Aryaman Mishra

19BCE1027

Sniper (Single payload attack)

This uses a single set of payloads. It targets each payload position in turn, and places each payload into that position in turn. Positions that are not targeted for a given request are not affected - the position markers are removed and any enclosed text that appears between them in the template remains unchanged. This attack type is useful for fuzzing a number of request parameters individually for common vulnerabilities. The total number of requests generated in the attack is the product of the number of positions and the number of payloads in the payload set.

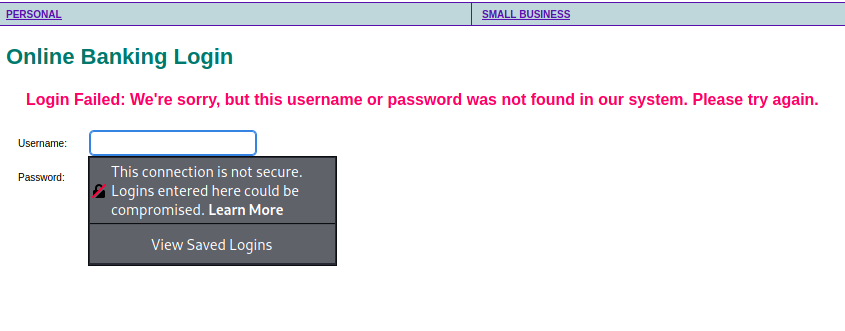
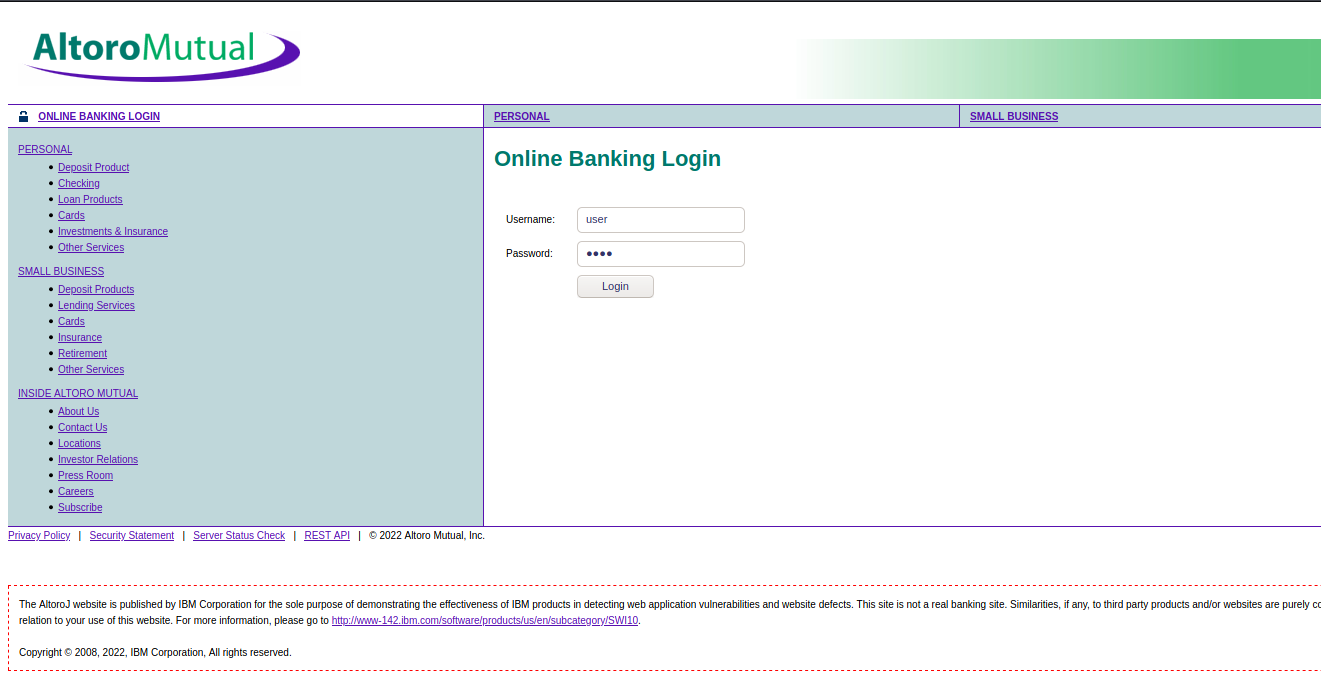
Battering ram (Single payload attack)

This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once. This attack type is useful where an attack requires the same input to be inserted in multiple places within the request (e.g. a username within a Cookie and a body parameter). The total number of requests generated in the attack is the number of payloads in the payload set.

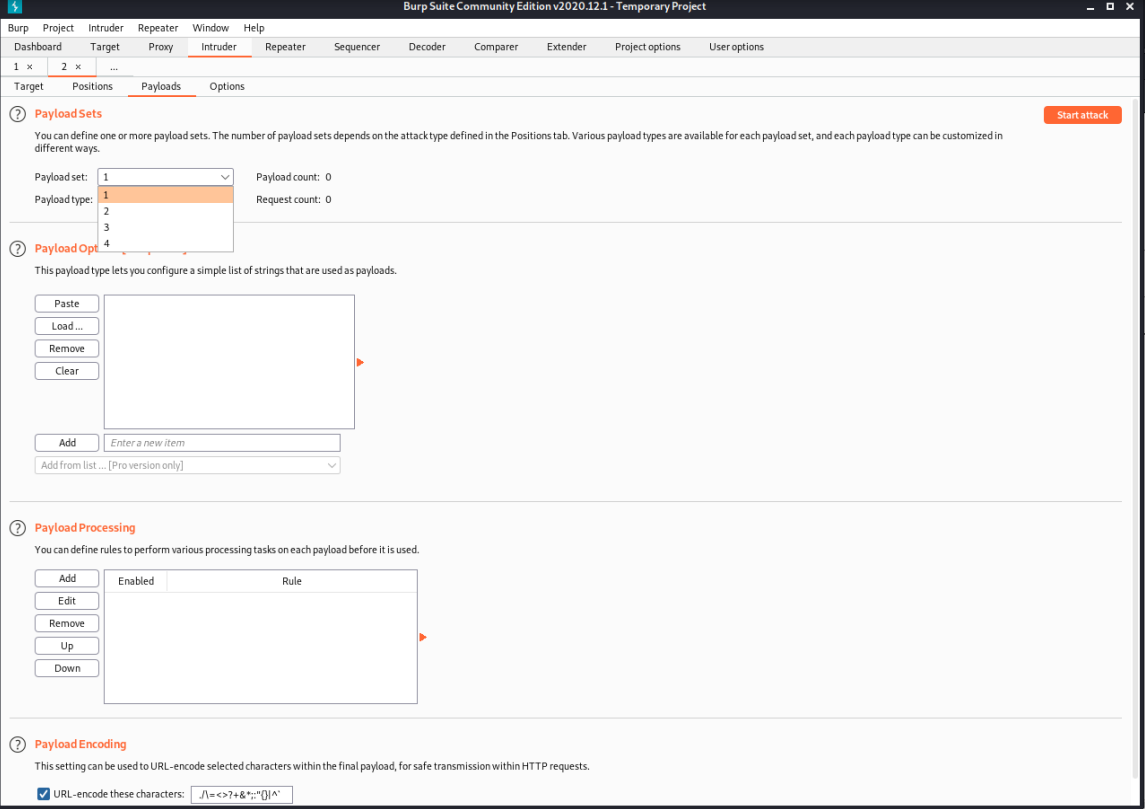
Pitchfork

This uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through all payload sets simultaneously, and places one payload into each defined position. In other words, the first request will place the first payload from payload set 1 into position 1 and the first payload from payload set 2 into position 2; the second request will place the second payload from payload set 1 into position 1 and the second payload from payload set 2 into position 2, etc. This attack type is useful where an attack requires different but related input to be inserted in multiple places within the request (e.g. a username in one parameter, and a known ID number corresponding to that username in another parameter). The total number of requests generated in the attack is the number of payloads in the smallest payload set.

Cluster bomb

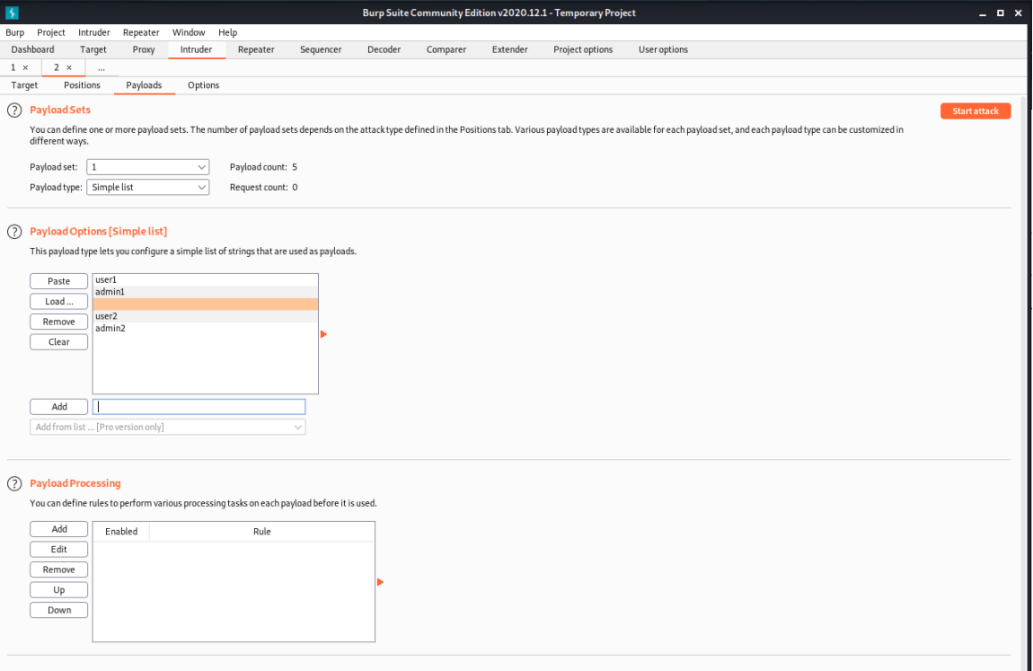
This uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn, so that all permutations of payload combinations are tested. I.e., if there are two payload positions, the attack will place the first payload from payload set 2 into position 2, and iterate through all the payloads in payload set 1 in position 1; it will then place the second payload from payload set 2 into position 2, and iterate through all the payloads in payload set 1 in position 1. This attack type is useful where an attack requires different and unrelated or unknown input to be inserted in multiple places within the request (e.g. when guessing credentials, a username in one parameter, and a password in another parameter). The total number of requests generated in the attack is the product of the number of payloads in all defined payload sets - this may be extremely large. 

Pitchfork



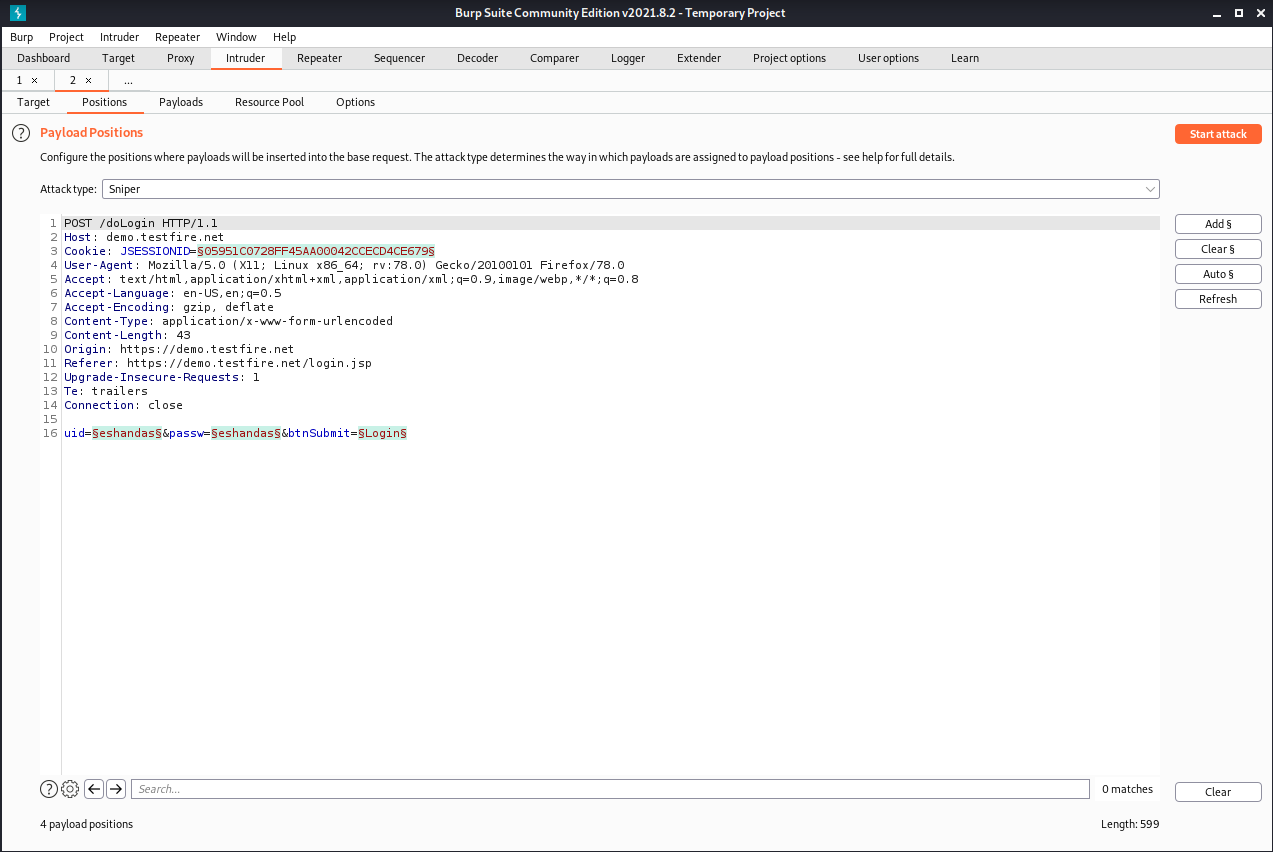
Cluster Bomb

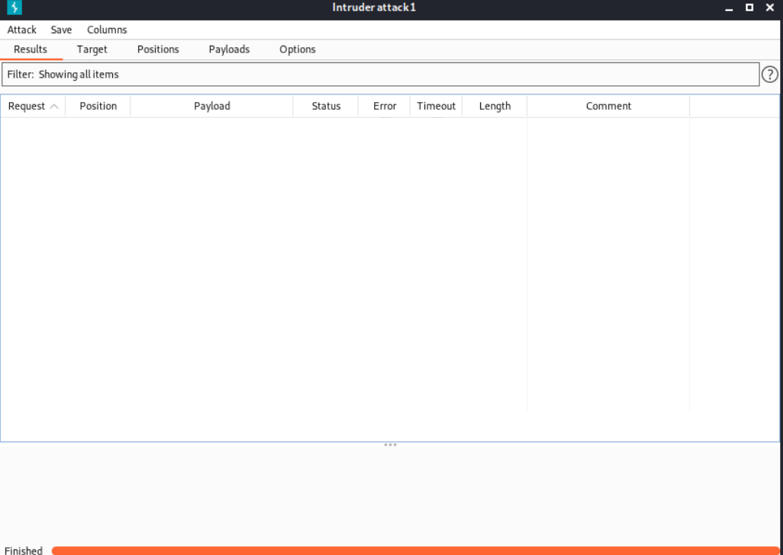
Payload

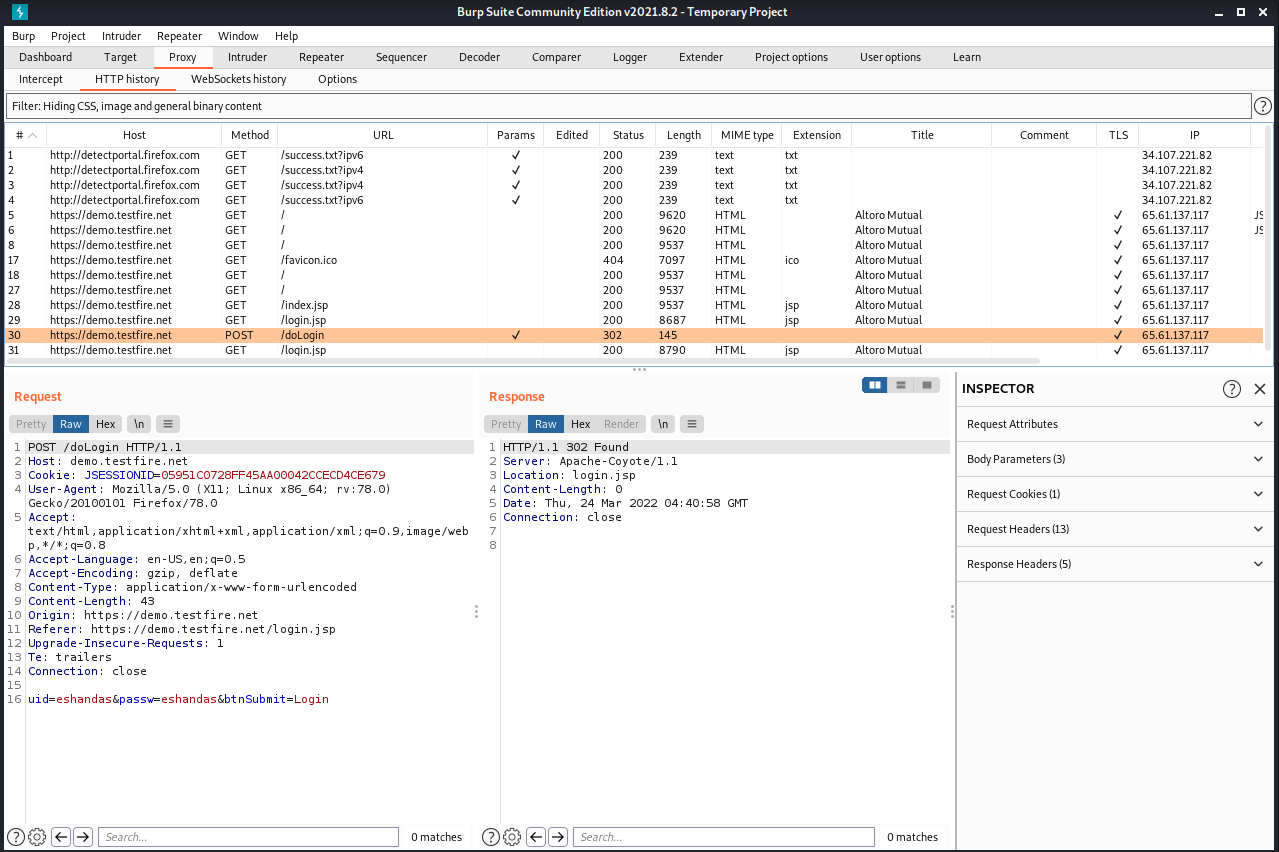


For sniper attack

Start attack

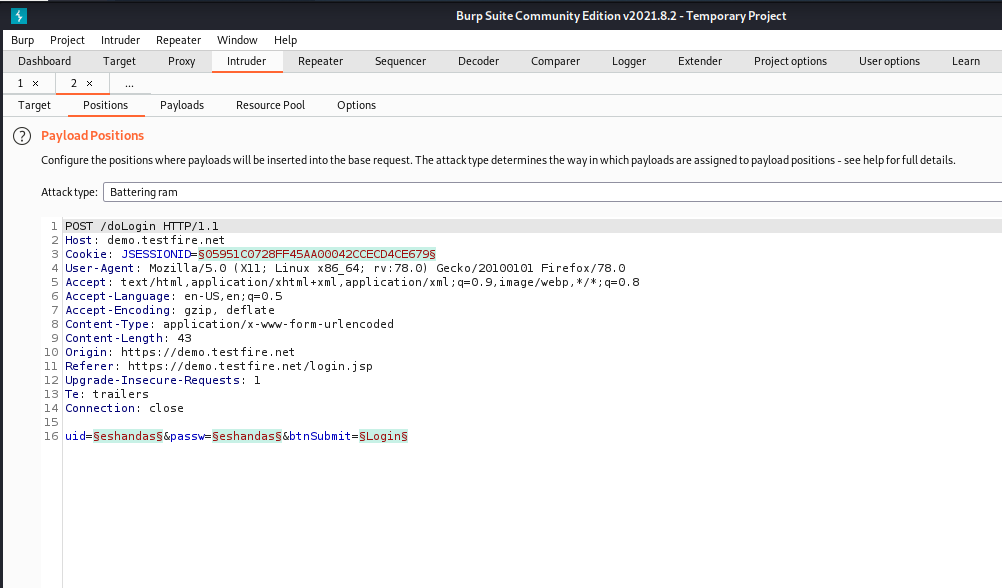


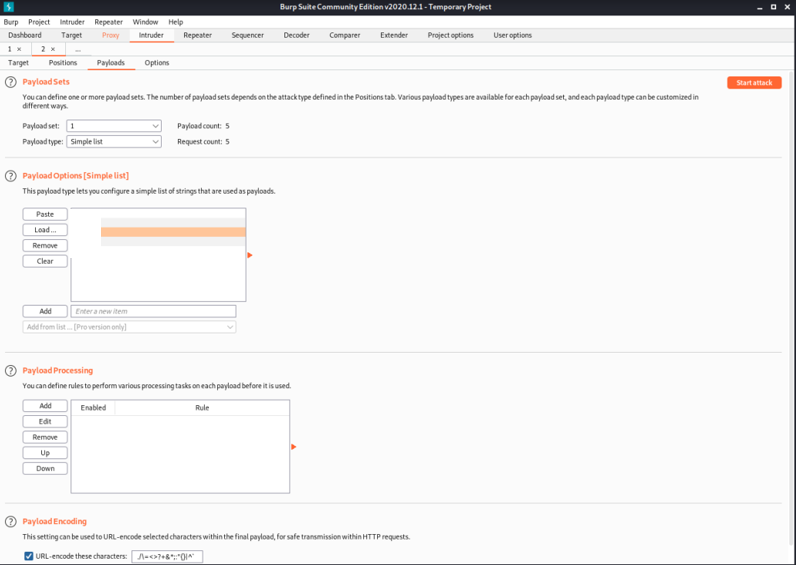


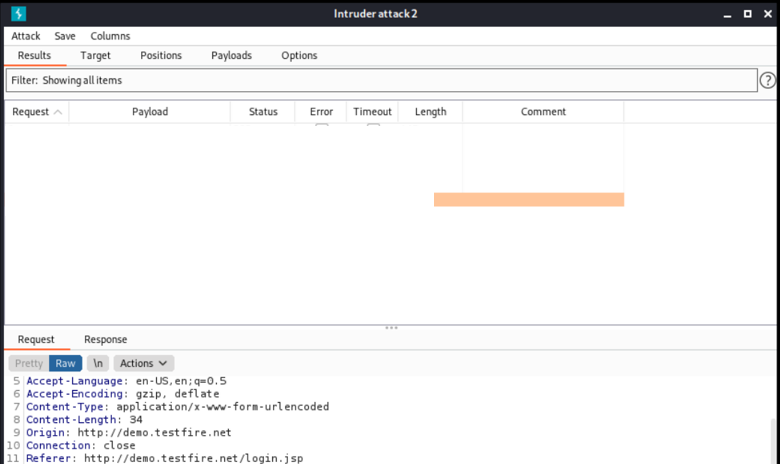


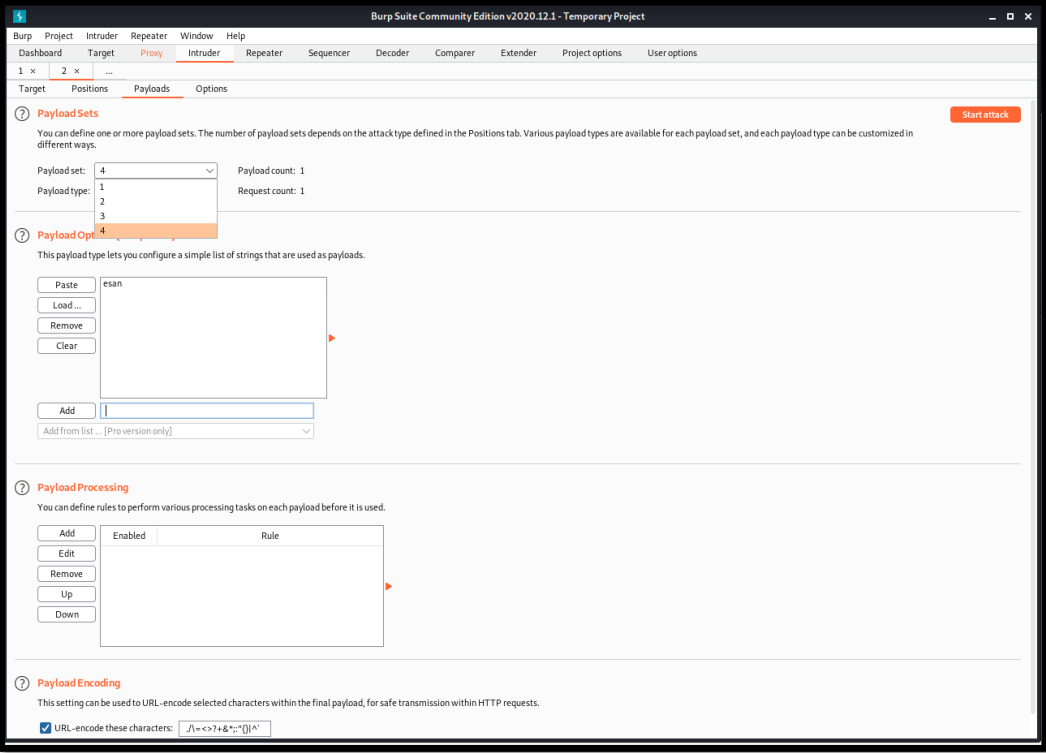
Demo website 4 attacks and Own website 4 attacks

Battering ram attack

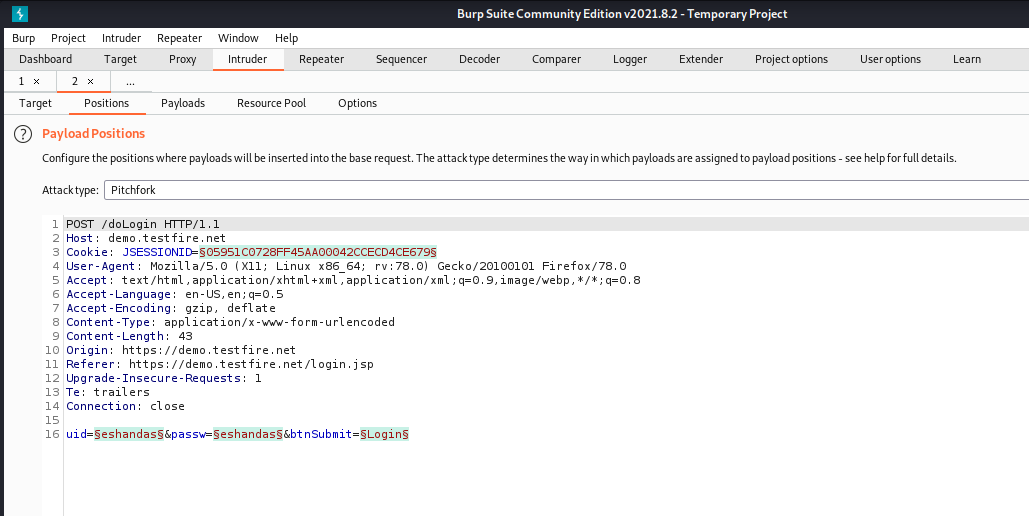


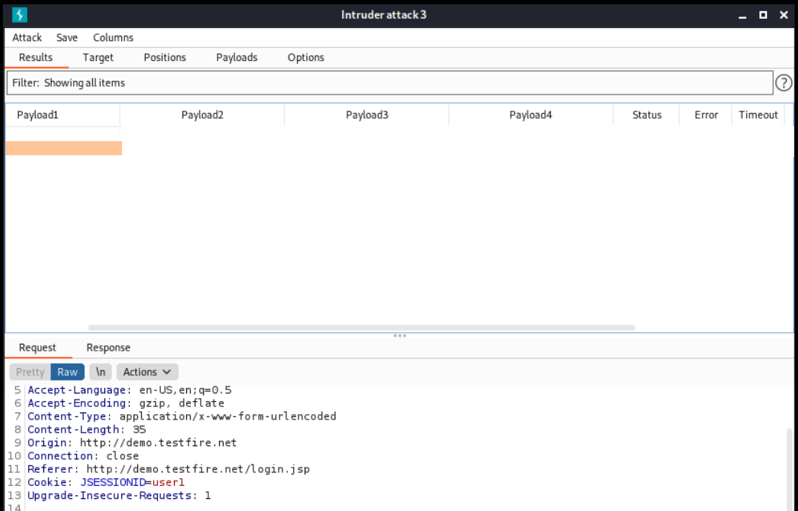




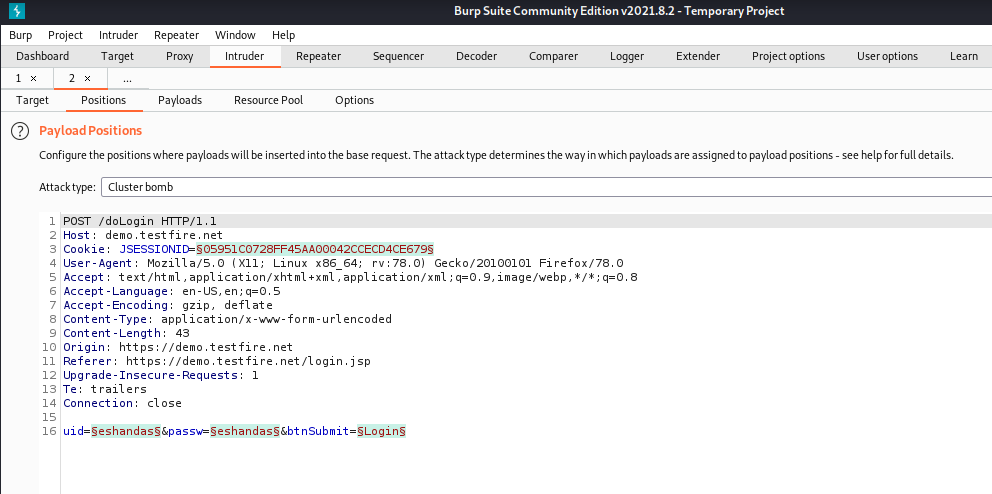


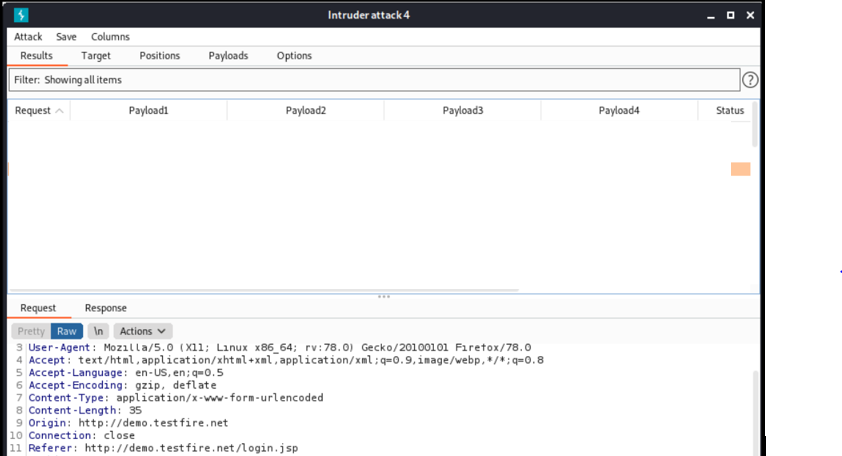
Pitchfork attack ()



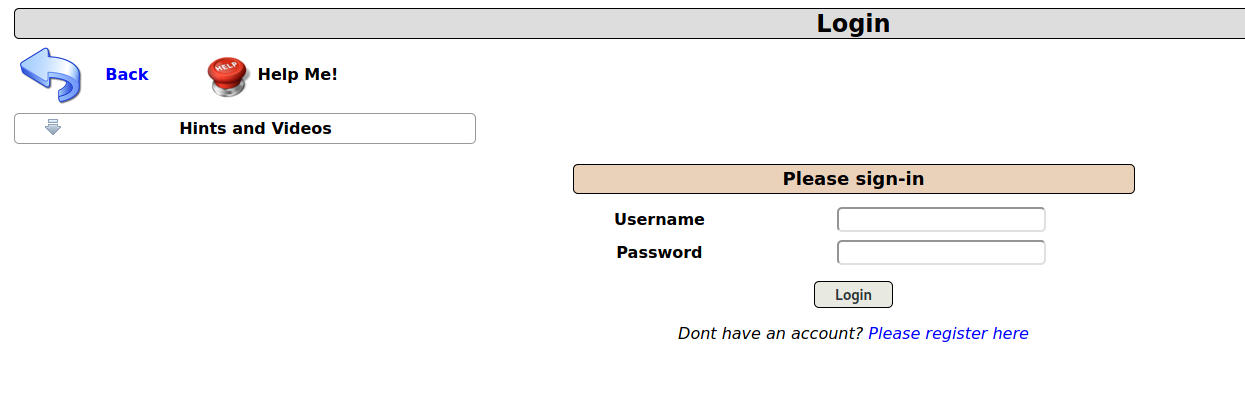


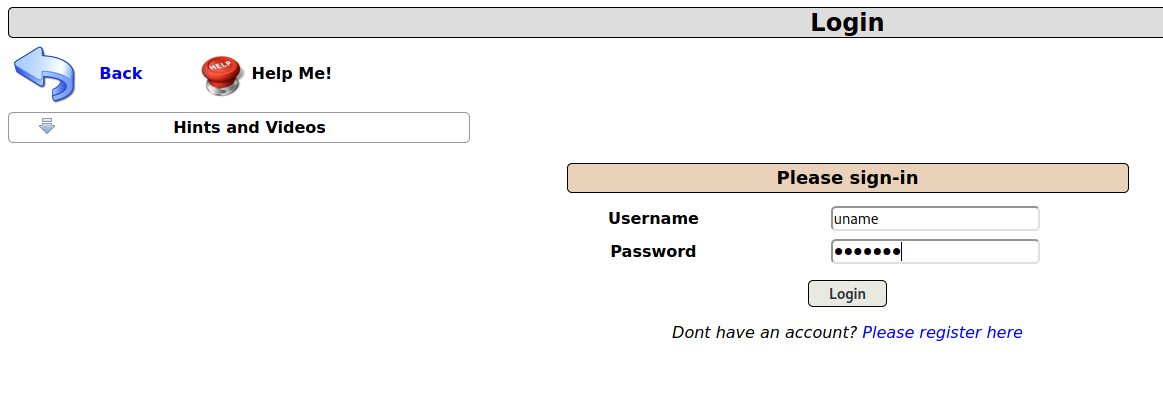
Clustering Bomb Attack





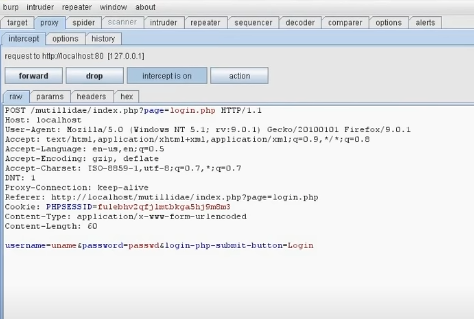
OWN website experiments



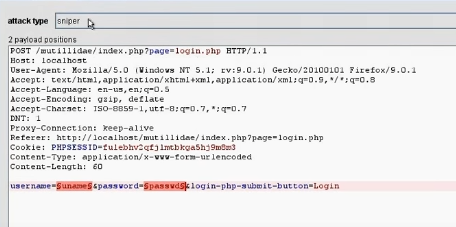


Username:uname

Password:pass123



Click on ‘send to intruder.’ And turn intercept off.

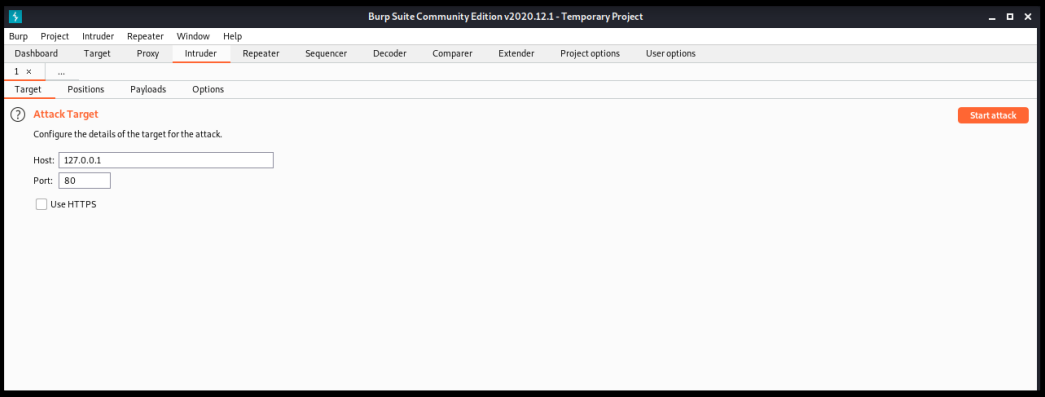


Login the website Quickstore Admin Portal (Self-made website)

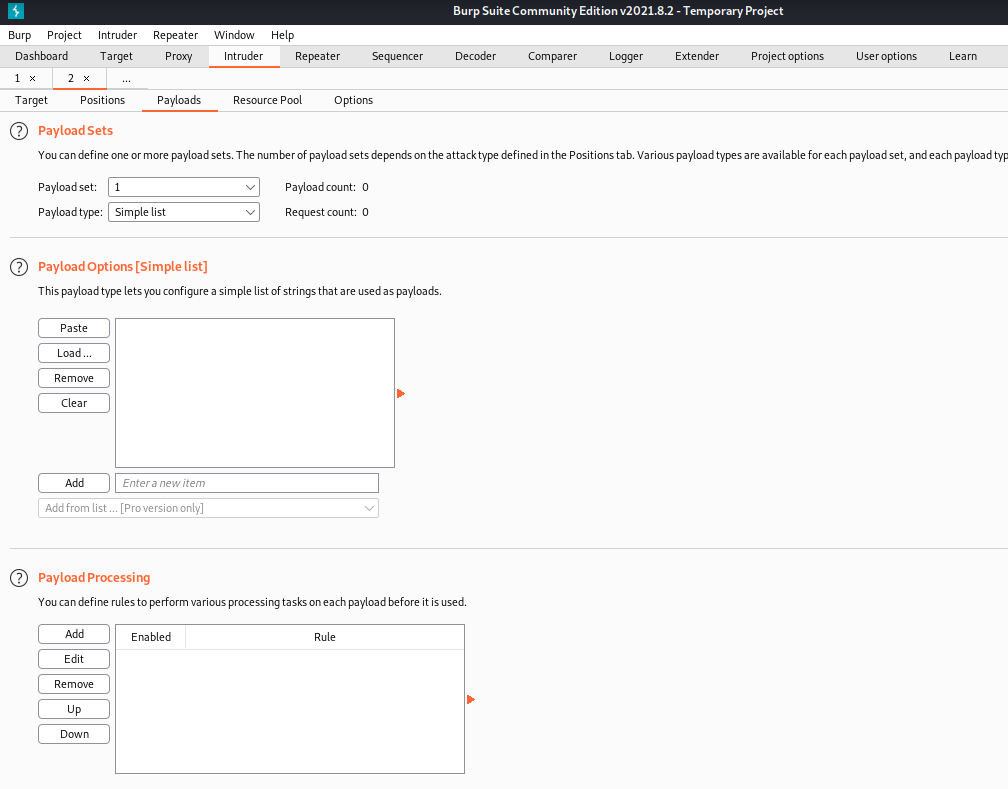
Go to burpsuite then choose Intruder and then select target

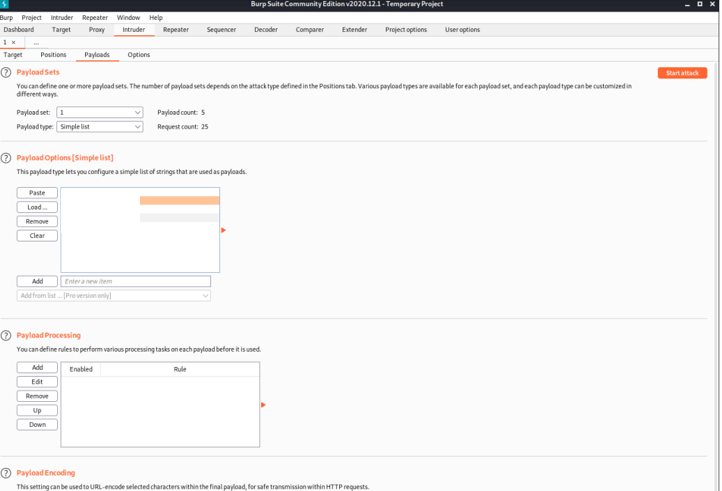
Again set target host as 127.0.0.1

Port :80

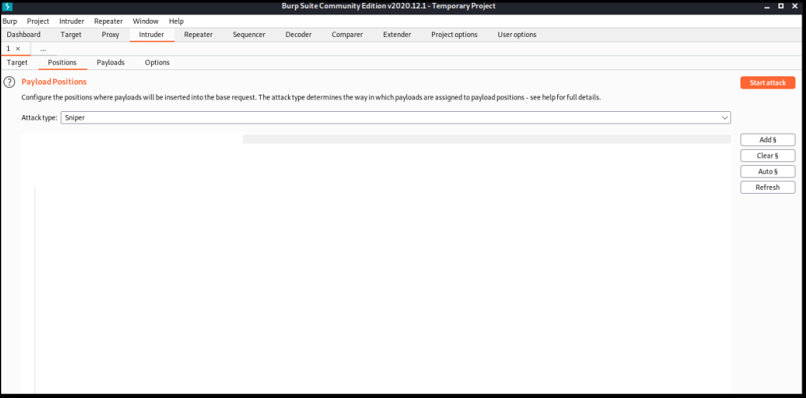


Go to payloads section and payloads as per attack type

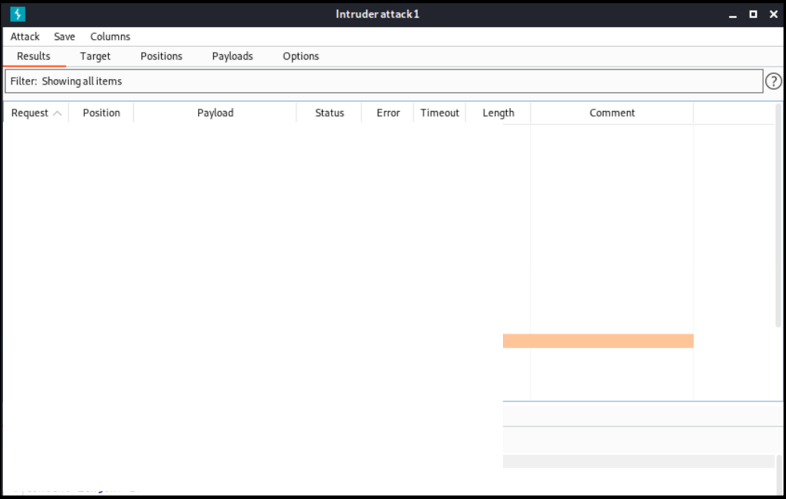




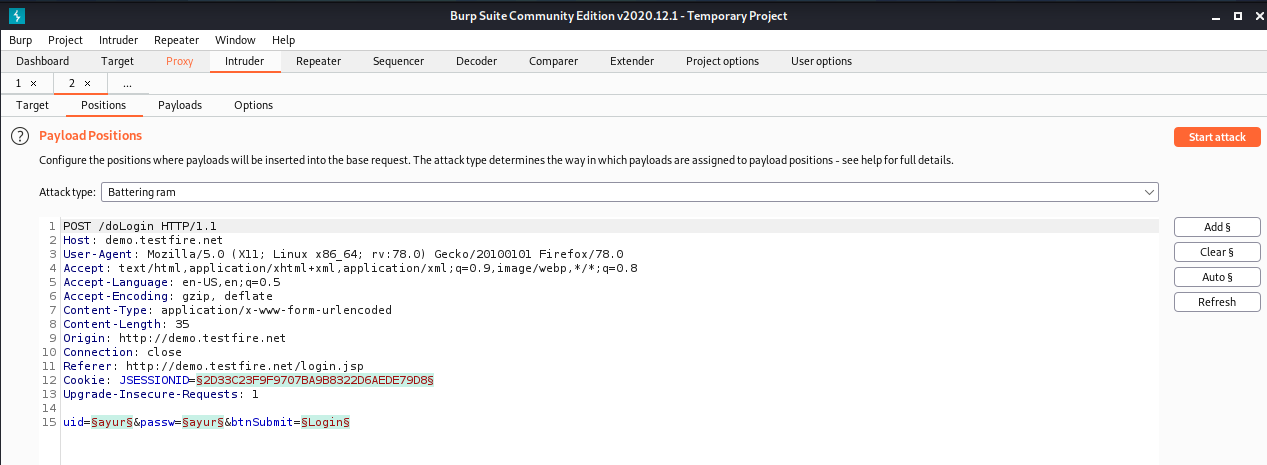
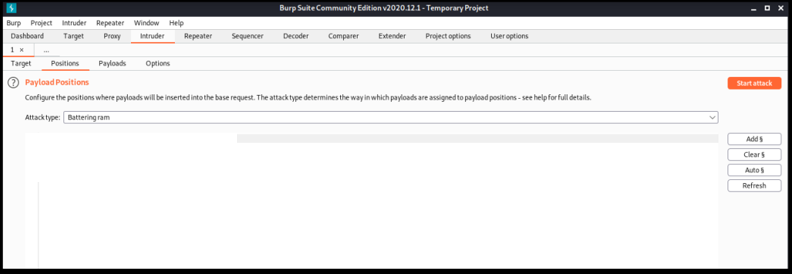
Set attack type: sniper

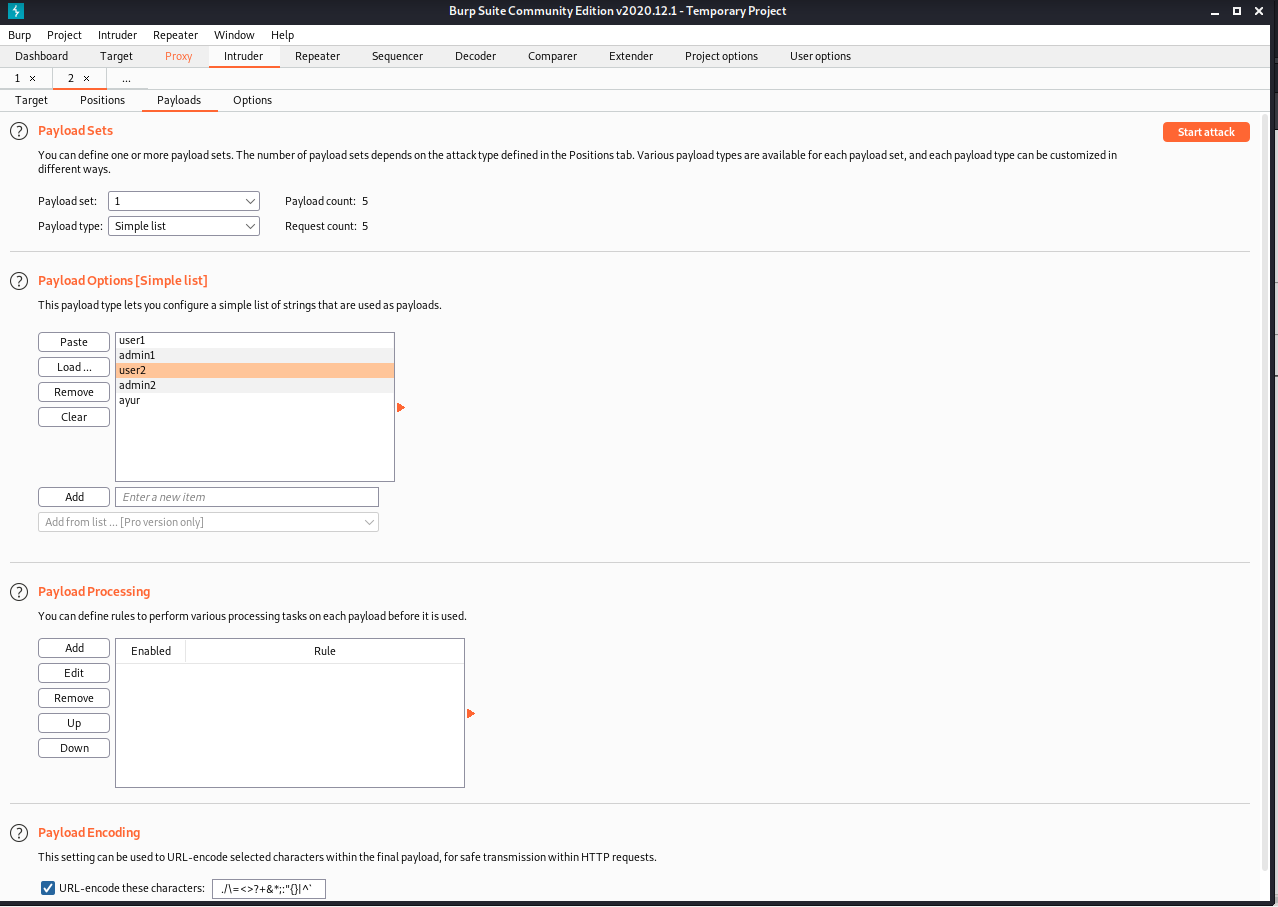


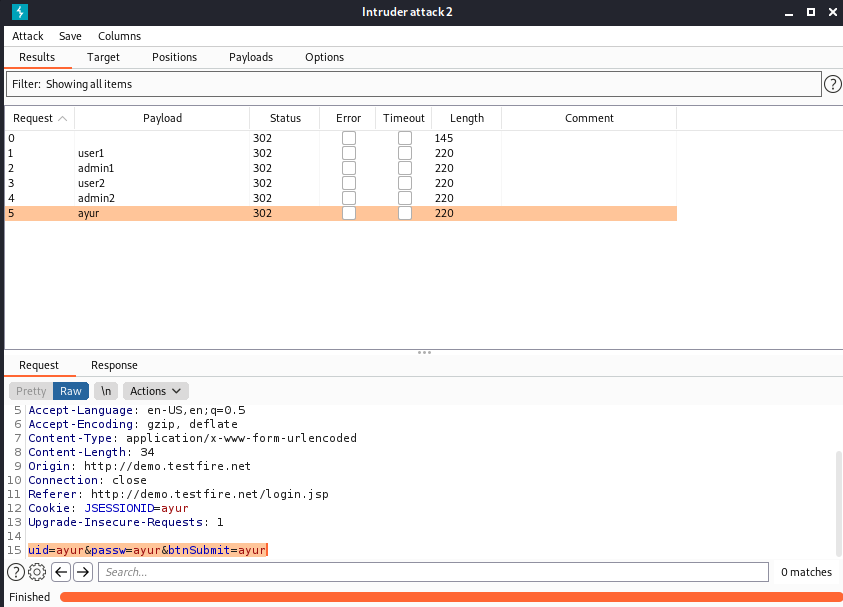
Start Attack

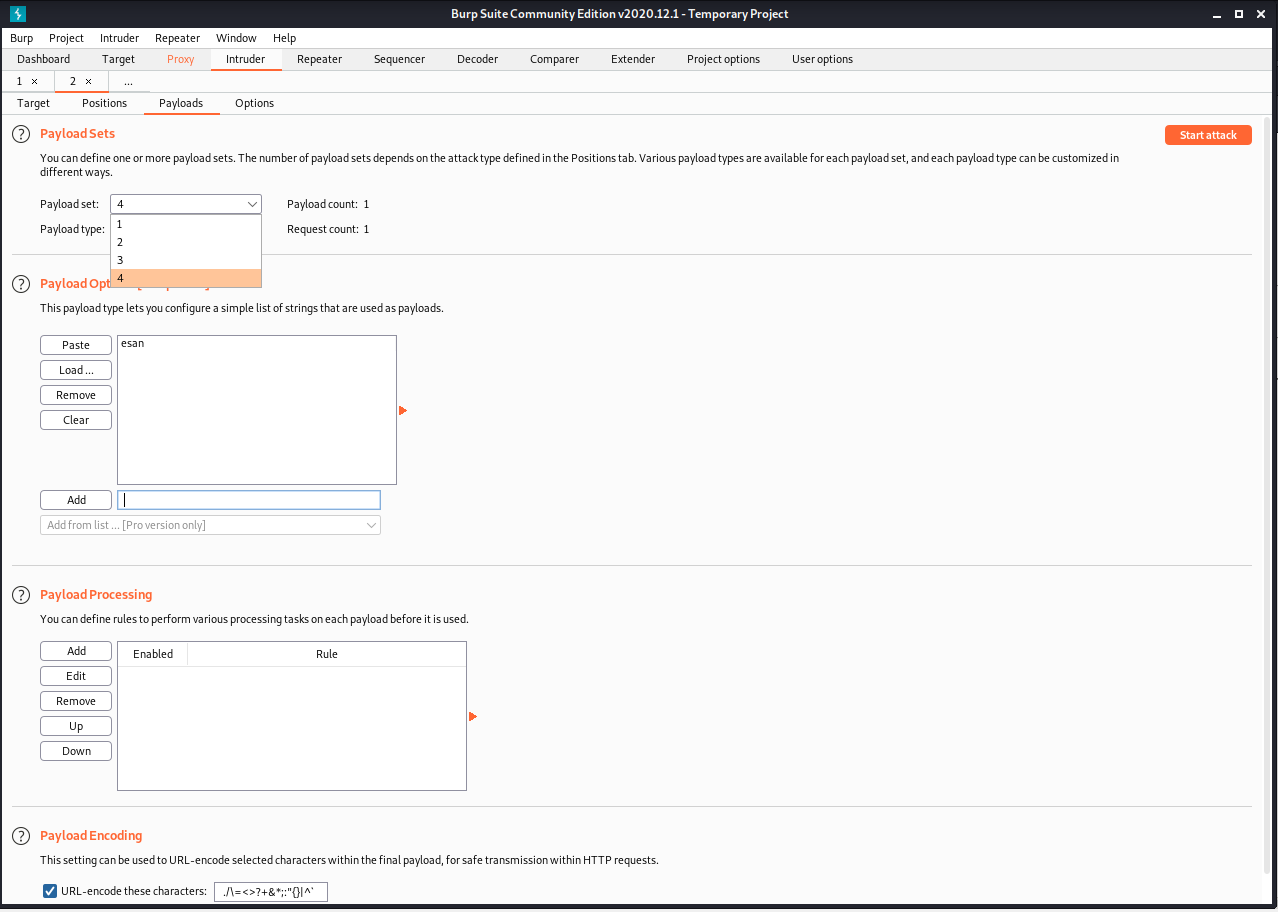


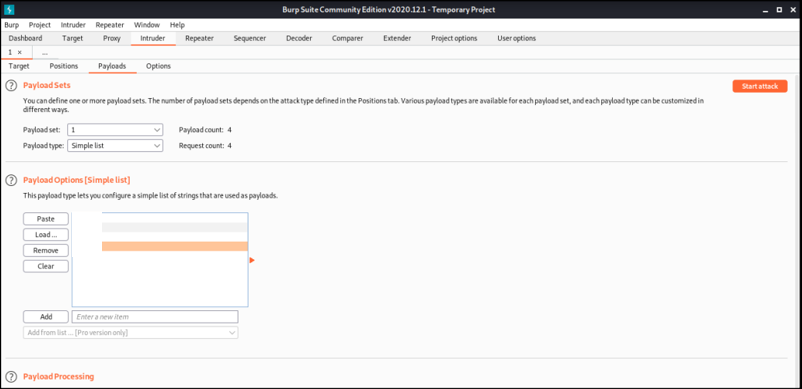
Battering ram attack





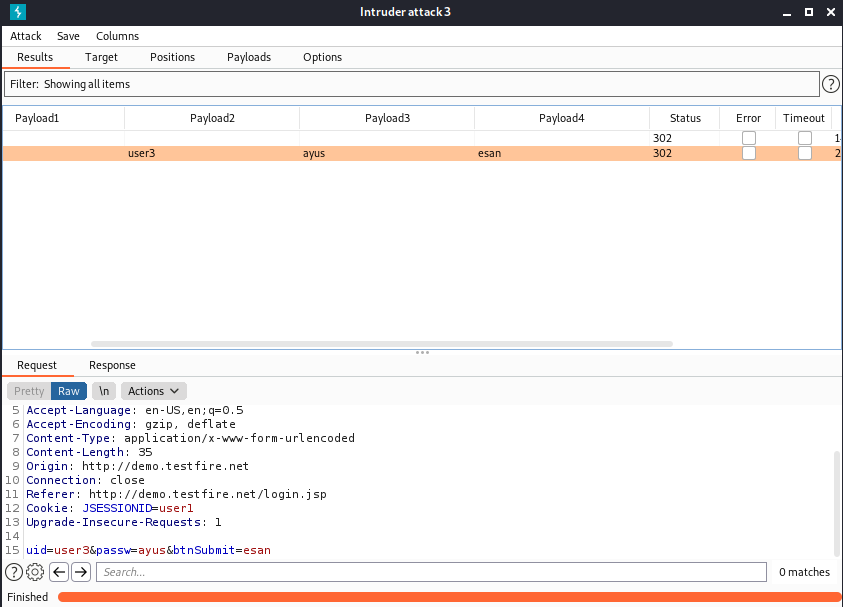
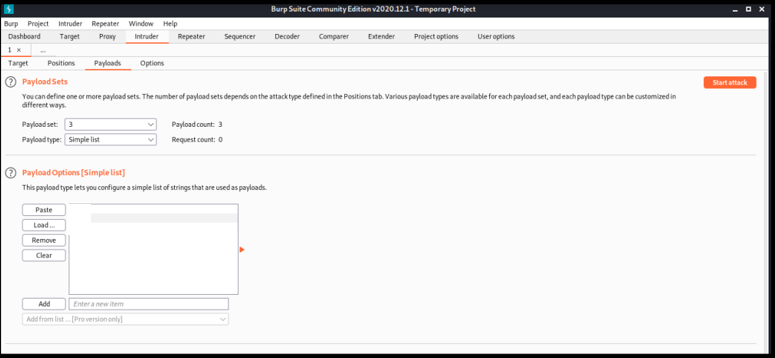


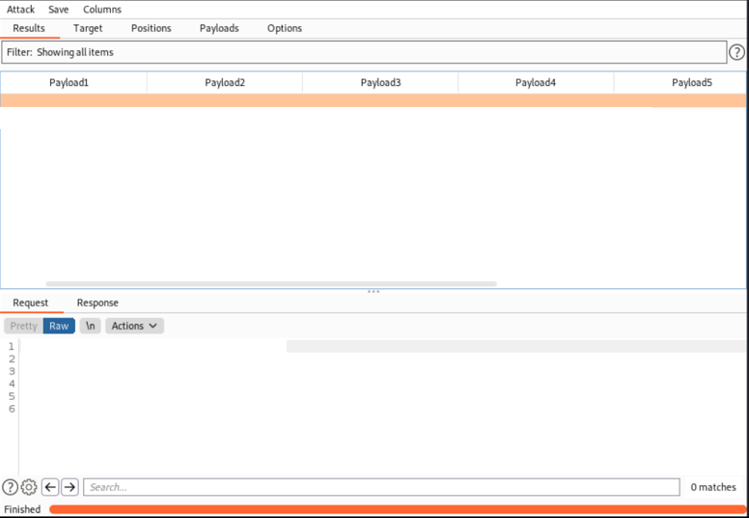




Pitchfork attack

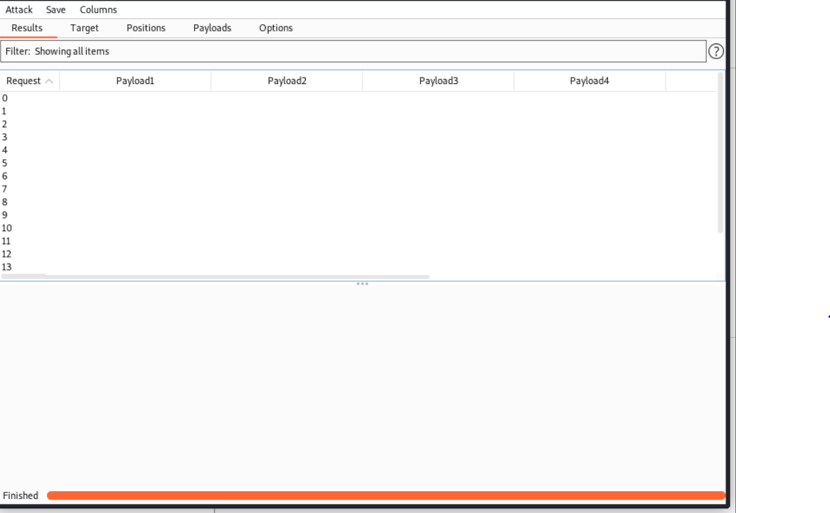
Provide different values for payloads and click on start attack

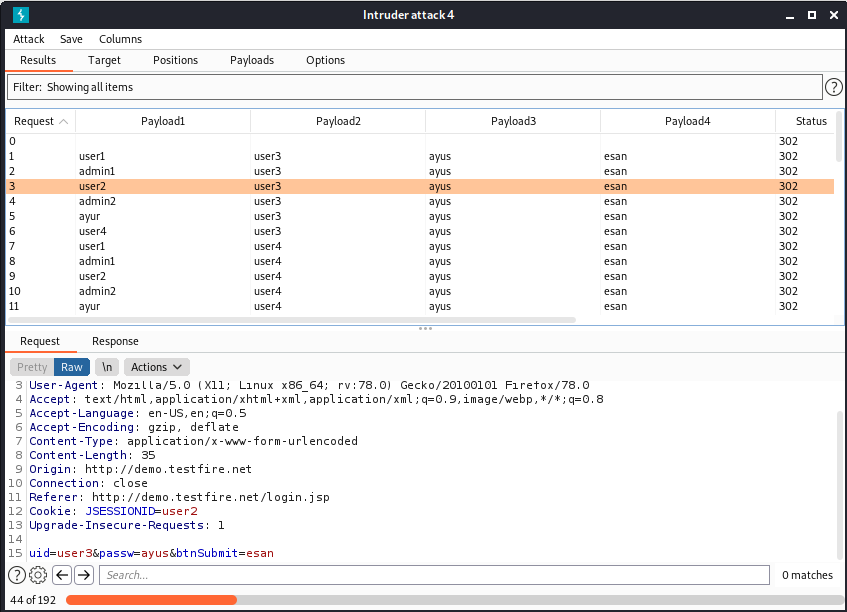




Clustering Bomb attack

Provide different values for payloads and click on start attack





Result: **All the attacks were successfully executed on a demo website and a self- made demo website used for login.**