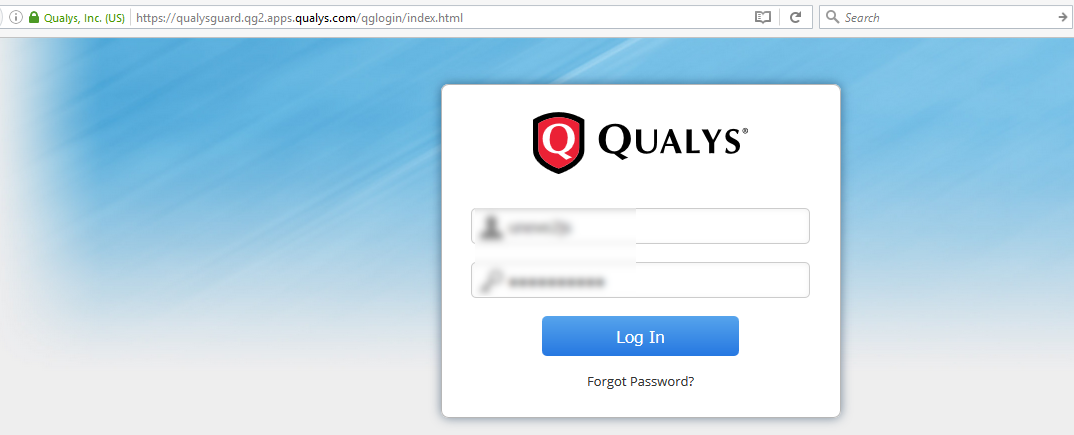
**Vulnerability in Qualys Guard Online Scanner Web Application**

Vulnerability: Improper Cache Control

Improper cache control :- In this phase, we check that the logout function is properly implemented, and that it is not possible to “reuse” a session after logout. We also check that the application automatically logs out a user when that user has been idle for a certain amount of time, and that no sensitive data remains stored in the browser cache. The logout function must ensure that all session tokens (e.g., cookies) are properly destroyed or made unusable, and that proper controls are enforced at the server side to prevent the reuse of session tokens.

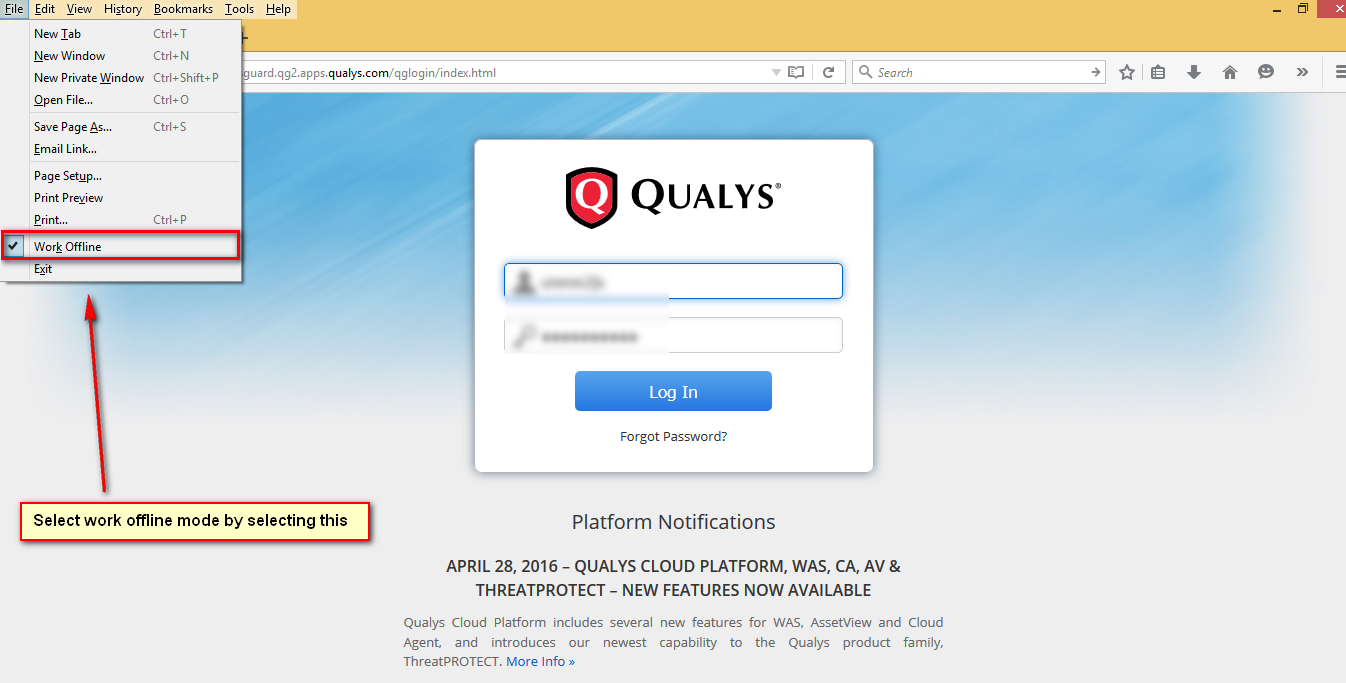
POC:

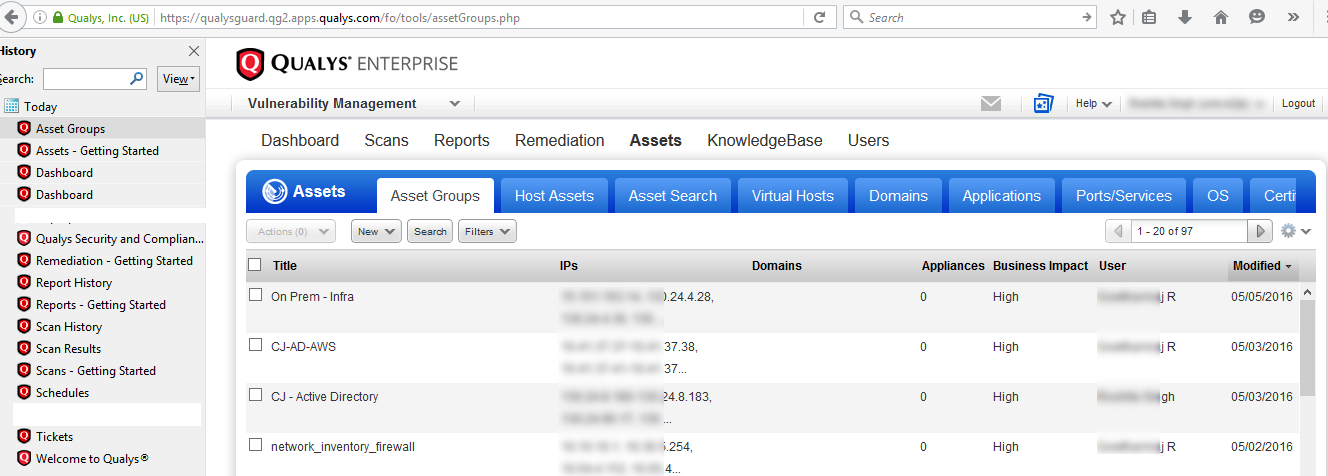
Step 1: Open the URL <https://qualysguard.qg2.apps.qualys.com/qglogin/index.html> in firefox browser and then login to the application with valid credentials.

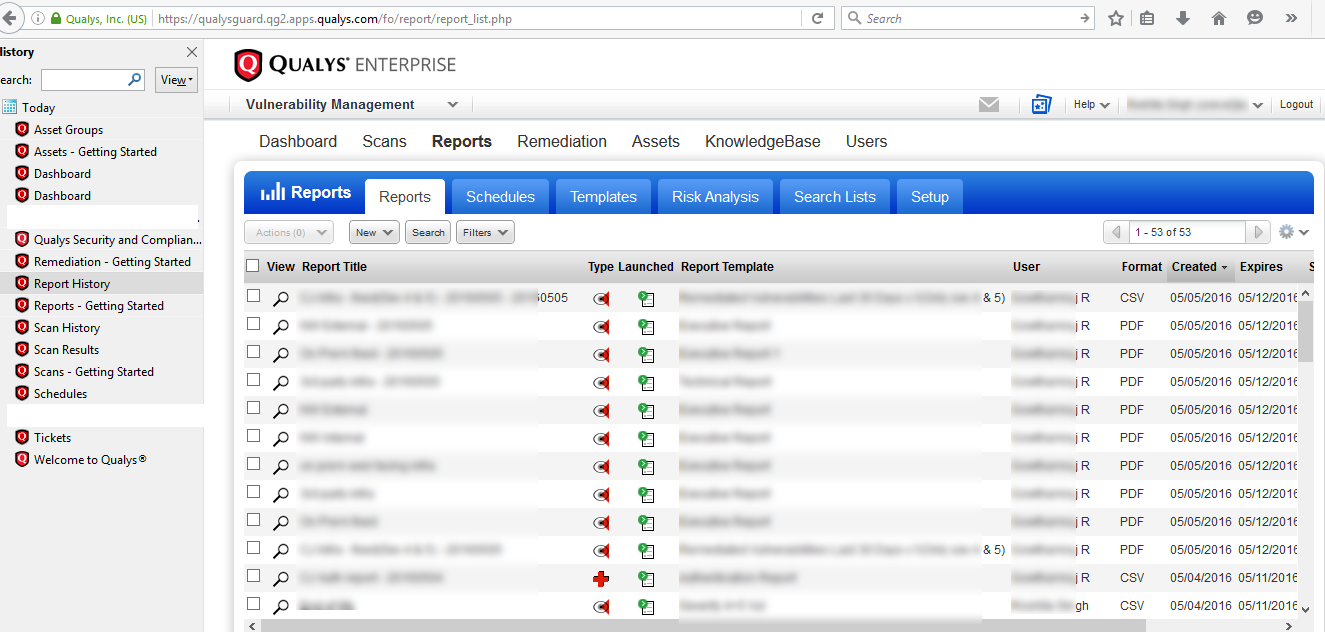


Step 2: After logging into the application browse some of the pages then logout of the application.

Step 3: Now go to menu of firefox and turn on work-offline mode by File🡪Work Offline.



Step 4: Now open history(ctrl+h) and try to open the internal authenticate pages and observe that we will be able to browse most of the pages.



Impact: By using this vulnerability attacker can see sensitive information line vulnerabilities found and IP Address/Web Application details and others.

How to Fix this:

Add this code to the application web pages, when you add this code to the application then every time when browser tries to login to the application it will revalidate the request.

<meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate" />

<meta http-equiv="Pragma" content="no-cache" />

<meta http-equiv="Expires" content="0" /

For more details visit the site:

<https://www.owasp.org/index.php/Testing_for_Logout_and_Browser_Cache_Management_(OWASP-AT-007)>

Below is a video link shown how it was done:

<https://youtu.be/O_IvOh3n9k>