# Composr CMS 10.0.13
# Cross Site Scripting(XSS)
# Assigned CVE Number:
# CVE-2018-6518

## Proof-of-Concept

**Submitted by:**
**Author: Faiz Ahmed Zaidi**
**Organization: Provensec LLC**
**Website: www.provensec.com**
**Email: faizzaidi17@gmail.com**
**LinkedIn: https://www.linkedin.com/in/faizzaidi/**

**National Vulnerability Database**

(https://nvd.nist.gov/cvss/v2-calculator)

Overall CVSS Score: 3.3

CVSS v2 Vector(AV:N/AC:M/Au:S/C:P/I:N/A:N/E:F/RL:U/RC:C)

# Proof-of-Concept

Hello,

I would like to report a vulnerability that I discovered in Composr CMS version (composr_quick_installer-10.0.13), which can be exploited to perform Cross-Site Scripting (XSS) attacks. The vulnerability exists due to insufficient sanitization in the "site_name" parameters uses HTTP POST method passed to "/adminzone/index.php?page=admin-setupwizard&type=step3" Script. The exploitation example below uses the "confirm()" JavaScript function to display "1" word.

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source; the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

---

**Vulnerability Type:**
Cross Site Scripting (XSS)

---

**Vendor of Product:**
Composr CMS

---

**Affected Product Code Base:**
Composr CMS(https://compo.sr/) - Composr CMS version composr_quick_installer-10.0.13.

---

**Affected Component:**
http://localhost:880/composr_quick_installer-10.0.13/adminzone/index.php?page=admin-setupwizard&type=step3

---

**Attack Type:**

Remote

---

**Attack Vectors:**

**Steps:**

1. Install of Composr CMS.

2. It will ask for some details like delete install.php, etc.

3. In step wizard, step 3 having some details which are filled by a user.

URL: http://localhost:880/composr_quick_installer-10.0.13/adminzone/index.php?page=admin-setupwizard&type=step3

4. Insert XSS payload site_name parameter.Here, payload I used ""><img src=x onerror=confirm(1);>".

5. Complete the step wizard.

6. Now login with your setup credentials.

7. XSS gets executed on the "site_name" parameter is vulnerable to XSS.

**PoC's:**

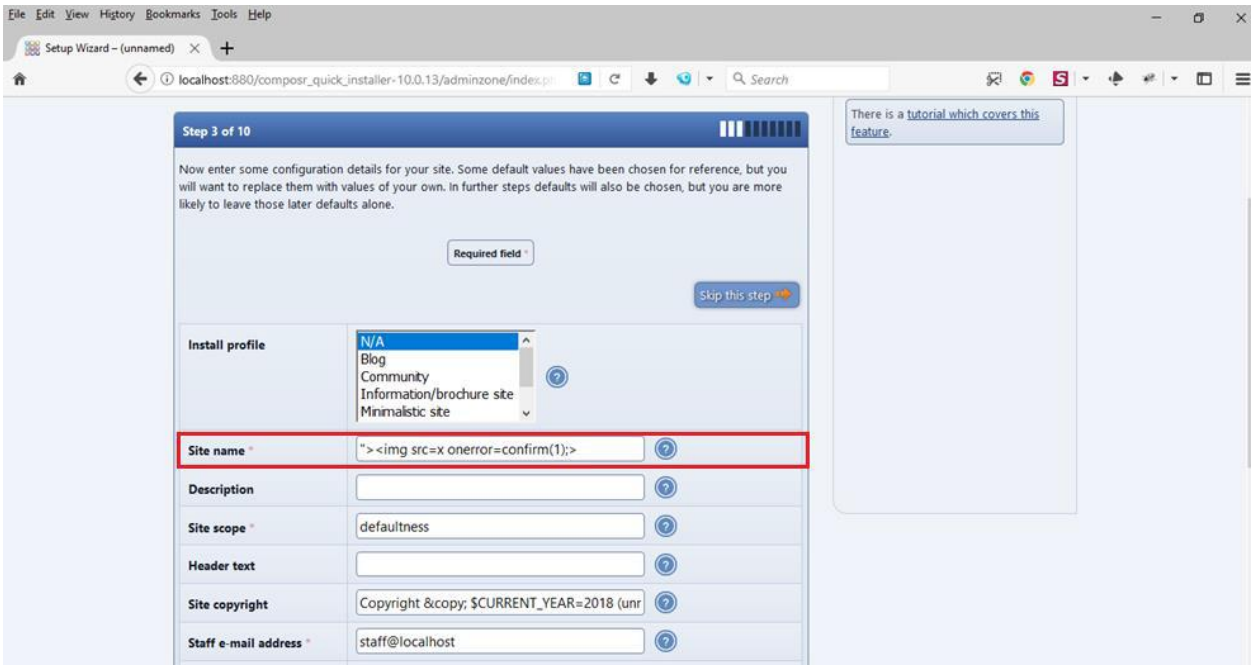
File Edit View History Bookmarks Tools Help
Setup Wizard – (unnamed)
localhost:880/composr_quick_installer-10.0.13/adminzone/index.p
Search
Step 3 of 10
Now enter some configuration details for your site. Some default values have been chosen for reference, but you will want to replace them with values of your own. In further steps defaults will also be chosen, but you are more likely to leave those later defaults alone.
There is a tutorial which covers this feature.
Required field *
Skip this step
Install profile
N/A
Blog
Community
Information/brochure site
Minimalistic site
Site name *
"><img src=x onerror=confirm(1);>
Description
Site scope *
defaultness
Header text
Site copyright
Copyright © $CURRENT_YEAR=2018 (unr
Staff e-mail address *
staff@localhost

Fig 1.1

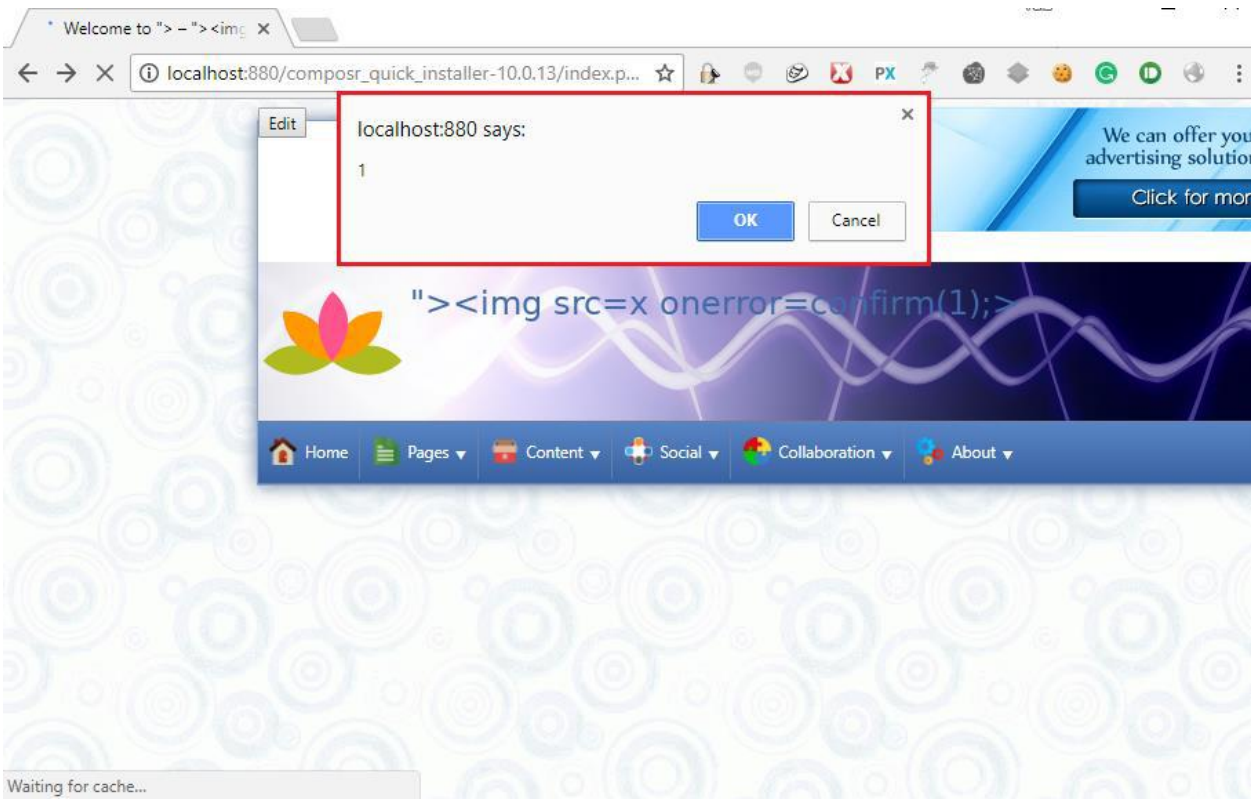
Welcome to "> – "><img
localhost:880/composr_quick_installer-10.0.13/index.p...
Edit
localhost:880 says:
1
OK
Cancel
We can offer you advertising solutio
Click for mor
"><img src=x onerror=confirm(1);>
Home
Pages
Content
Social
Collaboration
About
Waiting for cache...

Fig 1.2

---

**Reference:**

https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

---

**Discoverer:**

Author: Faiz Ahmed Zaidi Organization: Provensec LLC

Website: https://www.provensec.com/