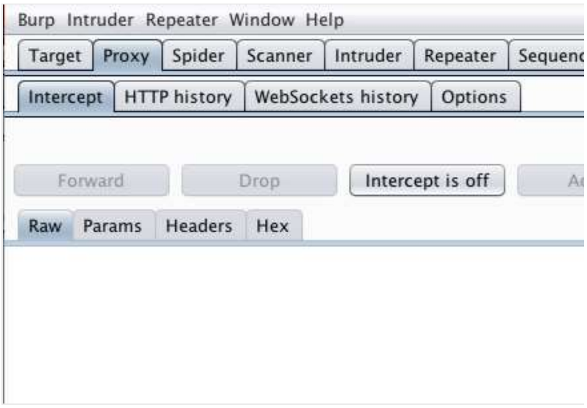
Using Burp's "Request in Browser" Function to Test for Access Control Issues

Comparing the application's contents when accessed in different user contexts sometimes requires each page to be tested individually, to confirm wheth access controls are being applied. One way to perform this testing manually is to walk through a process several times in your browser and use your pro switch the session token supplied in different requests to that of a less-privileged user.

However, you can often dramatically speed up this process by using the "Request in browser" feature of Burp Suite. This tutorial demonstrates the use o function on a version of a WordPress web application. The version of WordPress we are using is taken from OWASP's Broken Web Application Project. how to download, install and use this project.

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

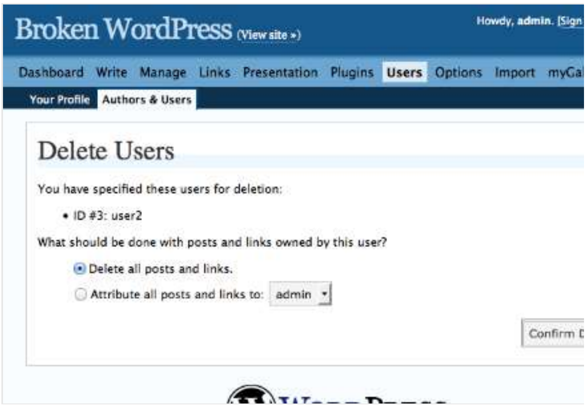
With intercept turned off in the Proxy "Intercept" tab, visit the login page of the application you are testing in your browser.


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequenc
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Ac
Raw Params Headers Hex

Login using the higher privileged account, in this example using the credentials admin : admin.

Walk through the process or area of the application you are testing.

The request/response will be captured in Burp's Site map and Proxy history.


Broken WordPress (View site »)
Howdy, admin. [Sign
Dashboard Write Manage Links Presentation Plugins Users Options Import myGa
Your Profile Authors & Users

Delete Users

You have specified these users for deletion:

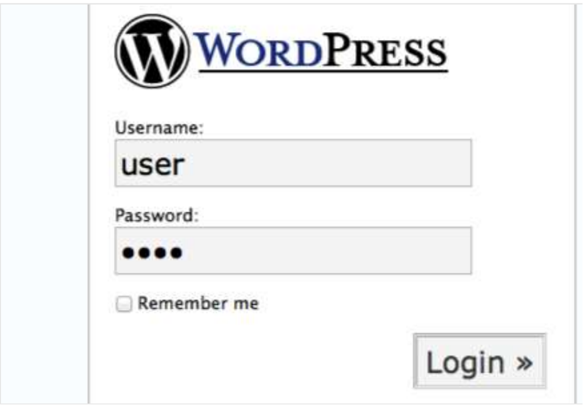
- ID #3: user2

What should be done with posts and links owned by this user?

● Delete all posts and links.

○ Attribute all posts and links to: admin

Log out of the application and log in using the lower-privileged account (or none at all).



Username: user

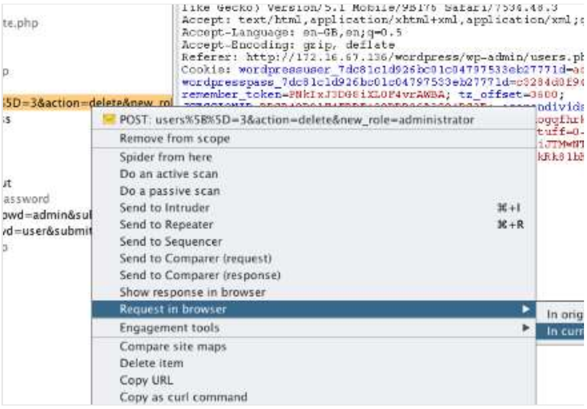
Password: ●●●●

□ Remember me

Locate the area you are testing in Burp's Site map or HTTP history.

Right click on the entry to bring up the context menu.

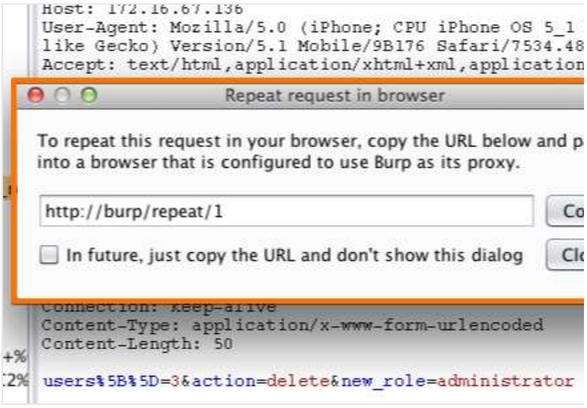
Click "Request in browser", then "In current session".



```
like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3
Accept: text/html,application/xhtml+xml,application/xml;
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.67.136/wordpress/wp-admin/users.ph
Cookie: wordpressuser_7dc81c1d926bc01c04797533eb27771d=a
wordpresspass_7dc81c1d926bc01c04797533eb27771d=c3284d0f9
remember_token=PNkIxJ3DG8iXL0P4vrAWBA; tz_offset=3600;
```

The "Request in browser" pop up window allows you to copy the URL of the required page.

Click the "Copy" button.



```
Host: 172.16.67.136
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1
like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48
Accept: text/html,application/xhtml+xml,application
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 50

users%5B%5D=3&action=delete&new_role=administrator
```

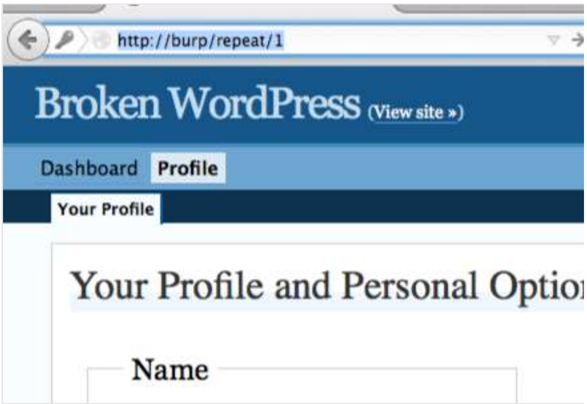
Repeat request in browser

To repeat this request in your browser, copy the URL below and p into a browser that is configured to use Burp as its proxy.

http://burp/repeat/1

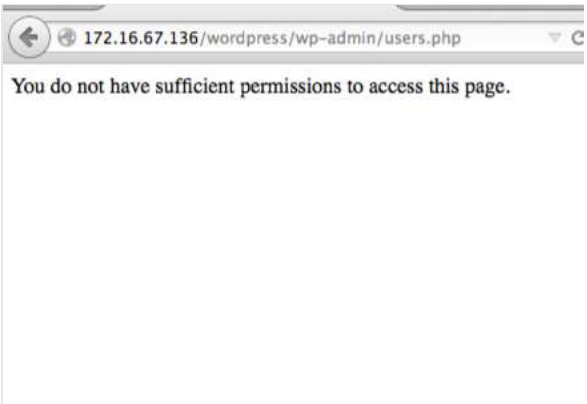
□ In future, just copy the URL and don't show this dialog

Post the URL in to your browser to attempt to access the individual page your are testing.



http://burp/repeat/1
Broken WordPress (View site »)
Dashboard
Profile
Your Profile
Your Profile and Personal Optio
Name

In this example we are denied access to the page. It would appear that appropriate access controls are in place for this class of user.



You do not have sufficient permissions to access this page.

Related articles:

Getting started With Burp Proxy

Using Burp's site map

Burp Proxy history

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

PortSwig

Follow us