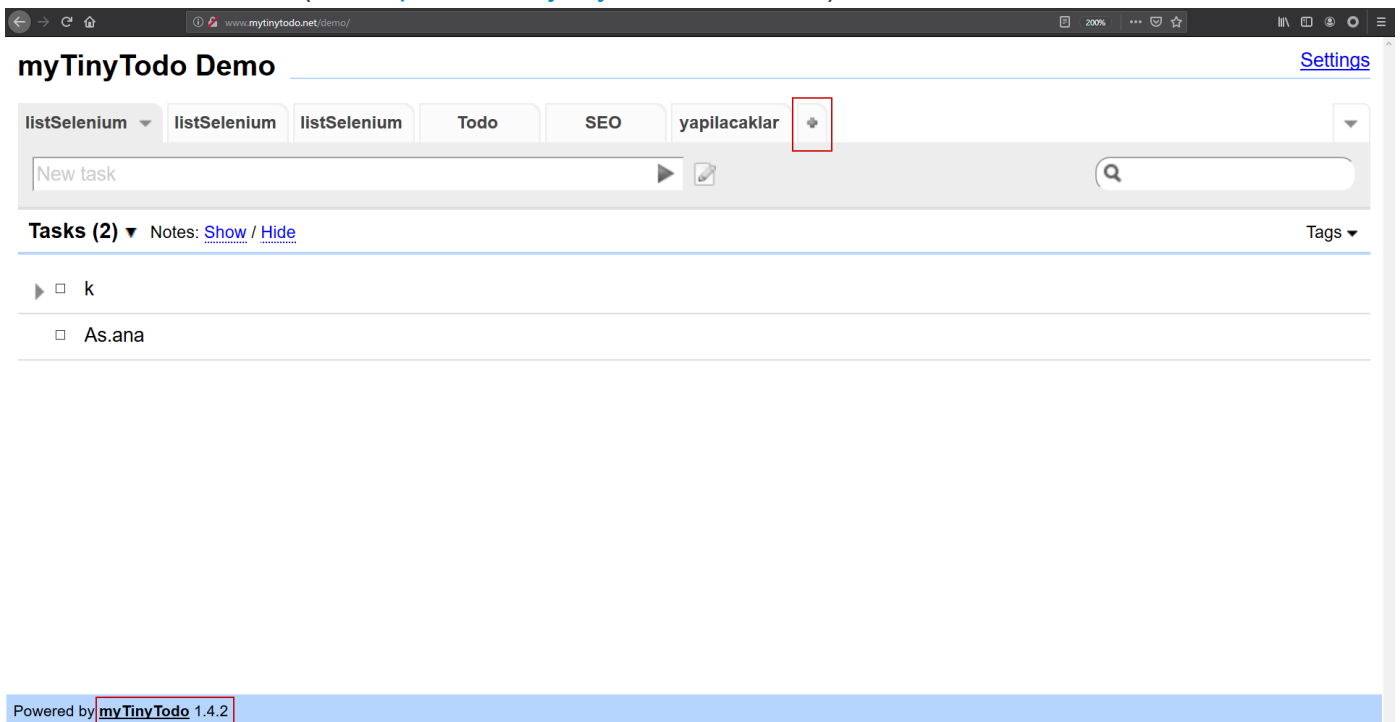# CSV Injection with the export feature

Description:

A vulnerability in the file upload feature allows attackers to send
malicious csv files. By using the Microsoft Excel DDE function an
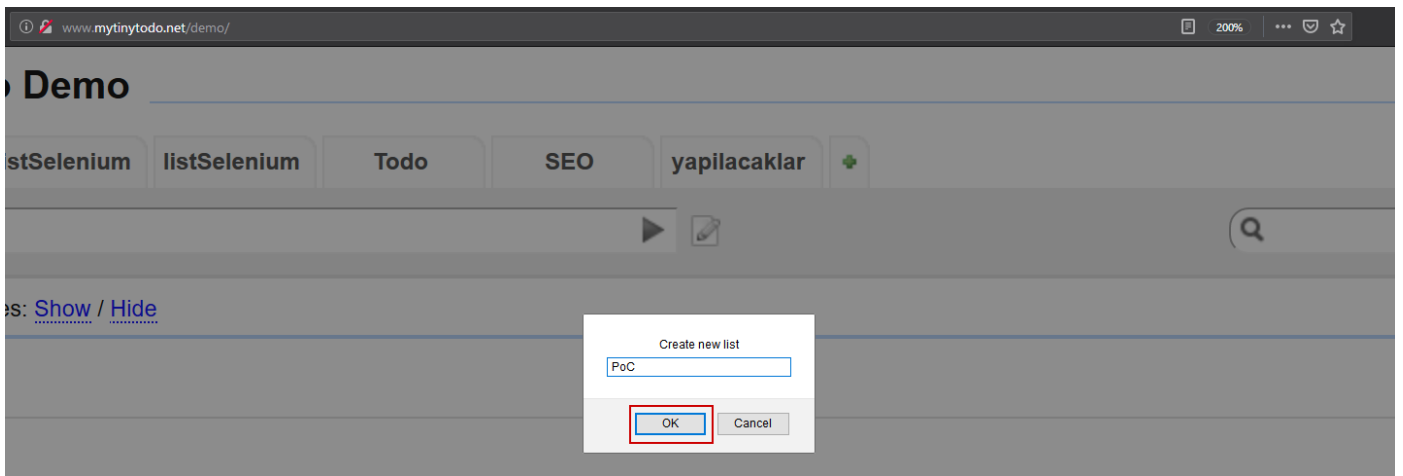attacker can launch arbritary commands on the victims system.
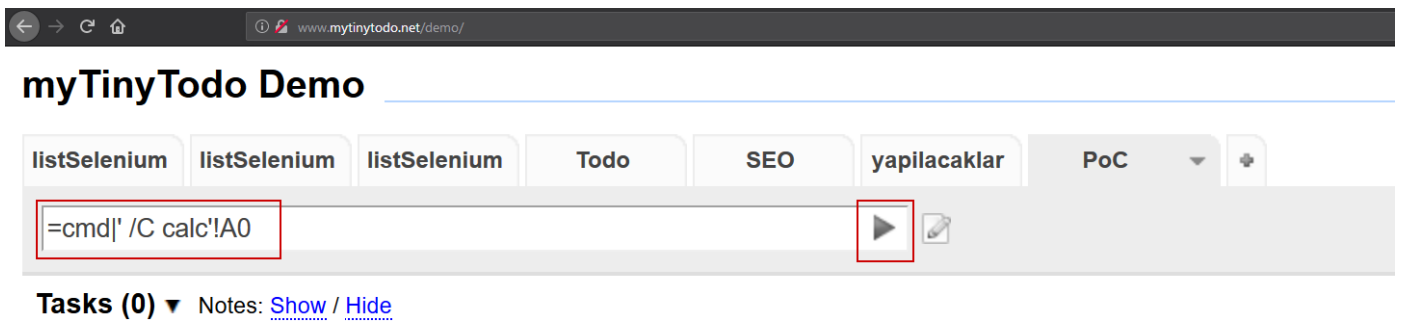
Version

1.3.3 <= 1.4.3

PoC:

1. Go to victim website (ex. http://www.mytinytodo.net/demo/)
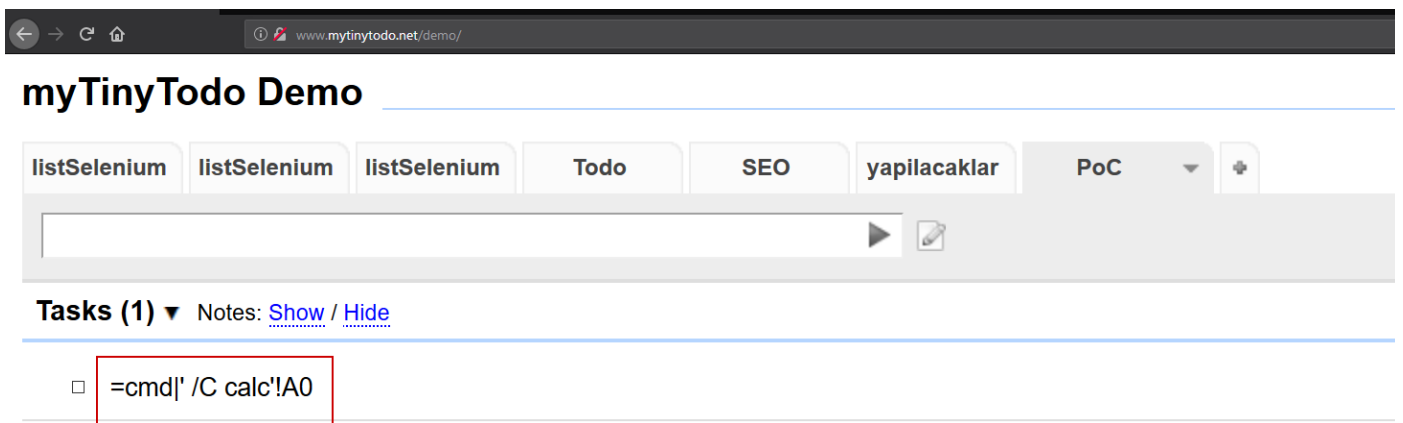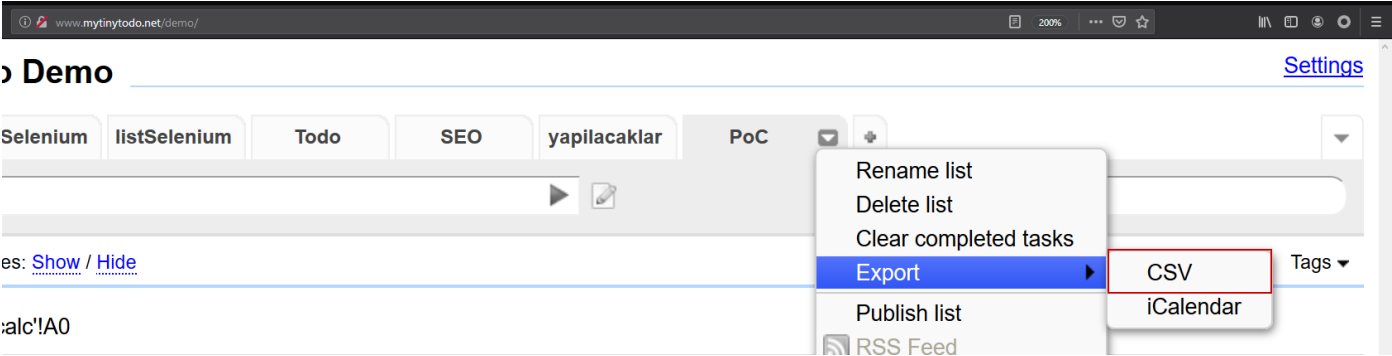

2. Create new list

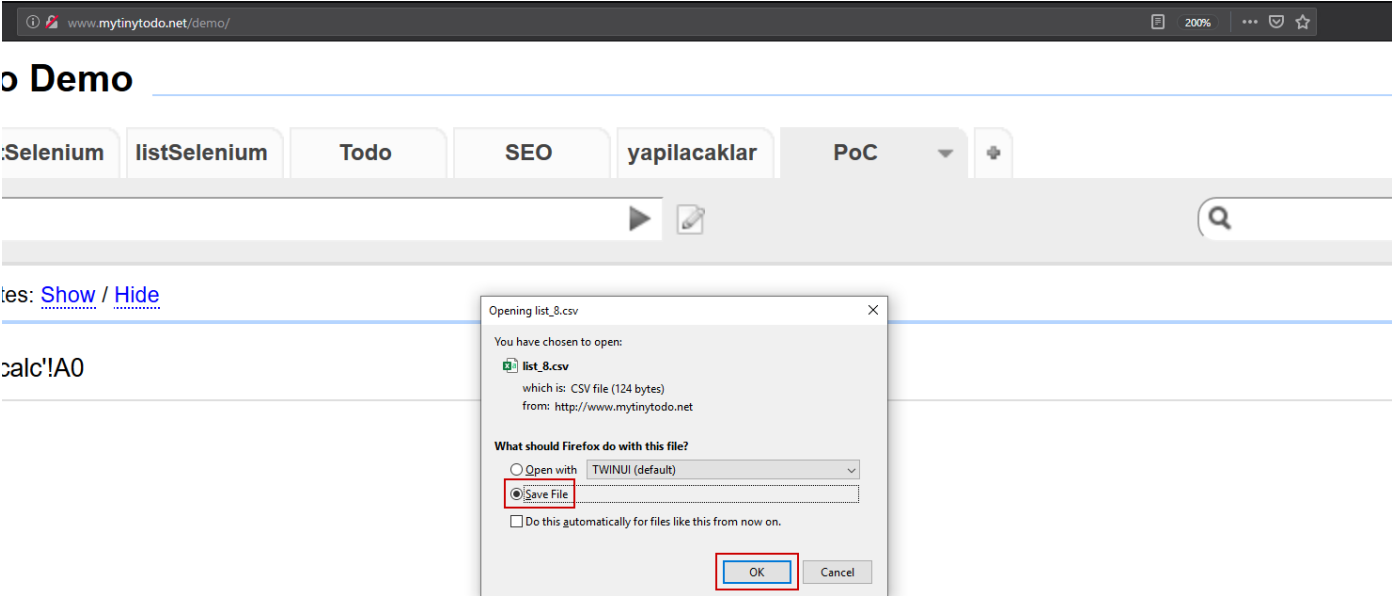3. Insert `=cmd|' /C calc'!A0` and click add

4. The malicious code will saved

5. Export as CSV

6. Click OK to download

7. The malicious will run automically

Todo Demo

Calculator

Standard

History   Memory

0

There's no history yet

MC	MR	M+	M-	MS
%	√	x^2	⅟x	
CE	C	⌫	÷	
7	8	9	×	
4	5	6	−	
1	2	3	+	
±	0	.	=	

AutoSave Off

File   Home   Insert   Page Layout   Formulas   Data   Review   View   Hel

Paste   Cut   Copy   Format Painter

Clipboard   Font   Alignment

A1

Wrap T   Merge

Comments

Ideas

Ideas

Microsoft Excel

This wo
If you

Update   Don't Update   Help

Calculate

10%