Lab name: [Information disclosure on debug page](https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-on-debug-page)

Severity: High

Lab description:

* This lab focuses on the debug page that discloses sensitive information about the application.
* This application reveals the sensitive internal application information such as server paths. These details can help attackers to attack application using privilege escalation or other known vulnerabilities.

Impact:

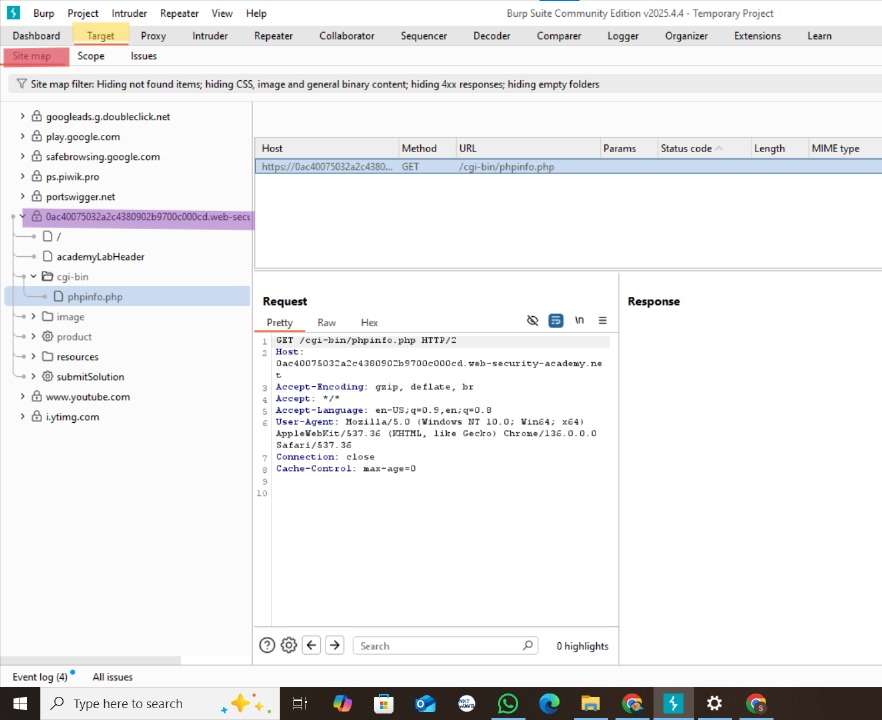
* Details of the server page and PHP files, code resources are revealed.
* Due to this there is lots of potential that attacks can happen using those end points.
* Confidentiality is impacted here, leading to high severity.

Recommendation:

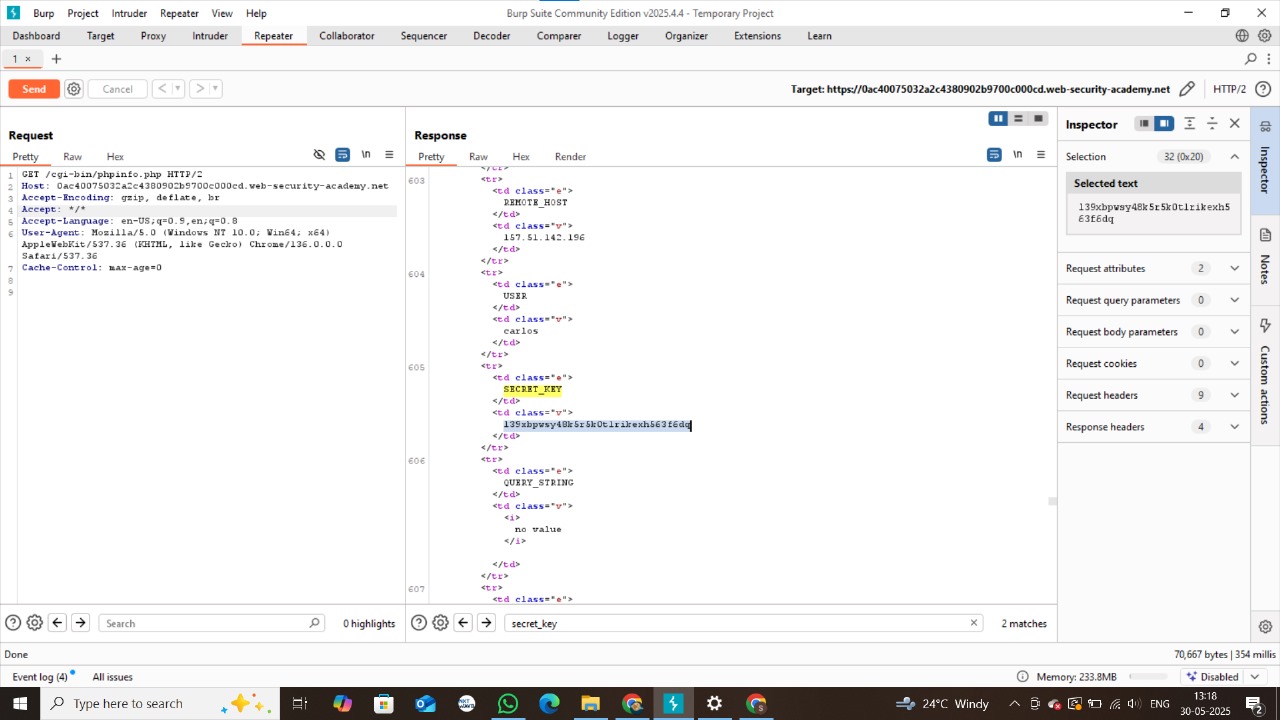
* Restrict access to sensitive tools and pages using authentication, setting up session time-outs and such things implementing access controls
* Ensure developer options are disabled for the end-user.
* Application should be developed using security measures.

Steps to reproduce:

* After accessing the lab, go to burp suite.
* Now switch to target tab -> site map. There access the lab’s link and notice all the files that can be accessed.



* Send the *cgi-bin/phpinfo.php* to repeater and see the response.



* Notice that there is SECRET\_KEY tag that is only visible in the HTML page of the response.
* Submit the key and lab is done.