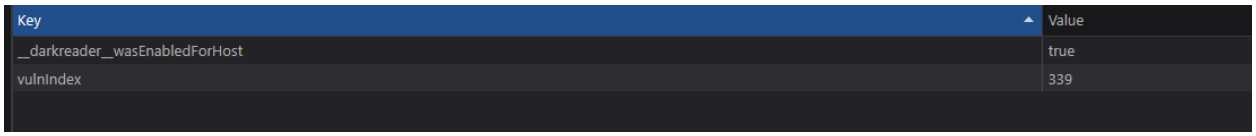
Inspect the webpage and look through the javascript. At the very bottom, there is the following code:

```
// Inject DOM comment into vulnerable form
document.querySelectorAll("form").forEach((form, idx) => {
  if ((idx + 1) === parseInt(sessionStorage.getItem("vulnIndex"))) {
    form.appendChild(document.createComment(" TO DO: fix this "));
  }
});
```

This indicates that there is one text box that is vulnerable, which is randomly chosen during each session of the website.

Check the session storage:



Scroll down to the user indicated by session storage:

Inject the following SQL query: ‘OR 1=1-- and it results in the following popup: