**SCENARIO**

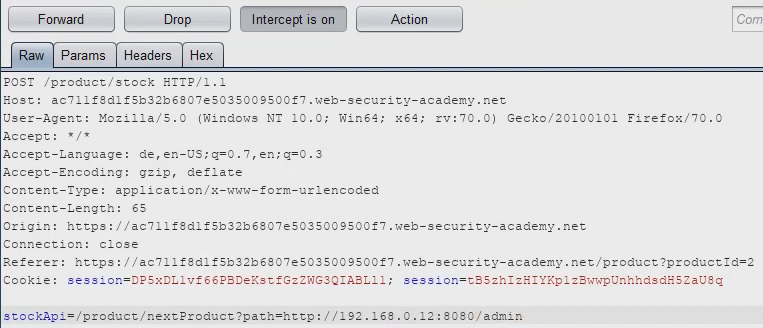
The application uses a stock check system that retrieves data from an internal endpoint. However, we notice that the URL parsing has some inconsistencies, hinting at a possible SSRF vulnerability.

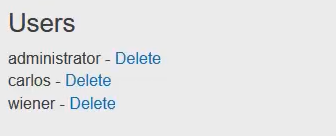
**PROCEDURE**

1. Choosing a product and invoking its stock check, we analyze the intercepted request. On changing the stockApi parameter to the localhost, we spot URL parsing anomalies.
2. Through multiple tests, we ascertain that the URL parser can be fooled using double URL encoding.
3. Harnessing this vulnerability, we access the internal admin interface and subsequently delete the targeted user.

**PAYLOAD**

Manipulated URL using double URL encoding, such as http://localhost:80%2523@stock.weliketoshop.net/admin/delete?username=carlos.

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Strict URL Parsing:** Employ robust URL parsing libraries and ensure URLs don't accept or act upon unnecessary components.
2. **Whitelisting:** Only allow specific pre-defined URLs to be accessed by the stock check feature.
3. **Encode and Sanitize:** Ensure all input data, especially URLs, are properly encoded and sanitized before use.