

[Open in app](#)[Get started](#)

Published in Cybersecurity@ValueLabs



ValueLabs

[Follow](#)

Aug 23 · 2 min read · [Listen](#)

[Save](#)

# EspoCRM 7.1.8 is vulnerable to Cross Site Scripting

**Affected Product and Version:** EspoCRM 7.1.8

**Description:** EspoCRM is an open-source CRM (customer relationship management) software written in PHP. This web application enables users to see and manage company relationships. EspoCRM version 7.1.8 is vulnerable to Cross Site Scripting, allowing attackers to run malicious JavaScript on the browser. Administrator users can import contacts through the CSV file. Attackers can craft a CSV file containing JavaScript payloads and send it to the Administrator. JavaScript payload gets executed on import.

**Impact:** The attacker may access the session ID of the victim and send it to a remote server. Under this situation, the attacker may use this session ID to get control of the Administrator user and perform all the actions an administrator can perform. The attacker can deface the website and steal the credentials of the administrator user.

## Steps to reproduce:

1. Craft a CSV file containing a malicious JavaScript payload





Open in app

Get started

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	salutation	firstName	lastName	middleName	name	accountId	accountName	emailAddress	emailAddress	phoneNumber	phoneNumber		
2	Mr.	ffff"><script>alert(999)</script>	notepad!	<script>al	#REF!							8.99E+09	
3													
4													
5													
6													
7													
8													
9													
10													
11													

2. Log in to the application as an administrator user. Navigate to Administrator>> Import

3. Click New import and choose the CSV file (as shown in step 1) containing the malicious payload

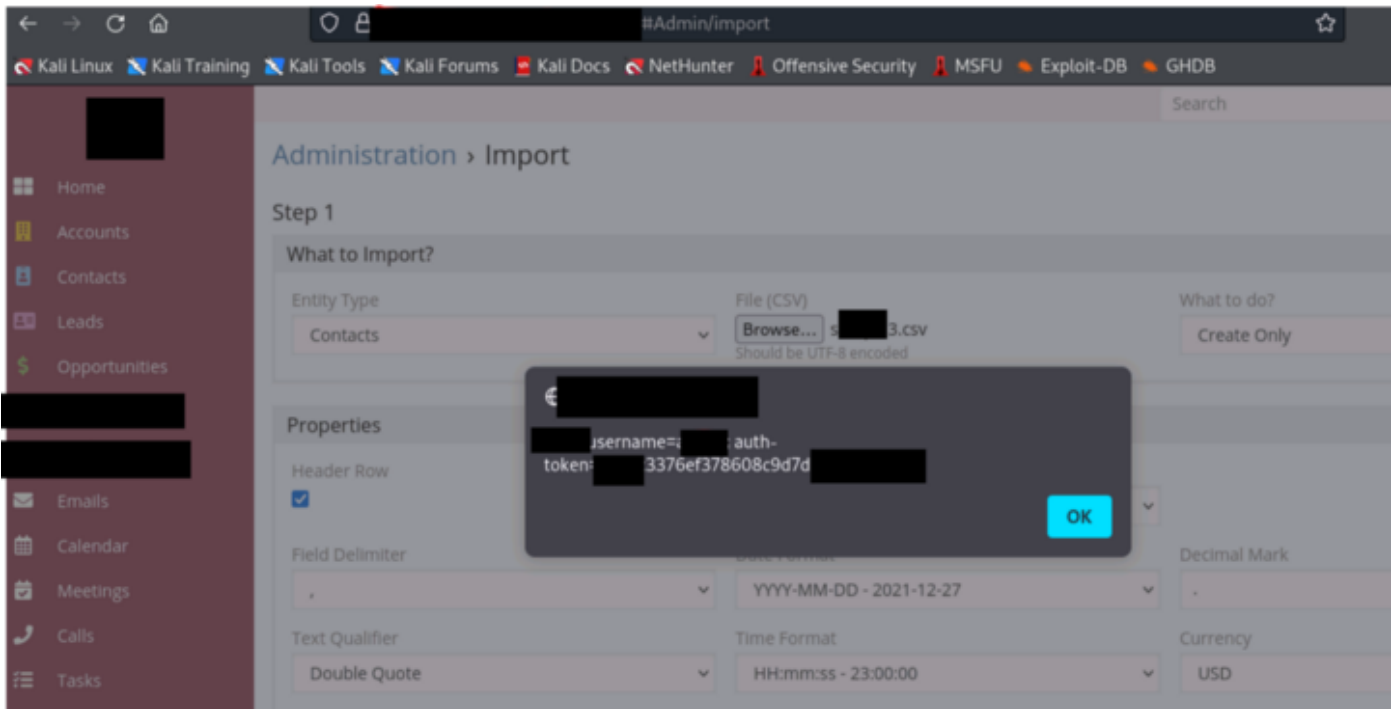
4. Observe that payload gets executed on the browser

The screenshot shows a web application interface for importing data. A modal dialog is open, displaying a JavaScript alert: "says 999". The background interface includes a sidebar with navigation links (Home, Accounts, Contacts, Leads, Opportunities, Emails, Calendar, Meetings, Calls, Tasks) and a main content area titled "Administration > Import". The "Step 1" section, "What to Import?", shows "Entity Type" as "Person" and "File (CSV)" as "Choose File". The "Properties" section includes settings for "Header Row" (checked), "Field Delimiter" (comma), "Text Qualifier" (Double Quote), "Person Name Format" (First Last), "Date Format" (YYYY-MM-DD - 2021-12-27), "Time Format" (HH:mm:ss - 23:00:00), "Timezone" (UTC), "Decimal Mark" (.), and "Currency" (USD). There are also checkboxes for "Execute in idle (for big data; via cron)" and "Skip searching for duplicates", and a "Silent Mode" toggle.



[Open in app](#)

[Get started](#)



## Remediation:

Upgrade to the latest stable version of EspoCRM 7.1.9

[About](#) [Help](#) [Terms](#) [Privacy](#)

[Get the Medium app](#)





[Open in app](#)

Get started

