SCENARIO

The application contains a reflected cross site scripting vulnerability in the home page as it reflects the user supplied input in canonical tags and escape angle brackets when we press a combination of keys together. We will try to trigger an alert message by injecting a payload into the application.

**PROCEDURE**

1. Go to the vulnerable application and inspect the source of the HTML page and we can find the href tag enclosed with canonical relation.
2. Canonical tag tells the browser that if you find a lot of copies of the required page then this is the original page.
3. In our scenario we can see that our page’s URL is enclosed with canonical tag so we will break out of it.
4. Then we will inject the payload which will force the browser to trigger an alert whenever a particular combination of keys is pressed.

**PAYLOAD**

/?'accesskey='x'onclick='alert(“HACKED!”)

**REMEDIATION**