Using Burp to Test for Sensitive Data Exposure Issues

Sensitive Data Exposure vulnerabilities can occur when a web application does not adequately protect sensitive information from being disclosed to attac
This can include information such as credit card data, medical history, session tokens, or other authentication credentials.

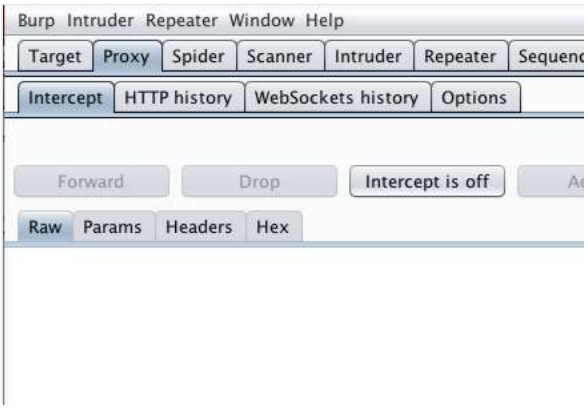
It is often said that the most common flaw is failing to encrypt data. One example of this vulnerability is the cleartext submission of a password. This is or
many vulnerabilities detected by Burp Scanner.

In this example we will demonstrate how to use the Scanner to check a login function page. The login page is taken from an old, vulnerable version of
"WordPress".

The version of "WordPress" we are using is taken from OWASP's Broken Web Application Project. Find out how to download, install and use this project

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

In the Burp Proxy "Intercept" tab ensure "Intercept is off".



Visit the web application you are testing in your browser.

Access the log in page of the web application.

Return to Burp.

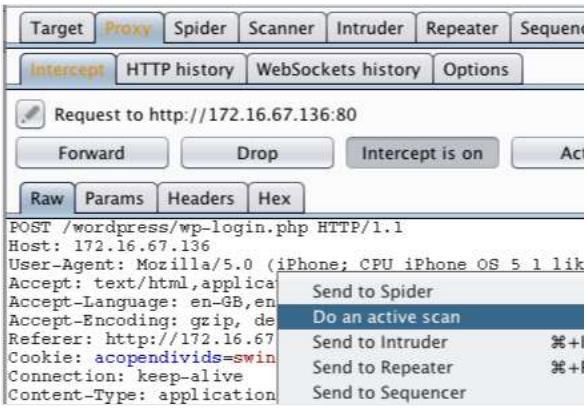
In the Proxy Intercept tab, ensure "Intercept is on".

Enter login details in to the login form and submit the request. In this example by clicking "Login".

Return to Burp. The raw request details should now be displayed in the Proxy "Intercept" tab.

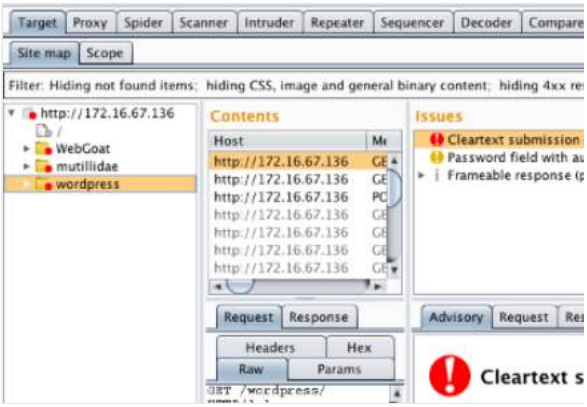
Right click on the request to bring up the context menu and click "Do an active scan."

Note: You can also send requests to the Scanner via the context menu in any location where HTTP requests are shown, such as the site map or Proxy history.

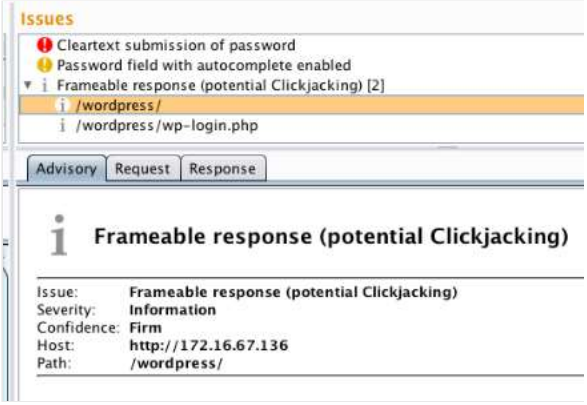


The results of the scan are displayed in the Target "Site map" tab.

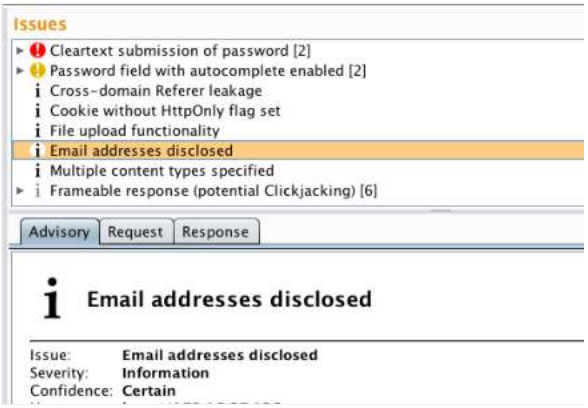
In this example the Scanner has detected that the application has an issue; "Cleartext submission of password".



By clicking on an individual issue you can view a description of the vulnerability and suggested remediation in the "Advisory tab". The full request and response are also shown.



Burp Scanner checks for a variety of types of data exposure, including SSH keys, credit card numbers and email addresses, etc.



Related articles:

Getting started with Burp Proxy

Getting started with Burp Scanner