Lab name: [CORS vulnerability with trusted null origin](https://portswigger.net/web-security/cors/lab-null-origin-whitelisted-attack)

Severity: High

Lab description:

* This lab demonstrates a **CORS misconfiguration** where the server incorrectly trusts the Origin: null.
* Some browsers send null as the origin when requests are made from **sandboxed iframes**, **files opened locally**, or **PDFs**.
* If the server allows CORS requests from Origin: null, attackers can exploit this to read sensitive data.

Impact:

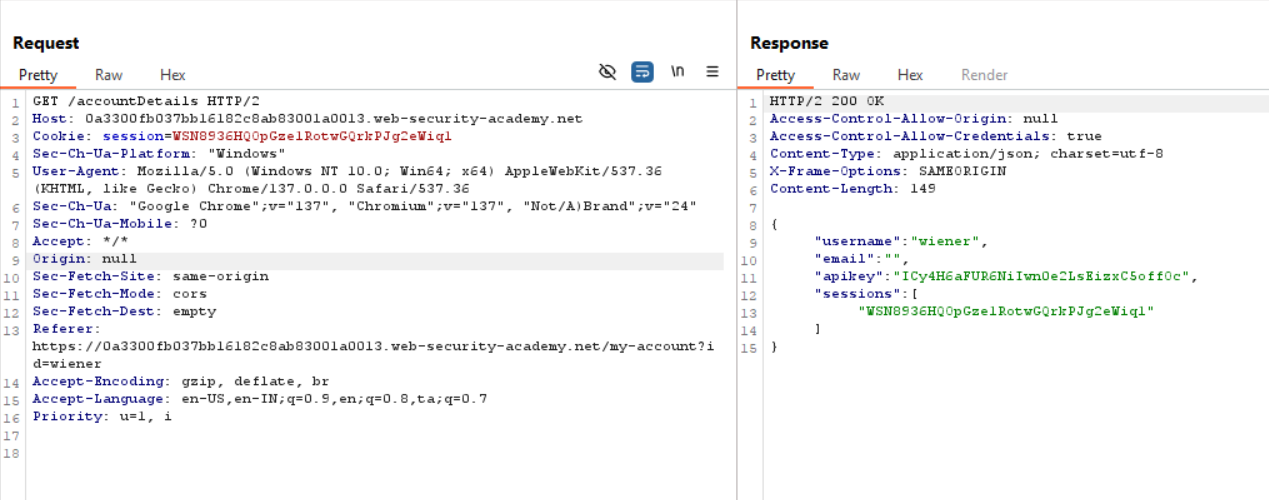
* An attacker can craft a malicious web page, host it locally or in a sandboxed iframe, and trick users into opening it.
* The browser sends a CORS request with Origin: null.
* The vulnerable server treats null as a trusted origin and responds with sensitive data.
* This breaks the Same-Origin Policy, exposing user data like email, profile info, or tokens.
* Attackers can steal data from authenticated users silently.
* This can also affect internal tools or systems opened in file:// URLs or from PDFs.

Recommendations:

* Never allow Access-Control-Allow-Origin: null unless there’s a **very specific reason** and it’s tightly controlled.
* Implement a strict **whitelist of allowed origins** and block all others.
* Do not use wildcards or loose CORS policies, especially with sensitive data.
* Use browser security headers and server-side checks to prevent abuse.
* Log and monitor CORS requests, especially those with unusual origins.
* Review application CORS settings regularly for misconfigurations.

Steps to reproduce:

* 1. Access the lab and login with the username and password provided.
  2. Notice that the details are retrieved in the /accountDetails request.
  3. Set a header Origin with null value and send the request. This is accepted by the server.



* 1. Now in the body of the exploit server, write a code to retrieve user details, store and deliver it to the victim.
  2. Now in he access log we can find the Admin’s API key.



* 1. Decode the key in burpsuite to get the API key and submit the solution to solve the lab.

