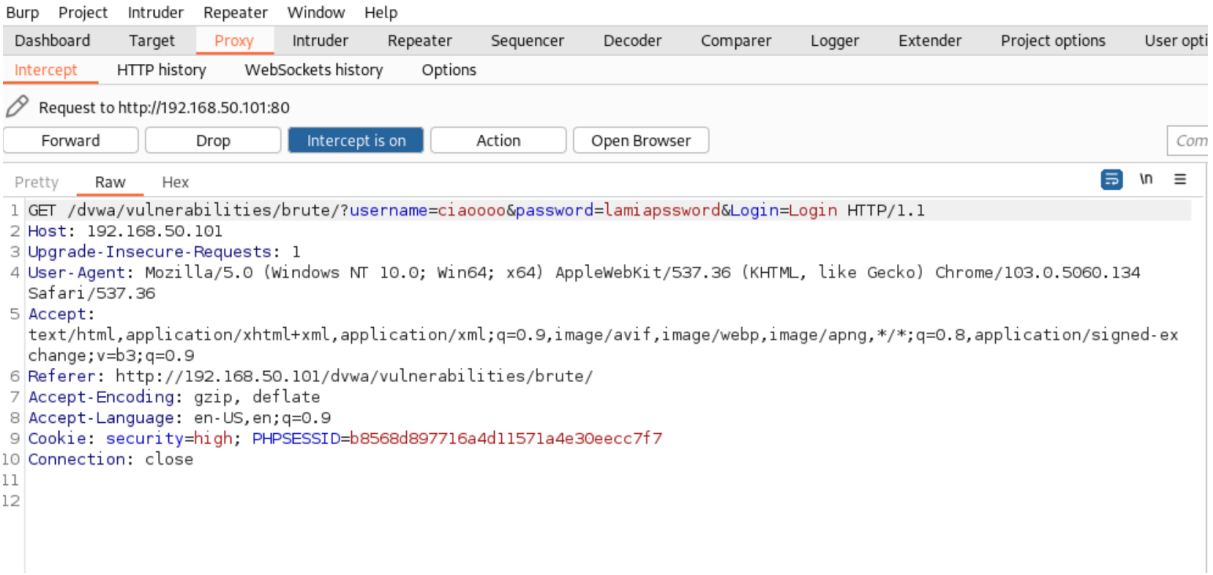
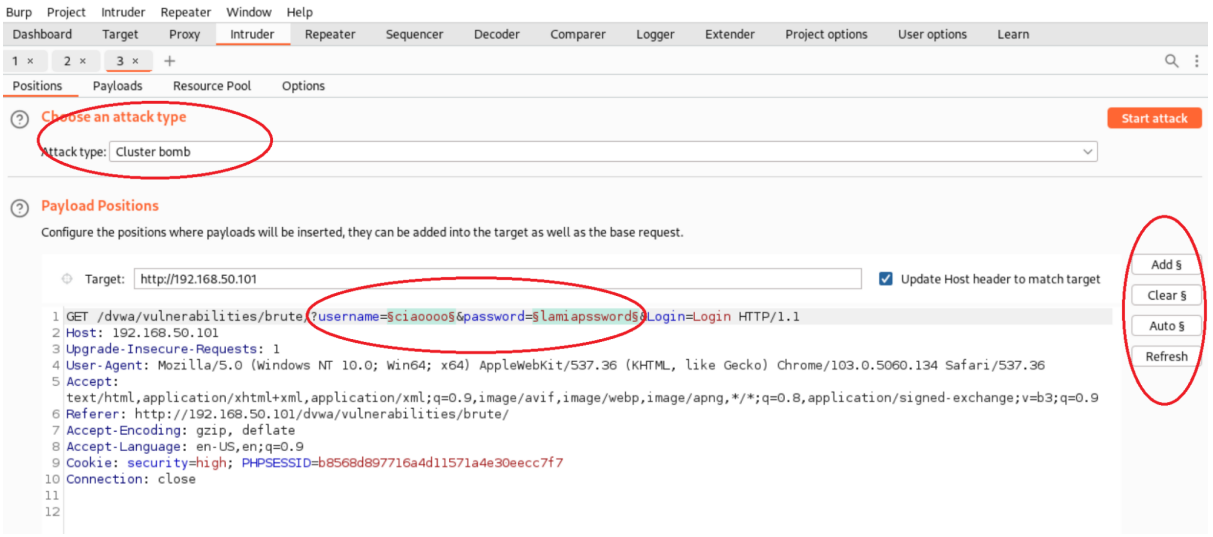
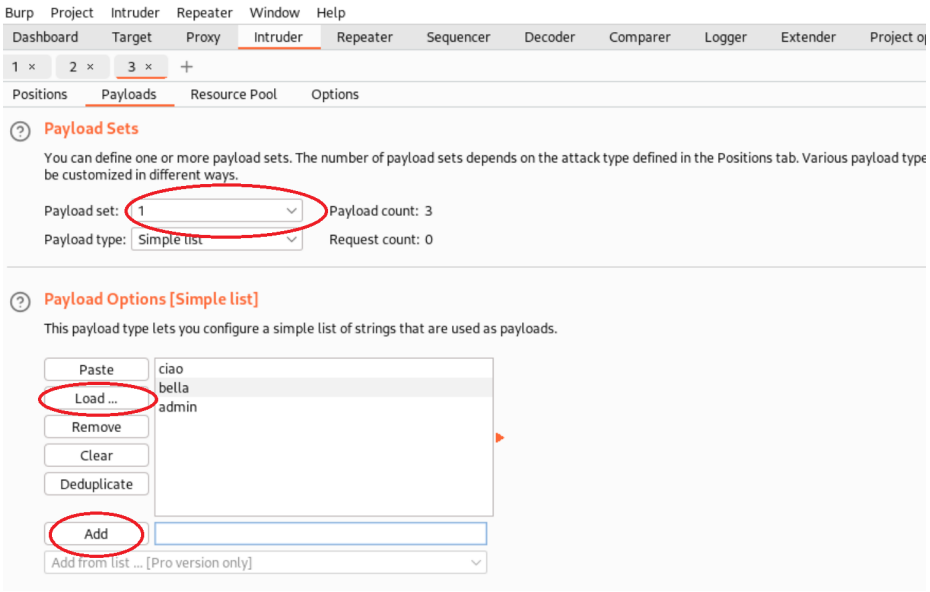
Per effettuare un brute force da Burpsuite verso dvwa rechiamoci alla pagina desiderata (in questo caso la pagina interna di DVWA dedicata al Brute Force) utilizzando il browser Chromium del programma e dopo aver attivato l'interceptor proviamo a effettuare un login (ovviamente non conosciamo le credenziali, ma quello che ci interessa è vedere la richiesta che viene effettuata).



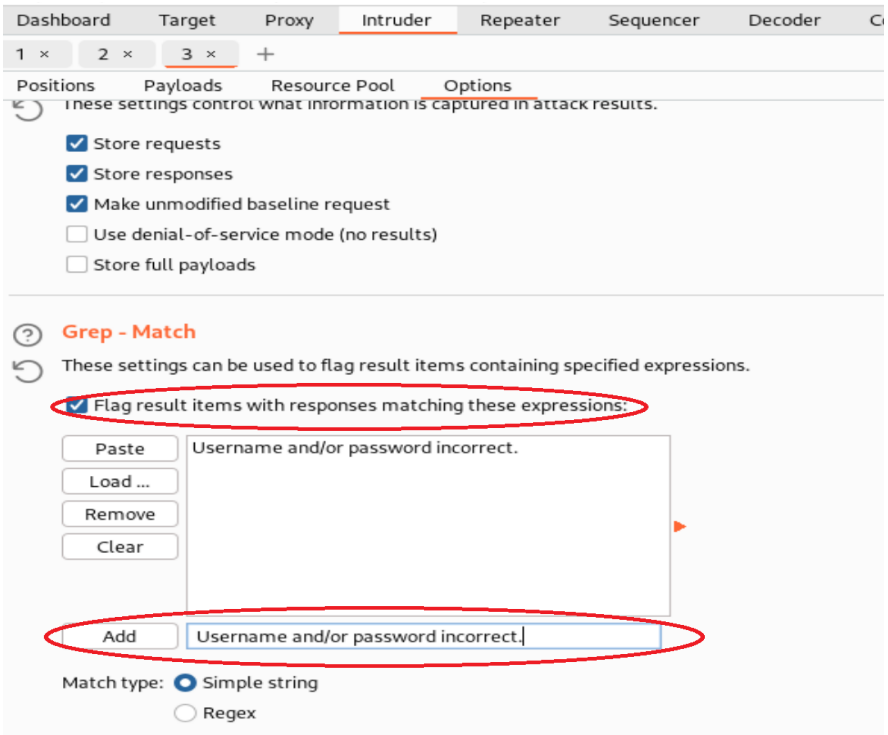
Una volta ottenuta tale richiesta possiamo smettere di intercettare il traffico dati e mandare la richiesta all'intruder utilizzando il tasto *Action*.



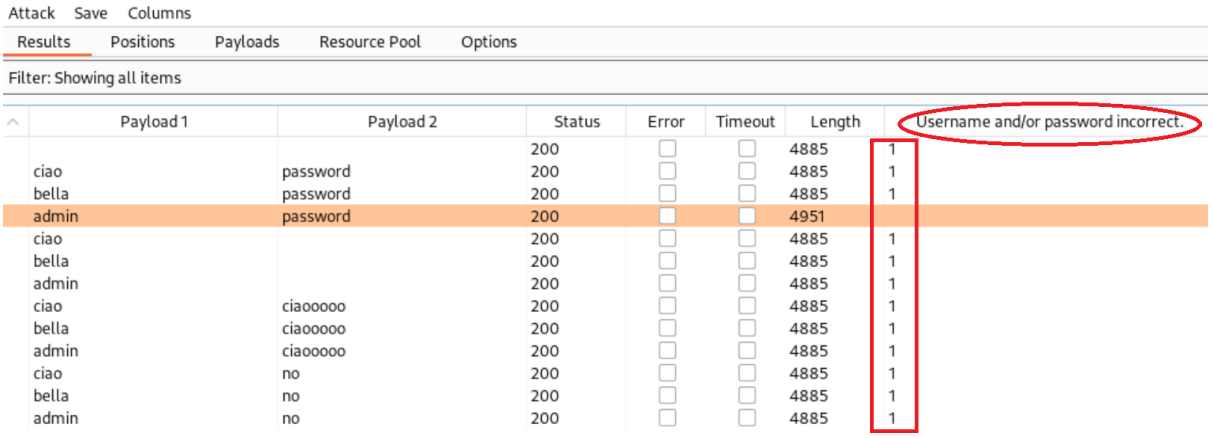
Vediamo che la richiesta è stata copiata all'interno della schermata di selezione dei payload. Scegliamo *cluster bomb* come tipo di attacco (così che il programma provi tutte le combinazioni di user e password delle liste che gli forniremo). Ora il programma ha gia selezionato tutti i parametri che è possibile variare come payloads, utilizziamo *clear* per pulire tutto, e selezioniamo i campi successi a username e password (ovvero dove Burpsuite inserirà i valori delle liste per effettuare il brute force) utilizzando *Add.* In soldoni basta selezionare come payloads le credenziali errate che abbiamo inserito all'inizio.
ATTENZIONE: ricordiamoci l'ordine con cui abbiamo aggiunto tali parametri, ci servirà nel prossimo step.



Ora spostiamoci nella sezione payloads dell'intruder.
Personalmente ho aggiunto come primo payload lo username.
Quindi con *payload set 1* vado a completare la lista sottostante con i possibili username che voglio che il programma utilizzi. Si può importare una lista utilizzando *load* o aggiungere singoli valori con *Add.* Ora ripetiamo tale operazione con *payload set 2* e andiamo a riempire la lista con le possibili password che vogliamo provare.



Come ultimo step, dobbiamo configurare un parametro che ci serve per sapere se il login è andato a buon fine o no con certezza. Utilizziamo il messaggio di errore che ci viene fornito quando sbagliamo il login ovvero *"Username and/or password incorrect."*. Nella sezione *Options- grep match* aggiungiamo manualmente la frase di login errati. Sembra paradossale andare a indagare sui login che non sono riusciti, ma ci basterà vedere quali risultati **non** contengono tale frase per garantire che il login sia andato a buon fine. Ora possiamo avviare l'attacco (in alto a destra).



Payload 1	Payload 2	Status	Error	Timeout	Length	Username and/or password incorrect.
		200	☐	☐	4885	1
ciao	password	200	☐	☐	4885	1
bella	password	200	☐	☐	4885	1
admin	password	200	☐	☐	4951	
ciao		200	☐	☐	4885	1
bella		200	☐	☐	4885	1
admin		200	☐	☐	4885	1
ciao	ciaooooo	200	☐	☐	4885	1
bella	ciaooooo	200	☐	☐	4885	1
admin	ciaooooo	200	☐	☐	4885	1
ciao	no	200	☐	☐	4885	1
bella	no	200	☐	☐	4885	1
admin	no	200	☐	☐	4885	1

Otteniamo in risposta tutte le combinazioni provate e se andiamo a analizzare il flag da noi inserito vediamo che l'unica coppia di credenziali che non ha ricevuto la frase di errore è proprio quella delle credenziali corrette.