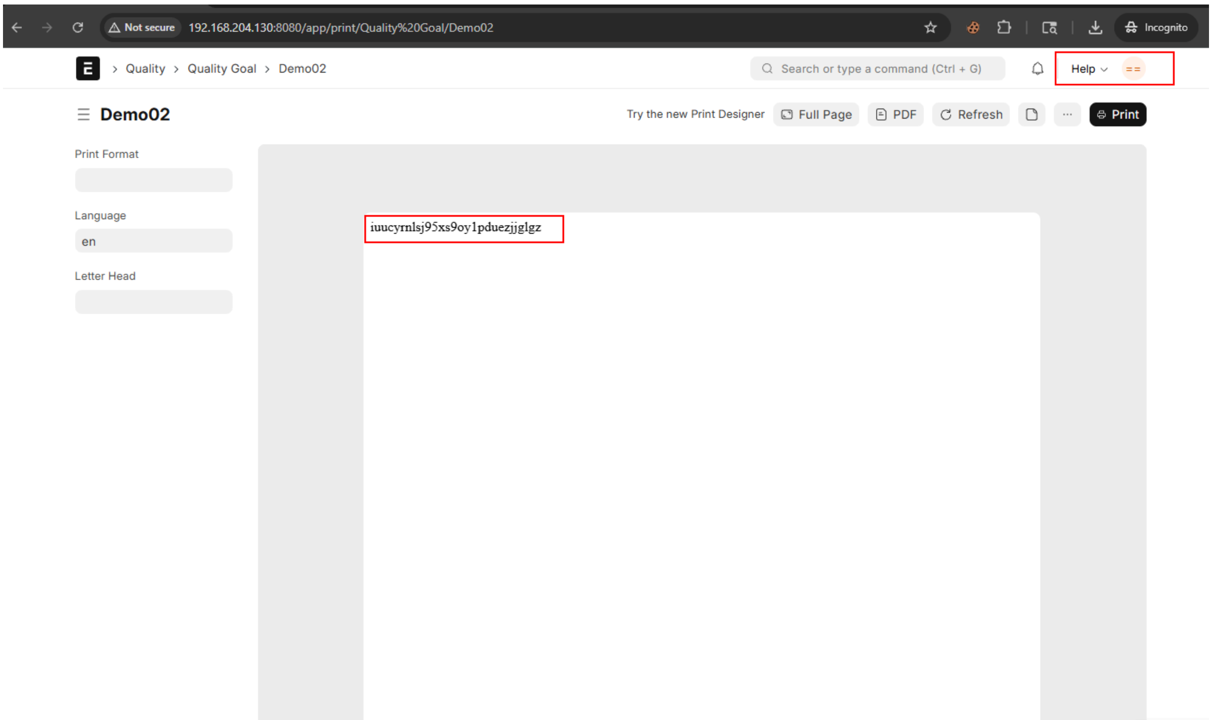
Quality Goal

Demo02

Goal:	Demo02	Weekday:	Monday
Monitoring Frequency:	None	Date:	1

Sr	Objective	Target
1	See Informations	See Informations

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


Not secure
192.168.204.130:8080/app/print/Quality%20Goal/Demo02
Incognito
Quality > Quality Goal > Demo02
Search or type a command (Ctrl + G)
Help
Try the new Print Designer
Full Page
PDF
Refresh
Print

Demo02

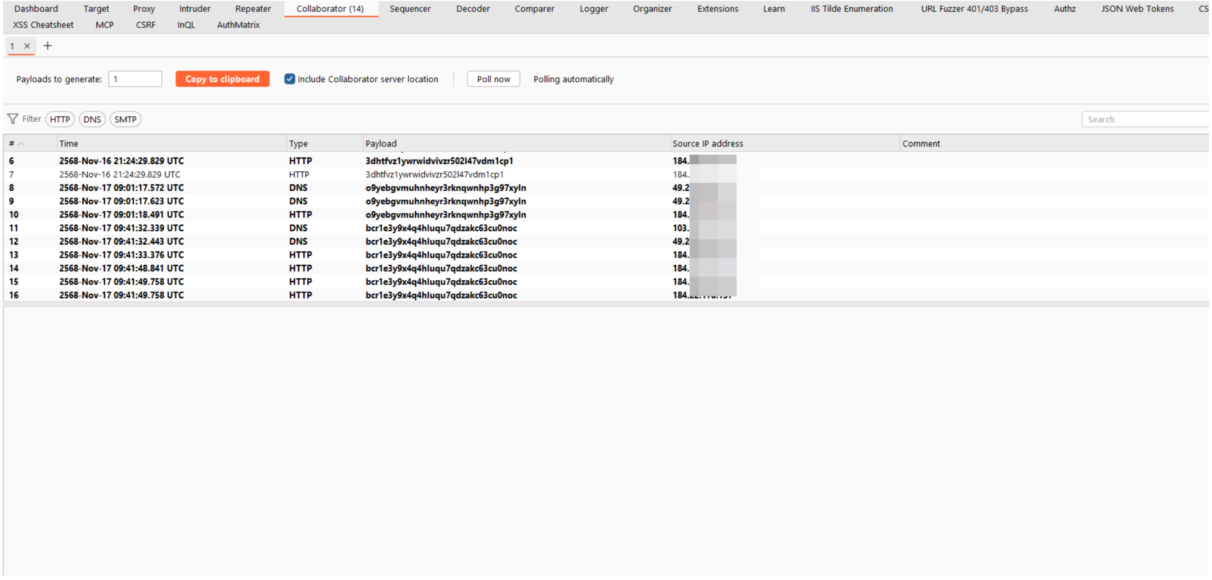
Print Format

Language: en

Letter Head

iuucyrnlsj95xs9oy1pduezjjglgz

Collaborator:



Payloads to generate: 1

☑ Include Collaborator server location

Polling automatically

#	Time	Type	Payload	Source IP address	Comment
6	2568-Nov-16 21:24:29.829 UTC	HTTP	3dhtfvz1ywrwidvivzr502l47vdm1cp1	184.[redacted]	
7	2568-Nov-16 21:24:29.829 UTC	HTTP	3dhtfvz1ywrwidvivzr502l47vdm1cp1	184.[redacted]	
8	2568-Nov-17 09:01:17.572 UTC	DNS	o9yebgvmuhnheyr3rknqwnhp3g97xyln	49.2[redacted]	
9	2568-Nov-17 09:01:17.623 UTC	DNS	o9yebgvmuhnheyr3rknqwnhp3g97xyln	49.2[redacted]	
10	2568-Nov-17 09:01:18.491 UTC	HTTP	o9yebgvmuhnheyr3rknqwnhp3g97xyln	184.[redacted]	
11	2568-Nov-17 09:41:32.339 UTC	DNS	bcr1e3y9x4q4hluqu7qdzakc63cu0noc	103.[redacted]	
12	2568-Nov-17 09:41:32.443 UTC	DNS	bcr1e3y9x4q4hluqu7qdzakc63cu0noc	49.2[redacted]	
13	2568-Nov-17 09:41:33.376 UTC	HTTP	bcr1e3y9x4q4hluqu7qdzakc63cu0noc	184.[redacted]	
14	2568-Nov-17 09:41:48.841 UTC	HTTP	bcr1e3y9x4q4hluqu7qdzakc63cu0noc	184.[redacted]	
15	2568-Nov-17 09:41:49.758 UTC	HTTP	bcr1e3y9x4q4hluqu7qdzakc63cu0noc	184.[redacted]	
16	2568-Nov-17 09:41:49.758 UTC	HTTP	bcr1e3y9x4q4hluqu7qdzakc63cu0noc	184.[redacted]	