Setup-PTest

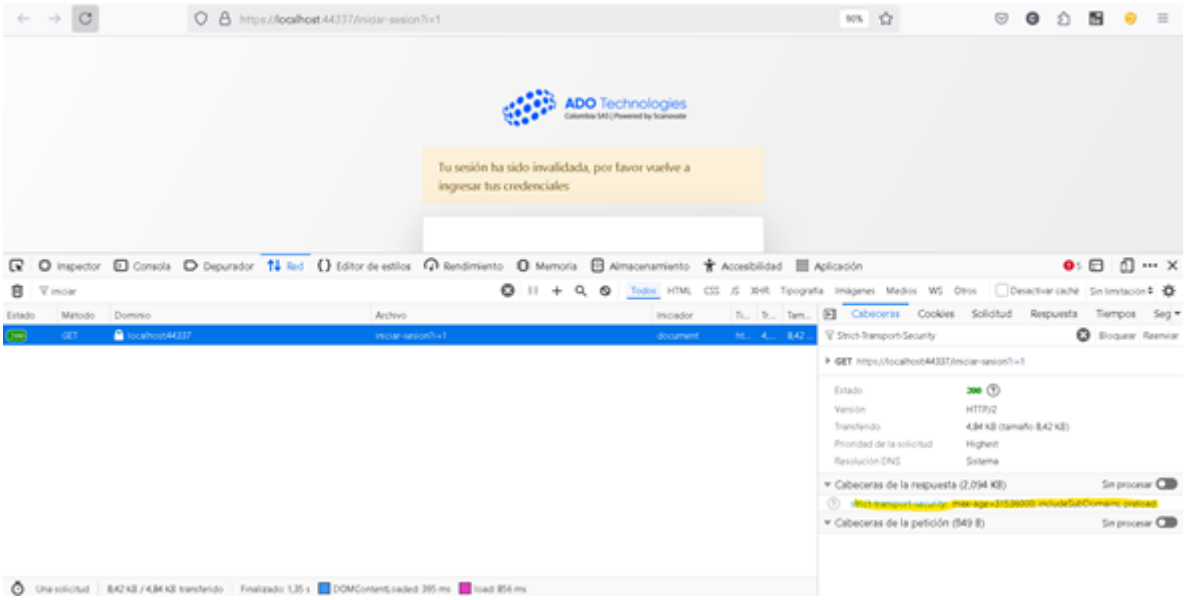
1. **HTTP Strict Transport Security (HSTS) Policy Not Enabled**

    1.1. The header is added to the responses from the server.

    ```
    response.AddHeader("Strict-Transport-Security", "max-age=31536000; includeSubDomains; preload");
    ```

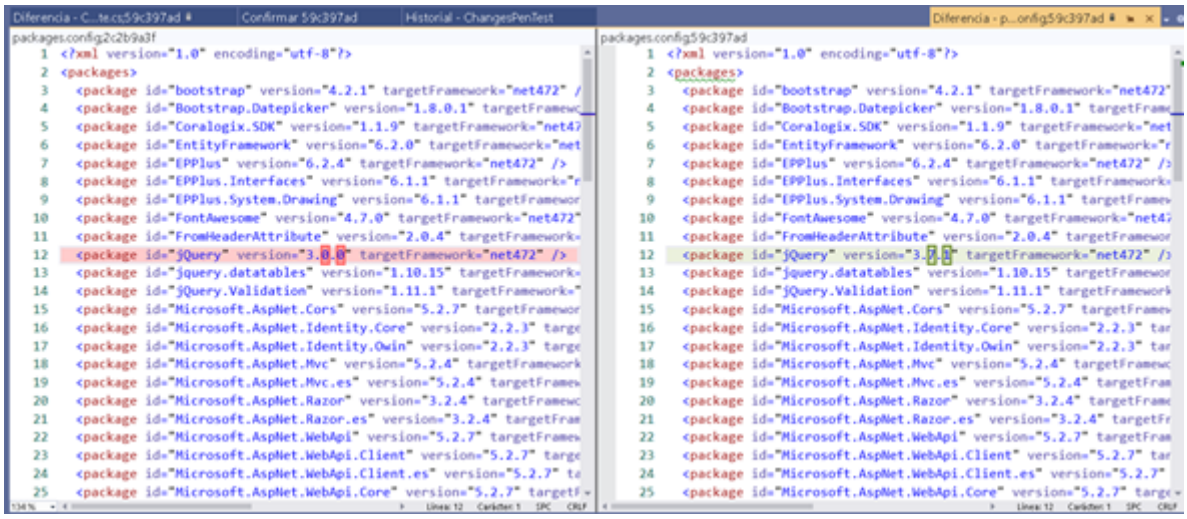
    |

    And it can be evidenced in the site's response:

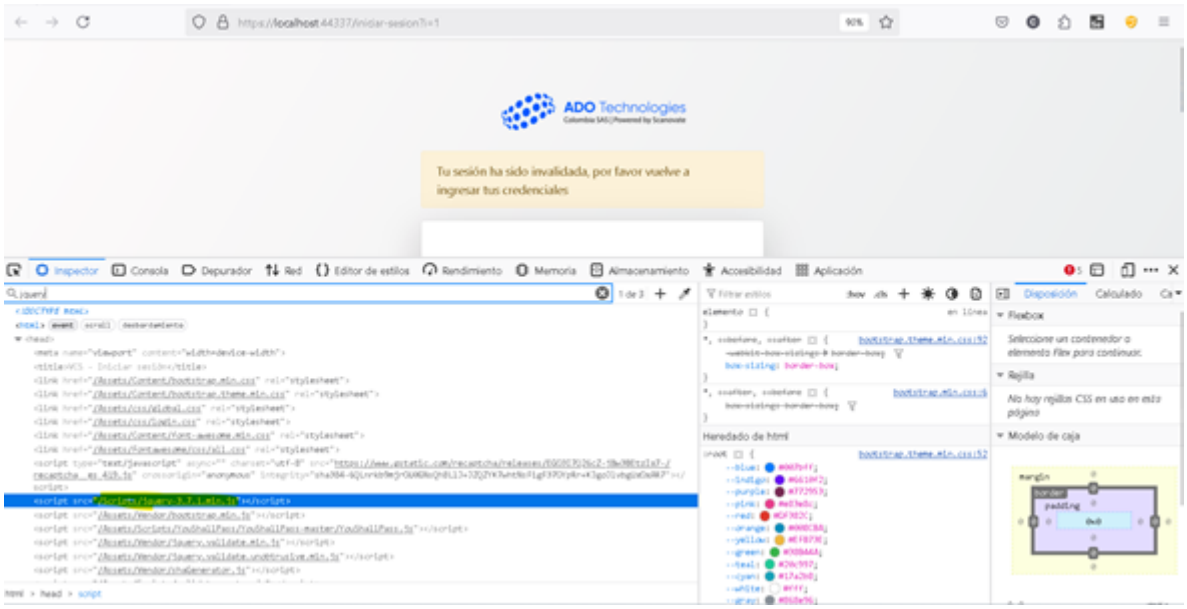
    

2. **Vulnerable JavaScript Libraries**

    2.1. Jquery library upgraded to the latest version

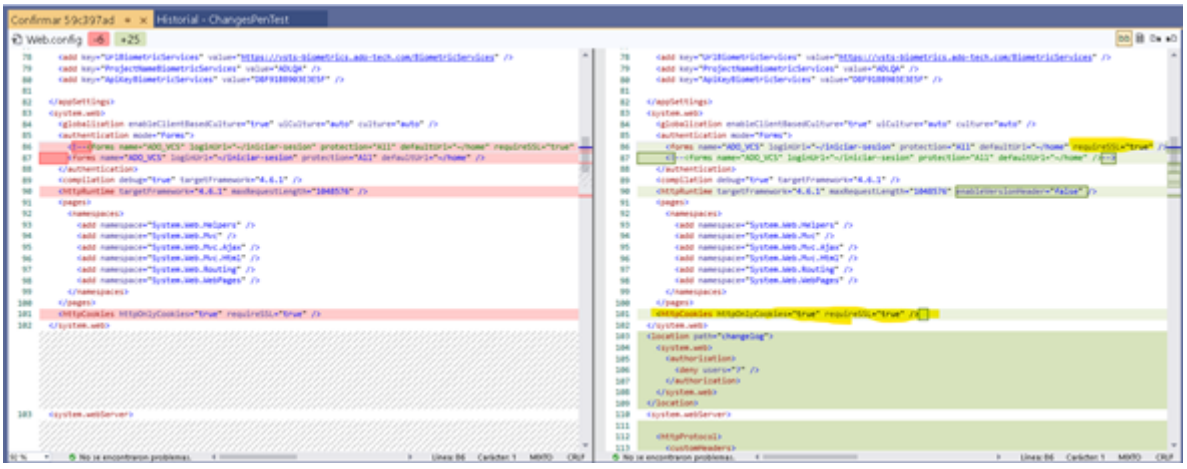


and the references are updated in the code as evidenced by the page loading

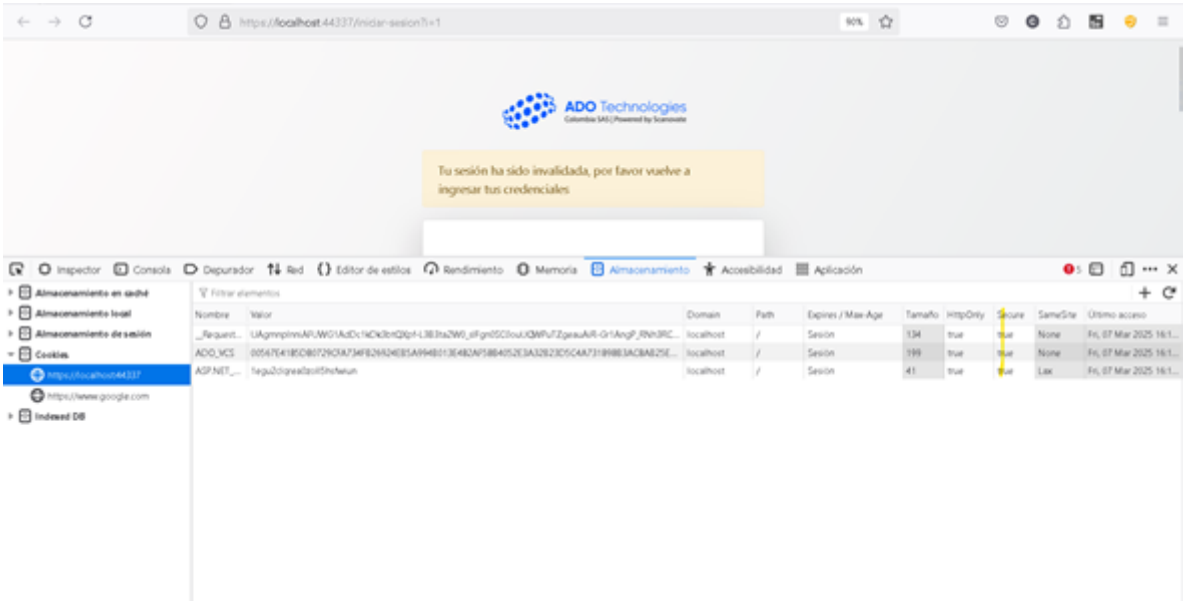


3. **Cookies Not Marked as Secure**

3.1. In the Forms tag, the attribute requireSSL=true is added and the httpCookies tag is added.

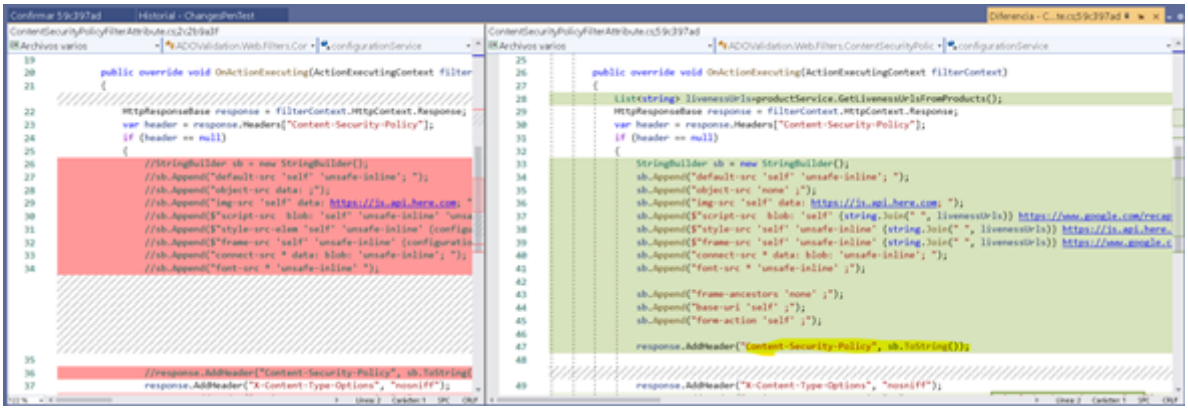


And on the site it can be seen that now all cookies are marked as secure.

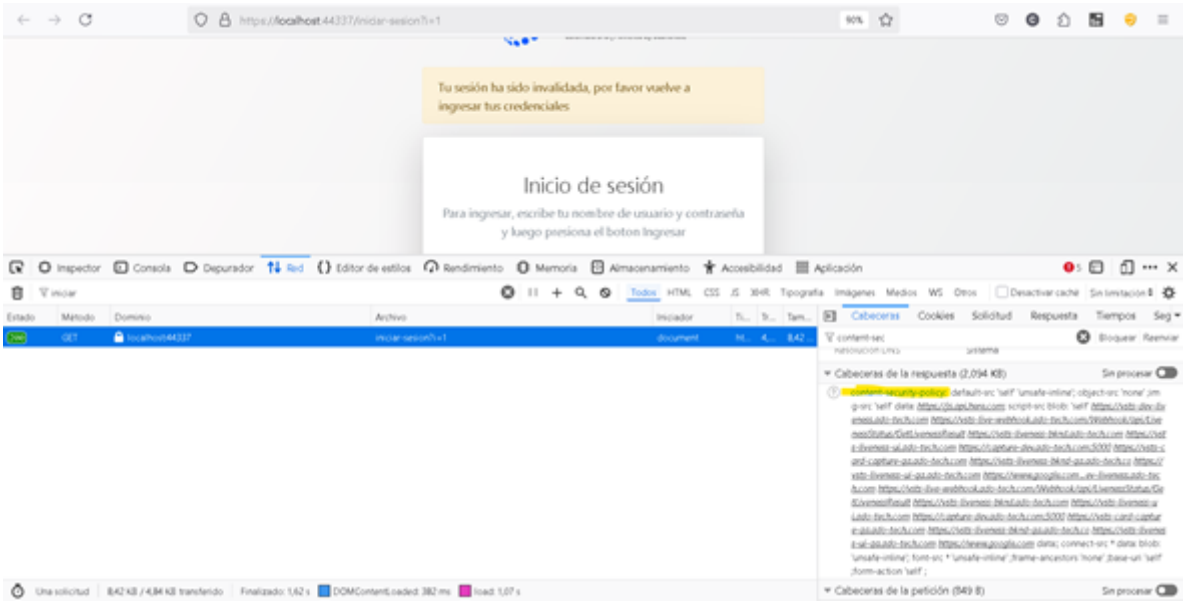


4. **Content Security Policy (CSP) Not Implemented**

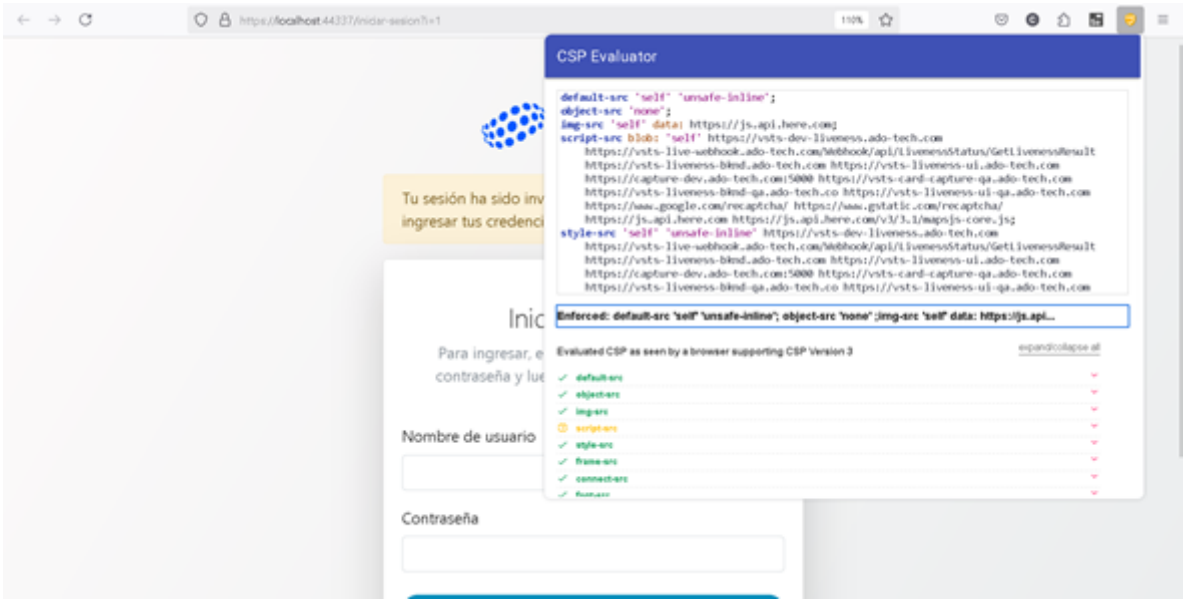
4.1. The CSP is added through the code



And it is evident in the site headers

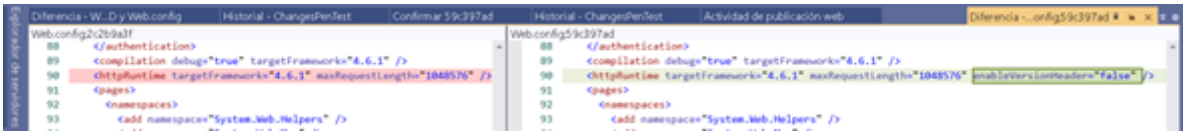


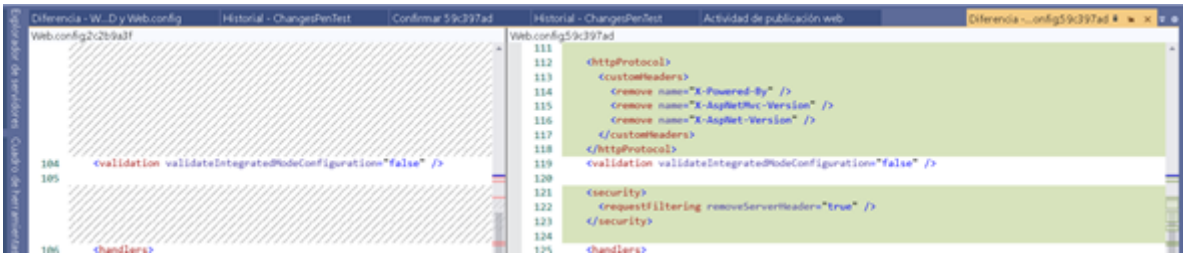
In addition, the Google CSP validator is installed, and a positive result is obtained on the site.



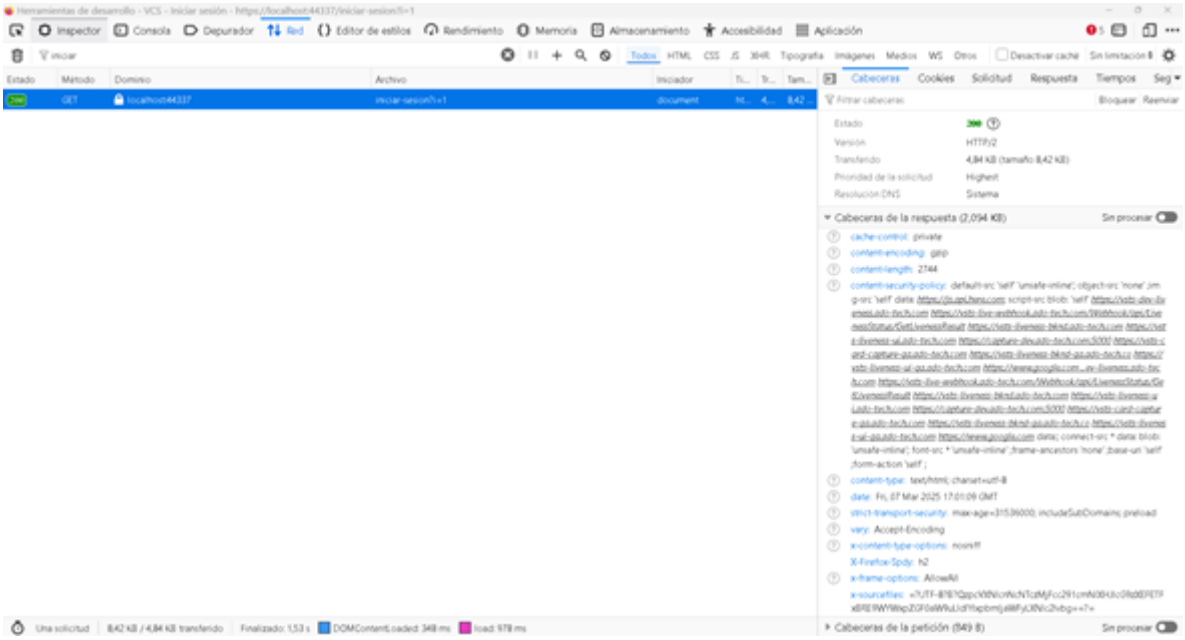
5. **Information Disclosure**

5.1. The following tags and tag attributes are added to hide the header with server and code information

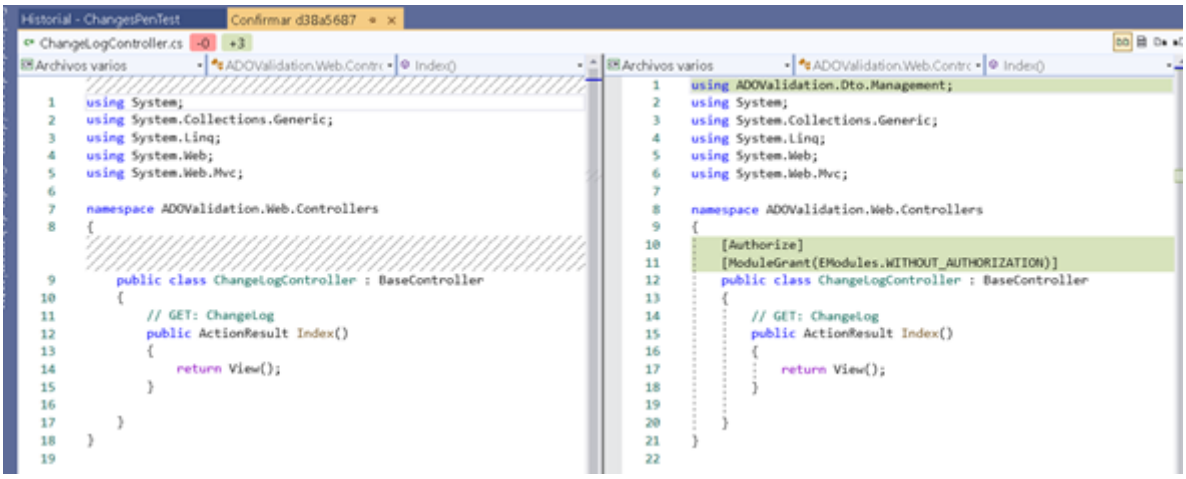




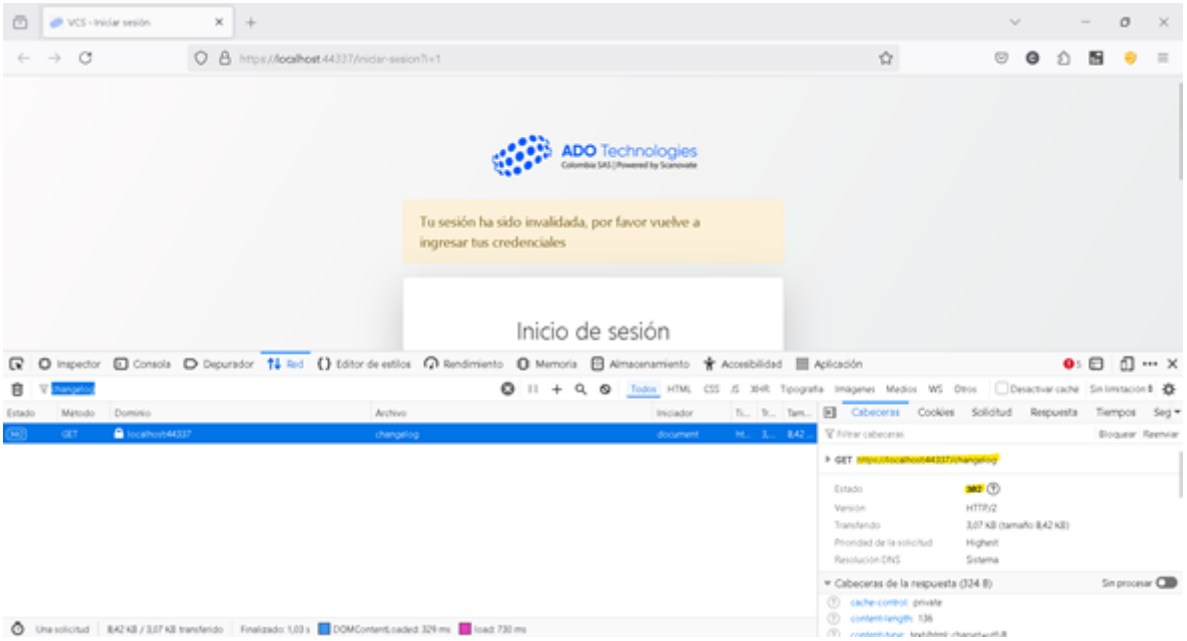
And as can be seen in the response headers there are no longer headers with server data and framework versions.



To control access to the changelog, access is controlled by the following code



And as you can see it is not possible to access without logging in.



Revision #2
Created 10 March 2025 20:07:50 by Admin
Updated 10 March 2025 20:17:43 by Admin