

Using Burp's Site Map to Test for Access Control Issues

The easiest and most effective way to test an application's **access controls** is to access the application using different accounts. Testing an application's controls thoroughly in this manner is a time-consuming process. Burp can help you automate some of the work involved.

Burp Suite lets you map the contents of an application using two different user contexts. You can then compare the results to see exactly where the content accessed by each user is the same or different. This tutorial uses a version of WordPress taken from OWASP's Broken Web Application Project. [Find out how to download, install and use this project.](#)

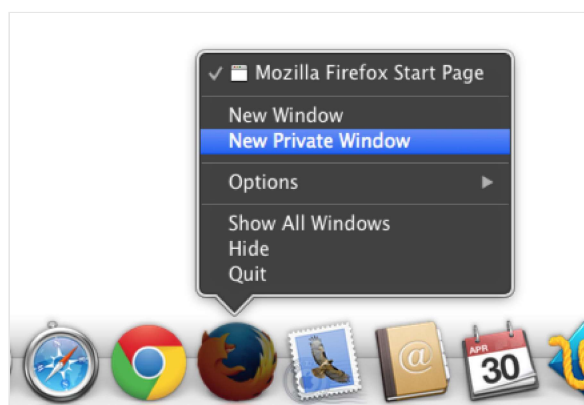
First, ensure that Burp is correctly **configured with your browser**.

With intercept turned off in the **Proxy "Intercept"** tab, visit the login page of the application you are testing in your browser.



Ensure you open your browser in "Private" or "Incognito" mode.

This will stop the browser from caching data or reusing any existing user context.



Browse all the application's content within one user context.

In this example we have accessed the navigational links at the top of the page, logged in with the credentials user2 : user2.

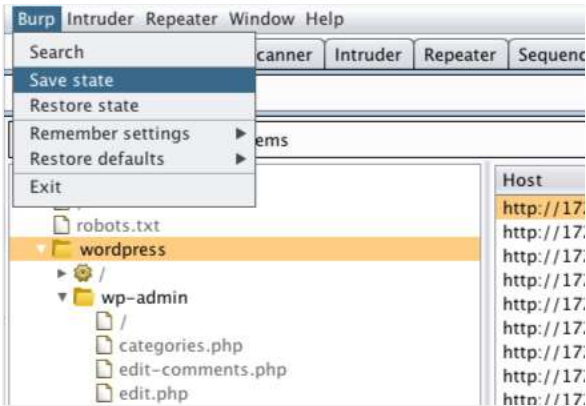
(Note: The user2 account was created for the purposes of this tutorial.)



Go to the **Target "Site map"** tab. The site map will be populated with request/response interactions with the application.

In this example we have saved the site map in a Burp state file.

It is also possible to have Burp dynamically rerequest the first site map in a new session context.



Next, sign out of the application and return to the login page.

Log in to the second account you wish to compare. In this example we have used the credentials user : user, a default account with this version of WordPress.

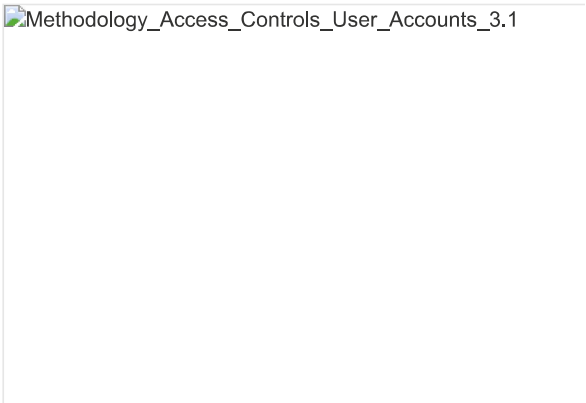


In Burp, return to the "Site map" tab.

Right click on the host and click "Delete host" to clear the Site map.

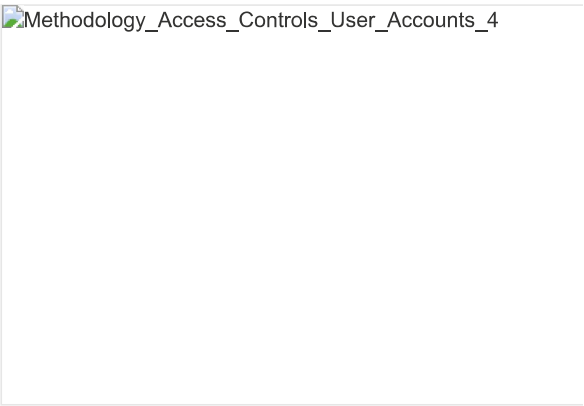


Access the area or functionality of the application that you are testing.



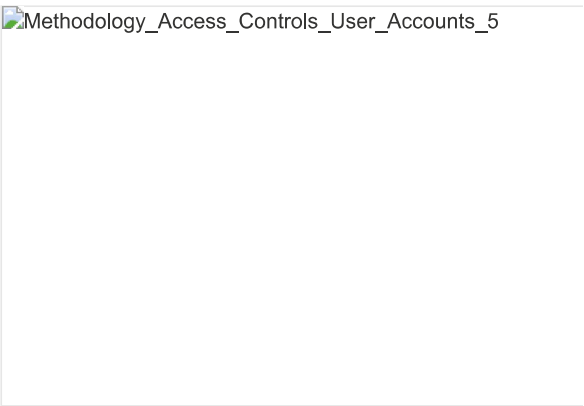
Burp's Site map will again populate with interactions with the application.

Right click on the application title in the Target "Site map" tab and click "compare site maps".



The "Compare site maps" window will pop up.

For "Site Map 1" select "Use current site map and click "Next".



In the next options window you can configure your comparison further.

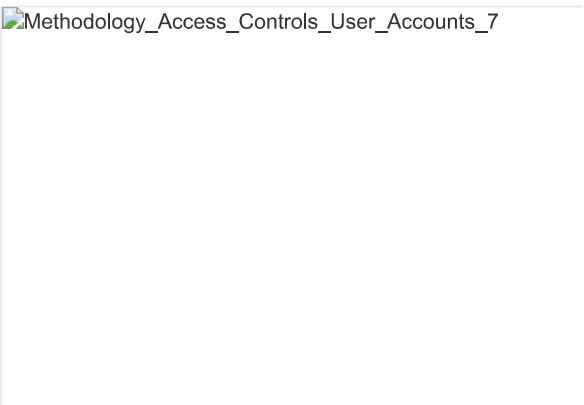
Consider what you wish to include in your comparison, select the appropriate option/s and click "Next".



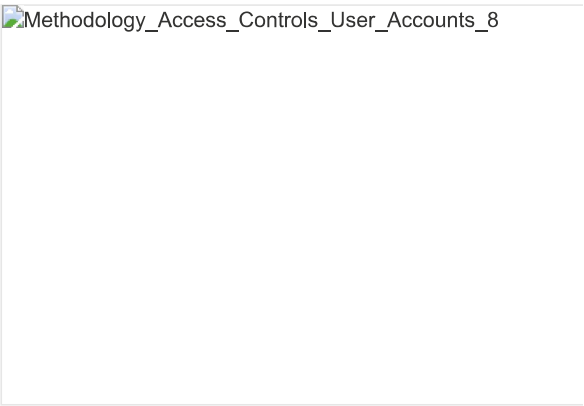
Next you will need to configure your second site map.

In this example, "Site Map 2" will be loaded from the from previously saved Burp state file.

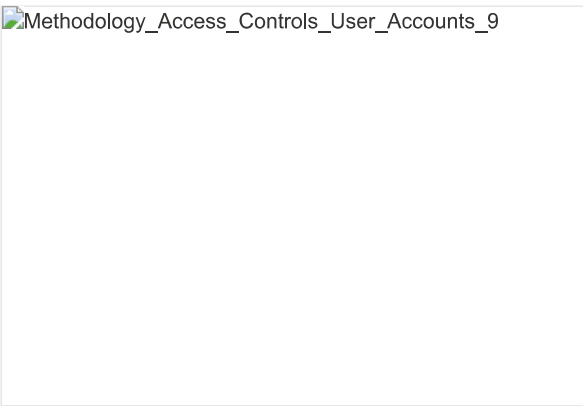
Select "Load from Burp state file" and click next.



Select the appropriate file from the load file window and click "Open".

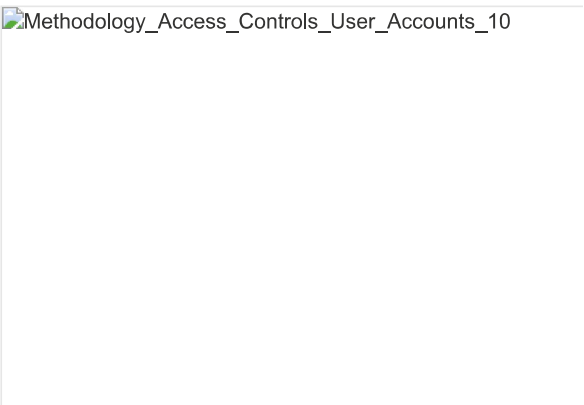


Ensure that the correct file appears in the "Compare" site map window and click "Next".

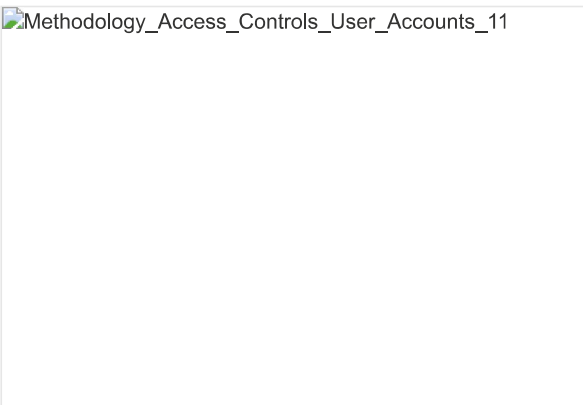


As with "Site Map 1", you are able to configure your comparison in the next options window.

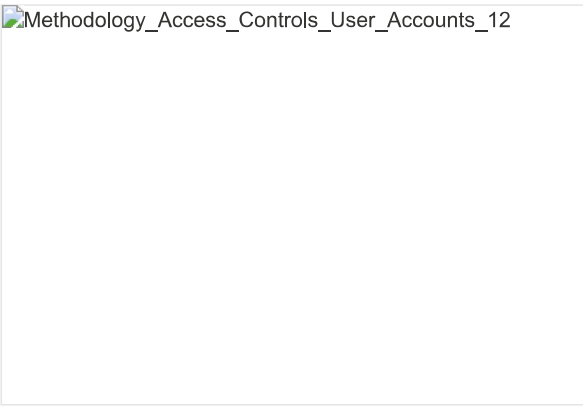
Select the appropriate configuration options and click "Next".



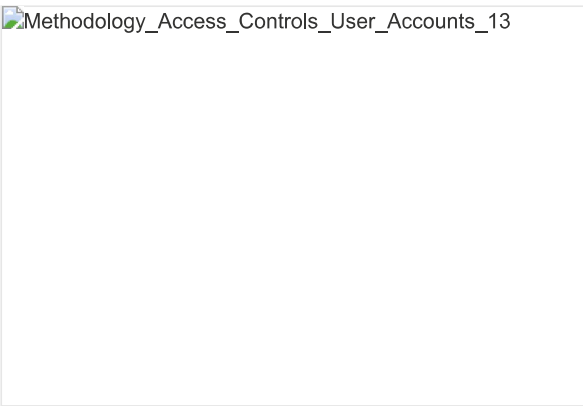
The "Request Matching Window" window will pop-up.
In this example we have retained the default settings, which work effectively for most situations.
Use the default settings or use the options to customize your request matching rules and click "Next".



The "Response Comparison" window allows you to configure how Burp handles features such as response headers when performing site map comparisons. Configure the setting appropriately and click "Next".



The "Compare sites maps" window will now display both site maps. Explore the content of both site maps and compare them to assess their respective access control levels. In this example it is apparent that the "Admin" account ("Map 2") has a wider variety of links and accessible content from browsing the same area of the application's functionality.



Related articles:

- Getting started With Burp Proxy
- Using the Burp Target tool

Burp Suite

Web vulnerability scanner
Burp Suite Editions
Release Notes

Vulnerabilities

Cross-site scripting (XSS)
SQL injection
Cross-site request forgery
XML external entity injection
Directory traversal
Server-side request forgery

Customers


Organizations
Testers
Developers


Company

About
PortSwigger News
Careers
Contact
Legal
Privacy Notice

Insights

Web Security Academy
Blog
Research
The Daily Swig

PortSwigger Logo

 Follow us

© 2020 PortSwigger Ltd

