**SCENARIO**

The application possesses a stock check functionality that internally retrieves data. However, a potential Server Side Request Forgery (SSRF) vulnerability exists that could grant unintended access to the internal admin panel.

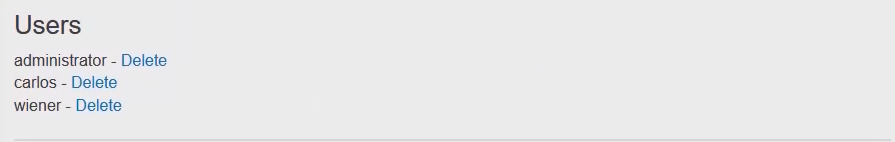
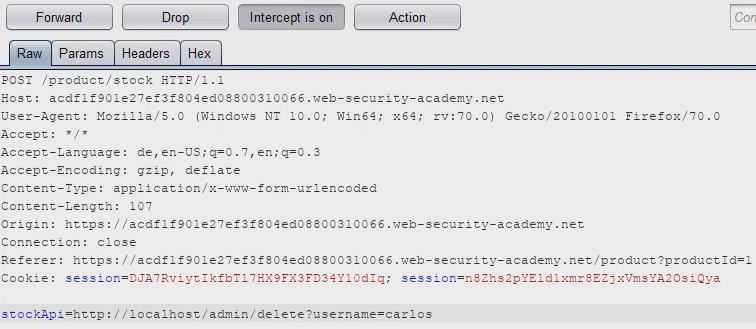
**PROCEDURE**

1. We attempt to directly navigate to /admin, realizing that direct access is denied.
2. Moving to a product, we select "Check stock". In doing so, we intercept the request using Burp Suite and redirect it to Burp Repeater.
3. In the Repeater, we modify the stockApi parameter's URL to target the localhost admin URL. The response exposes the administrative interface.
4. Carefully analyzing the HTML, we pinpoint the exact URL endpoint responsible for deleting users.

**PAYLOAD**

Targeting http://localhost/admin via the stockApi parameter and subsequently utilizing http://localhost/admin/delete?username=carlos to execute the deletion.

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Restrict Outbound Calls:** Limit the domains or IP addresses the stock check feature can call out to.
2. **Input Validation:** Rigorously validate and sanitize the input given to the stockApi parameter.
3. **Enhanced Logging:** Monitor for and alert about suspicious requests or patterns that might indicate an exploit attempt.