## Using Burp to Test for Components with Known Vulnerabilities

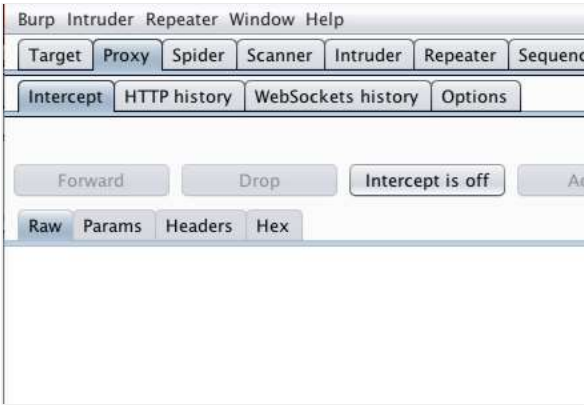
To determine whether your application is vulnerable it is important to keep abreast of the security status of the components that it uses. Vulnerabilities ar reported to central clearing houses such as CVE and NVD.

Attackers are able to identify a weak component through scanning or manual analysis of a web application. You can simulate this process using Burp. In example we assess one potential vulnerability of a web server.

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

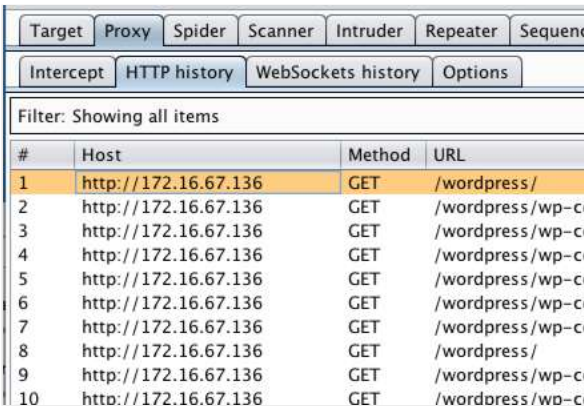
Ensure Burp Proxy "Intercept is off".

Visit the web application you are testing in your browser.




Next, click the “HTTP history” tab.

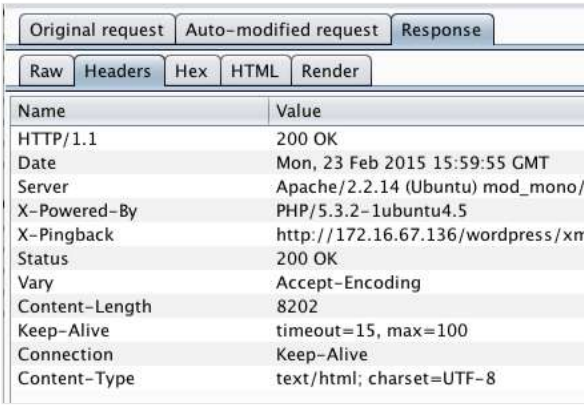
In the HTTP history table select one of the captured request and response rows.




Click the “Response” tab.

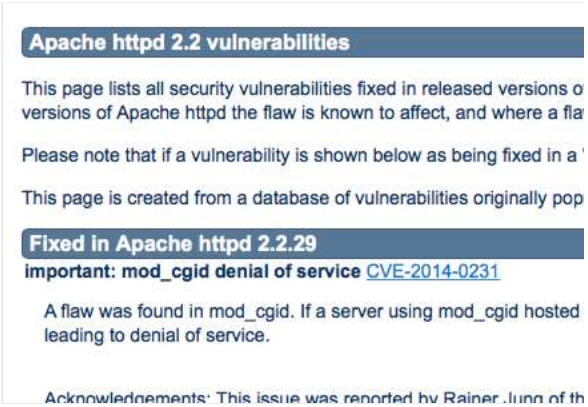
Information regarding the web server used by the web application is provided in the response.

From either the “Raw” or “Headers” tab, make a note or copy the Server name and version number.



With the server information at your disposal you can now use a search engine or one of the central clearing houses to check whether your web server has any known vulnerabilities.


Vulnerable components are usually fixed in a later version of the software. Upgrading or patching any components used by your web application is critical when securing your applications.




Additionally, it is possible to use the "Software Version Reporter" from the BApp store to passively scan for server software version numbers.


Related articles:

Getting started with Burp Proxy

Getting started with Burp Scanner