SCENARIO

The application contains a simple DOM based cross site scripting vulnerability in the home page which uses jQuery's **$()** selector function to auto-scroll to a given post, whose title is passed via the **location.hash** property, so we will try to exploit it by delivering an exploit using our exploit server to force the application to show the print dialog box.

**PROCEDURE**

1. Go to the vulnerable web application’s home page.
2. Open the element inspector tab and got to debugger tab in that.
3. In there we can see that location.hash value is passed and is used to scroll to any given post.
4. Now go to the exploit server and paste the following payload into the body of your exploit, then store the exploit, test the exploit and in the end deliver the exploit to the victim to force the application into viewing a print page dialog box in the victim’s browser.

**PAYOAD**

<iframe src="https://YOUR-LAB-ID.web-security-academy.net/#" onload="this.src+='<img src=0 onerror=print()>'"></iframe>

**REMEDIATION**