1. login cross-site scripting

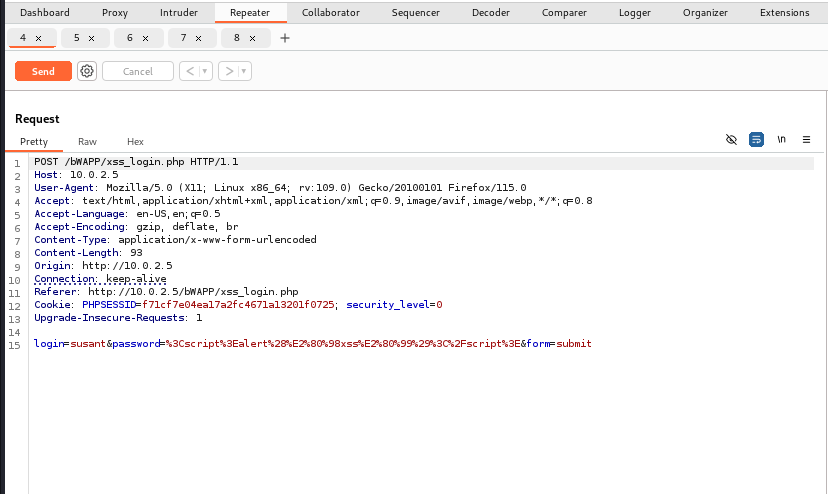




The vulnerability lies in how the $message variable is constructed and echoed back to the user. User-supplied input ($row["login"] and $row["secret"]) is directly concatenated into the HTML response without proper escaping or validation.

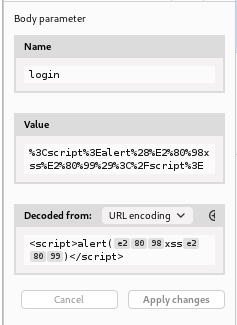


After that, the data in HTTP history is sent to the repeater in burpsuite.

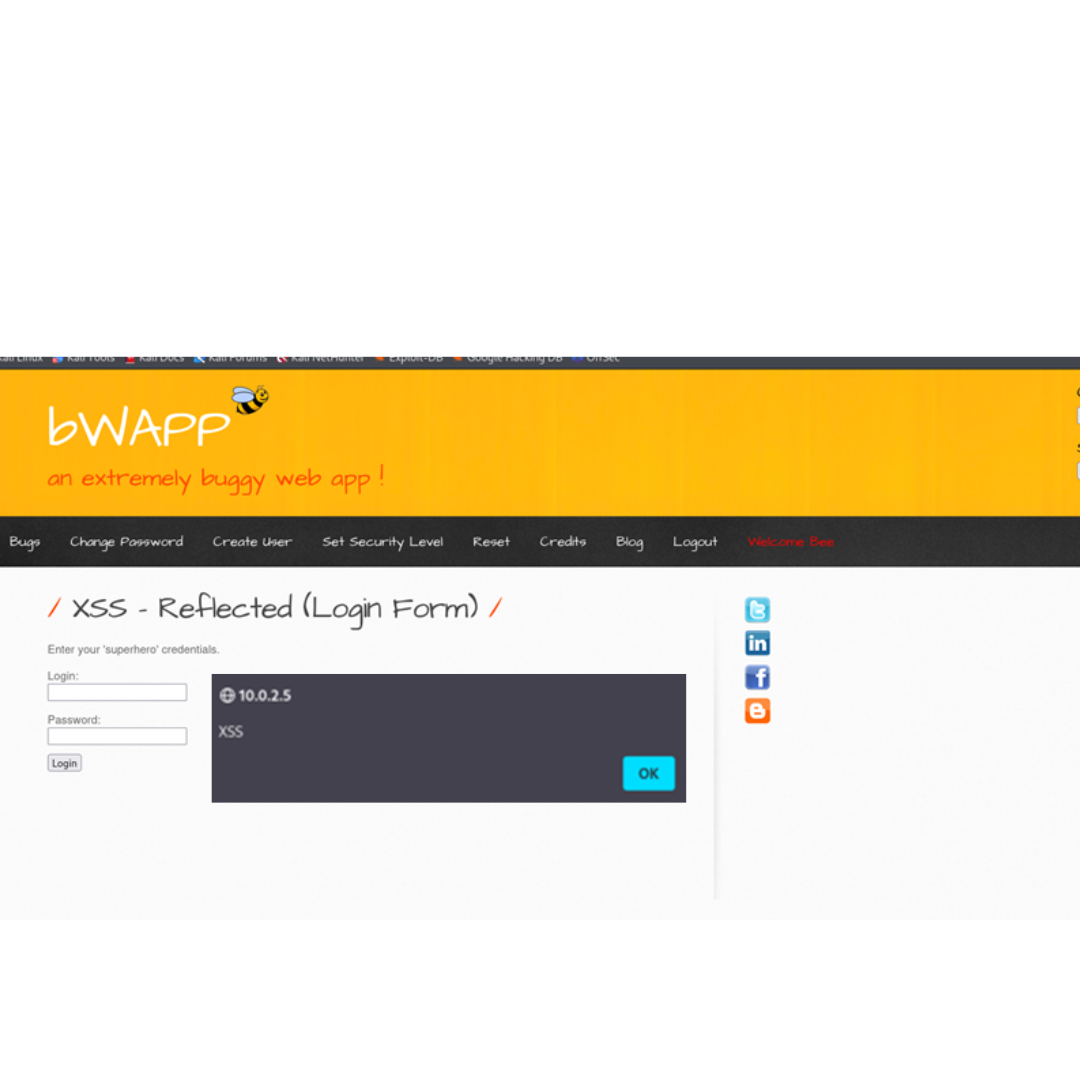


In the response tab of Burp Suite, look for the HTML code that includes your payload.

The <script>alert('XSS')</script> is a part of the response successfully.



Then the URL is copied from the browser and the alert box is generated in the browser.



So, the reflected login XSS vulnerability is successfully found.