Lab name: [Authentication bypass via information disclosure](https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-authentication-bypass)

Severity: Critical

Lab description:

* This lab focusses on exploiting login page’s vulnerability using the leaked information that helps in identifying valid endpoints and gain unauthorized access.
* Should observe HTTP headers to exploit the vulnerability.

Impact:

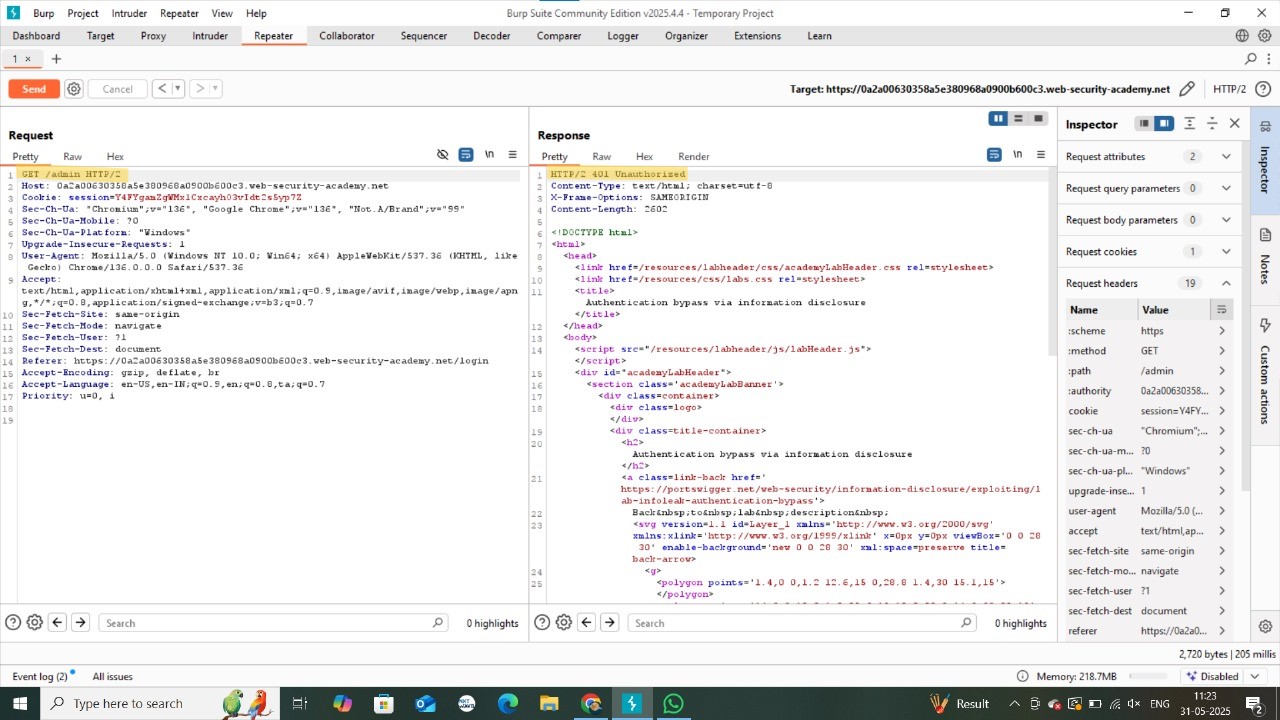
* Unauthorized access can be done to the admin page itself, so confidentiality and integrity can be affected.
* The attackers may also get access some other URLs which might have access to important files or directories.
* Privilege escalation can happen because there is one login Id and password given, through which attackers can exploit the application.
* Reputation and compliance risks are high.
* Here confidentiality and integrity impacts are high. Thus, there is high severity.

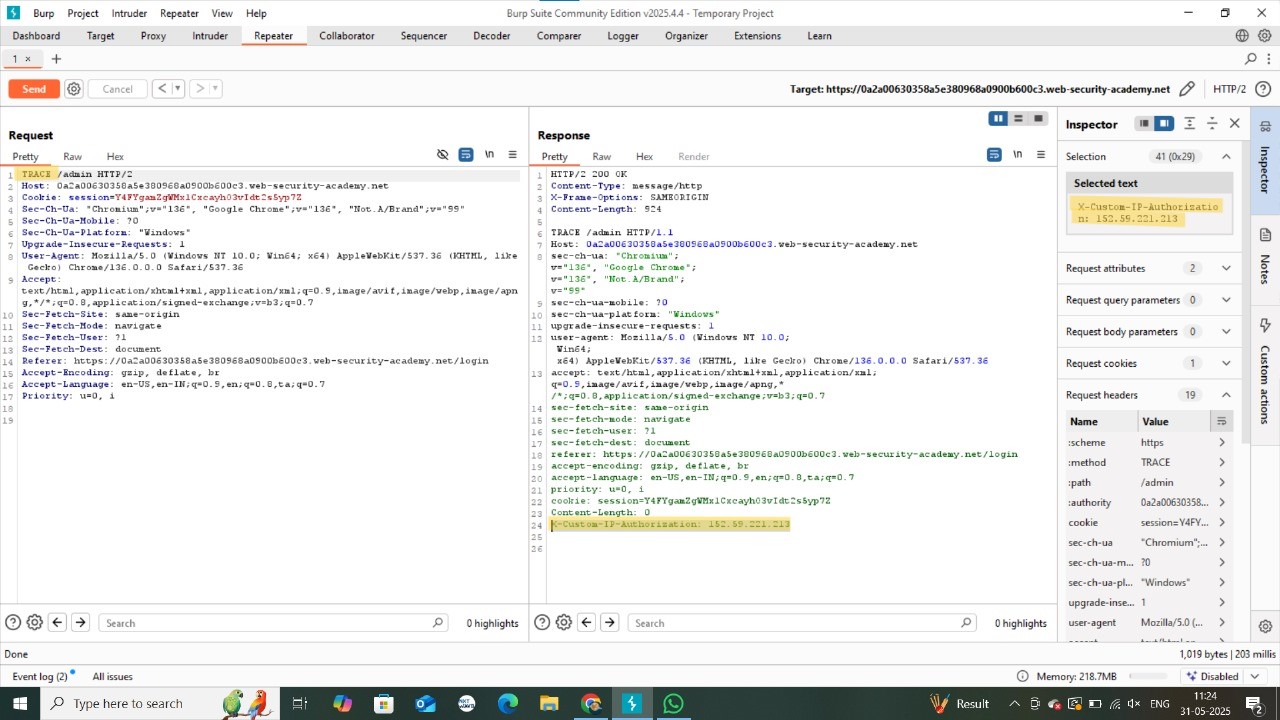
Recommendations:

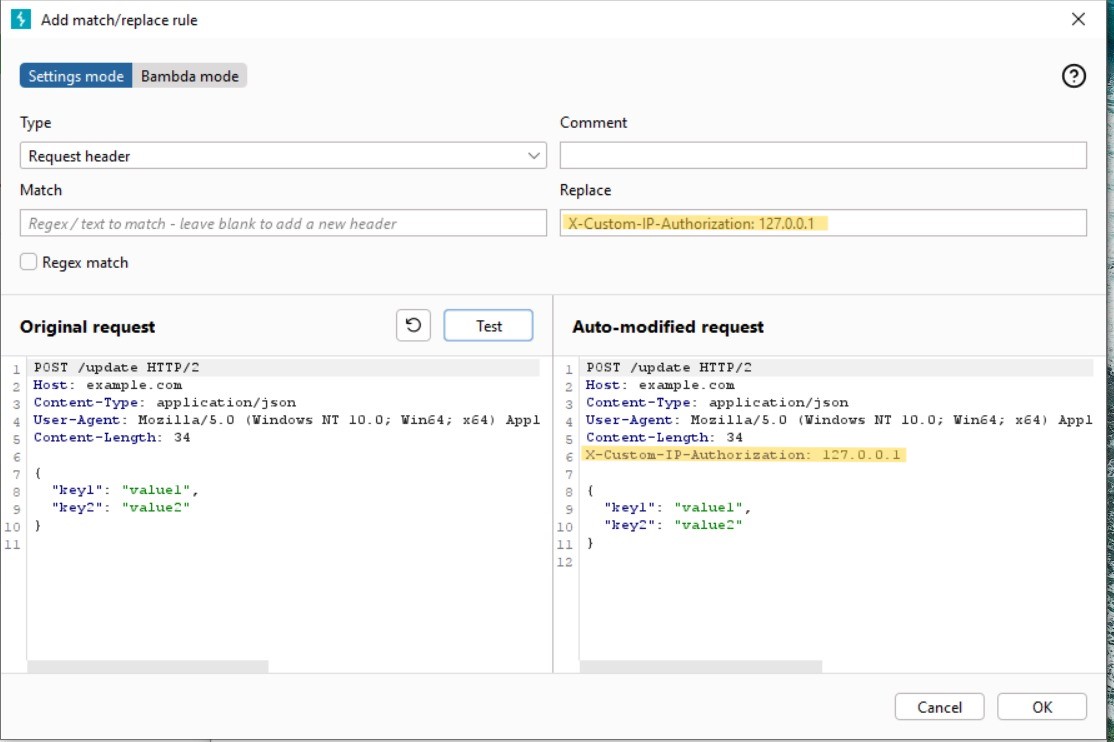
* Avoid exposing security headers to the client
* Avoid trusting Ip addresses for authentication, enforcement of valid session tokens makes the application secure
* Enable only needed HTTP request methods, disabling TRACE request would be better solution in this case
* Show only generic error messages
* Validate headers each time when a request is made.
* Removal of sensitive comments in the HTML documents will be a secure method

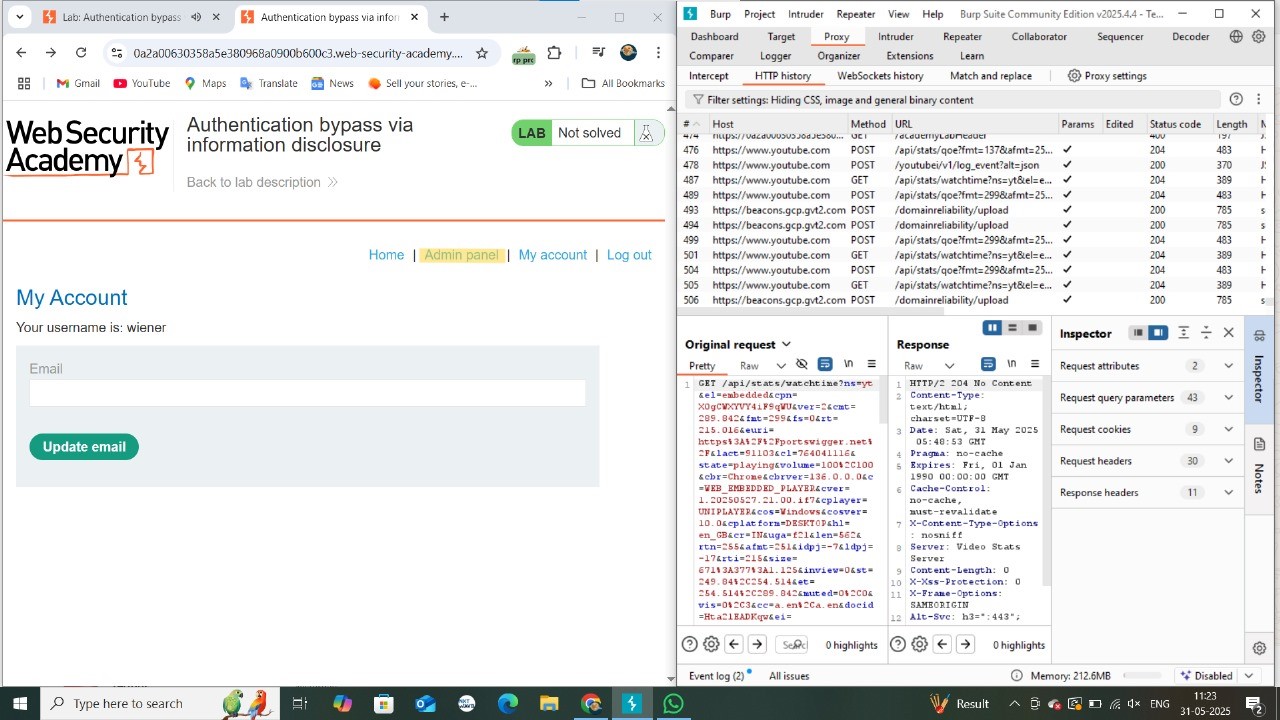
Steps to reproduce:

* Access the lab and start the burp.
* Now we can see a request with GET request and ‘/’ in the URL, send this request to the repeater.
* Now change URL to /admin, it is noticeable that there is error code 401 with unauthorized access, it also reveals that it should be requested from a trusted IP address, also try with TRACE request method, it is going to show the IP address header, which can be customized.





* Now we move to Match and replace in the proxy tab and in replace tab we add our IP address (127.0.0.1) using ‘*X-Custom-IP-Authorization: 127.0.0.1*’.
* Now every request that is sent to the server will go along with this header, in which the server thinks that this is a request from Administrator



* Now Admin panel is shown once after reloaded.
* Enter into admin panel and delete *Carlos* user. Thus, lab solved.

