**SCENARIO**

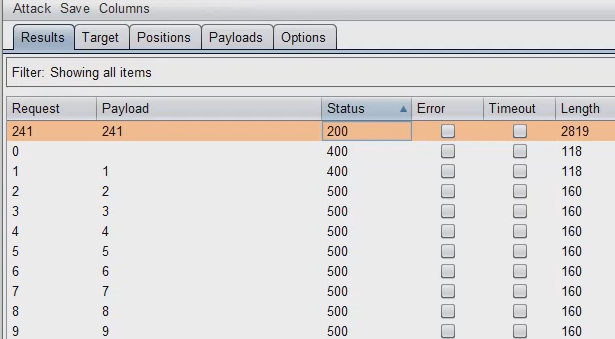
The application's stock check functionality probes data from an internal mechanism. We suspect that this can be manipulated to scan the internal network.

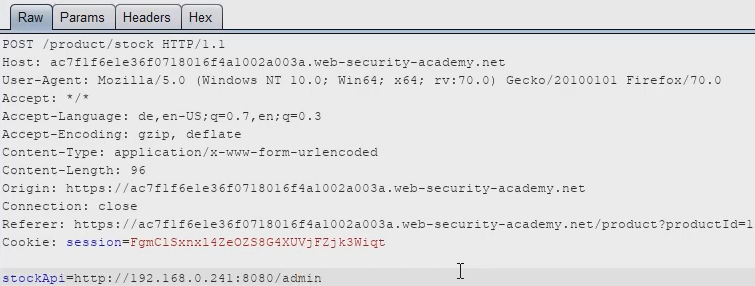
**PROCEDURE**

1. Upon selecting a product, we initiate the "Check stock" feature. This request is intercepted and redirected to Burp Intruder.
2. Within Intruder, we prepare to scan the internal IP range, modifying the stockApi parameter to initiate the scan.
3. We launch the attack, targeting IP addresses in the internal 192.168.0.X range on port 8080.
4. Scanning results identify an admin interface, which we subsequently use to delete the target user.

**PAYLOAD**

Scanning payload that cycles through the 192.168.0.X IP range on port 8080.

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. **Limit Internal Access:** Prevent the stock check feature from accessing internal IP addresses or ports.
2. **Rate Limiting:** Implement rate limiting to deter or hinder potential scanning attempts.
3. **Implement Proper Network Segmentation:** Isolate critical internal services from areas of the network accessible by web applications.