

BROKEN AUTHENTICATION – PASSWORD ATTACKS

SECURITY LEVEL -low

Go to Challenge

Login using given credentials,

The screenshot shows the bWAPP web application interface. At the top, there's a navigation bar with links for 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', 'Logout', and 'Welcome Bee'. On the right side of the header, there are dropdown menus for 'Choose your bug' (set to 'bWAPP v2.2') and 'Set security level' (set to 'low'). Below the header, the main content area has a yellow background with the text 'an extremely buggy web app!' and a bee logo. The title 'Broken Auth - Password Attacks' is displayed above a form. The form contains fields for 'Login' (with 'bee' entered) and 'Password' (with 'bug' entered), along with a 'Login' button. To the right of the form are social media sharing icons for Twitter, LinkedIn, Facebook, and Email. A green success message 'Successful login!' is visible below the form. At the bottom of the page, a footer bar includes a license notice: 'bWAPP is licensed under CC BY-NC-ND © 2014 MME BVBA / Follow @MME_BVBA on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?'.

Try login through wrong password

This screenshot shows the same bWAPP interface as the previous one, but with a failed login attempt. The 'Login' field still contains 'bee' and the 'Password' field contains 'test'. Below the form, a red error message 'Invalid credentials! Did you forgot your password?' is displayed. The rest of the page, including the menu, social sharing icons, and footer, remains identical to the successful login screenshot.

Now we will use Burp Suite to intercept the request.

Intercept the request of the login page, send it to “Intruder” to carry out the attack.

The screenshot shows the Burp Suite interface on the left and a browser window on the right. In the browser, the URL is https://bwapp.hakhub.net/ba_pwd_attack. The page title is "Choose your bug: bWAPP v2.2 Hack". It says "Set your security level: low" and "an extremely buggy web app!". Below that is a form titled "/ Broken Auth - Password A". It has fields for "Login:" containing "bee" and "Password:" containing "test". A red message at the bottom says "Invalid credentials! Did you forget your password?". The Burp Suite interface shows a captured POST request to "/ba_pwd_attacks_1.php" with the same login and password values.

In “Intruder -> Positions”,

Choose Attack type → Cluster Bomb

For payload position, select <login_value> and <password_value> (in this case bee and test)

'Add §'

The screenshot shows the Burp Suite interface on the left and a browser window on the right. The browser page is identical to the one in the previous screenshot. The Burp Suite interface shows the "Intruder" tab selected. Under "Payload positions", the "Target" is set to <https://bwapp.hakhub.net>. The "Attack type" is set to "Cluster bomb". The "Payload positions" section highlights the "login" and "password" fields in the request body. The request body is identical to the one in the first screenshot, with "login=bee&password=test&form=submit". The browser shows the same "Invalid credentials!" message.

Go to “Intruder -> payloads”

Payload set 1 -

{for payload position “login”}

Clear the default list and add few random login usernames

The screenshot shows the Burp Suite interface with the "Intruder" tab selected. In the "Payloads" section, a payload set is configured with a count of 5 and a simple list type. Below this, a list of payloads contains "bee", "bug", "admin", "abc", and "xyz". The "Payload processing" section is empty. To the right, a browser window displays a "bWAPP - Broken Authentication" page. The URL is https://bwapp.hakhub.net/ba_pwd_attack. The page has a yellow header with "Choose your bug" and "bWAPP v2.2". It features a "Set your security level:" dropdown set to "low". A red annotation on the page says "an extremely buggy web app!". The main content area shows a login form with fields for "Login" (containing "bee") and "Password" (containing "test"). A message at the bottom says "Invalid credentials! Did you forget your password?".

Payload set 2 -

{for payload position “password”}

Clear the default list and add few random and common passwords

The screenshot shows the Burp Suite interface with the "Intruder" tab selected. In the "Payloads" section, a payload set is configured with a count of 5 and a simple list type. Below this, a list of payloads contains "bee", "bug", "admin", "password", and "xyz". The "Payload processing" section is empty. To the right, a browser window displays a "bWAPP - Broken Authentication" page. The URL is https://bwapp.hakhub.net/ba_pwd_attack. The page has a yellow header with "Choose your bug" and "bWAPP v2.2". It features a "Set your security level:" dropdown set to "low". A red annotation on the page says "an extremely buggy web app!". The main content area shows a login form with fields for "Login" (containing "bee") and "Password" (containing "test"). A message at the bottom says "Invalid credentials! Did you forget your password?".

Go to “Intruder -> Settings”

Look for following settings

The screenshot shows the Burp Suite interface. On the left, the 'Intruder' tab is selected. Under 'Grep - Match', there is a checkbox 'Flag result items with responses matching these expressions:' which is checked. Below it, a text input field contains the string 'Invalid credentials! Did you forget your pas...'. On the right, a browser window displays a login page for 'bWAPP - Broken Authentication'. The URL is https://bwapp.hakhub.net/ba_pwd_attack. The page says 'Choose your bug' and 'Set your security level: low'. It features a logo of a bee and the text 'an extremely buggy web app!'. Below the logo are links for 'Bugs', 'Change Password', 'Create User', and 'Set Security Level'. A form for logging in with 'Login:' set to 'bee' and 'Password:' set to 'test' is shown. An error message 'invalid credentials! Did you forget your password?' is displayed below the form.

Now go back to “Intruder -> Payloads”

And start attack

After attack is finished, sort the length column

Click on “bee” and “bug” credentials → Response -> Render

The screenshot shows the Burp Suite interface with the 'Results' tab selected. A table lists various credentials and their corresponding response lengths. The row for 'bee' and 'bug' has the number '200' in the 'Length' column and is highlighted with a red border. Below the table, there are tabs for 'Request', 'Response' (which is selected), and 'Render'. The 'Render' tab shows the response from the 'bWAPP' application. The page title is 'Welcome Bee'. The main content area says '/ Broken Auth. - Password Attacks /' and contains a login form with 'Login:' set to 'bee' and 'Password:' set to 'test'. A green message box at the bottom left says 'Successful login!' with a dashed border. The status bar at the bottom left says 'Finished'.

CHALLENGE SOLVED...!!