**SCENARIO**

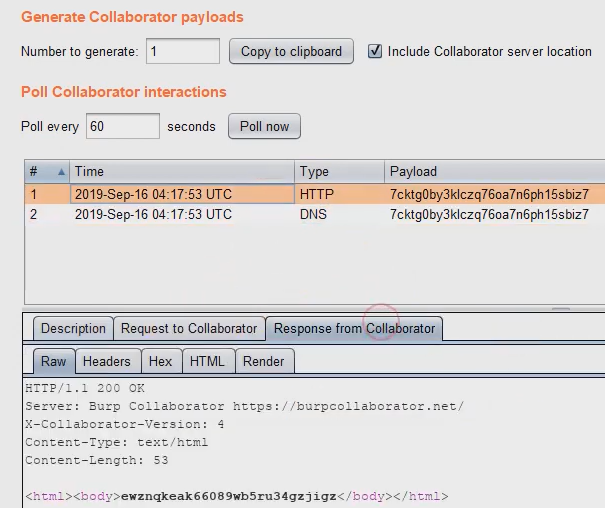
The website incorporates an analytics software which, upon loading a product page, fetches the URL specified in the Referer header. This behavior may be exploitable.

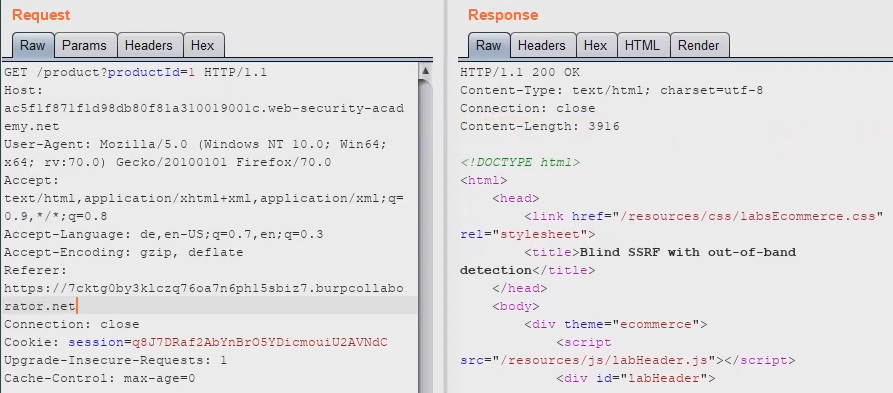
**PROCEDURE**

1. Accessing a product, we intercept its request, sending it over to Burp Repeater.
2. Within the Repeater, the Referer header is altered to a Burp Collaborator generated domain.
3. Monitoring the Collaborator client, we notice several interactions initiated by the application, confirming the potential exploit.

**PAYLOAD**

Modified Referer header to a unique domain generated by Burp Collaborator.

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Validate Headers:** Ensure that all HTTP headers, especially the Referer header, undergo thorough input validation.
2. **Limit Outbound Requests:** Control the outbound requests the analytics software can make, disallowing unintended destinations.
3. **Isolation:** Ensure the analytics software operates in a restricted environment, limiting its potential actions if exploited.