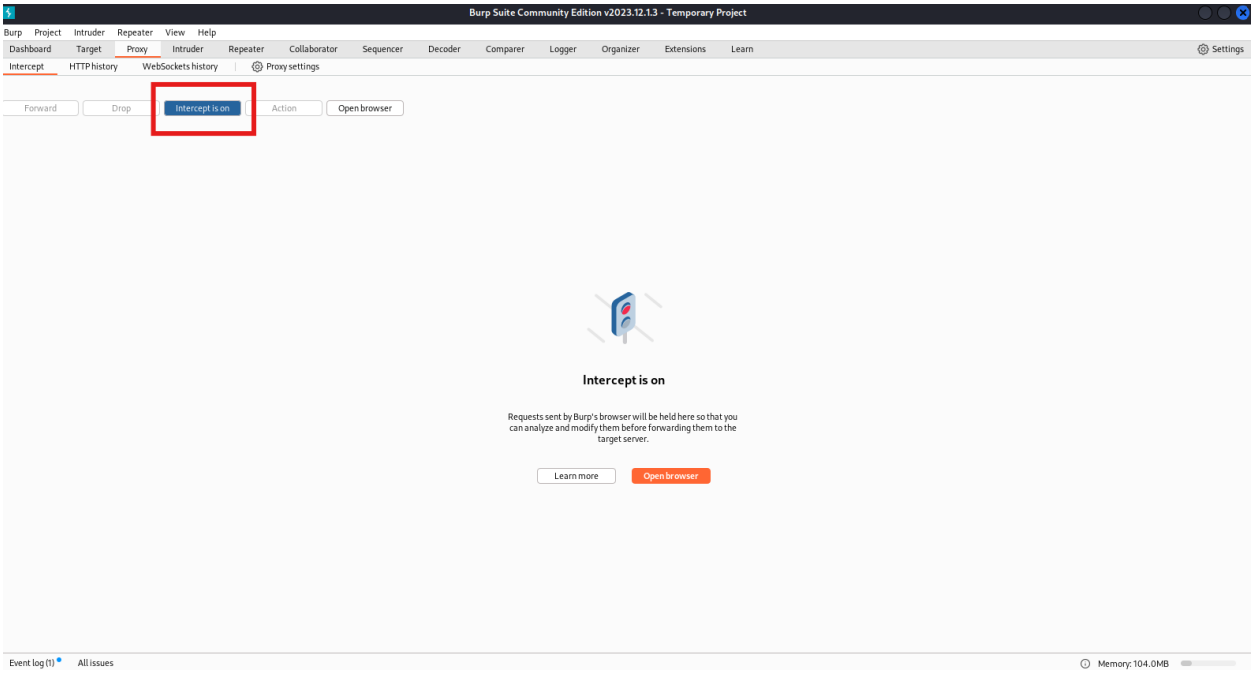
Burp Suite: Brute Force Attack

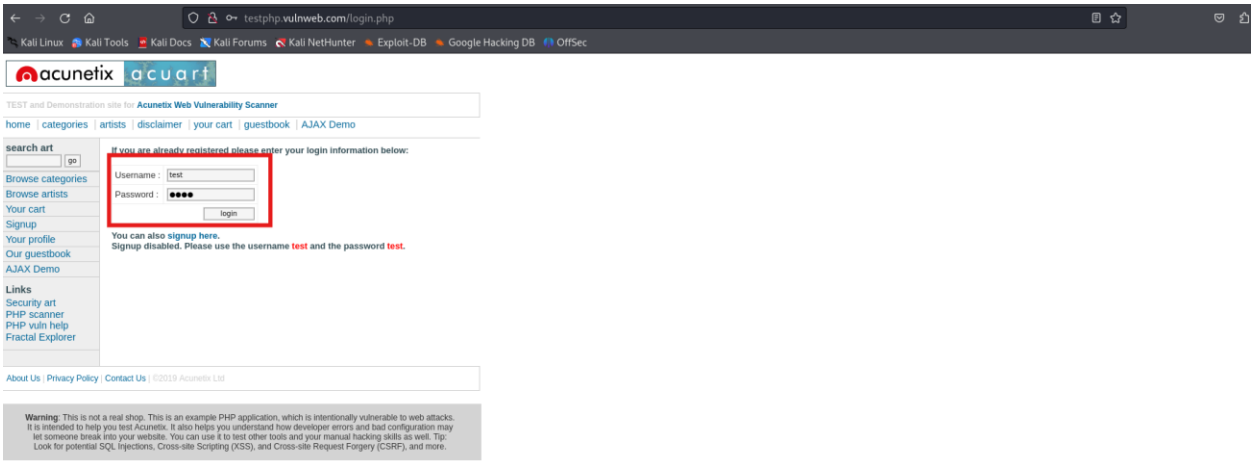
A brute force attack using Burp Suite involves utilizing the Intruder tool to systematically guess valid credentials or discover hidden information by trying numerous possible inputs. The process starts by setting up Burp Suite as a proxy and configuring the browser to route traffic through it, allowing Burp Suite to capture HTTP/S requests and responses. The tester navigates to the target login page or form and submits a test request, which is intercepted and sent to the Intruder tool. In Intruder, the tester identifies and marks the positions where payloads (such as usernames and passwords) will be inserted. A list of potential inputs is configured as payloads, which the Intruder tool then systematically inserts into the marked positions and sends the requests to the server. The responses are analyzed to identify successful attempts, typically indicated by unique status codes or response messages. This methodical approach helps uncover valid credentials or sensitive information, highlighting potential security weaknesses in the application’s authentication or input validation mechanisms.

Examples: -

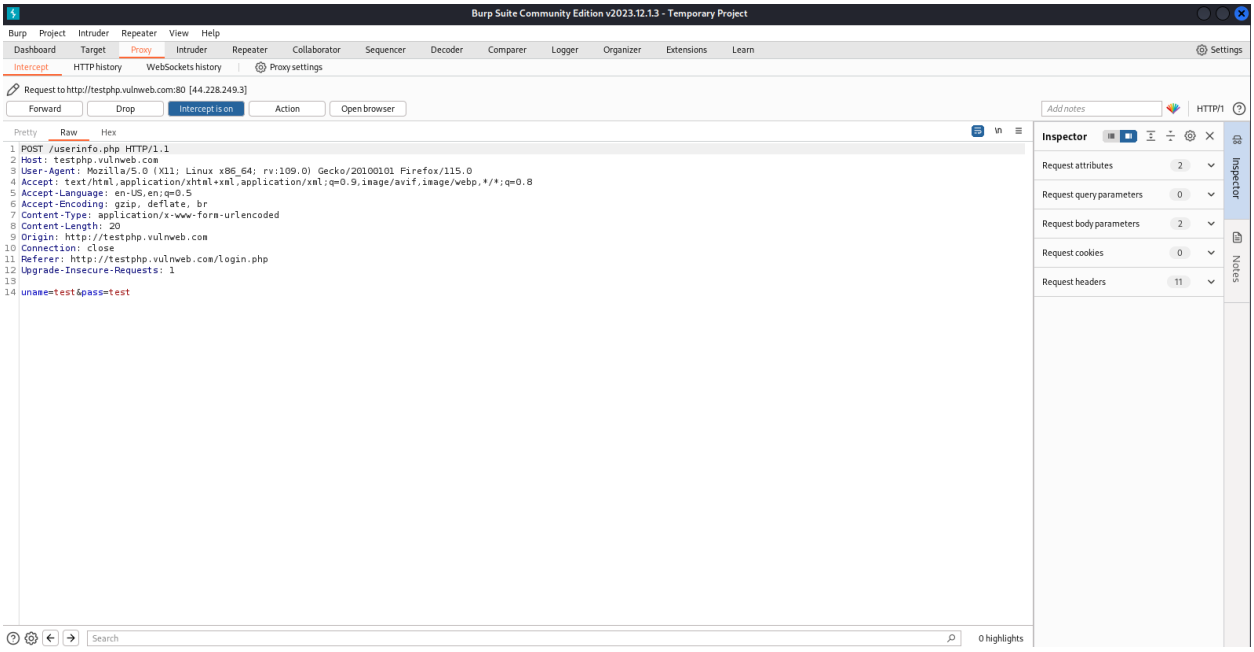
1. Firstly, open burp suite and turn on the intercept tab to intercept the http traffic of target webpage.



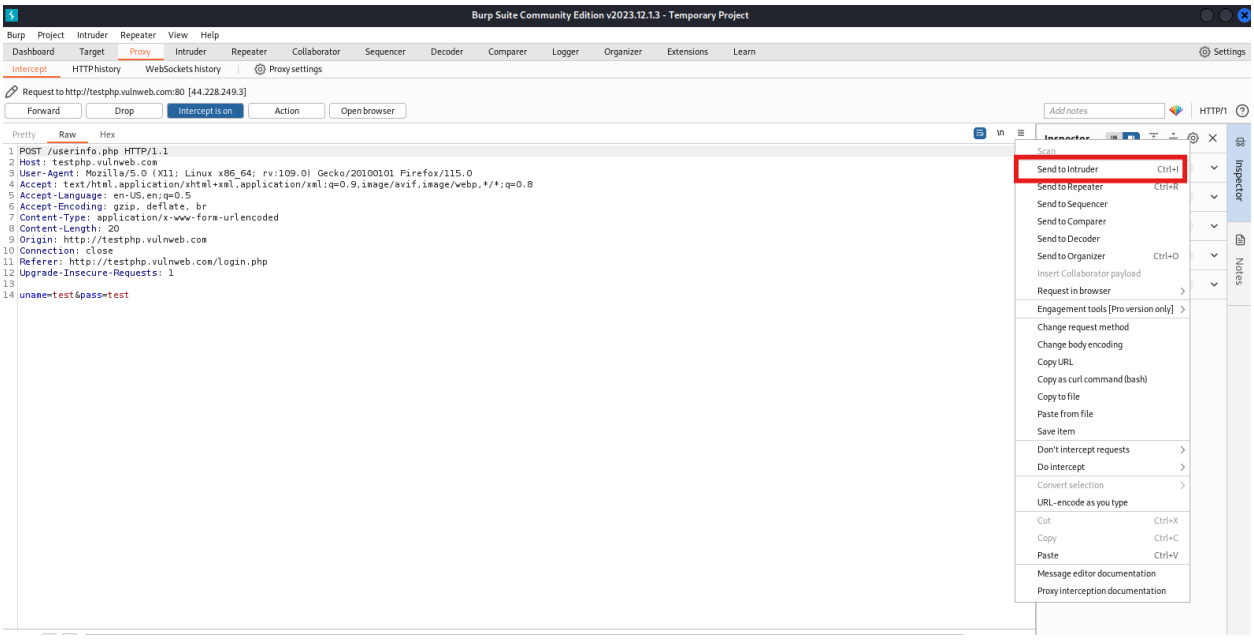
2. Now go to the target login webpage and fill up the possible credentials. Make sure to turn on browser's proxy.



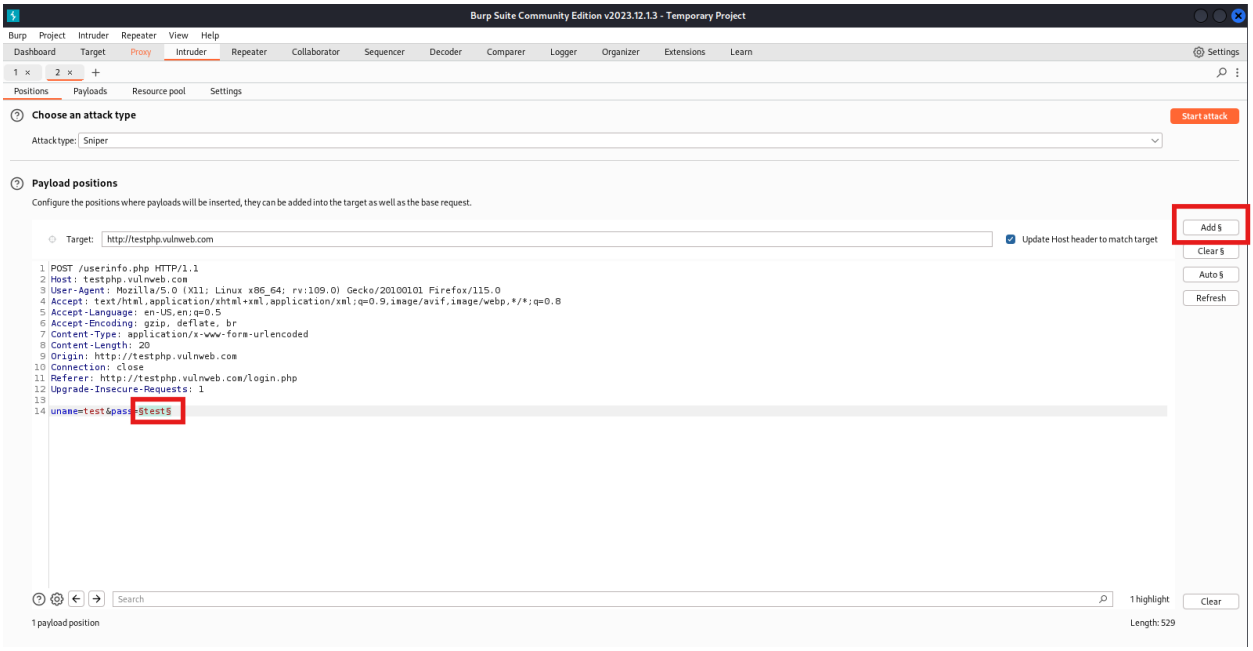
3. As soon as you hit the enter button you will redirected to the burp suite where we have captured the login request.



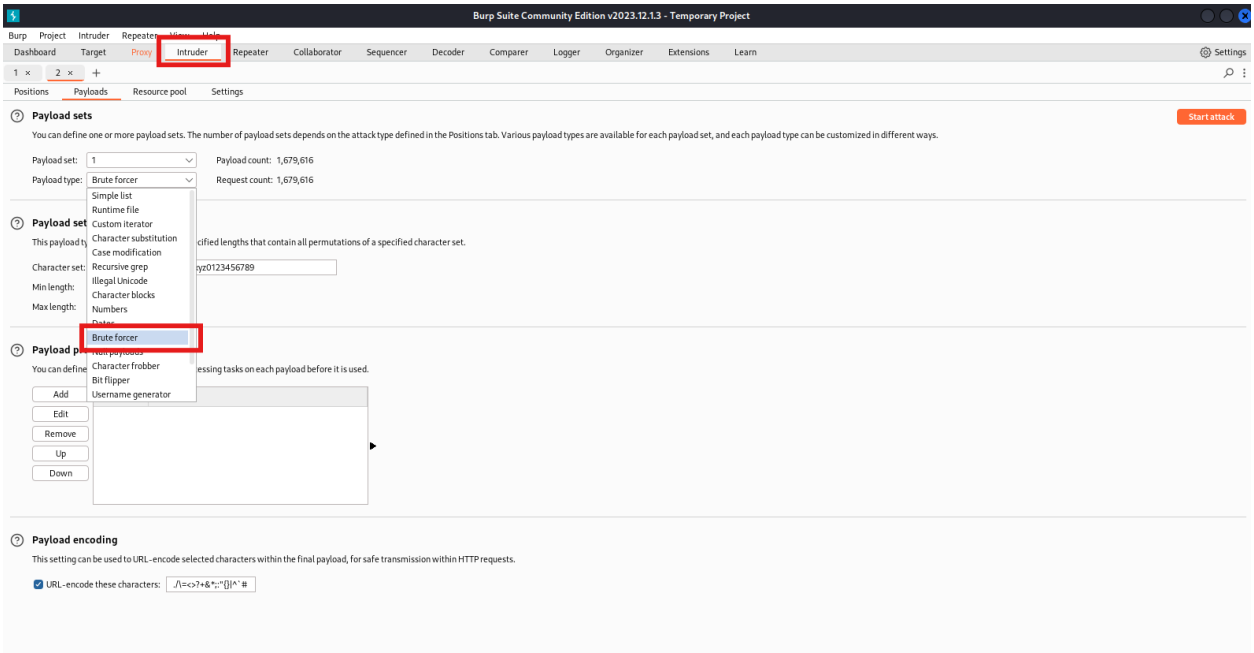
4. Now use the send to intruder button to specify the target.



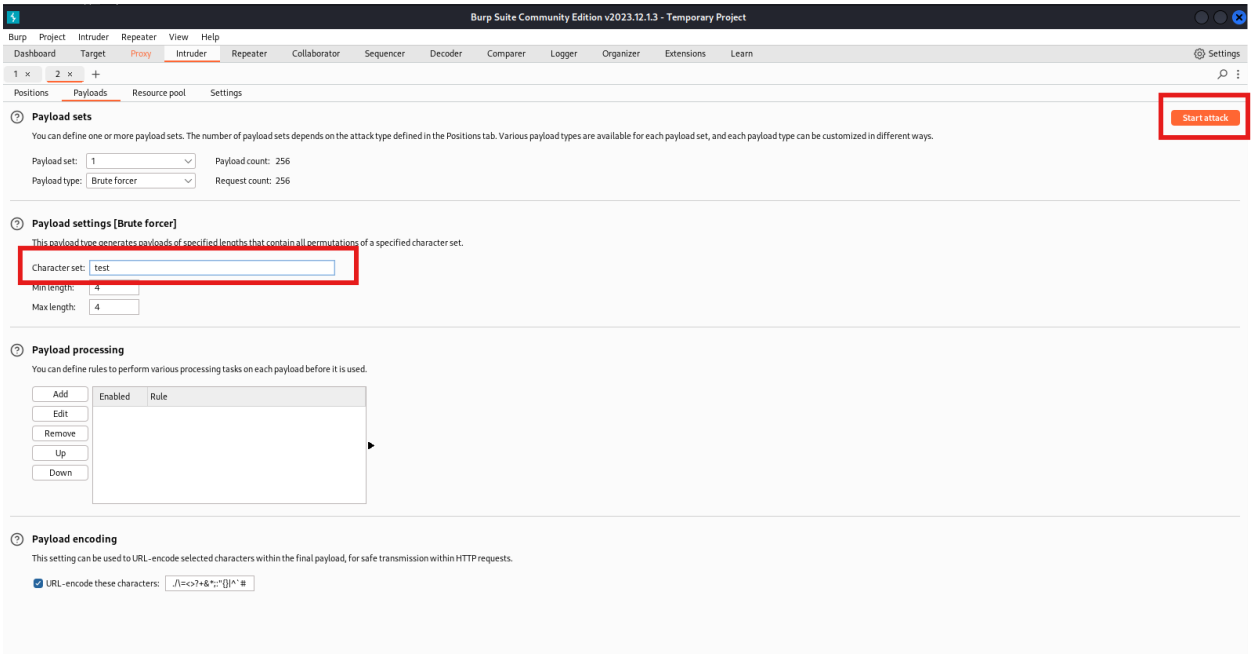
5. After sending it to intruder add dollar symbol to the password as we are going to brute force the password.



6. Now after setting the positions go to the payload tab to set the payload. Here we have to choose for the brute forcer option as we are going to perform a custom character brute force attack.



7. Now give the possible characters to perform the brute force attack. In my case I just provided it test as I want to save the time. The more character we provide the more time it will take.



8. At last we have the result as we can see our password is whom is having a uneven length.