Using Burp to Test for Missing Function Level Access Control

Anyone with network access to an application can send a request to it. Therefore, web applications should verify function level access rights for all reque actions by any user. If checks are not performed and enforced, malicious users may be able to penetrate critical areas of a web application without prope authorization.

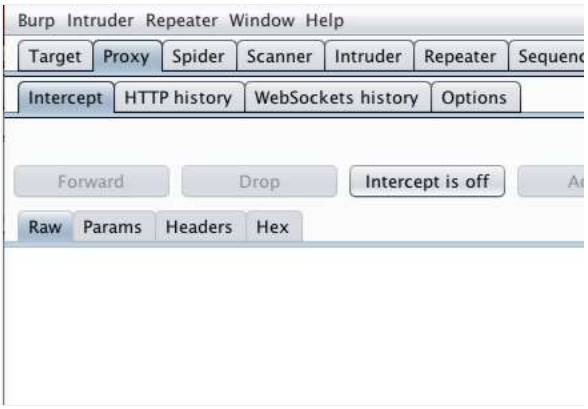
In this example we will demonstrate two typical access control attacks on a training web application (WebGoat).

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

Parameter Manipulation

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

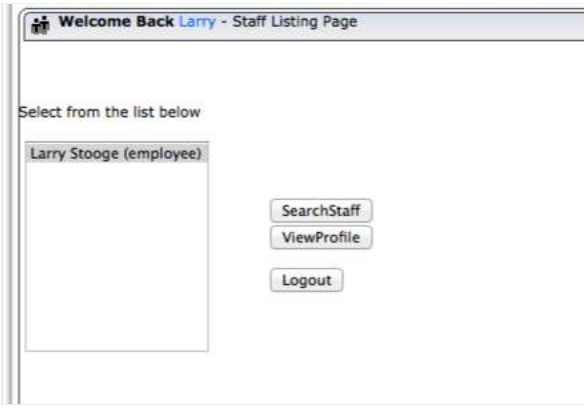
With intercept turned off in the Proxy "Intercept" tab, visit the web application you are testing in your browser.



The web application on this WebGoat page (Access Control Flaws - Stage 1: Bypass Business Layer Access Control Scheme) allows an employee to view their staff profile.

First, log in to one of the employee profiles.

In this example we are using "Larry".

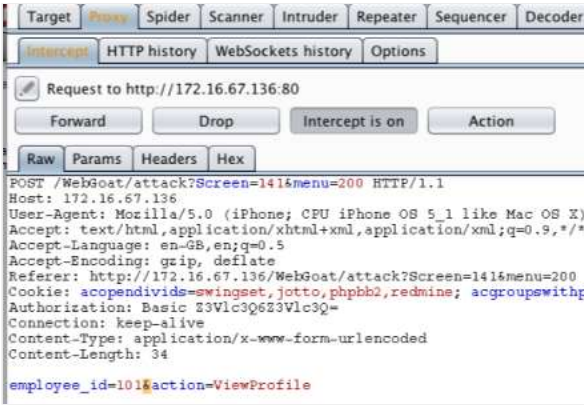


Return to Burp.

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

In your browser click the "View Profile" button.

Burp will capture the request, which can then be edited before being forwarded to the server.

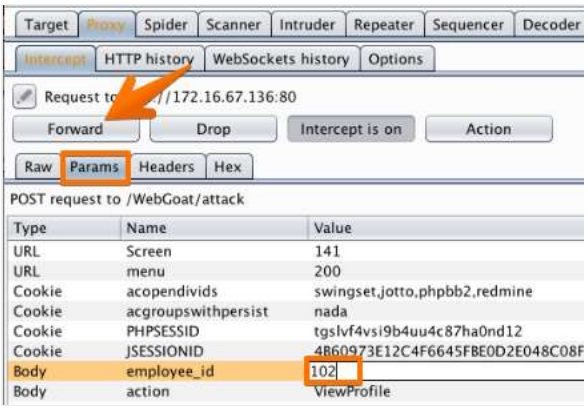


One way to easily locate and edit parameters is in the "Params" tab.

In this example we are changing the "employee_id" from "101" to "102".

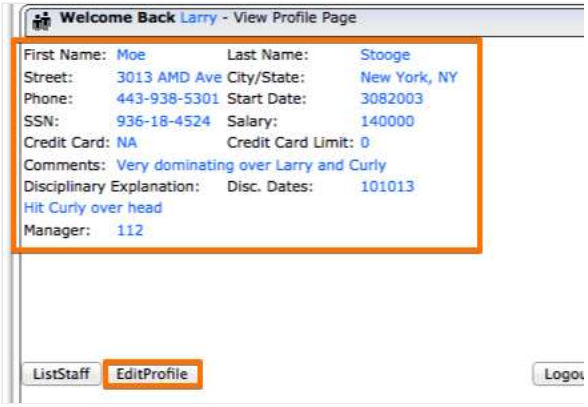
Once the request has been edited, use the "Forward" button to forward the request.

In this example you will need to click the forward button more than once to get the appropriate response from the server and view the results in the web application.



In the example, the application allows a user to access another user's employee profile page.

By editing the parameters in the request, the application's access controls have been bypassed.

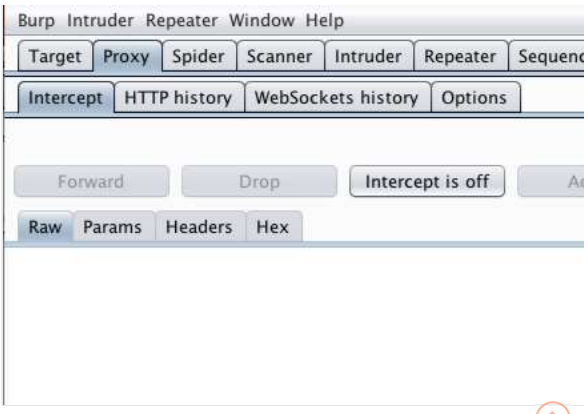


Forced Browsing

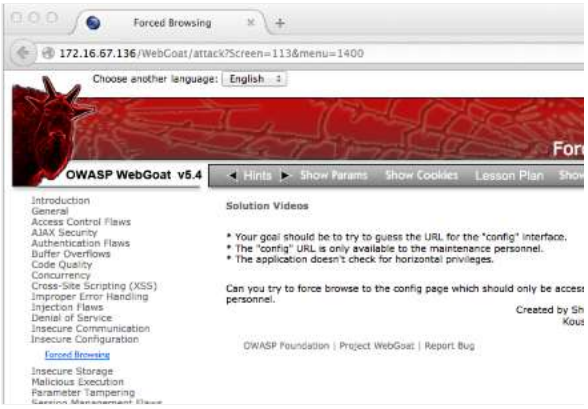
In this scenario the attacker uses forced browsing to access target URLs.

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

Ensure Proxy "Intercept is off".



In your browser, visit the page of the web application you are testing.



Return to Burp.

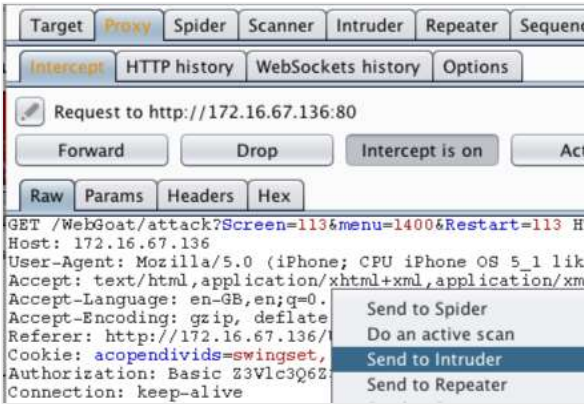
In the Proxy "Intercept" tab, ensure "Intercept is on".

In your browser, resubmit the request to visit the page you are testing.

You can now view the intercepted request in the Proxy "Intercept" tab.

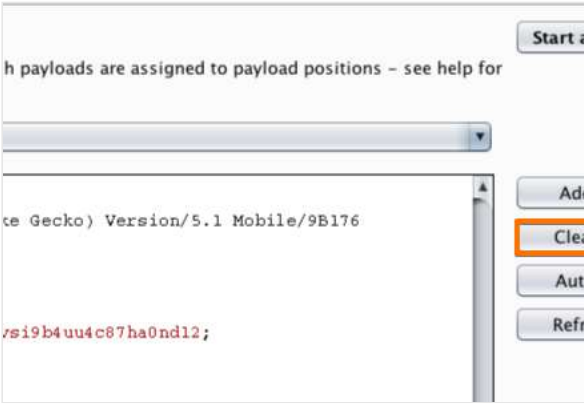
Right click anywhere on the request to bring up the context menu.

Click "Send to Intruder".



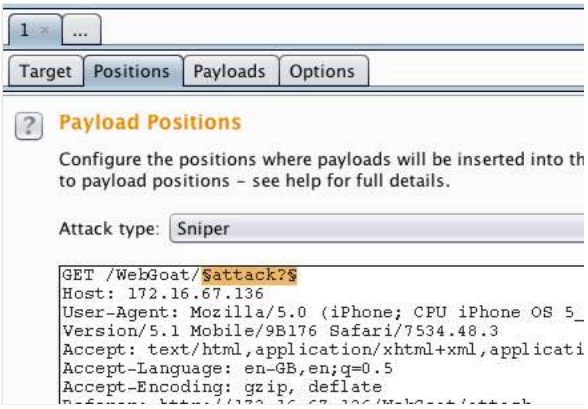
Go to the "Positions" tab under the "Intruder" tab.

Click the "Clear" button to clear the suggested payload positions.



In this attack we are attempting to locate and view files and directories.

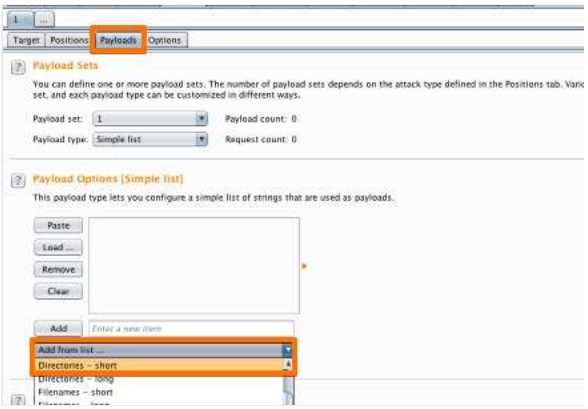
Select the file name in the URL and use the "Add" button to position the payload.



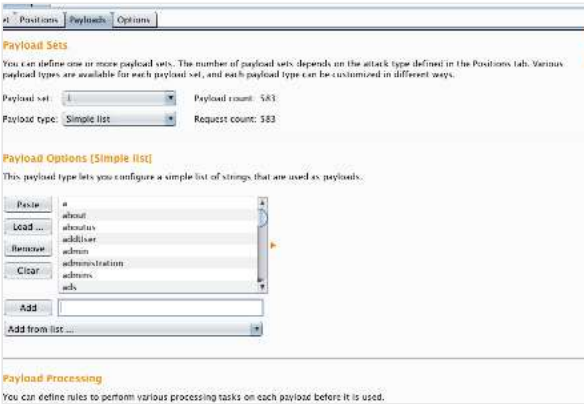
Go to the "Payloads" tab.

"Payload type" in the "Payload sets" options should be set to "Simple list".

In the "Payload Options [Simple list]" from the dropdown menu "Add from list...", select "Directories - short" and "Filenames - short".



Click the "Start Attack" button.

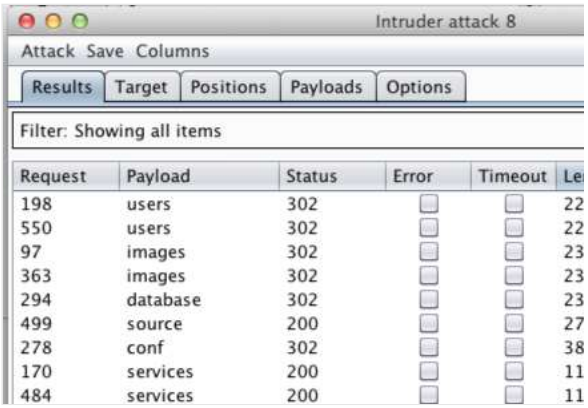


An "Intruder Attack" window will pop up with the results of the attack.

You can sort the results using the column headers.

In this example we will use "Length". Click the "Length" column header.

"Status" would also be a useful method of organizing this results table.

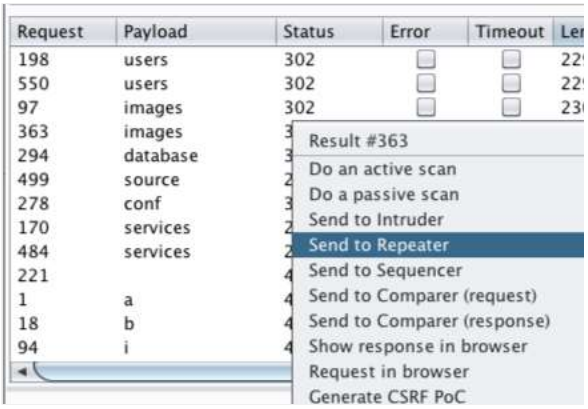


By sorting by "Length" or by "Status" we have enumerated some interesting results.

Send any results that warrant further investigation to Burp Repeater.

Right click on each individual result to bring up the context menu.

Click "Send to Repeater"



Go to the "Repeater" tab.

Click "Go" to follow the request.

In this example you have to use the "Follow redirection" button to follow the applications redirect and view the response.

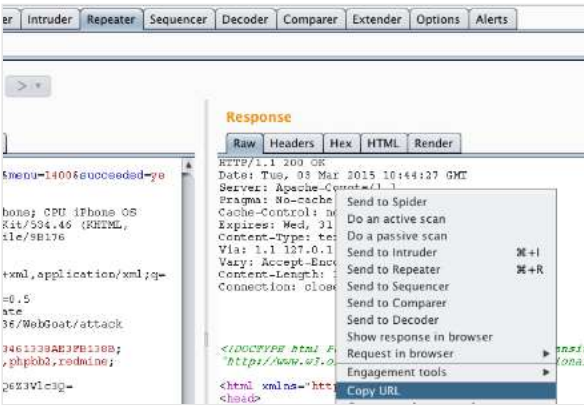
In some of the results, forwarding the redirect leads to a 404 response, indicting there is no issue with this vulnerability.

The "/conf" payload provides a redirect to a "200 ok" response.

You can view the response beneath the "Response" header or right click anywhere within the response to bring up the context menu.

Click copy "Copy URL".

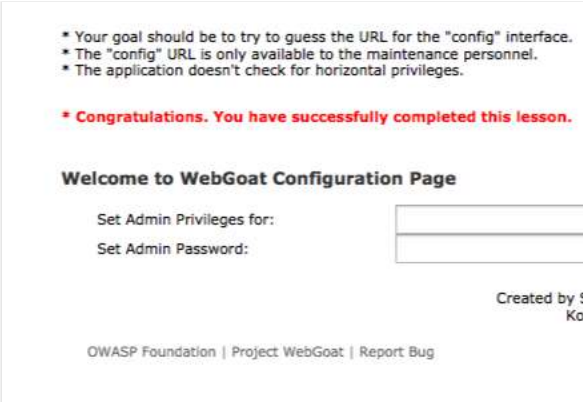
Paste the URL in to your browser to manually check the results.



In this example we are able to access the application's configuration page.

The application allows an unauthenticated user to configure administrative privileges and passwords for other users.

If an unauthenticated user can access URLs that should require authentication or hold sensitive information this is a security vulnerability.



Related articles:

- Using Burp Intruder
- Getting started with Burp Proxy
- Using Burp Repeater
- Getting started with Burp Scanner