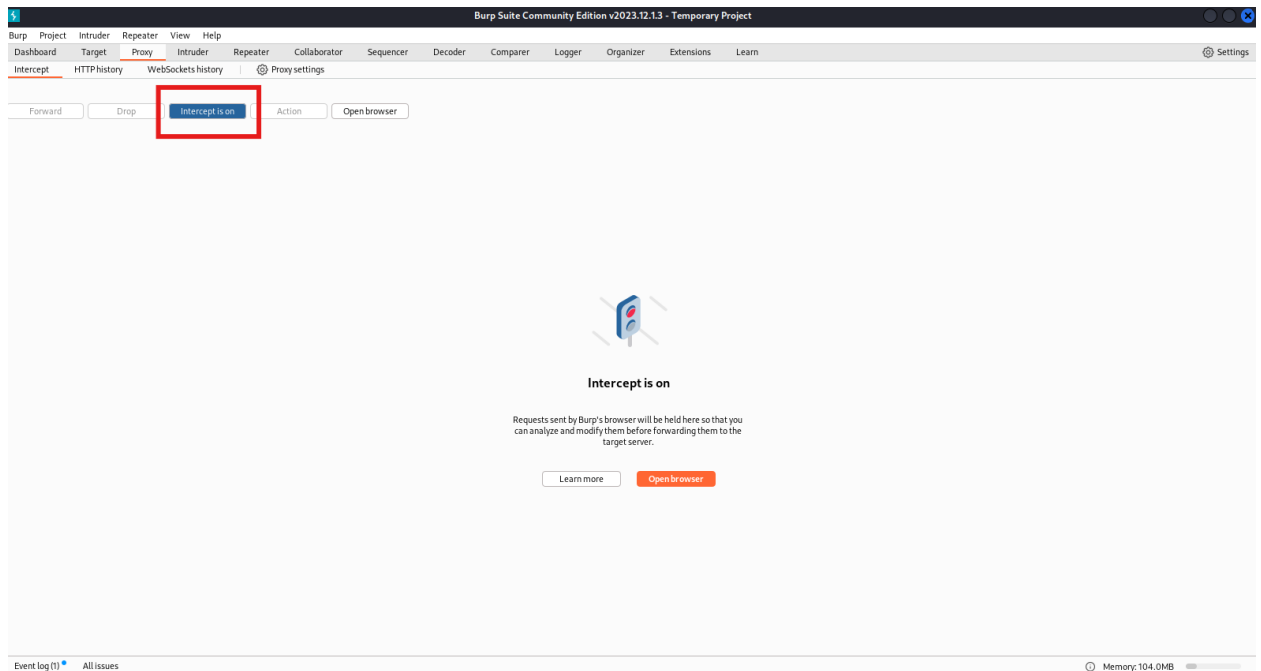


# Burp Suite: Brute Force Attack

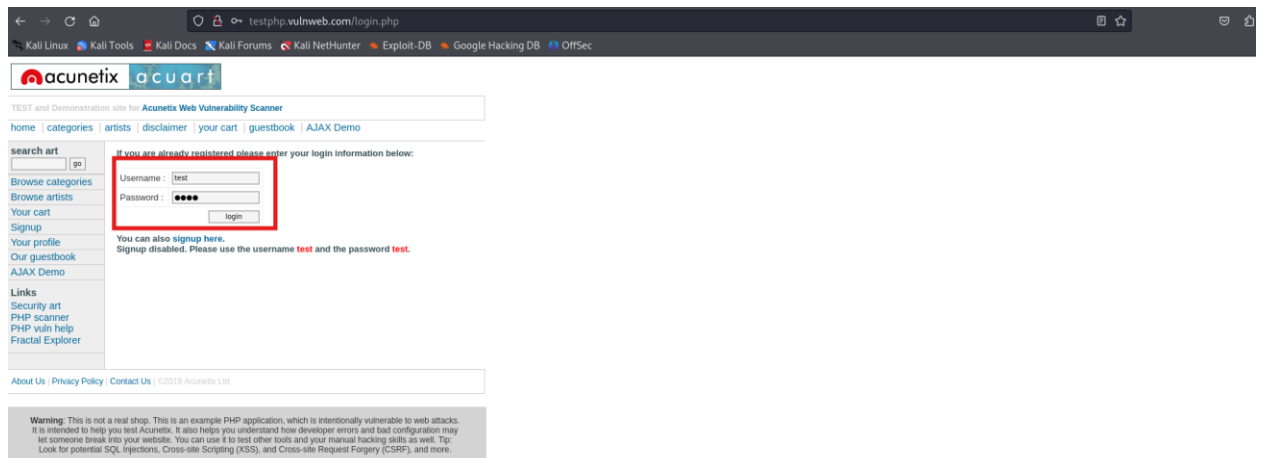
A brute force attack using Burp Suite involves utilizing the Intruder tool to systematically guess valid credentials or discover hidden information by trying numerous possible inputs. The process starts by setting up Burp Suite as a proxy and configuring the browser to route traffic through it, allowing 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: -

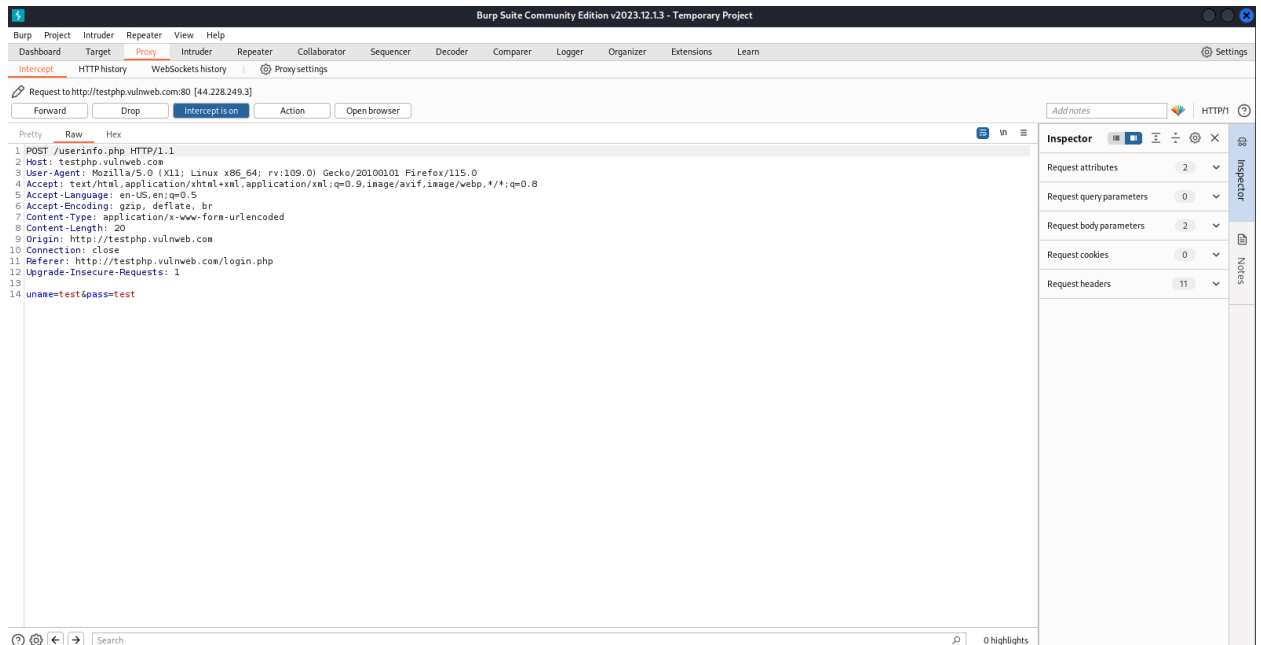
1. Firstly, open burp suite and turn on the intercept tab to intercept the http traffic of target webpage.



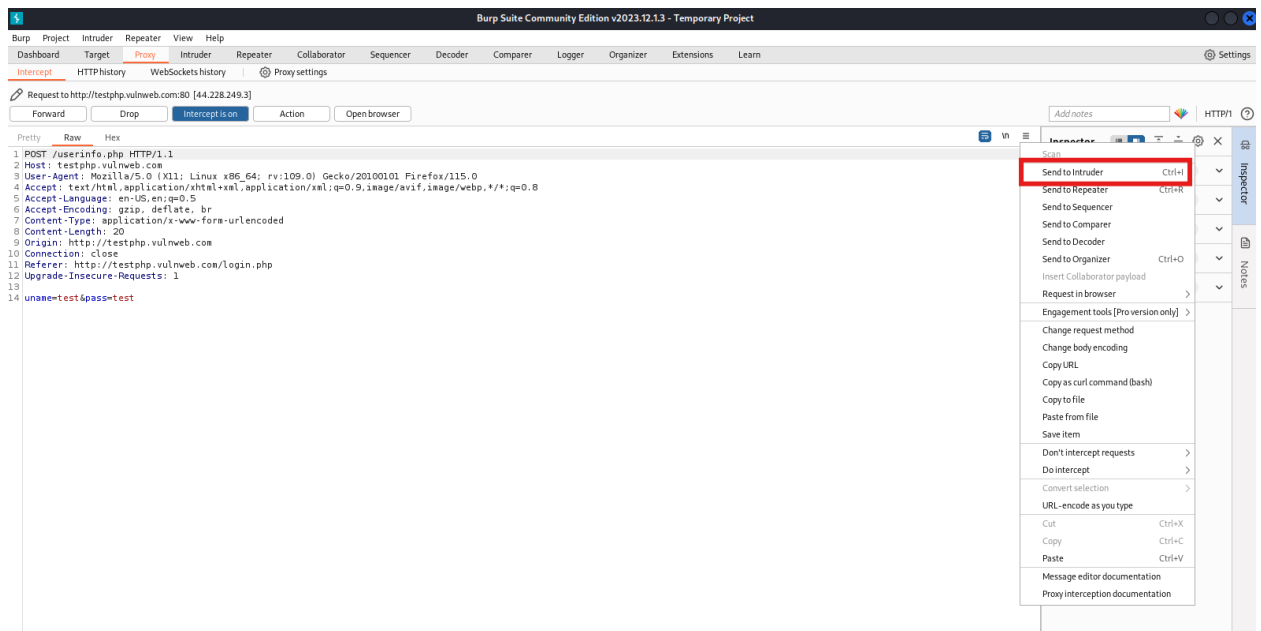
2. Now go to the target login webpage and fill up the possible credentials. Make sure to turn on browser's proxy.



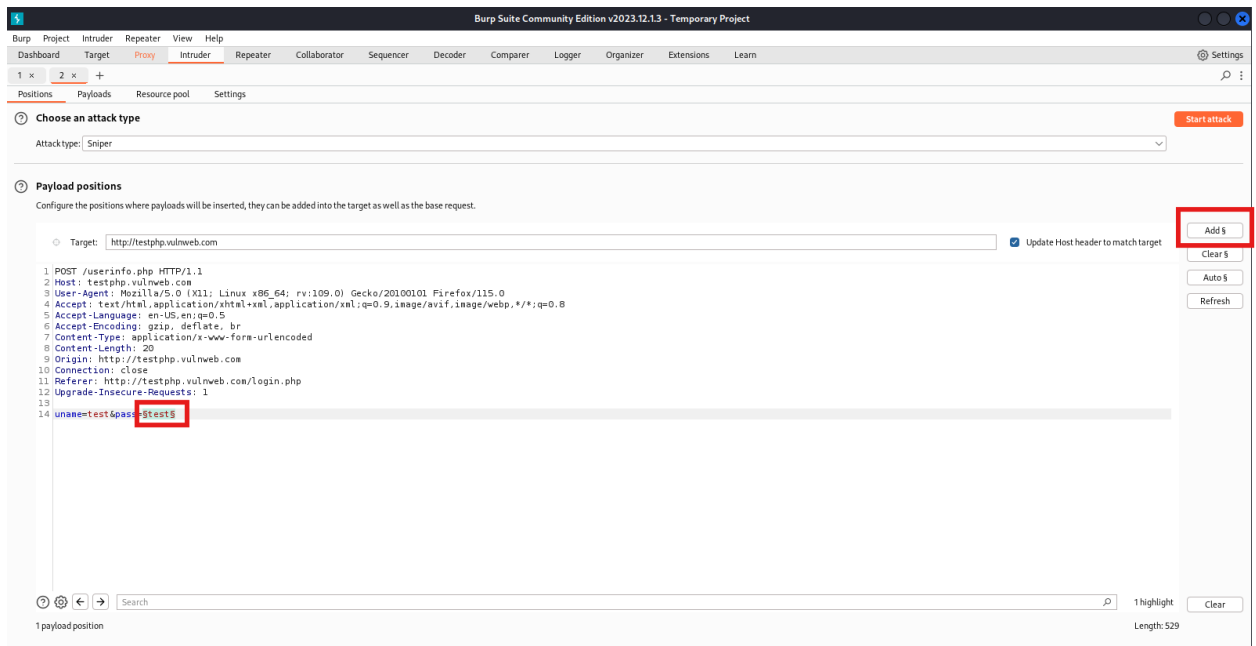
3. As soon as you hit the enter button you will be redirected to the burp suite where we have captured the login request.



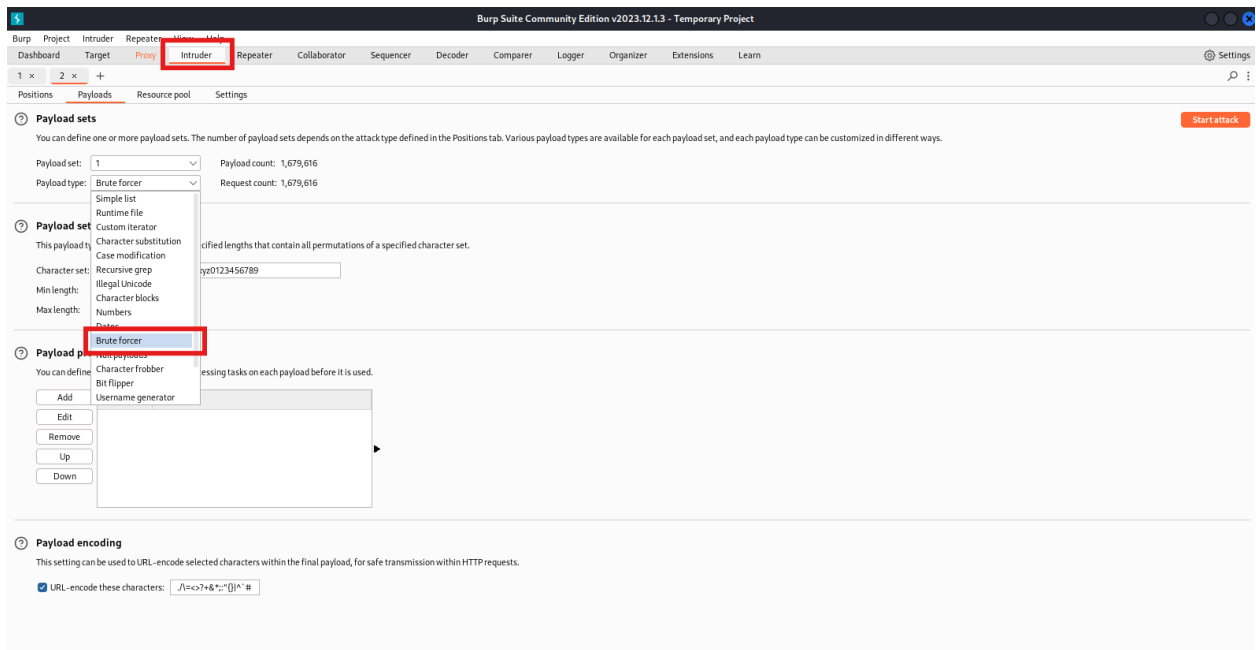
4. Now use the send to intruder button to specify the target.



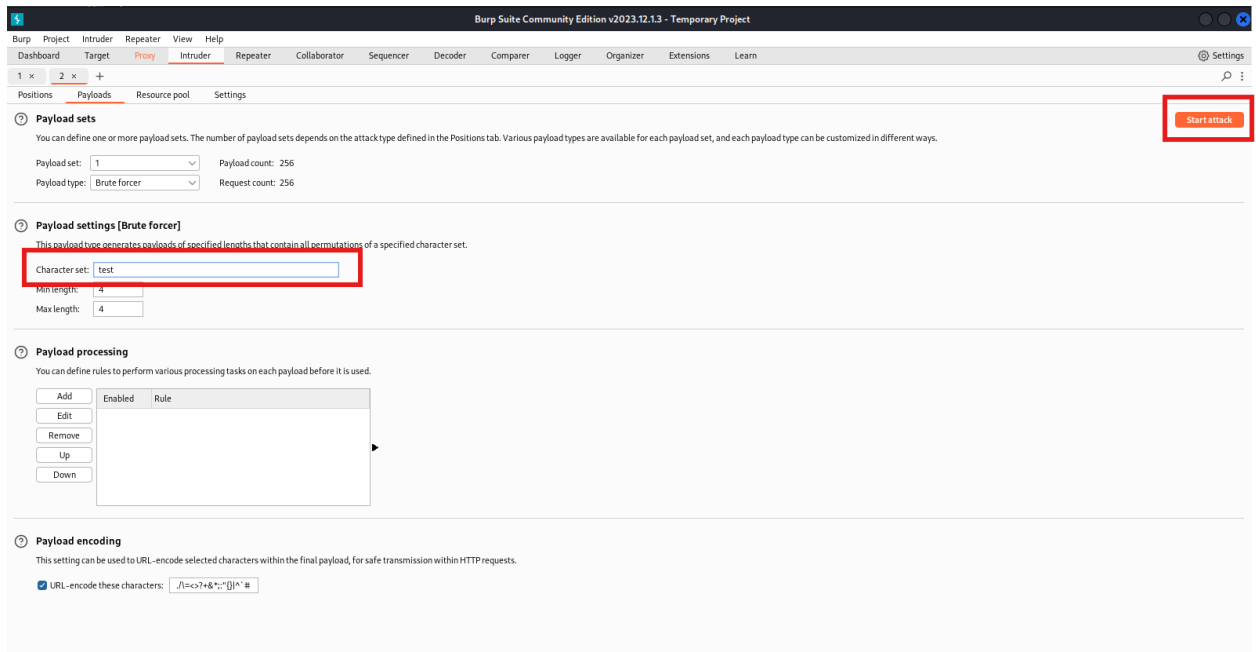
5. After sending it to intruder add dollar symbol to the password as we are going to brute force the password.



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.

3. Intruder attack of http://testphp.vulnweb.com

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Requ...	Payload	Status code	Error	Timeout	Length	Comment
14	eeet	302			258	
15	seet	302			258	
16	tset	302			258	
17	eset	302			258	
18	sset	302			258	
19	ttst	302			258	
20	etst	302			258	
21	asse	302			258	
22	test	200			6242	
23	sest	302			258	
24	sest	302			258	
25	tsst	302			258	
26	esst	302			258	

Request Response

Pretty Raw Hex

```
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 20
9 Origin: http://testphp.vulnweb.com
10 Connection: keep-alive
11 Referer: http://testphp.vulnweb.com/login.php
12 Upgrade-Insecure-Requests: 1
13
14 uname=test&pass=test
```

Finished

0 highlights