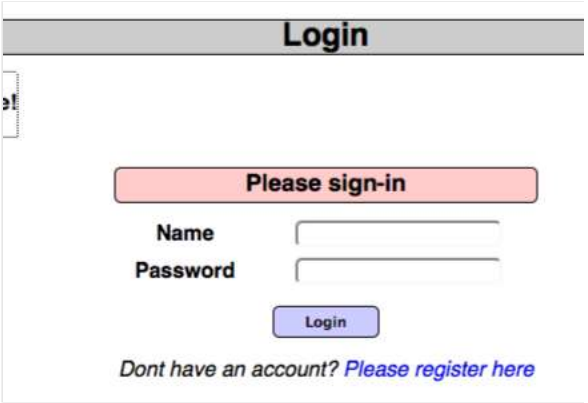
Using Burp to Brute Force a Login Page

Authentication lies at the heart of an application's protection against unauthorized access. If an attacker is able to break an application's authentication fu then they may be able to own the entire application.

The following tutorial demonstrates a technique to bypass authentication using a simulated login page from the "Mutillidae" training tool. The version of "Mutillidae" we are using is 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.

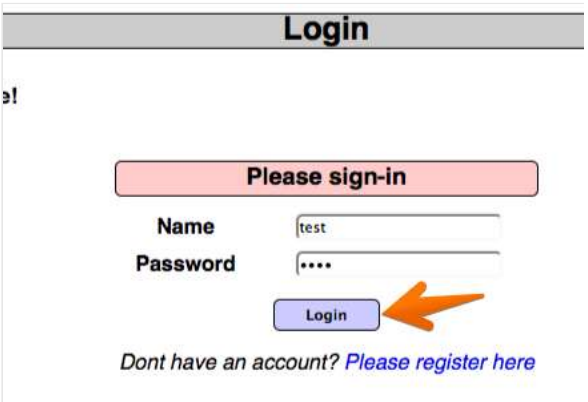
In the Burp Proxy tab, ensure "Intercept is off" and visit the login page of the application you are testing in your browser.



Return to Burp.

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

In your browser enter some arbitrary details in to the login page and submit the request.

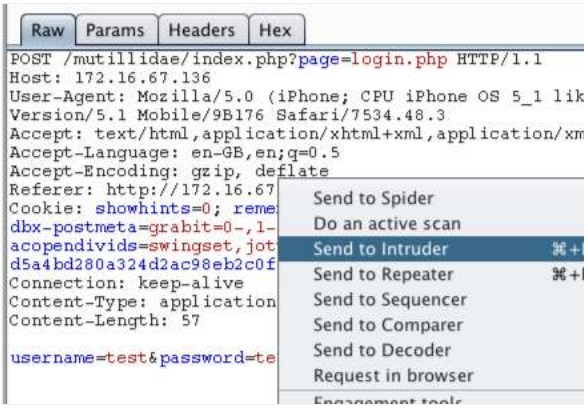


The captured request can be viewed in the Proxy "Intercept" tab.

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

Then click "Send to Intruder".

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

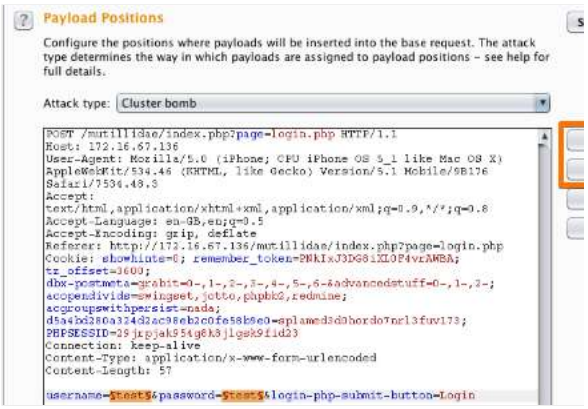


Go to the Intruder "Positions" tab.

Clear the pre-set payload positions by using the "Clear" button on the right of the request editor.

Add the "username" and "password" parameter values as positions by highlighting them and using the "Add" button.

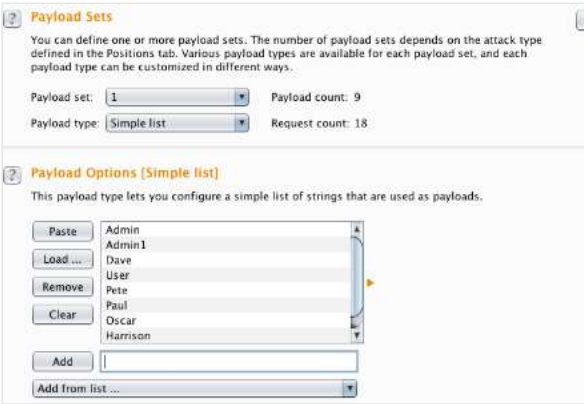
Change the attack to "Cluster bomb" using the "Attack type" drop down menu.



Go to the "Payloads" tab.

In the "Payload sets" settings, ensure "Payload set" is "1" and "Payload type" is set to "Simple list".

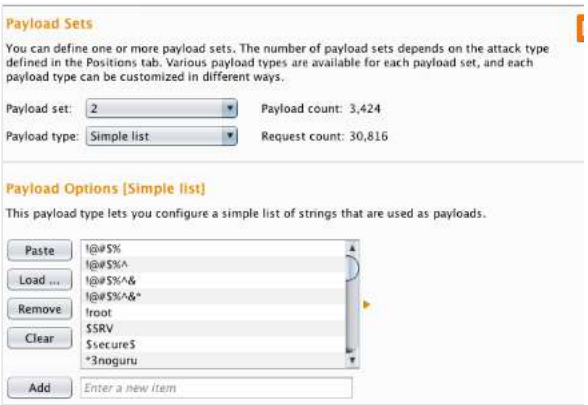
In the "Payload options" settings enter some possible usernames. You can do this manually or use a custom or pre-set payload list.



Next, in the "Payload Sets" options, change "Payload" set to "2".

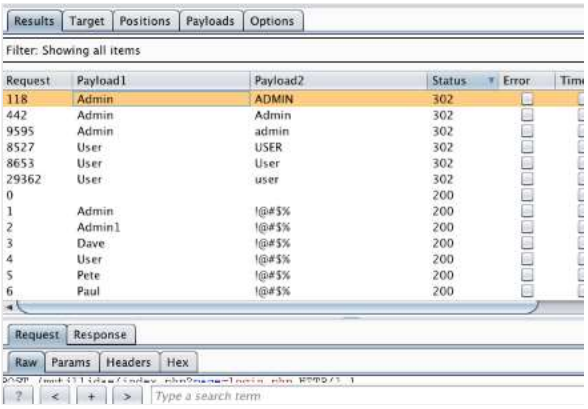
In the "Payload options" settings enter some possible passwords. You can do this manually or using a custom or pre-set list.

Click the "Start attack" button.



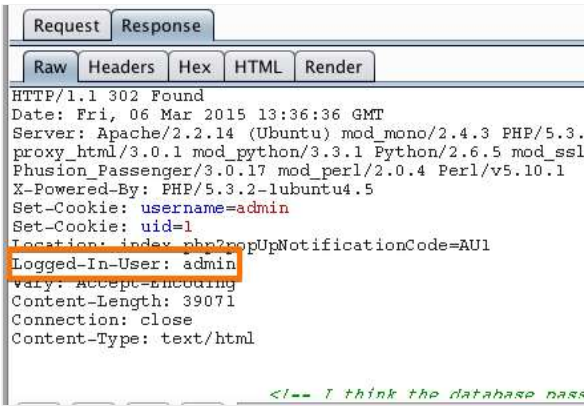
In the "Intruder attack" window you can sort the results using the column headers.

In this example sort by "Length" and by "Status".



The table now provides us with some interesting results for further investigation.

By viewing the response in the attack window we can see that request 118 is logged in as "admin".



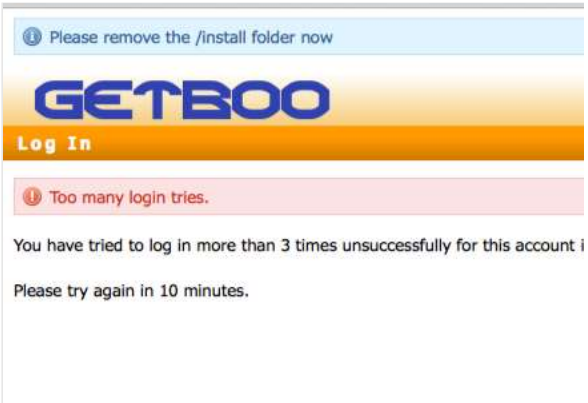
To confirm that the brute force attack has been successful, use the gathered information (username and password) on the web application's login page.

Account Lock Out

In some instances, brute forcing a login page may result in an application locking out the user account. This could be the due to a lock out policy based on a certain number of bad login attempts etc.

Although designed to protect the account, such policies can often give rise to further vulnerabilities. A malicious user may be able to lock out multiple accounts, denying access to a system.

In addition, a locked out account may cause variances in the behavior of the application, this behavior should be explored and potentially exploited.



Verbose Failure Messages

Where a login requires a username and password, as above, an application might respond to a failed login attempt by indicating whether the reason for the failure was an unrecognized username or incorrect password.

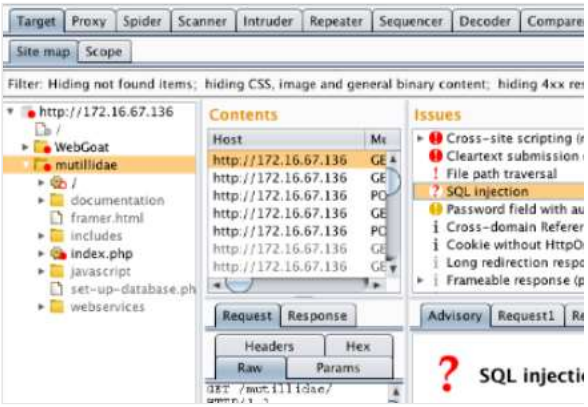
In this instance, you can use an automated attack to iterate through a large list of common usernames to enumerate which ones are valid.

A list of enumerated usernames can be used as the basis for various subsequent attacks, including password guessing, attacks on user data or sessions, or social engineering.

Scanning a login page

In addition to manual testing techniques, Burp Scanner can be used to find a variety of authentication and session management vulnerabilities.

In this example, the Scanner was able to enumerate a variety of issues that could help an attacker break the authentication and session management of the web application.



Related articles:

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