Description: Subrion CMS 4.2.1 has CSRF in panel/modules/plugins/

Affected Version: Subrion CMS v 4.2.1

About Subrion: Subrion is a Content Management System (CMS) which allows you to build websites for any purpose. Yes, from blog to corporate mega portal. It is a powerful web application which requires a server with PHP / MySQL to run. Subrion is a free and open source software distributed under the GPL v3.

Type of Vulnerability: CSRF

Discovered By: Nitin Goplani

CVE ID: 2019-7357

Vulnerability Description: CSRF is an attack which forces an end user to execute unwanted actions on a web application in which he/she is currently authenticated. With a little help of social engineering (like sending a link via email/chat), an attacker may force the users of a web application to execute actions of the attacker's choosing.

Subrion CMS is lacking CSRF Protection in plugin module which allows an attacker to activate/deactivate the plugins.

Severity: Medium

Vulnerable URL: http://<your server>/subrion/panel/modules/plugins/

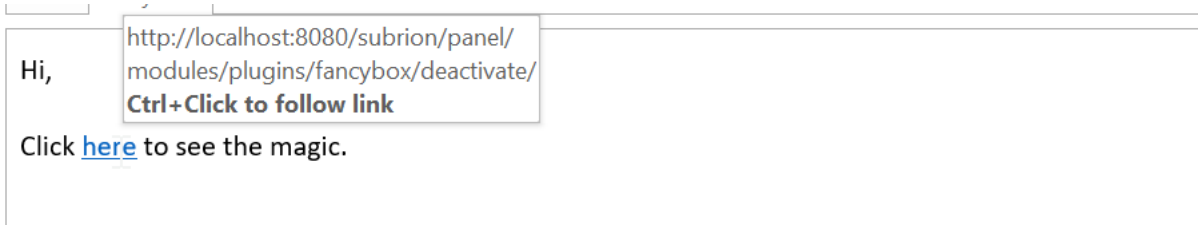
Steps to Reproduce:

1- Log into the Subrion CMS
2- Now go to panel/modules/plugins
3- Click on activate/deactivate plugin
4- Intercept the request and observe the CSRF Protection is missing
5- Create a CSRF Payload and wait for the victim to click 😊

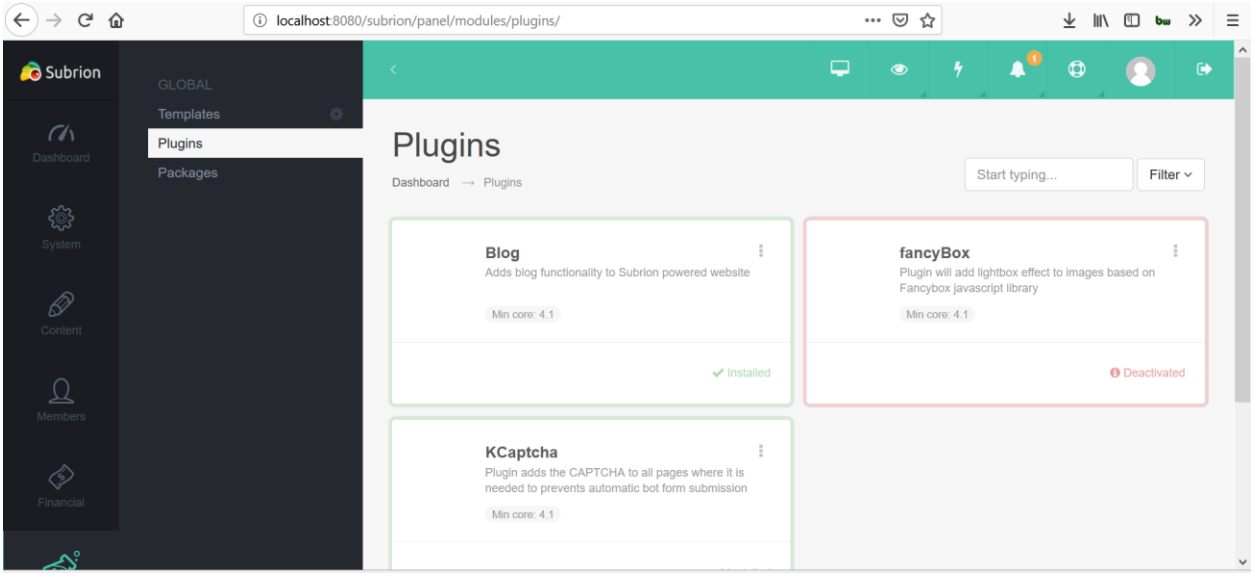
Screenshots:

Below screenshot confirms the CSRF Protection is missing

Below screenshot shows the CSRF Payload



Below screenshot confirms the plugin is now deactivated



Fix: It is recommended to:

- Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable
- Do not use the GET method for any request that triggers a state change.
- Check the HTTP Referer header to see if the request originated from an expected page.
- Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard