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

Severity: High

Lab description:

* This lab shows a CORS misconfiguration where the server reflects the value of the Origin header in the Access-Control-Allow-Origin response.
* If a malicious website sets its own domain in the Origin header, the server allows it, enabling cross-origin access.
* The goal is to use this to steal sensitive information from the victim’s account.

Impact:

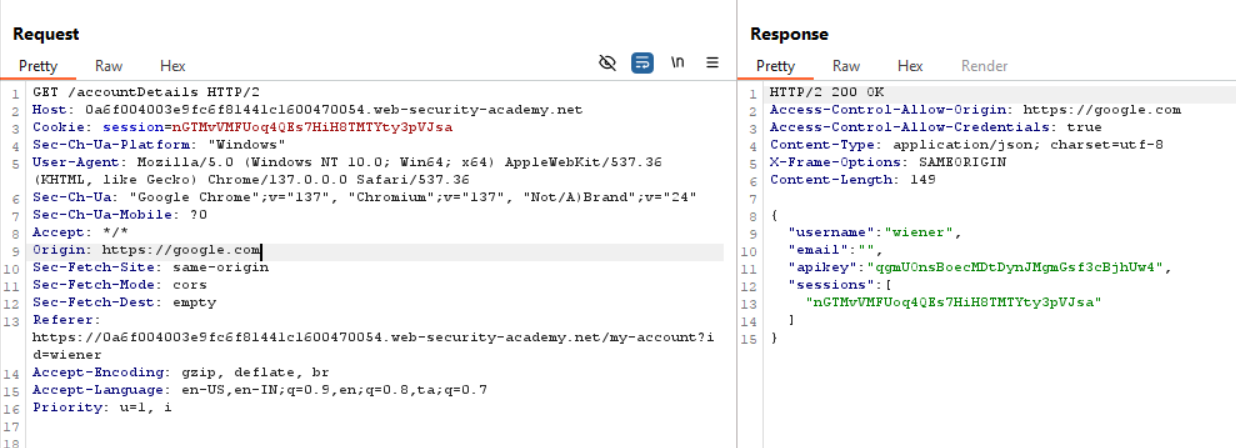
* Attackers can host a fake website and trick a logged-in user into visiting it.
* The fake site makes a hidden request to the vulnerable site with a custom Origin.
* The vulnerable site reflects this origin in the response, allowing the attacker to read private data.
* Sensitive user information like names, email addresses, or tokens can be stolen.
* The attack works silently, and users won’t notice anything unusual.
* This breaks the Same-Origin Policy, which is meant to protect user data.

Recommendations:

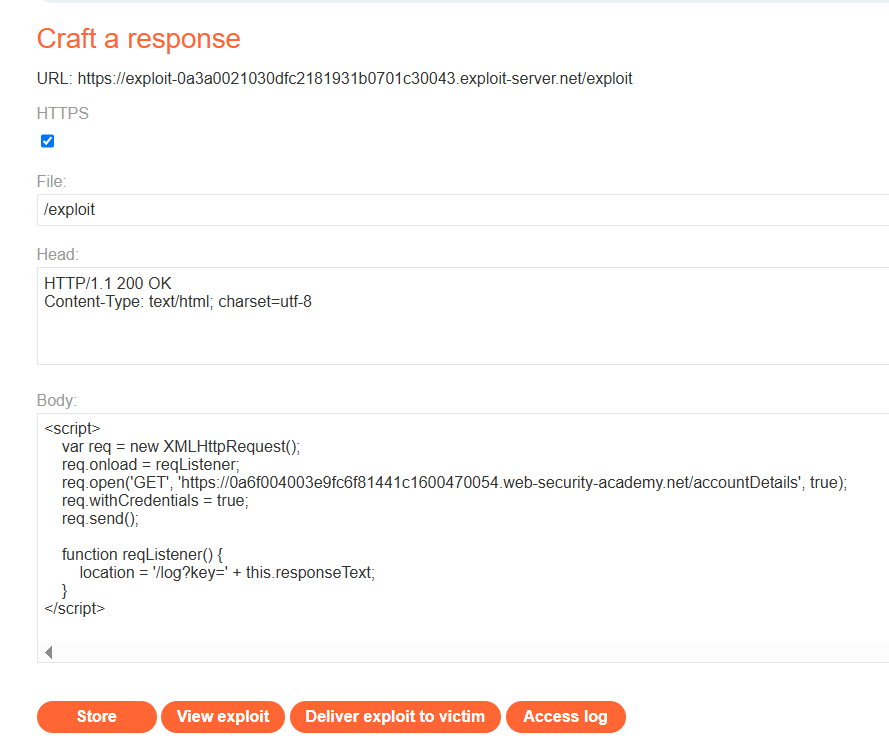
* Do **not reflect the Origin header value** directly in Access-Control-Allow-Origin.
* Allow only specific trusted domains by using a **strict CORS whitelist**.
* Avoid using Access-Control-Allow-Credentials: true unless absolutely necessary, and never with \* as the origin.
* Validate the Origin server-side before including it in the response.
* Regularly review and test CORS settings to prevent misconfigurations.
* Use security headers and browser policies to restrict unnecessary cross-origin access.

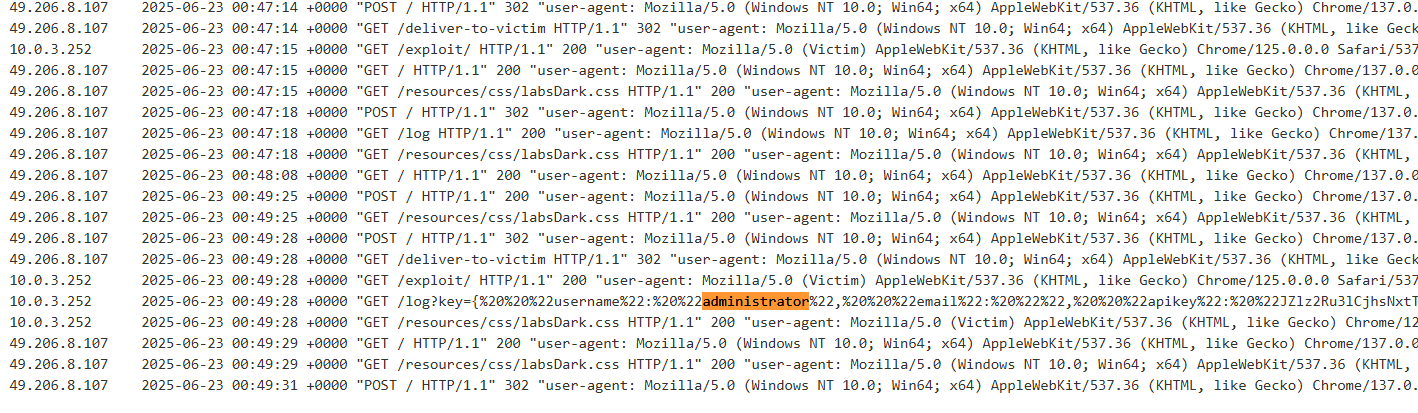
Steps to reproduce:

1. Access the lab and login using the username and password provided.
2. In the burpsuite, to the /accountDetails GET request, add a header *origin: google.com* and send the request. Notice the response accepts the origin.



1. In the body of exploit server, craft a code that retrives API from all the accounts.





1. Store and deliver to the victim, in the access log, it can be noticed that API of the administrator is encoded. Decode it using burpsuite decoder and submit the API key to solve the lab.

