Using Burp to Test for Open Redirections

Open redirections are potential vulnerabilities for web applications in which a redirection is performed to a location specified in user-supplied data. By rec or forwarding a user to a malicious web site, an attacker could attempt a phishing scam or to steal user credentials.

In this example we will demonstrate how to use Burp's Proxy, Spider and Repeater tools to check for open redirections. The application is ZAP-WAVE ar designed for evaluating security tools.

The version of ZAP-WAVE used in this tutorial is taken from OWASP's Broken Web Application Project. Find out how to download, install and use this pr

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

Ensure Burp Proxy "Intercept is on".

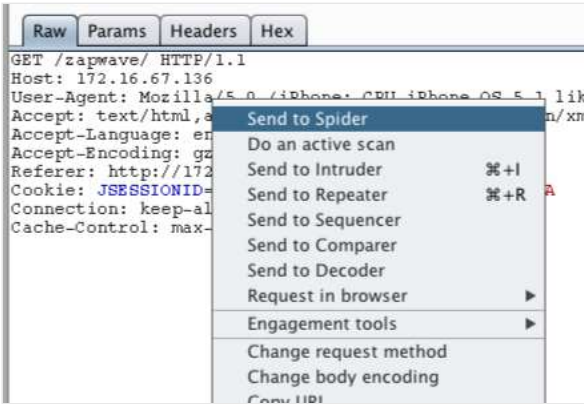
Visit the web application you are testing in your browser.

The Proxy "Intercept" tab should now show the intercepted request.

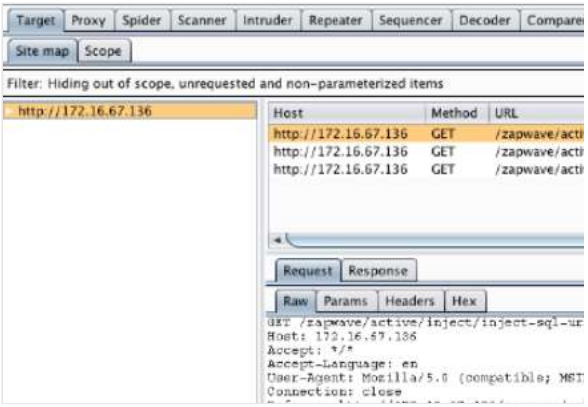
Bring up the context menu by right clicking anywhere on the request.

Click "Send to Spider", this will spider the web application and populate the "Site map".

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

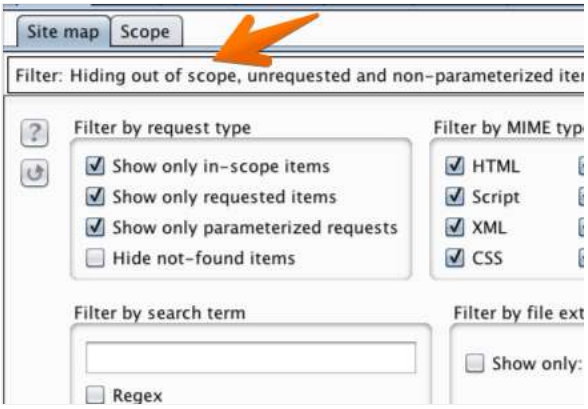


Click on the "Target" tab, then the "Site map" tab to view the spidered view of the web application.



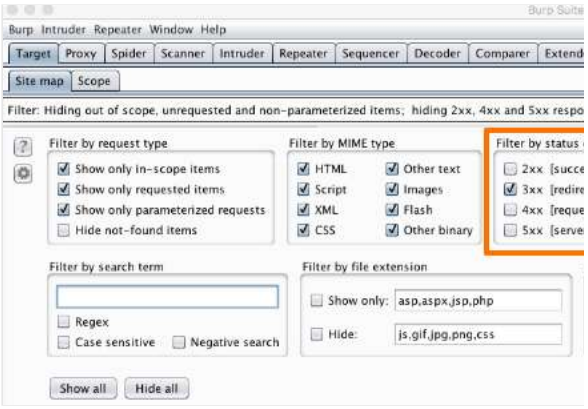
You can use the Site map filter to search for any redirects or forwards used by the Site map.

Click the "Filter" bar to bring up the filter options menu.



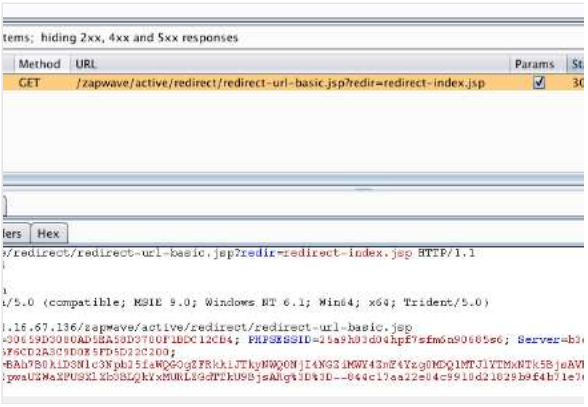
In this example we will "Filter by status code".

In this instance we are looking for the "3xx" class of status codes. These status codes indicate that further action has to be taken by the user agent to fulfil a request.



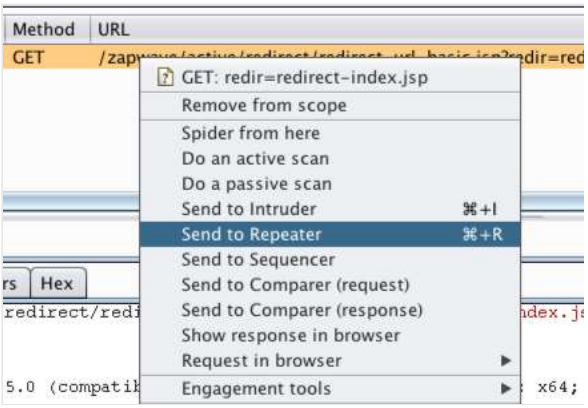
The "Site map" table should now only show HTTP requests of the "3xx" class.

You can now manually step through these requests to look for “interesting” URLs. These include any items in which the redirection target appears to be specified within a request parameter.



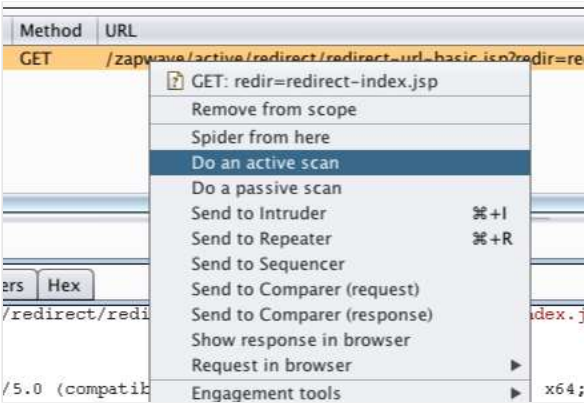
Send any HTTP requests that you wish to investigate further to the "Repeater" tab.

Right click on the request in the Site map table to bring up the context menu and click “Send to Repeater”.



Another way to investigate a request is to send it to Burp's Scanner.

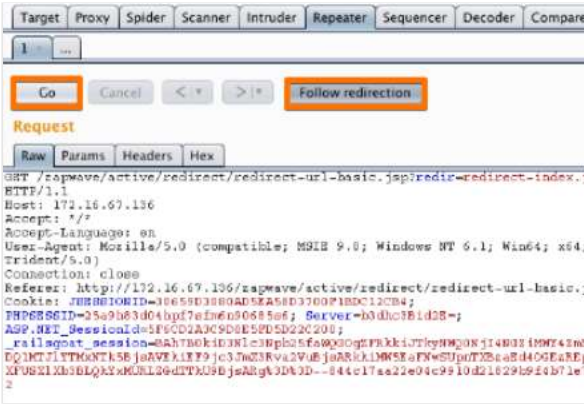
Right click on the request in the Site map table to bring up the context menu and click “Do an active scan”.



To continue with manual testing, go to the "Repeater" tab.

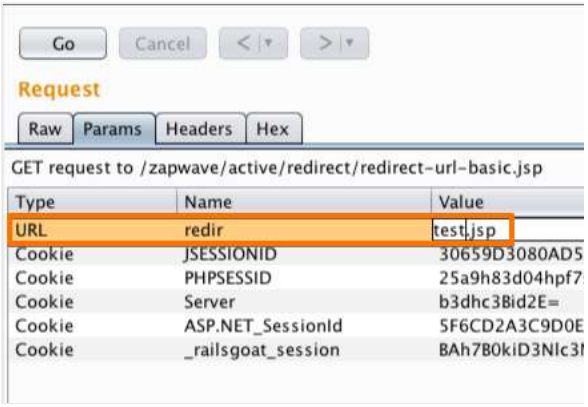
Click “Go” to check that the redirect occurs.

In this example you also need to click the "Follow redirection" button.



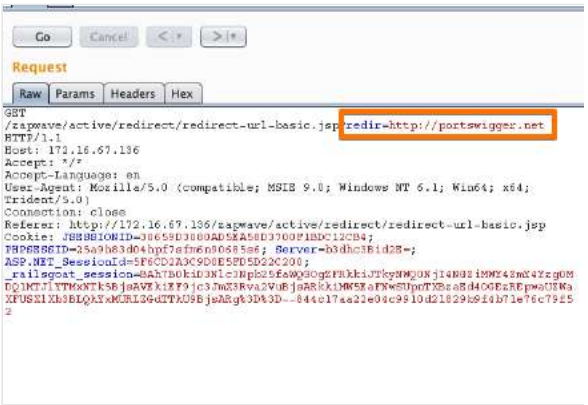
You can then try editing the URL parameter and clicking “Go” again to determine what effect this change might have.

If editing the URL causes a change in the location header in the response, the redirect may be "open" and vulnerable.



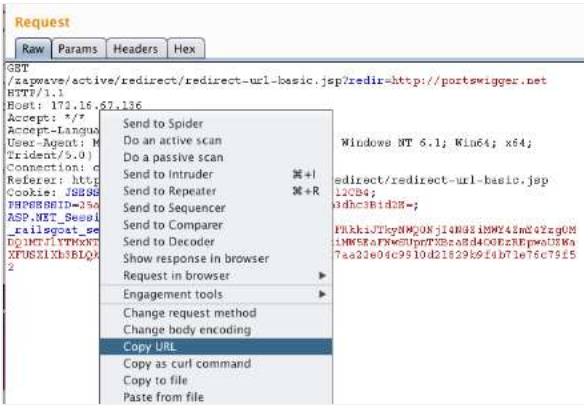
Try to change the value of the URL parameter to an external URL of your choice, on a different domain.

Click “Go” again to check if the URL is altered in the response.



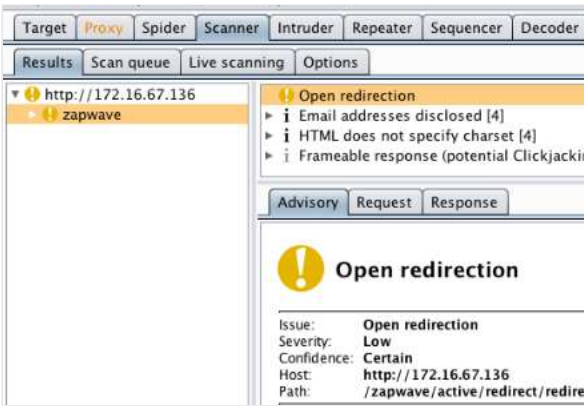
Finally, open an incognito tab in your browser and copy the redirect URL in to the address bar.

If the redirection to your external URL works, then the redirector is "open" and vulnerable.



In addition, Burp Scanner can be used to locate open redirection vulnerabilities.

In this example the Scanner submits a payload in to the "redir" parameter which causes a redirection to an arbitrary external domain.



Related articles:

- Getting started with Burp Proxy
- Using Burp Repeater
- Getting started with Burp Scanner
- Burp's target site map
- Getting started with Burp Spider