**SCENARIO**

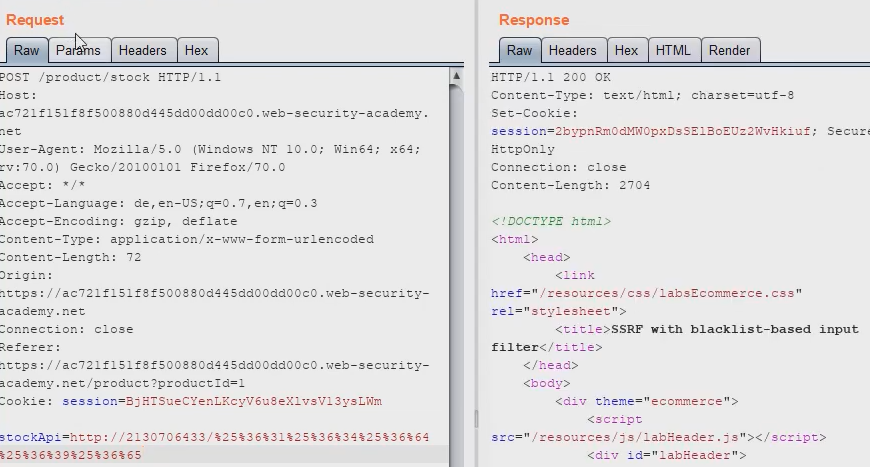
The application's stock check feature may be vulnerable to SSRF. Although there are defenses against this, we suspect they might be bypassable.

**PROCEDURE**

1. Initiating the stock check on a product, we intercept and analyze the request. We note that direct access to a different host is denied.
2. Exploring further, we find an open redirection vulnerability within the application's "next product" feature.
3. Combining these insights, we craft a URL exploiting the open redirection vulnerability to bypass the stock checker's limitations, subsequently accessing the internal admin interface.

**PAYLOAD**

Exploitation of open redirection via /product/nextProduct?path=http://192.168.0.12:8080/admin.

**PROOF OF CONCEPT**

**REMEDIATION**

1. **Prevent Open Redirects:** Ensure all user inputs undergo validation to avoid redirection to arbitrary URLs.
2. **Limit Internal Access:** Prohibit the stock check feature from accessing URLs other than its designated endpoint.
3. **Audit and Monitor:** Regularly review application logs to detect suspicious or anomalous activities.