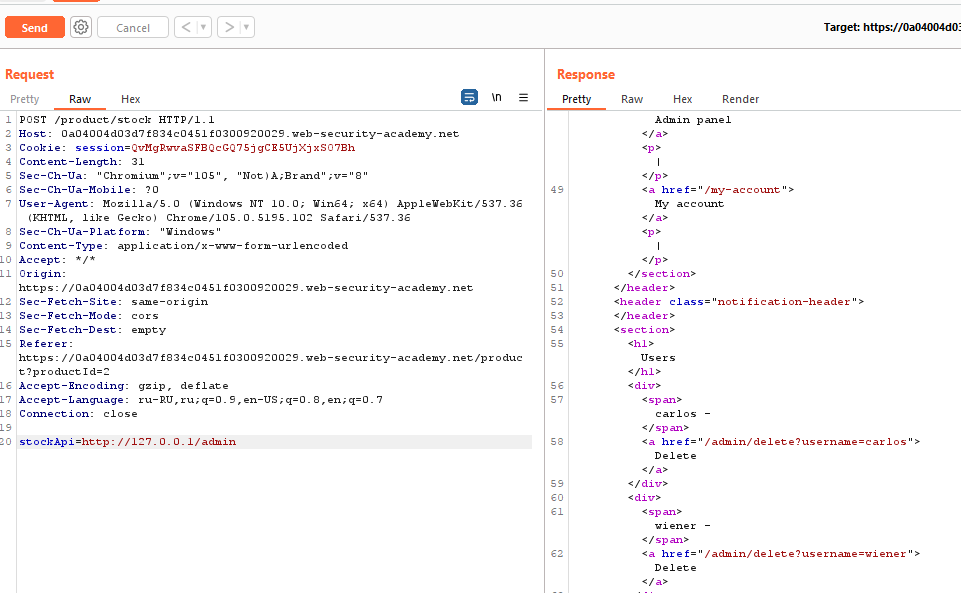
**Lab SSRF:**

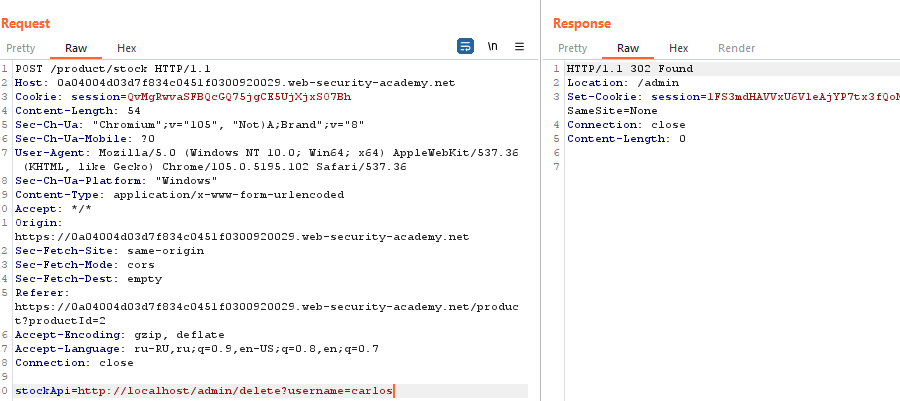
Выполнение примеров заданий на [сайте](https://portswigger.net/web-security/ssrf):

1. **Lab: Basic SSRF against the local server.**

stockApi=http://127.0.0.1/admin



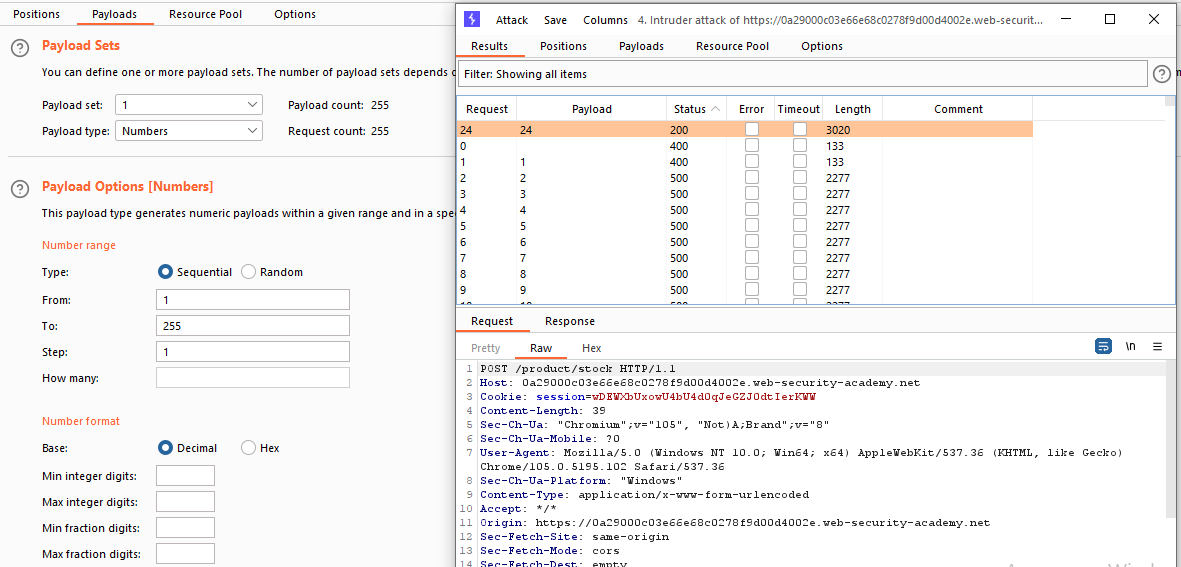
stockApi=http://localhost/admin/delete?username=carlos



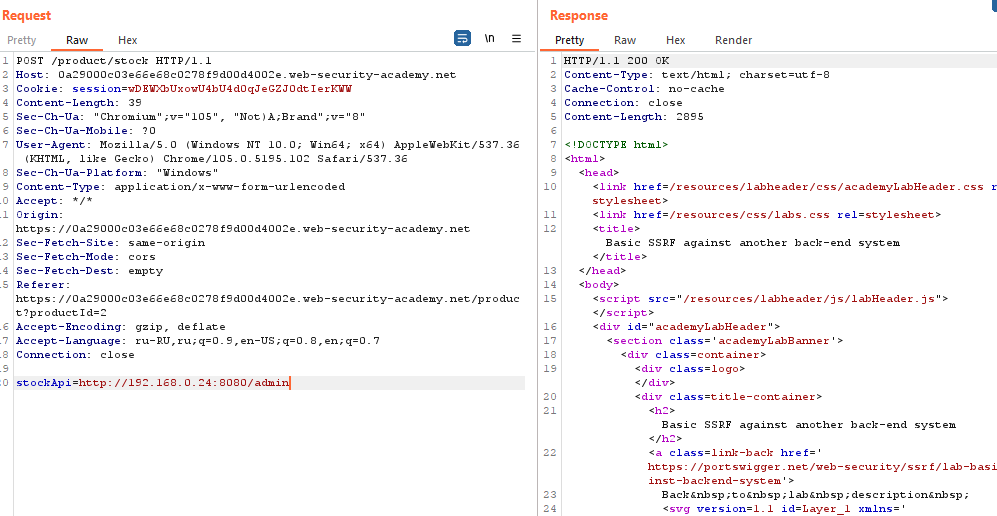
1. **Lab: SSRF against another back-end system**

Известен внутреннмй диапазон IP-адресов (192.168.0.х) и порт (8080) для интерфейса admin.

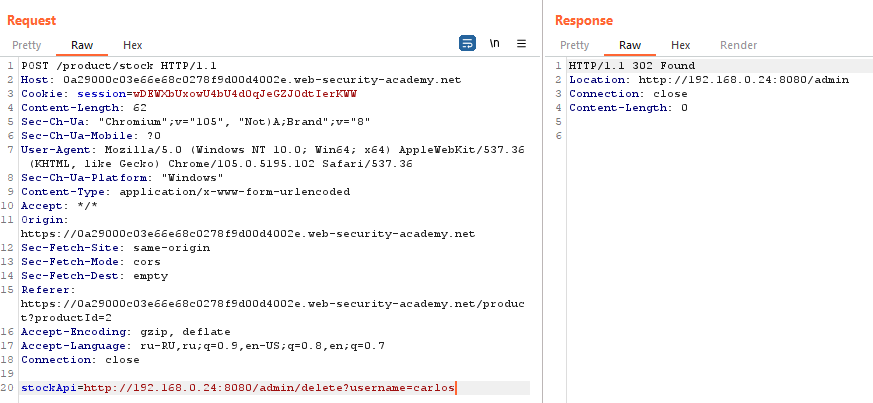
Запускаем сканирование IP-адресов (192.168.0.х) с шагом 1 и диапазоном от 1 до 255.



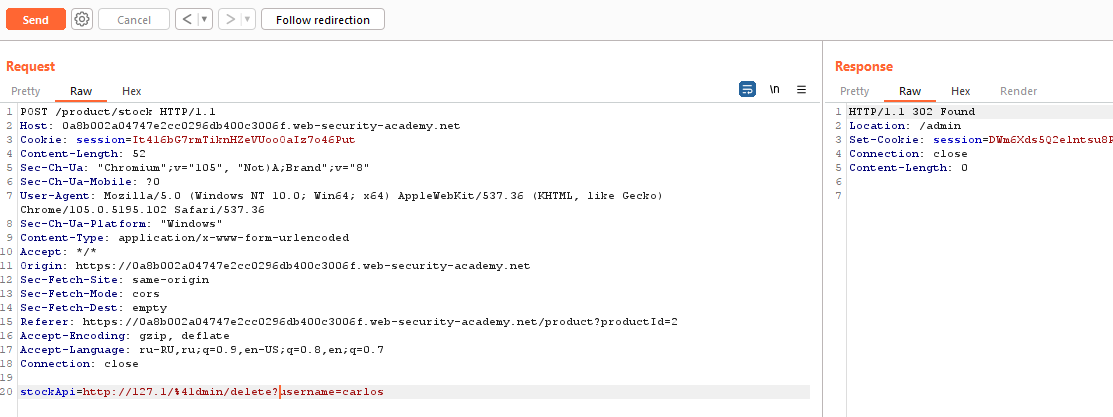
Отправляем запрос со статусом «200» в Repeater



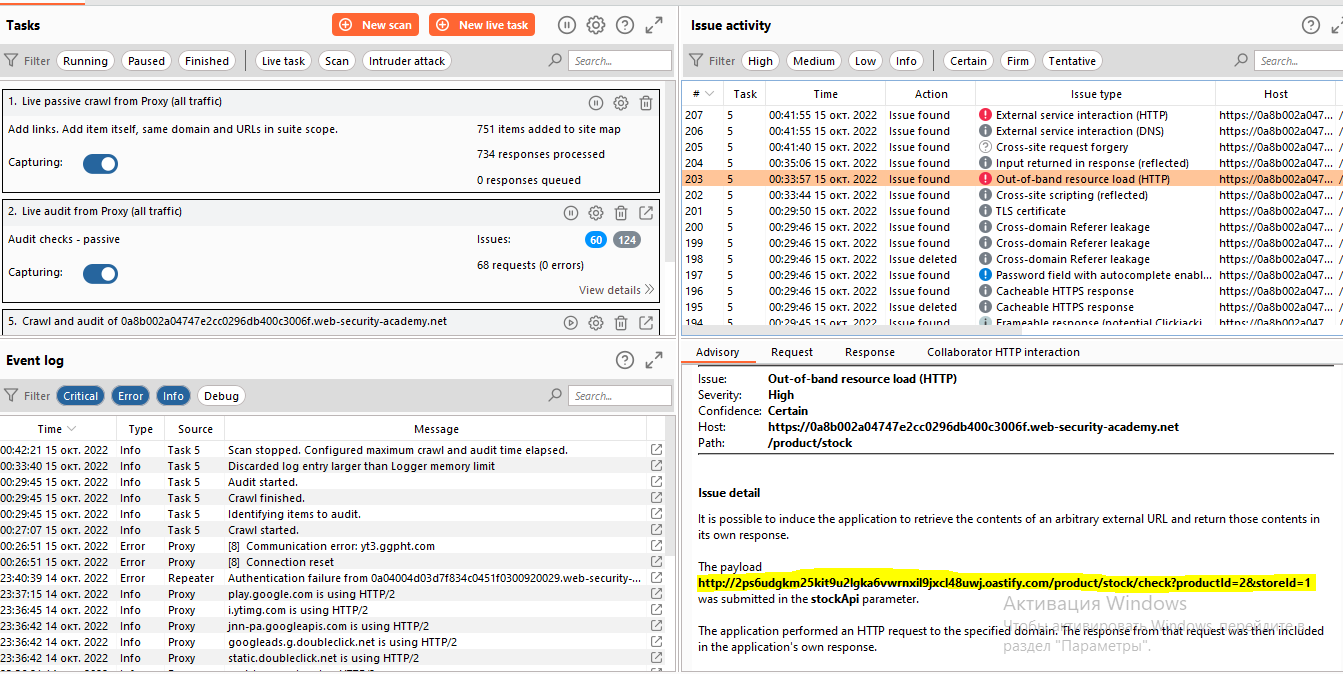
Изменим и отправим запрос: stockApi=http://192.168.0.24:8080/admin/delete?username=carlos



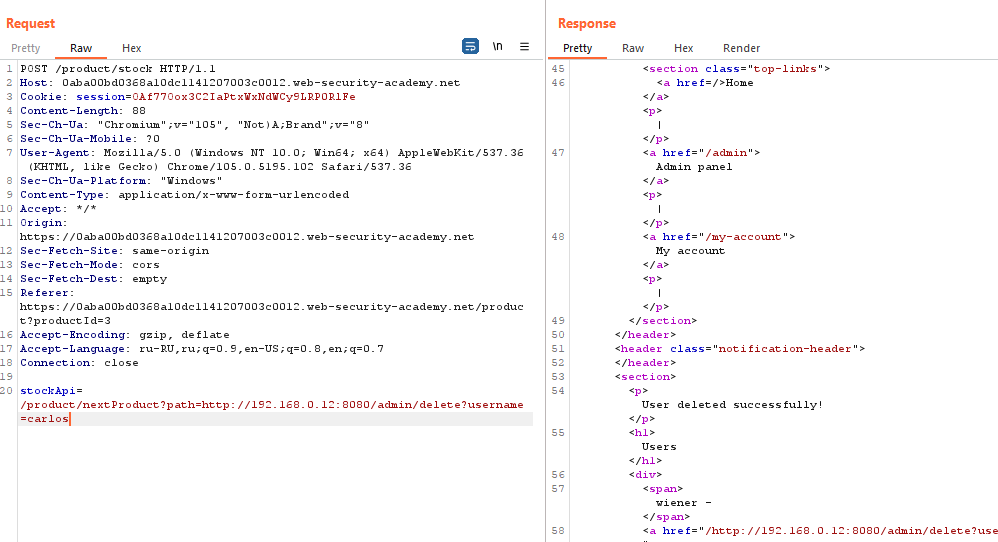
1. **SSRF with blacklist-based input filter**



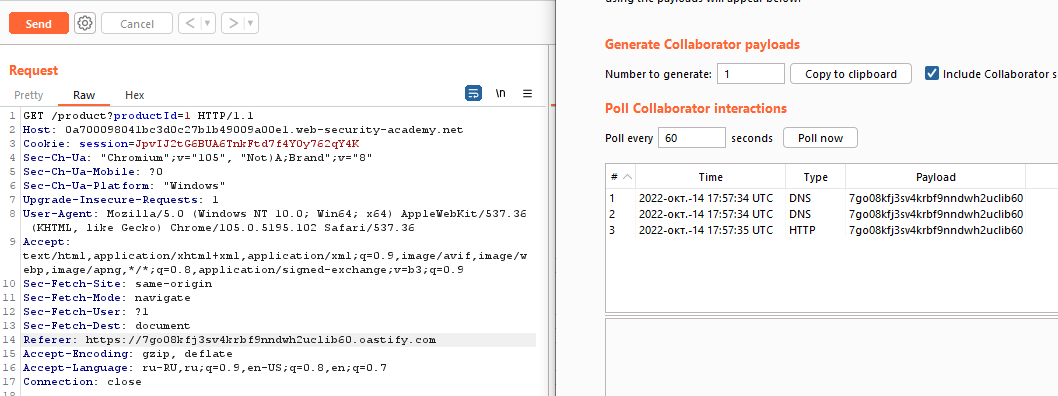
**Автоматизация:**



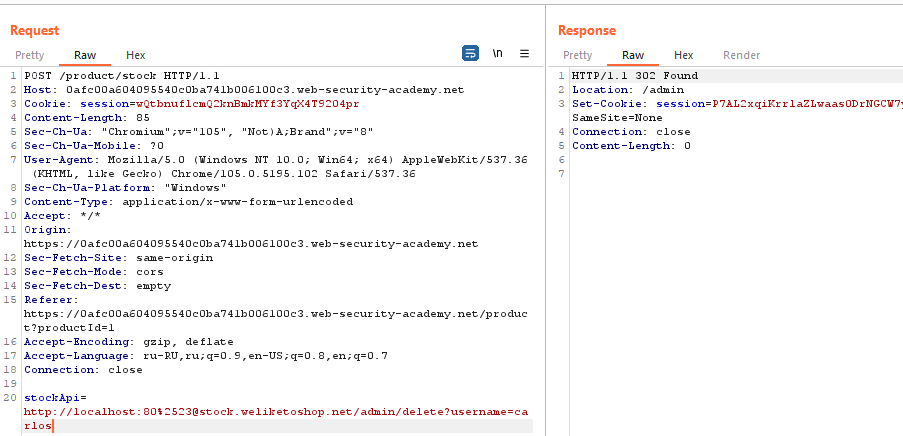
1. **SSRF with filter bypass via open redirection vulnerability**



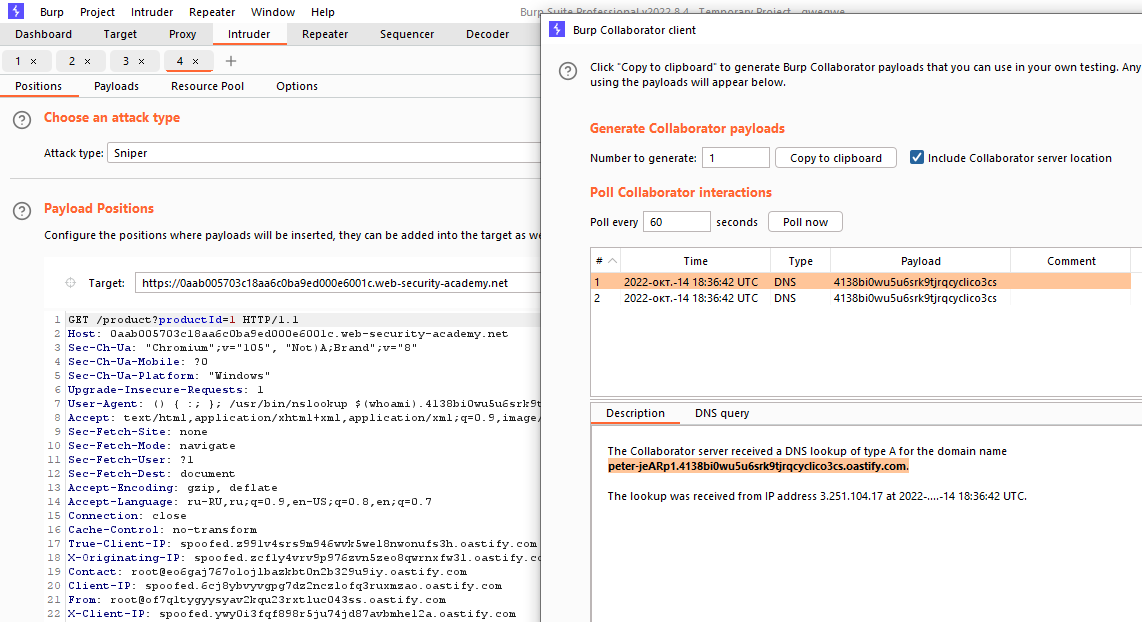
1. **Blind SSRF with out-of-band detection**

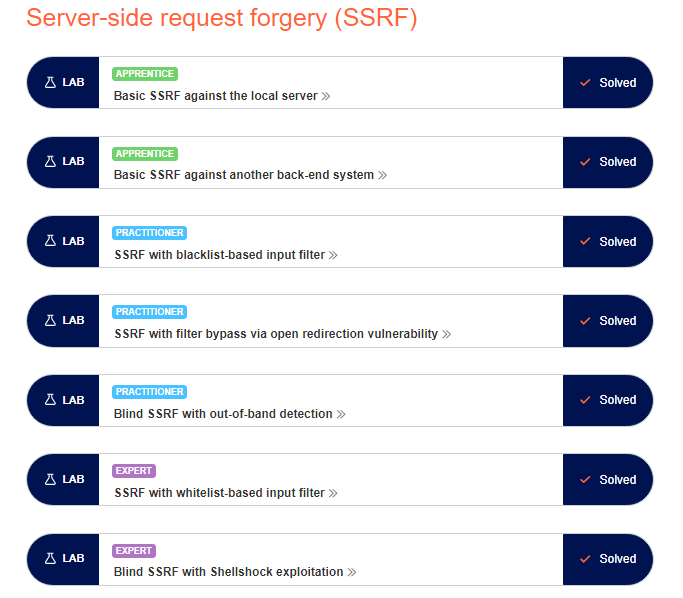


1. **SSRF with whitelist-based input filter**



1. **Blind SSRF with Shellshock exploitation**

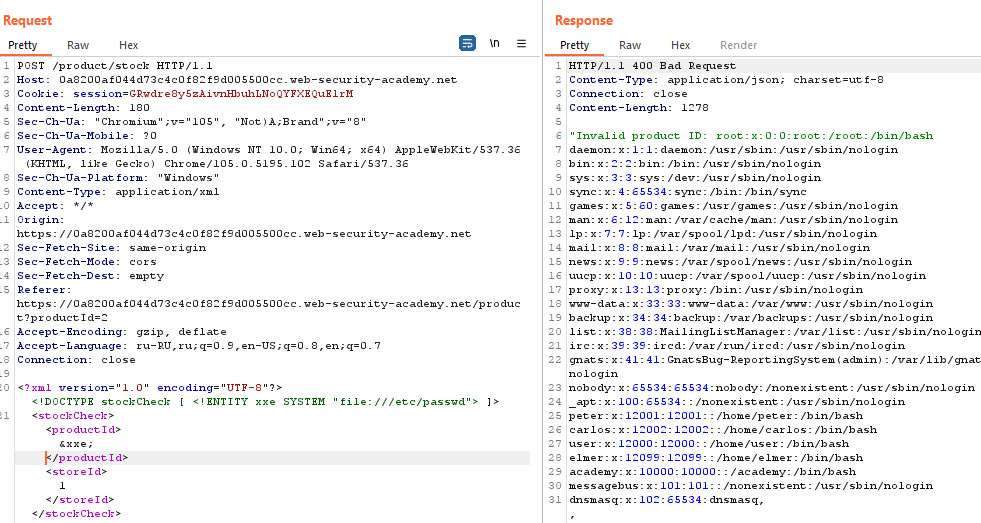




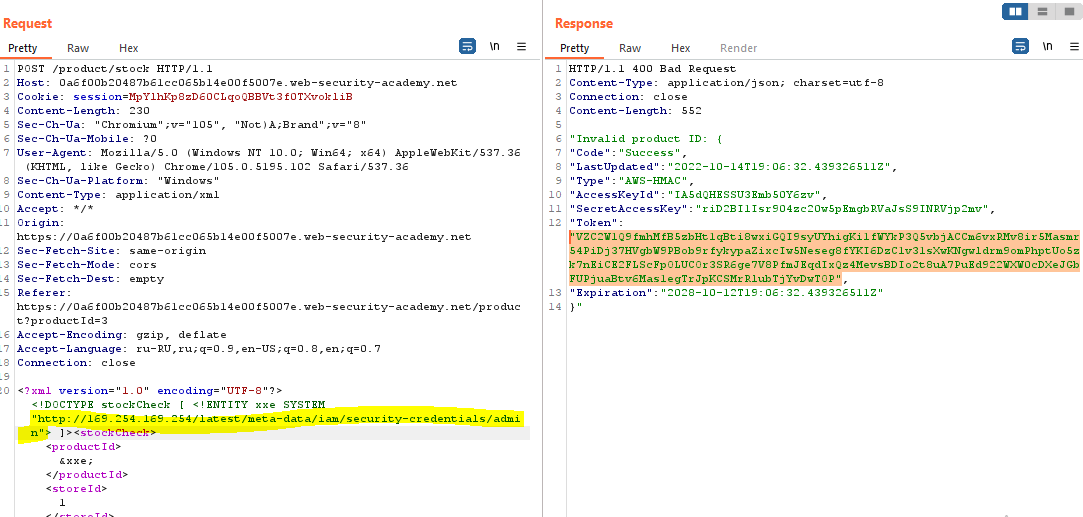
**Lab XXE:**

Выполнение примеров заданий на [сайте](https://portswigger.net/web-security/xxe/):

1. **Exploiting XXE using external entities to retrieve files.**



1. **Exploiting XXE to perform SSRF attacks.**



1. **Blind XXE with out-of-band interaction**

