

Benjamin Suljevic 4AHITS

18.04.2024

PortSwigger

- Burp Suite Community Edition installieren

API Testing

Exploiting an API endpoint using documentation

Lab: Exploiting an API endpoint using documentation

APPRENTICE



LAB

Not solved



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`.

Required knowledge

To solve this lab, you'll need to know:

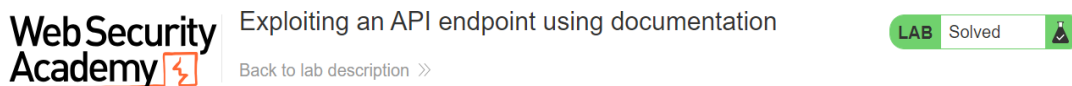
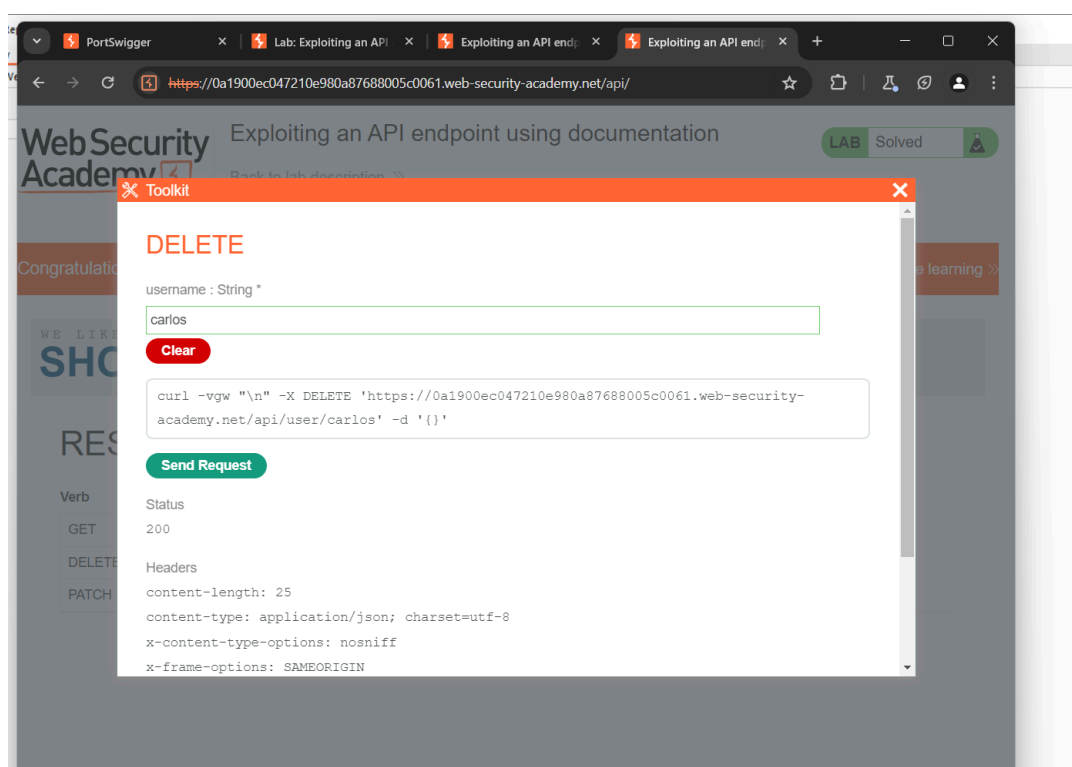
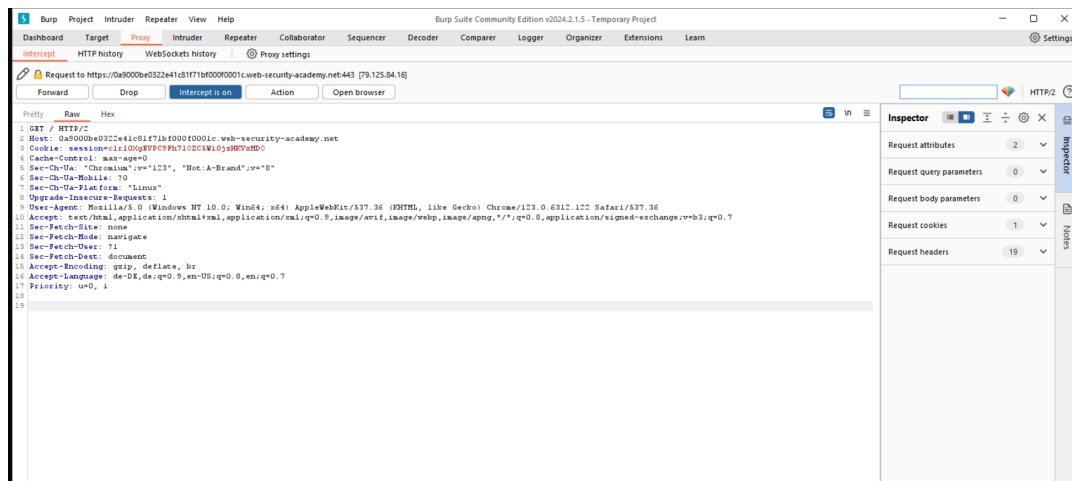
- What API documentation is.
- How API documentation may be useful to an attacker.
- How to discover API documentation.

These points are covered in our [API Testing Academy](#) topic.



ACCESS THE LAB

Den Link den man bekommt dann im Burp Suite Browser öffnen und unter Proxy **Intercept off** muss auf on geschaltet werden dann ebenfalls auf die Option Forward gehen+



Finding and exploiting an unused API endpoint

Lab: Finding and exploiting an unused API endpoint

PRACTITIONER

LAB

Not solved



To solve the lab, exploit a hidden API endpoint to buy a **Lightweight I33t Leather Jacket**. You can log in to your own account using the following credentials: `wiener:peter`.

Required knowledge

To solve this lab, you'll need to know:

- How to use error messages to construct a valid request.
- How HTTP methods are used by RESTful APIs.
- How changing the HTTP method can reveal additional functionality.

These points are covered in our [API Testing Academy](#) topic.



ACCESS THE LAB

Das Produkt was man ausgewählt hat jetzt noch suchen

The screenshot shows the Burp Suite interface. At the top, there's a table of HTTP requests. The selected request is a GET to `/api/products/1/price`. A context menu is open over this request, showing options like 'Add to scope', 'Scan', 'Send to Intruder', 'Send to Repeater', 'Send to Sequencer', 'Send to Organizer', 'Send to Comparer (request)', 'Send to Comparer (response)', 'Show response in browser', 'Request in browser', 'Engagement tools [Pro version only]', and 'Show new history window'. The 'Send to Repeater' option is highlighted.

Den GET Request zu einem PATCH ändern

The screenshot shows the 'Request' tab in Burp Suite. The request is a PATCH to `/api/products/1/price`. The 'Host' is `0a8600090458150b8244a17100290000.web-security-academy.net`. The 'Cookie' is `session=h16N6YsxUCmzZCiyWfx612PJpnSCv2M9`. The 'Sec-Ch-Ua' header is `"Chromium";v="123", "Not:A-Brand";v="8"`. The 'Request' tab is selected, and the 'Raw' view is shown.