In one of the applications I came across a scenario where I can add links from external URLs (untrusted links)

The application has client side XSS escaping enabled, adding and executing direct XSS payloads did not work.

Since I can add URL from untrusted sources, below steps I have done to exploit the XSS via redirection link

1. Set up an Xampp server on localhost
2. Insert a .html file that can execute XSS payload
3. Verify if the file is accessible and executable via browser

<http://localhost:8000/testfiles/xss_payload.html>

1. Add this link into the target application form and save the form.
2. When the end user login into the application and click the embedded link, the XSS payload is executed and fetches the session cookies

