

# SureForms < 1.4.4 - Admin+ Stored XSS

## Description

The plugin does not sanitise and escape some of its Form settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the `unfiltered_html` capability is disallowed (for example in multisite setup).

## Proof of Concept

- 1) Create a new Blank Form
- 2) Put an Email block and change "Default value" field to `123" autofocus onfocus=ale`
- 3) The XSS will be triggered when accessing a page/post where the form is embed



## Affects Plugins

---

 [sureforms](#)

Fixed in 1.4.4 ✓

## References

---

### CVE

[CVE-2025-3514](#)

### URL

<https://research.cleantalk.org/cve-2025-3514/>

# Classification

---

Type

XSS

OWASP top 10

A7: Cross-Site Scripting (XSS)

CWE

CWE-79

CVSS

3.5 (low)

## Miscellaneous

---

Original Researcher

Dmitrii Ignatyev

Submitter

Dmitrii Ignatyev

Submitter website

<https://www.linkedin.com/in/dmitriy-ignatyev-8a9189267/>

Verified

Yes

WPVDB ID

fc3da503-a973-44d8-82d0-13539501f8c0

## Timeline

---

Publicly Published

2025-04-11 (about 22 days ago)

Added

2025-04-11 (about 22 days ago)

Last Updated

2025-04-11 (about 22 days ago)

Other

---

Published

2021-09-21

Title

[Special Text Boxes < 5.9.110 - Admin+ Stored Cross-Site Scripting](#)

Published

2024-07-10

Title

[WP GoToWebinar < 15.8 - Authenticated \(Subscriber+\) Stored Cross-Site Scripting](#)

Published

2025-04-22

Title

[Link Library < 7.8.1 - Authenticated \(Contributor+\) Stored Cross-Site Scripting](#)

Published

2022-06-28

Title

[Request a Quote < 2.3.9 - Admin+ Stored Cross-Site Scripting](#)

Published

2024-04-29

Title

[Adventure Journal <= 1.7.2 - Authenticated \(Contributor+\) Stored Cross-Site Scripting](#)



Vulnerabilities

About

For Developers

Other

WordPress

How it works

Status

Privacy

<a href="#">Plugins</a>	<a href="#">Pricing</a>	<a href="#">API details</a>	<a href="#">Terms of service</a>
<a href="#">Themes</a>	<a href="#">WordPress plugin</a>	<a href="#">CLI scanner</a>	<a href="#">Submission terms</a>
<a href="#">Our Stats</a>	<a href="#">Blog</a>		<a href="#">Disclosure policy</a>
<a href="#">Submit vulnerabilities</a>	<a href="#">Contact</a>		<a href="#">Privacy Notice for California Users</a>

---

In partnership with Jetpack

---

An [open source](#) endeavor [powered by](#) [WordPress](#) [Work With Us](#) [Press](#)