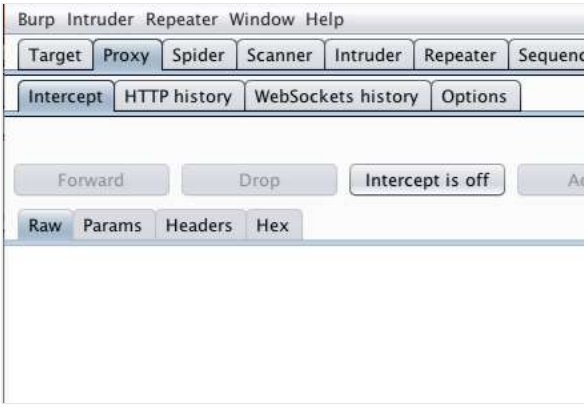
Using Burp to Test Session Token Handling

Regardless of how well session tokens are generated, the session mechanism of an application will be wide open to attack if those tokens are not handle carefully. For example, if tokens are disclosed to an attacker via some means, the attacker can hijack user sessions even if predicting the token is impos

The following tutorial demonstrates how to use Burp to test for session token handling issues.

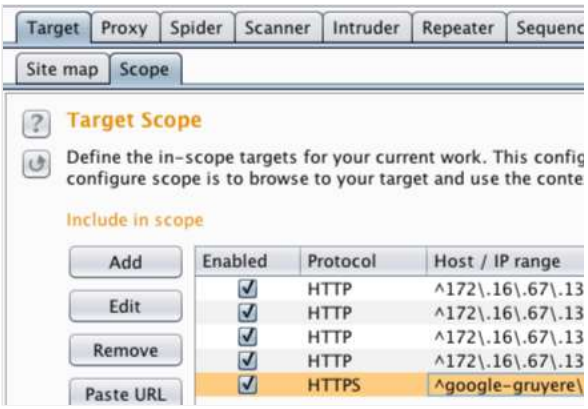
First, ensure that Burp is correctly configured with your browser.

With intercept turned off in the Proxy "Intercept" tab, visit the web application you are testing in your browser.



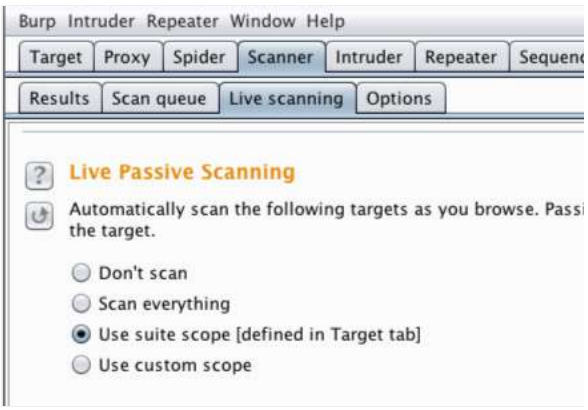
Go to the Target "Scope" tab.

Ensure that the target application is included in scope.



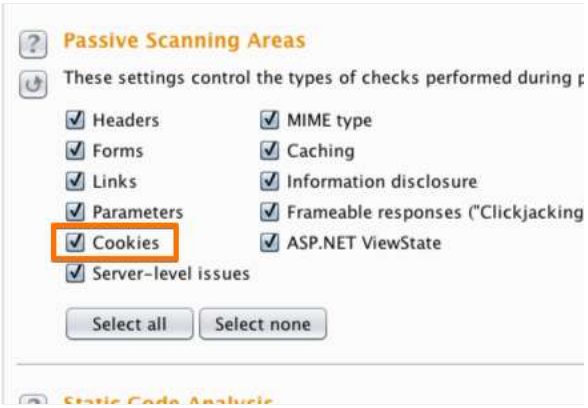
Go to the Scanner "Live Scanning" tab.

Ensure that live passing scanning is enabled for in-scope items.



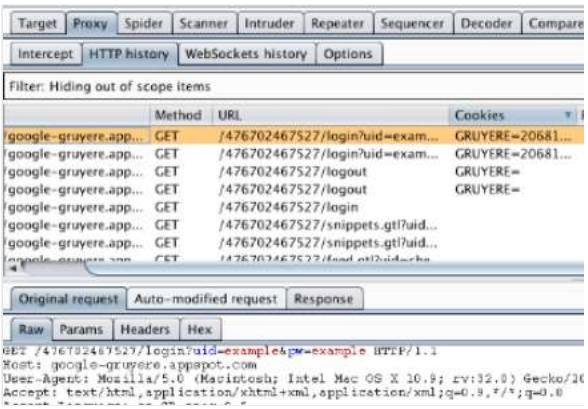
Go to the Scanner "Options" tab.

By selecting the appropriate scanning areas you can instruct Burp to scan for various session token handling issues, both actively and passively.



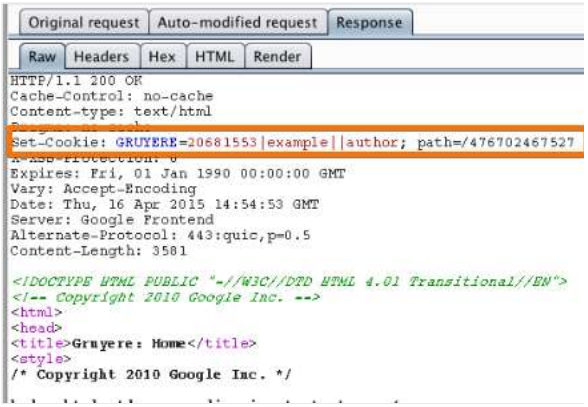
Walk through the application in the normal way from first access, through the login process, and then through all of the application's functionality.

A record can be kept of every URL visited in the "HTTP history" table. Pay particular attention to login functions and transitions between HTTP and HTTPS communications.



If cookies are being used as the transmission mechanism for session tokens, verify whether the "secure" flag has been set, preventing them from ever being transmitted over unencrypted connections.

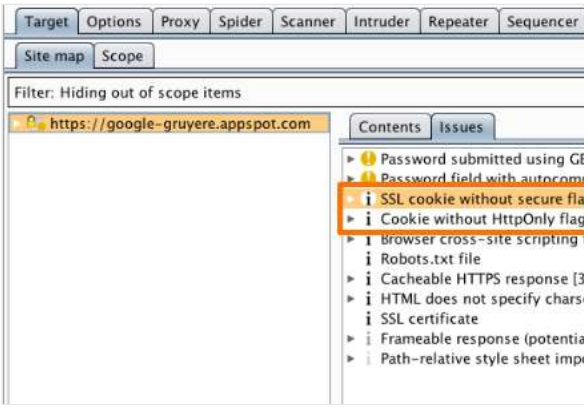
In this "Gruyere" example we can see that the secure flag has not been set.



Alternatively, go to the Scanner "Results" tab.

The Scanner's passive scan function detects session token management issues such as "SSL cookie without secure flag set" and "Cookie without HttpOnly flag set".

The Scanner also provides an advisory section with Issue detail, background and remediation.



Related articles:

Getting started with Burp Proxy

Getting started with Burp Scanner

Using Burp to attack session management