

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.

AltoroMutual

ONLINE BANKING LOGIN

PERSONAL

SMALL BUSINESS

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Username: user

Password: ••••

Login

Privacy Policy | Security Statement | Server Status Check | BEST API | © 2022 Altoro Mutual, Inc.

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW10>.

Copyright © 2008, 2022, IBM Corporation. All rights reserved.

PERSONAL

SMALL BUSINESS

Online Banking Login

Login Failed: We're sorry, but this username or password was not found in our system. Please try again.

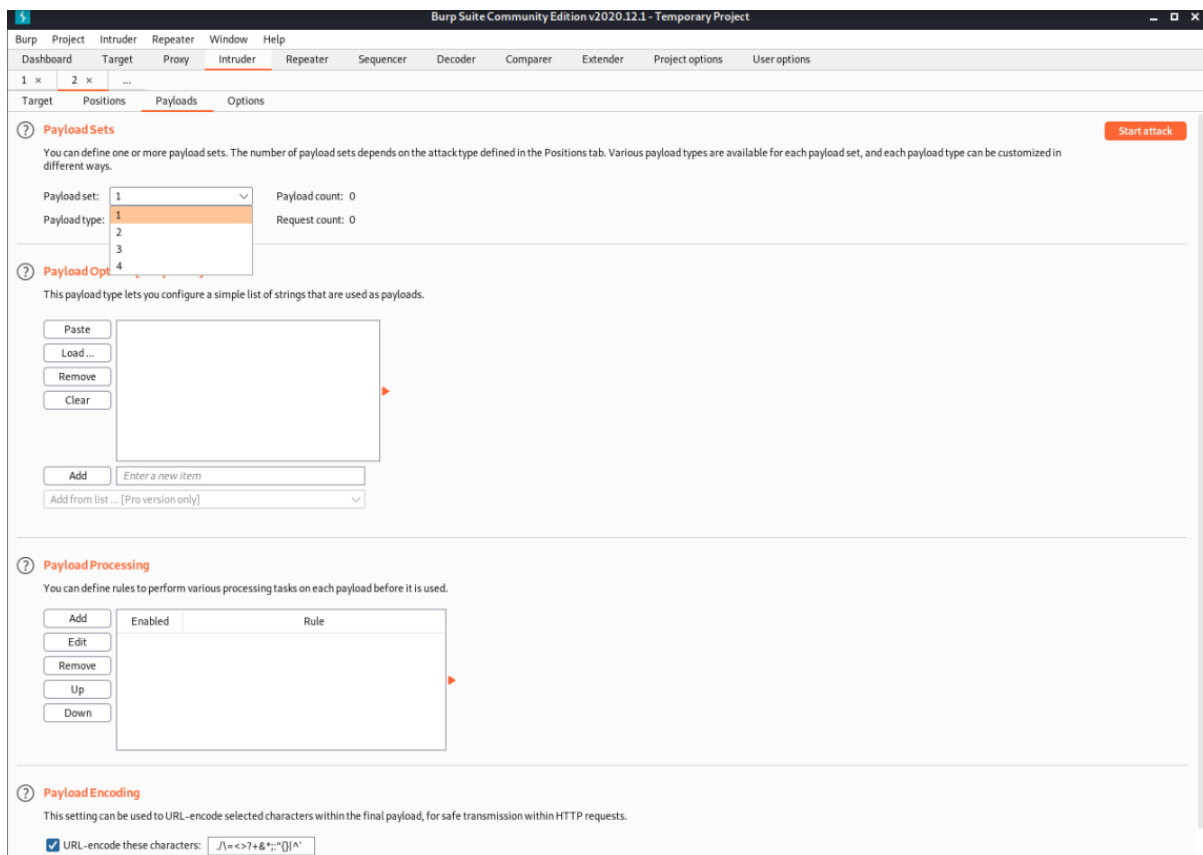
Username:

Password:

This connection is not secure.
Logins entered here could be compromised. [Learn More](#)

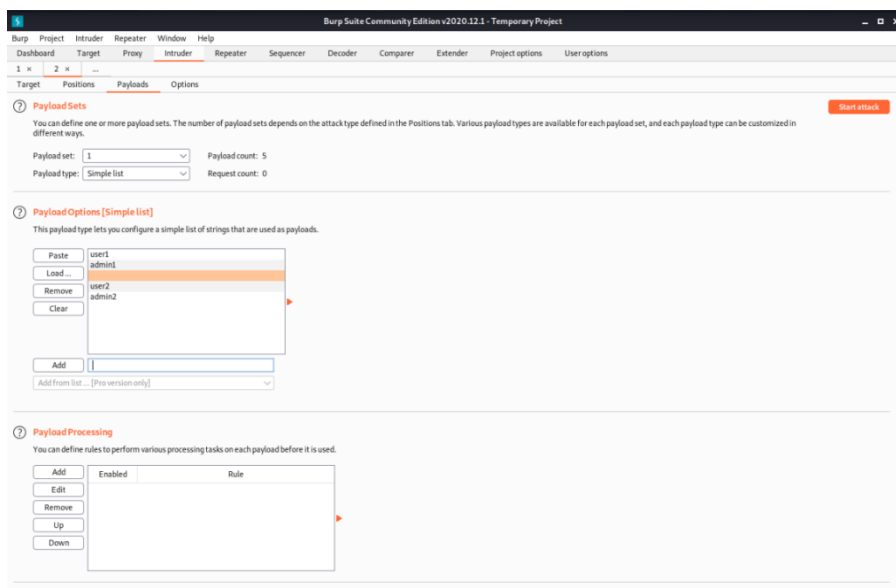
[View Saved Logins](#)

Pitchfork



Cluster Bomb

Payload



For sniper attack

Start attack

1 x2 x...

TargetPositionsPayloadsResource PoolOptions

1 POST /doLogin HTTP/1.1

2 Host: demo.testfire.net

3 Cookie: JSESSIONID=\$05951C0728FF45AA00042CCECD4CE6795

4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

6 Accept-Language: en-US,en;q=0.5

7 Accept-Encoding: gzip, deflate

8 Content-Type: application/x-www-form-urlencoded

9 Content-Length: 43

10 Origin: https://demo.testfire.net

11 Referer: https://demo.testfire.net/login.jsp

12 Upgrade-Insecure-Requests: 1

13 Te: trailers

14 Connection: close

15

16 uid=\$eshandas&passw=\$eshandas&btnSubmit=\$Login\$

Attack type: Sniper

Add \$

Clear \$

Auto \$

Refresh

0 matches

Clear

4 payload positionsLength: 599

AttackSaveColumns

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

Request ^	Position	Payload	Status	Error	Timeout	Length	Comment
-----------	----------	---------	--------	-------	---------	--------	---------

Finished

Burp Suite Community Edition v2021.8.2 - Temporary Project

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
1	http://detectportal.firefox.com	GET	/success.txt?ip=6	✓		200	239	text	txt				34.107.221.82
2	http://detectportal.firefox.com	GET	/success.txt?ip=4	✓		200	239	text	txt				34.107.221.82
3	http://detectportal.firefox.com	GET	/success.txt?ip=4	✓		200	239	text	txt				34.107.221.82
4	http://detectportal.firefox.com	GET	/success.txt?ip=6	✓		200	239	text	txt				34.107.221.82
5	https://demo.testfire.net	GET	/			200	9620	HTML		Altoro Mutual		✓	65.61.137.117 JS
6	https://demo.testfire.net	GET	/			200	9620	HTML		Altoro Mutual		✓	65.61.137.117 JS
8	https://demo.testfire.net	GET	/			200	9537	HTML		Altoro Mutual		✓	65.61.137.117
17	https://demo.testfire.net	GET	/favicon.ico			404	7097	HTML	ico	Altoro Mutual		✓	65.61.137.117
18	https://demo.testfire.net	GET	/			200	9537	HTML		Altoro Mutual		✓	65.61.137.117
27	https://demo.testfire.net	GET	/			200	9537	HTML		Altoro Mutual		✓	65.61.137.117
28	https://demo.testfire.net	GET	/index.jsp			200	9537	HTML	jsp	Altoro Mutual		✓	65.61.137.117
29	https://demo.testfire.net	GET	/login.jsp			200	8687	HTML	jsp	Altoro Mutual		✓	65.61.137.117
30	https://demo.testfire.net	POST	/doLogin	✓		302	145	HTML				✓	65.61.137.117
31	https://demo.testfire.net	GET	/login.jsp			200	8790	HTML	jsp	Altoro Mutual		✓	65.61.137.117

Request

1 POST /doLogin HTTP/1.1
 2 Host: demo.testfire.net
 3 Cookie: JSESSIONID=05951C0728FF45AA00042CCECD4CE679
 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 6 Accept-Language: en-US,en;q=0.5
 7 Accept-Encoding: gzip, deflate
 8 Content-Type: application/x-www-form-urlencoded
 9 Content-Length: 43
 10 Origin: https://demo.testfire.net
 11 Referer: https://demo.testfire.net/login.jsp
 12 Upgrade-Insecure-Requests: 1
 13 Te: trailers
 14 Connection: close
 15
 16 uid=eshandas&passw=eshandas&btnSubmit=Login

Response

1 HTTP/1.1 302 Found
 2 Server: Apache-Coyote/1.1
 3 Location: login.jsp
 4 Content-Length: 0
 5 Date: Thu, 24 Mar 2022 04:40:58 GMT
 6 Connection: close
 7
 8

INSPECTOR

Request Attributes
 Body Parameters (3)
 Request Cookies (1)
 Request Headers (13)
 Response Headers (5)

Demo website 4 attacks and Own website 4 attacks

Battering ram attack

Burp Suite Community Edition v2021.8.2 - Temporary Project

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x ...

Target Positions Payloads Resource Pool Options

Payload Positions

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: Battering ram

1 POST /doLogin HTTP/1.1
 2 Host: demo.testfire.net
 3 Cookie: JSESSIONID=\$05951C0728FF45AA00042CCECD4CE679\$
 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 6 Accept-Language: en-US,en;q=0.5
 7 Accept-Encoding: gzip, deflate
 8 Content-Type: application/x-www-form-urlencoded
 9 Content-Length: 43
 10 Origin: https://demo.testfire.net
 11 Referer: https://demo.testfire.net/login.jsp
 12 Upgrade-Insecure-Requests: 1
 13 Te: trailers
 14 Connection: close
 15
 16 uid=\$eshandas\$&passw=\$eshandas\$&btnSubmit=\$Login\$

Burp Suite Community Edition v2020.12.1 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x ...

Target Positions **Payloads** Options

1 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 type can be customized in different ways.

Payload set: 1 Payload count: 5
Payload type: Simple list Request count: 5

Start attack

2 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]

3 Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Edit Remove Up Down

Enabled Rule

4 Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☒ URL-encode these characters: /!@<>?+&*,;"'[]{}^`

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

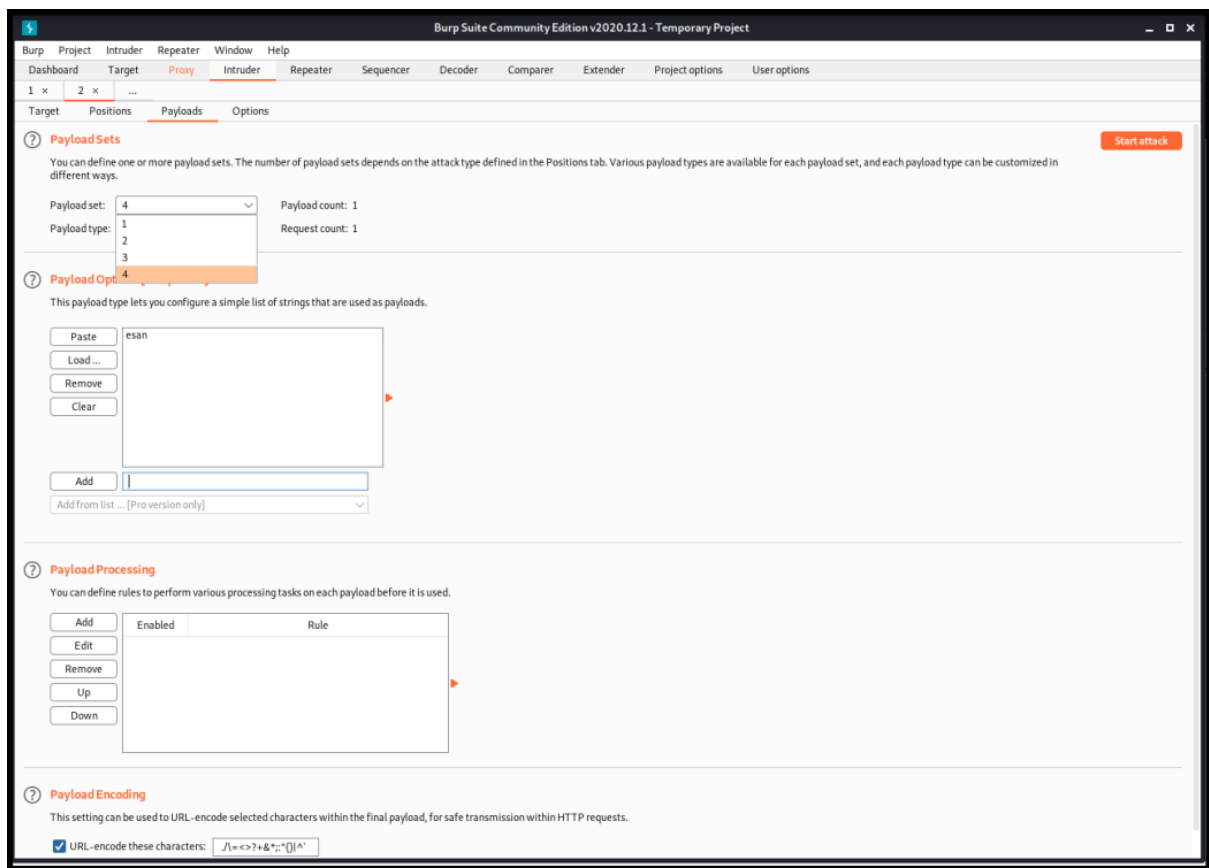
Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Comment

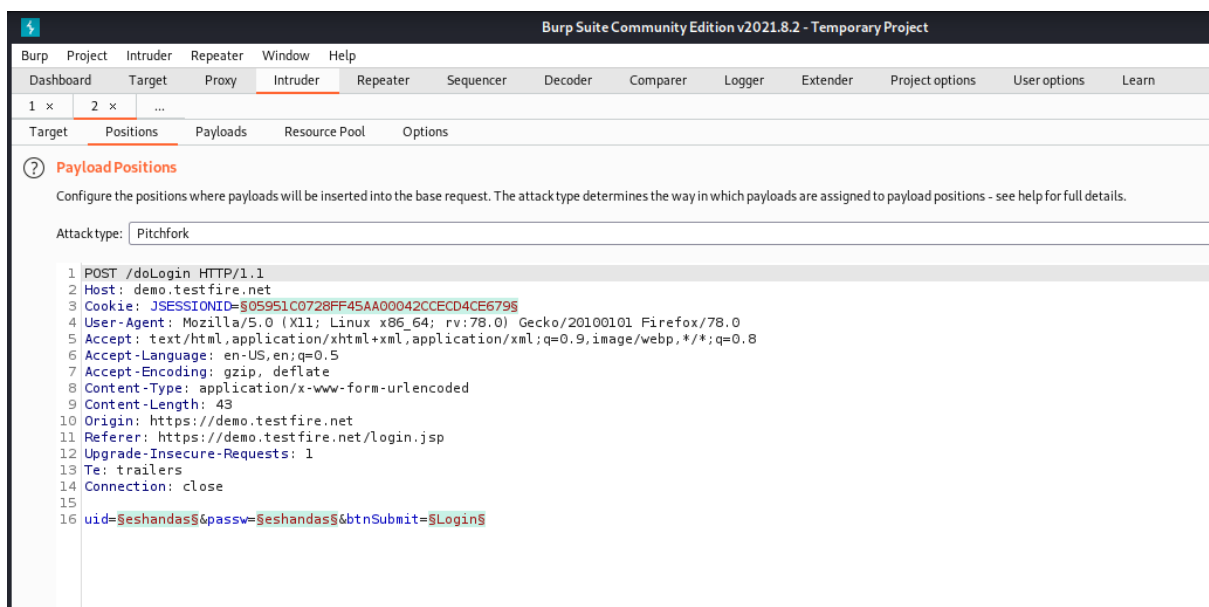
Request Response

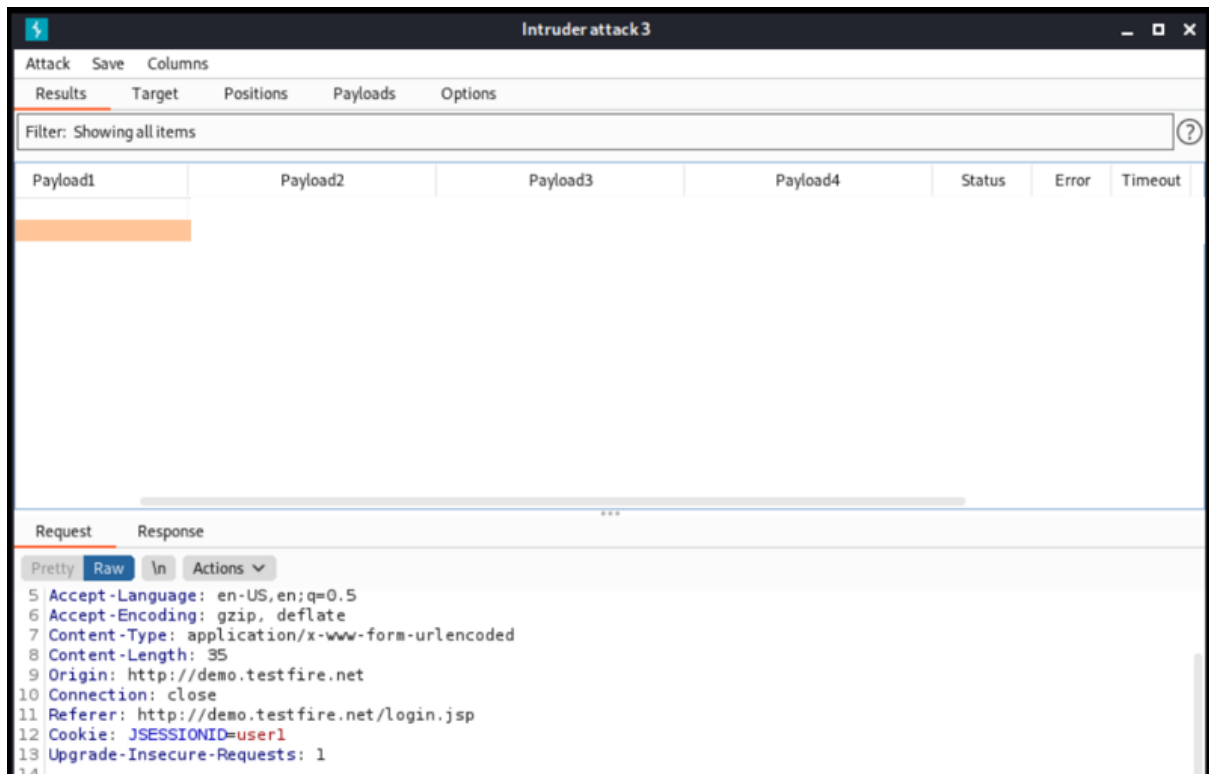
Pretty Raw In Actions

```
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 34
9 Origin: http://demo.testfire.net
10 Connection: close
11 Referer: http://demo.testfire.net/login.jsp
```

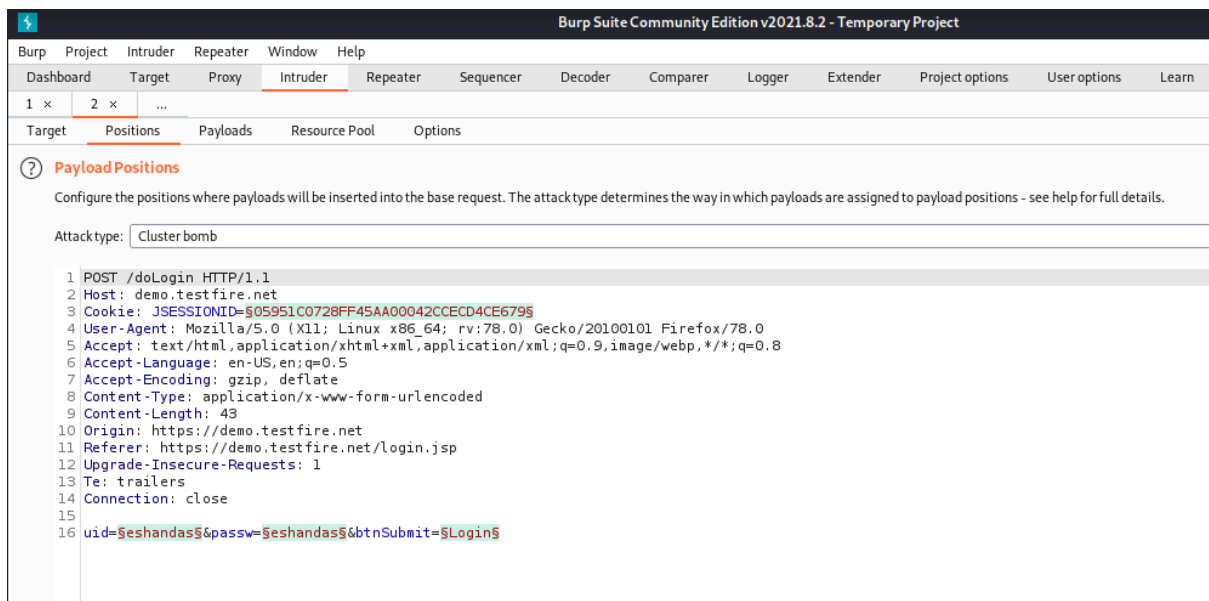


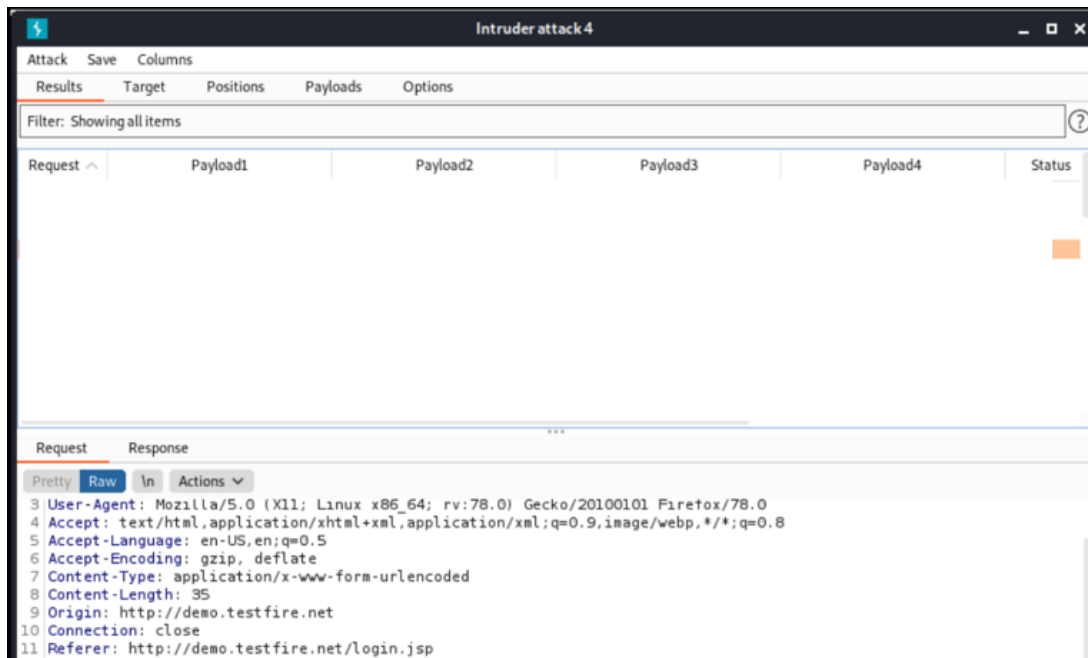
Pitchfork attack ()







Clustering Bomb Attack






OWN website experiments

Login

 **Back**  **Help Me!**

 **Hints and Videos**



Please sign-in


Username

Password

Dont have an account? [Please register here](#)

Login

 **Back**  **Help Me!**

 **Hints and Videos**

Please sign-in

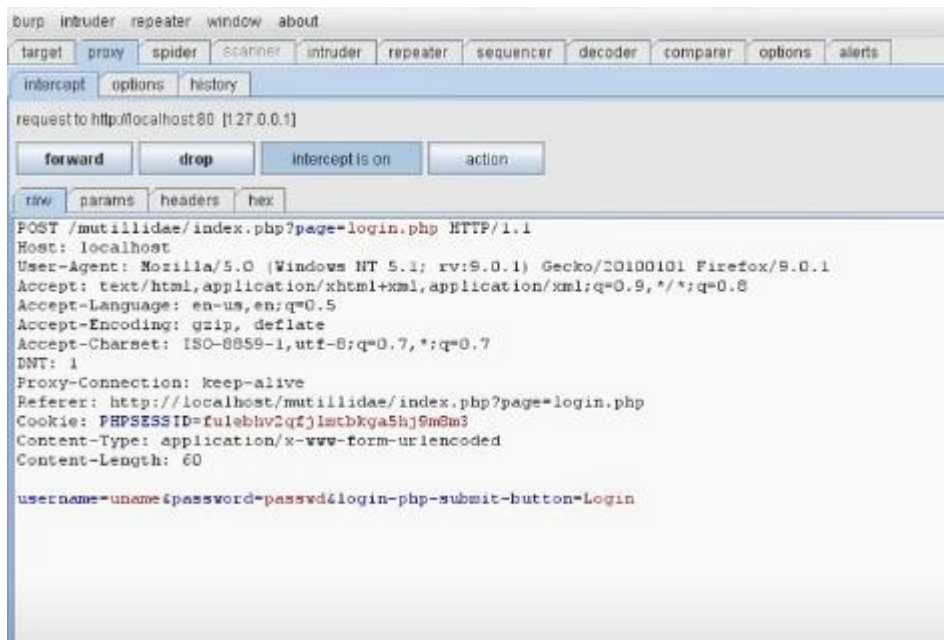
Username

Password

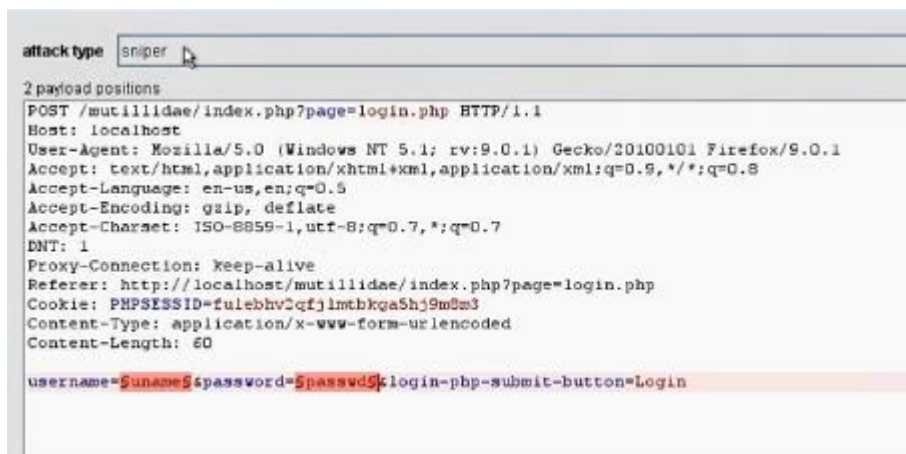
Dont have an account? [Please register here](#)

Username:uname

Password:pass123



Click on 'send to intruder.' And turn intercept off.

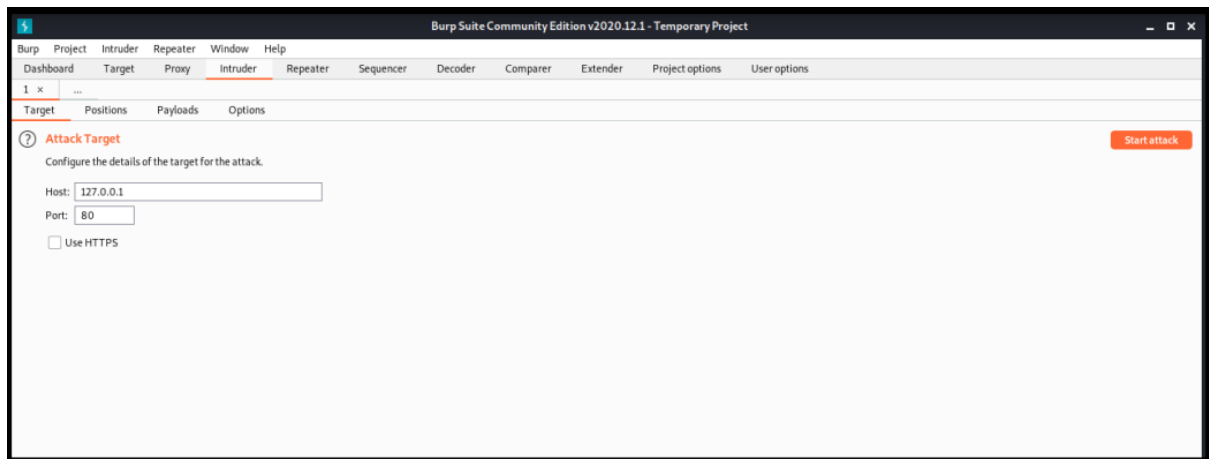


Login the website Quickstore Admin Portal (Self-made website)

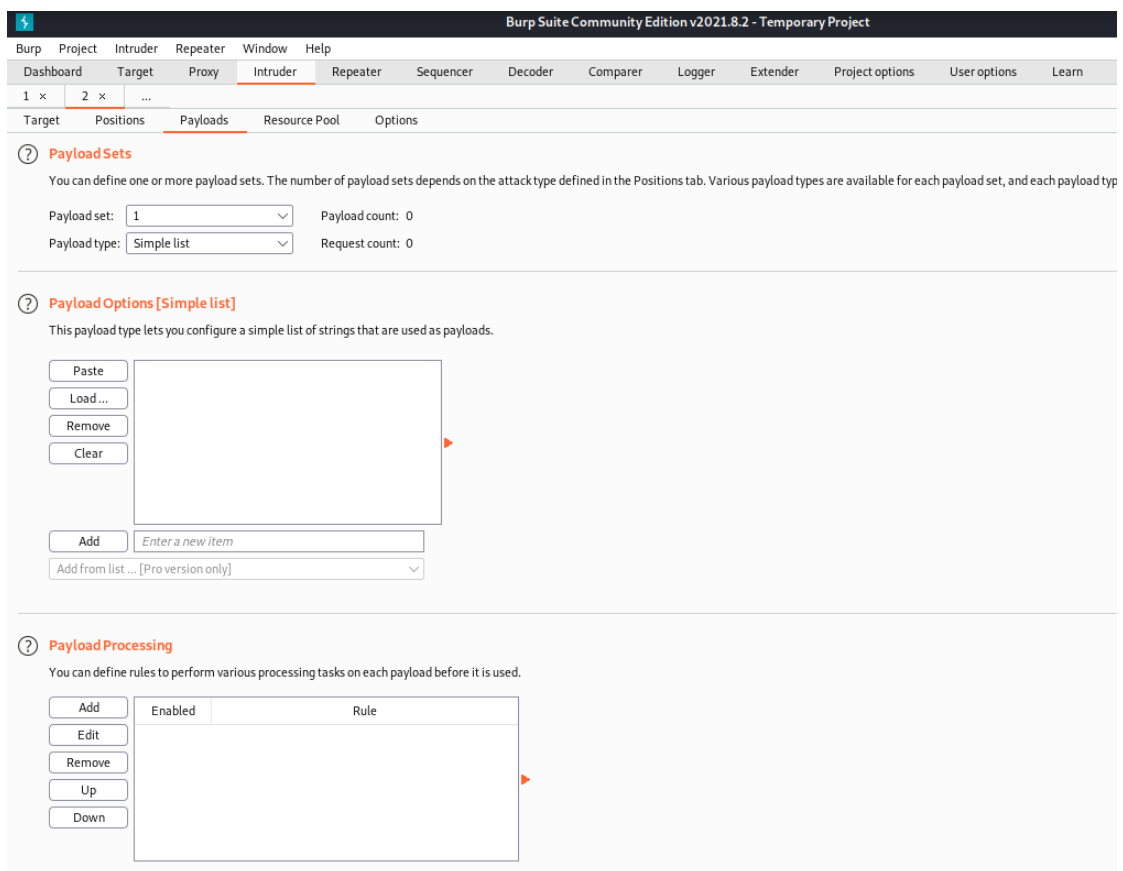
Go to burpsuite then choose Intruder and then select target

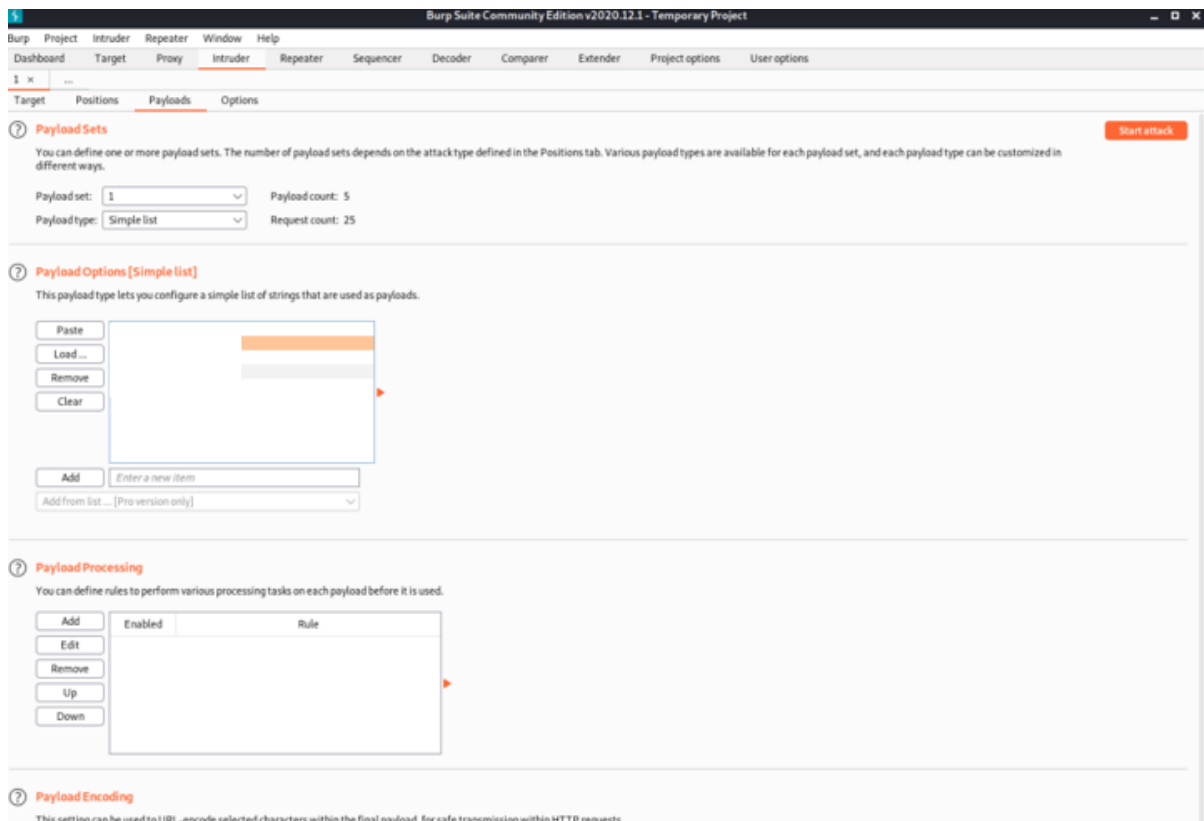
Again set target host as 127.0.0.1

Port :80

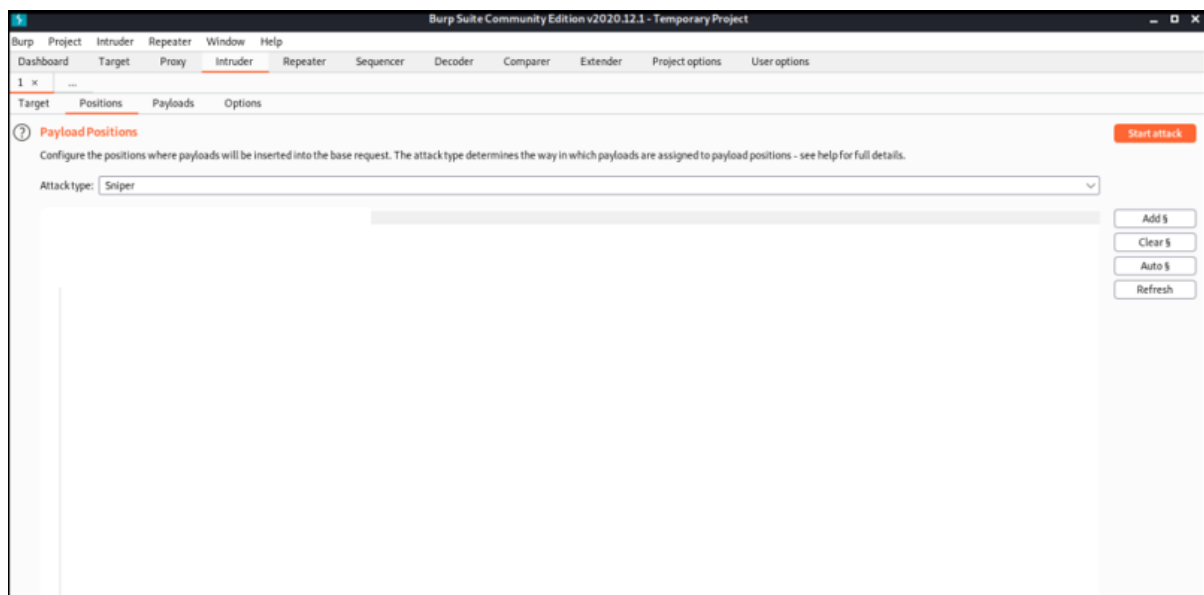


Go to payloads section and payloads as per attack type

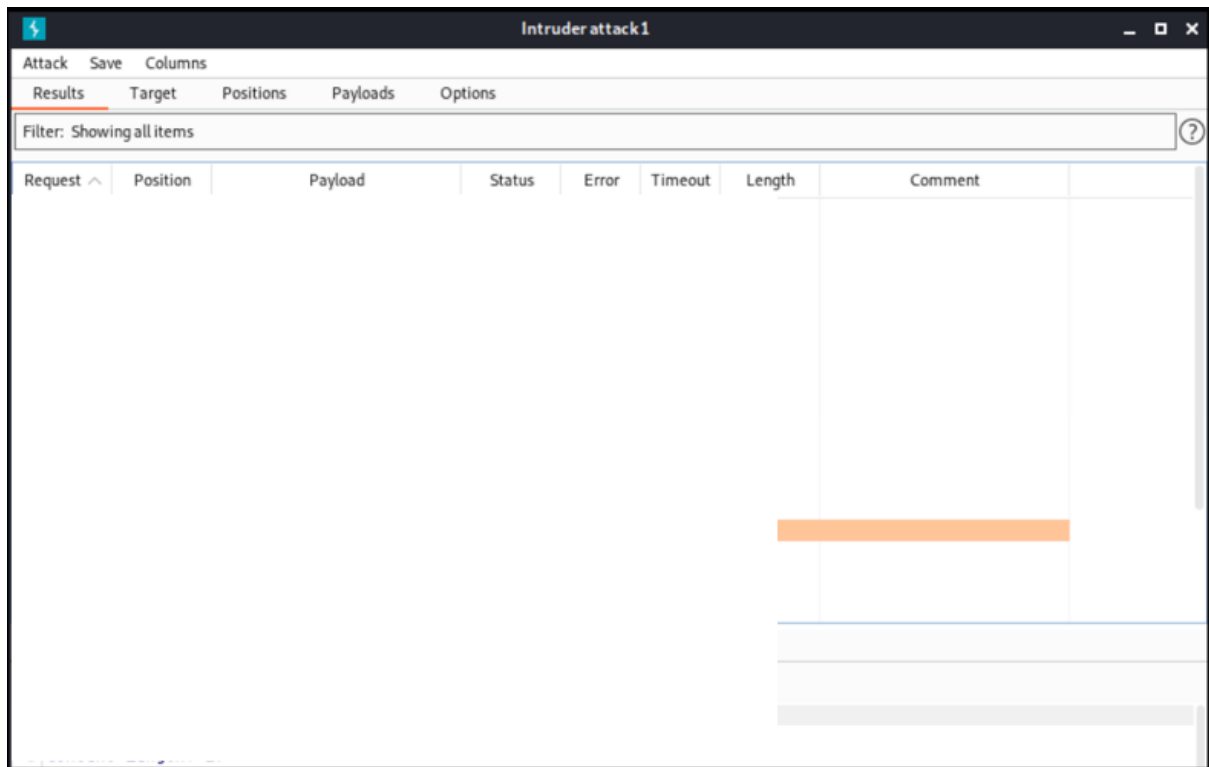




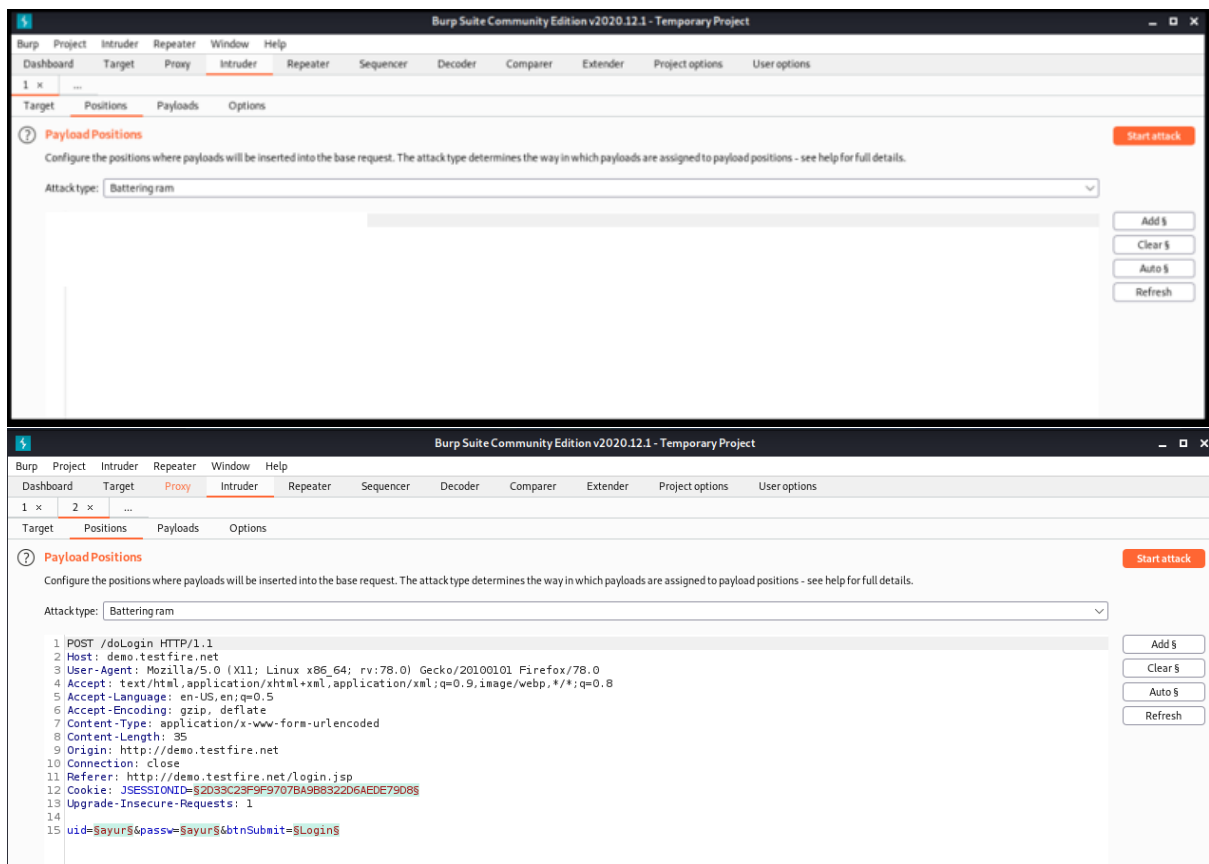
Set attack type: sniper



Start Attack



Battering ram attack



1

Burp Suite Community Edition v2020.12.1 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x ...

Target Positions Payloads Options

1 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 type can be customized in different ways.

Payload set: 1 Payload count: 5

Payload type: Simple list Request count: 5

2 Payload Options [Simple list]

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

Paste user1
Load ... admin1
Remove user2
Clear admin2
ayur

Add Enter a new item

Add from list ... [Pro version only]

3 Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule

Edit

Remove

Up

Down

4 Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☒ URL-encode these characters: [!<>?+&*";'{}|A*]

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Comment
0		302	<input type="checkbox"/>	<input type="checkbox"/>	145	
1	user1	302	<input type="checkbox"/>	<input type="checkbox"/>	220	
2	admin1	302	<input type="checkbox"/>	<input type="checkbox"/>	220	
3	user2	302	<input type="checkbox"/>	<input type="checkbox"/>	220	
4	admin2	302	<input type="checkbox"/>	<input type="checkbox"/>	220	
5	ayur	302	<input type="checkbox"/>	<input type="checkbox"/>	220	

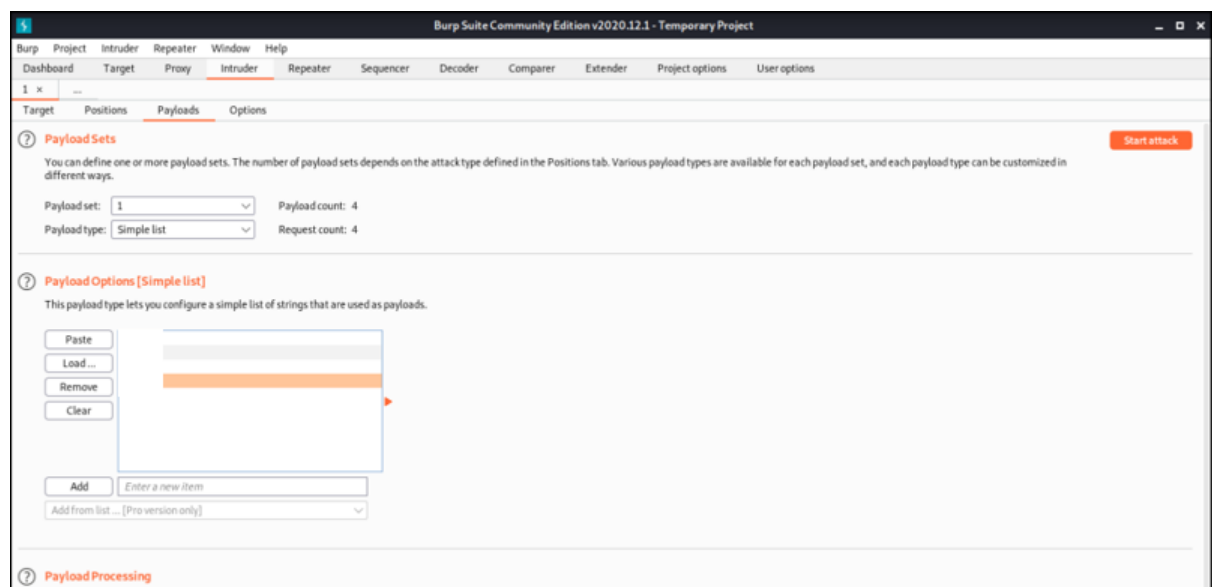
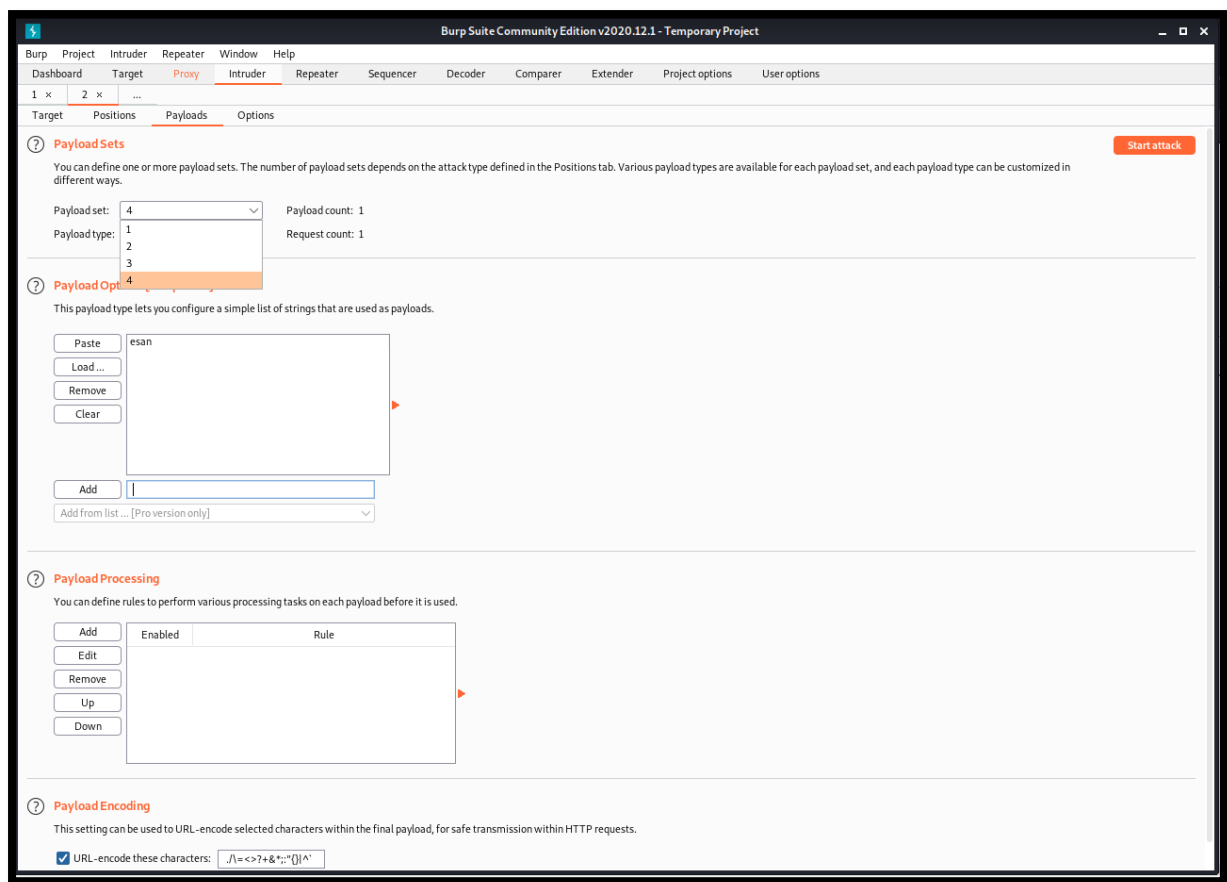
Request Response

Pretty Raw \n Actions

```
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 34
9 Origin: http://demo.testfire.net
10 Connection: close
11 Referer: http://demo.testfire.net/login.jsp
12 Cookie: JSESSIONID=ayur
13 Upgrade-Insecure-Requests: 1
14
15 uid=ayur&passw=ayur&btnSubmit=ayur
```

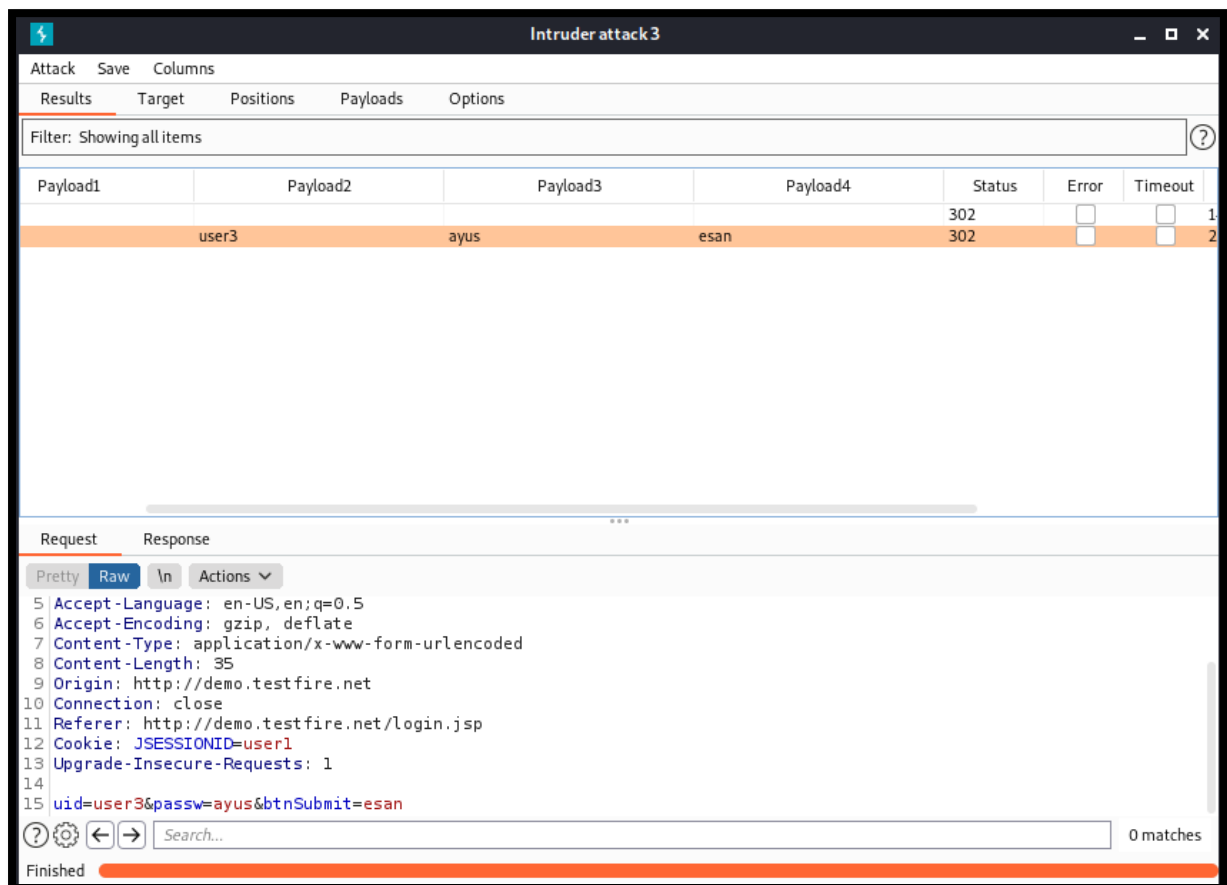
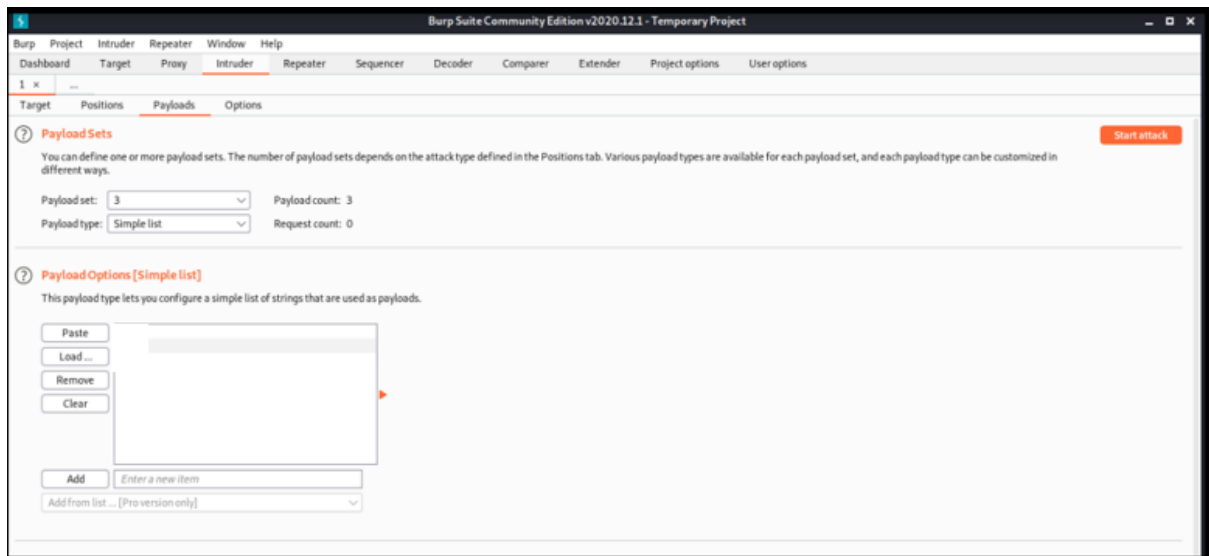
0 matches

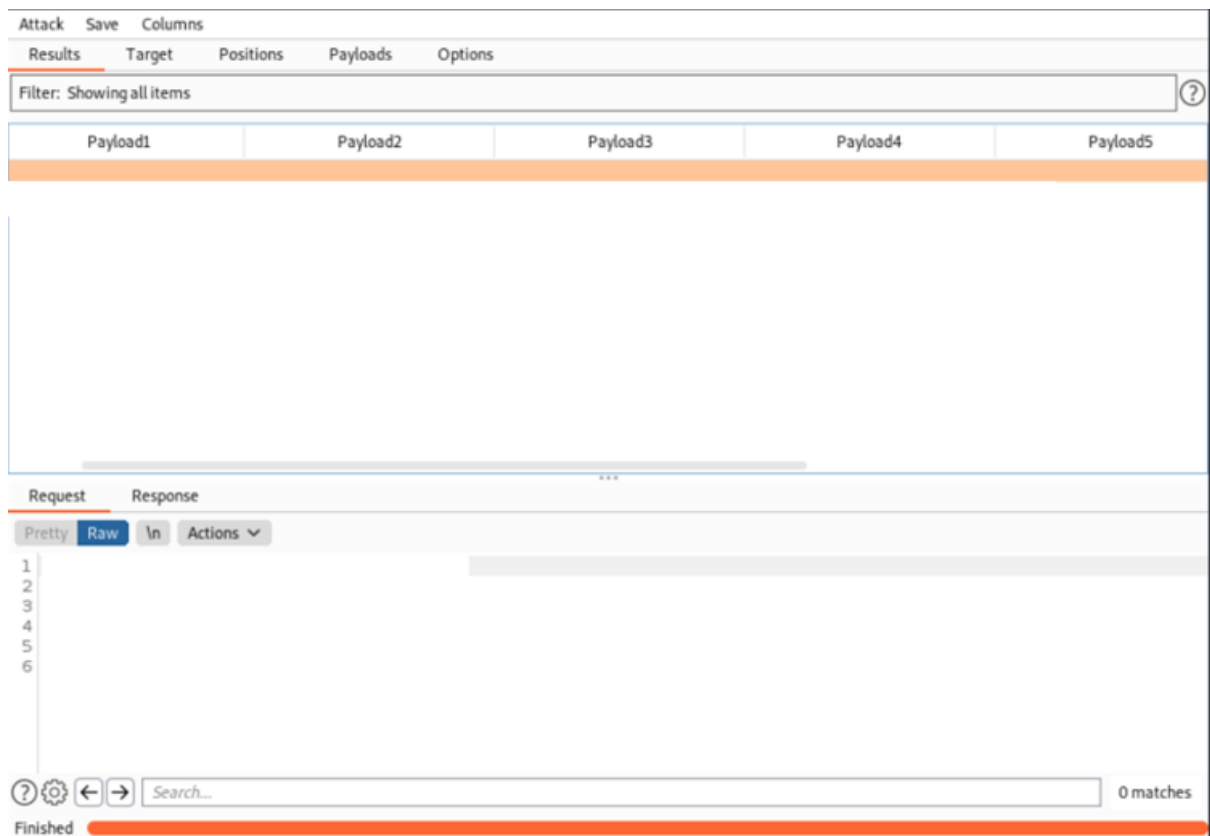
Finished



Pitchfork attack

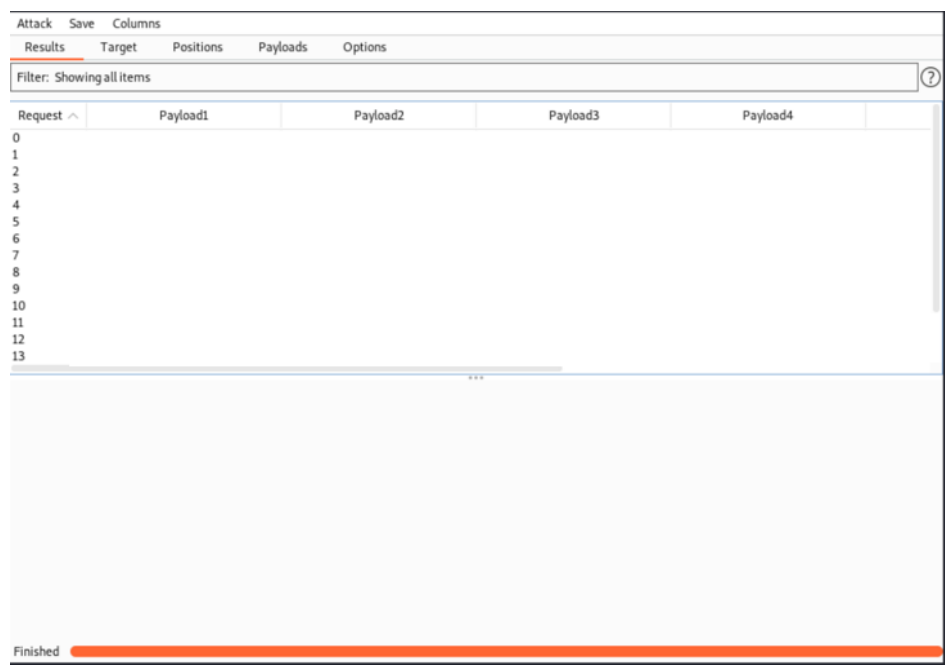
Provide different values for payloads and click on start attack





Clustering Bomb attack

Provide different values for payloads and click on start attack



Intruder attack 4

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request ^	Payload1	Payload2	Payload3	Payload4	Status
0					302
1	user1	user3	ayus	esan	302
2	admin1	user3	ayus	esan	302
3	user2	user3	ayus	esan	302
4	admin2	user3	ayus	esan	302
5	ayur	user3	ayus	esan	302
6	user4	user3	ayus	esan	302
7	user1	user4	ayus	esan	302
8	admin1	user4	ayus	esan	302
9	user2	user4	ayus	esan	302
10	admin2	user4	ayus	esan	302
11	ayur	user4	ayus	esan	302

Request Response

Pretty Raw In Actions

```
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 35
9 Origin: http://demo.testfire.net
10 Connection: close
11 Referer: http://demo.testfire.net/login.jsp
12 Cookie: JSESSIONID=user2
13 Upgrade-Insecure-Requests: 1
14
15 uid=user3&passw=ayus&btnSubmit=esan
```

44 of 192

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