SCENARIO

The application contains a simple stored cross site scripting vulnerability in the comment functionality which is shown to every user who views the injected blog so we will try to exploit it by injecting some payload containing malicious script in the comment box.

**PROCEDURE**

1. Go to the vulnerable web application.
2. Try to post any comment and study the request that is made to the server using BurpSuite’s Interceptor and we noticed that the request is sent using the URL.
3. So, we will modify the comment parameter with all the fields well filled except the comment in order to inject the payload to generate a basic alert on the page.
4. Now we get an alert, it is clear that we can exploit the application more by injecting reflected XSS.

**PAYOAD**

<script>alert("Hey!")</script>

**REMEDIATION**