

Typo-3 CMS V9.1.0
Persistent Cross Site
Scripting (XSS)
Assigned CVE Number:
CVE-2018-6905

Proof-of-Concept

Submitted by:

Author: Pradeep Jairamani

Website: <https://www.linkedin.com/in/pradeep-jairamani-167a1397/>

Proof-of-Concept

Hello,

I would like to report a vulnerability that I discovered in Typo3 CMS (TYPO3 cms-9.1.0), which can be exploited to perform persistent Cross-Site Scripting (XSS) attacks. The vulnerability exists due to insufficient sanitization in the site name field both parameters uses HTTP POST method passed to `"/index.php?route=%2Flogin"` script after logging in enter the payload in site name field and the payload will be executed at `"/index.php?route=%2Fmain"` . The exploitation example below uses the `"alert()"` JavaScript function to display "XSS" 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:
Typo3 CMS

Affected Product Code Base:
Typo3 CMS (https://typo3.org/) - Typo-3 CMS V9.1.0
https://forge.typo3.org/issues/84191

Affected Component:

http://localhost/typo3_src-9.1.0/typo3/index.php?route=%2Fmain

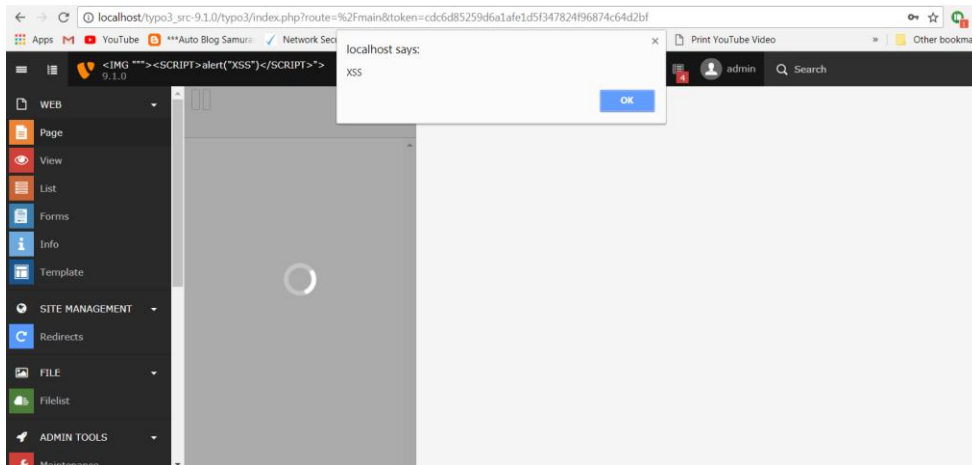
Attack Type:
Remote

Attack Vectors:

Steps:

1. Download TYPO3 unzip and start the installation process.
2. In installation Process under Process 4/5. The parameter site name is vulnerable to XSS.
3. Now complete the installation process.
4. Now Login with your credentials in typo3
`http://localhost/typo3_src9.1.0/typo3/index.php?route`
5. Now in left side panel click on "web" and select "page"
6. XSS payload gets executed on
`"http://localhost/typo3_src-9.1.0/typo3/index.php?route=%2Fmain" page`

POC are:



Reference:

[https://www.owasp.org/index.php/Crosssite_Scripting_\(XSS\)](https://www.owasp.org/index.php/Crosssite_Scripting_(XSS))

Discoverer:

Author: Pradeep Jairamani

Website: <https://www.linkedin.com/in/pradeep-jairamani-167a1397/>