BURP-SUITE

1. Configure Browser and Burp Suite

First, make sure your browser is set up to send its traffic through Burp Suite's proxy. You can verify this by visiting any website with Burp's intercept turned on to see if you capture the traffic.

---

2. Capture the Login Request

This step involves capturing the login attempt to analyze it.

1. In Burp Suite, go to the **Proxy → Intercept** tab and make sure the "Intercept is on" button is active.
2. In your browser, navigate to your WordPress login page: **https://wp.ktucyber.com/wp-login.php**.
3. Enter some incorrect details, like test for the username and test for the password, and click the "Log In" button.
4. Burp Suite will capture this request. It will be a POST request to /wp-login.php and will contain the username and password you entered.

---

3. Send the Request to Intruder

With the request captured in the Intercept tab, right-click anywhere in the request window and select **"Send to Intruder"** from the context menu. This will send the request to the Intruder tool for configuration.

---

4. Configure Intruder Positions

Now you need to tell Intruder which parts of the request to attack.

1. Go to the **Intruder → Positions** tab.
2. Click the **"Clear §"** button on the right to remove any default payload markers.
3. In the request editor, find the line with your login data (it will look something like log=test&pwd=test...).
4. Highlight the value test right after log= and click the **"Add §"** button.
5. Highlight the value test right after pwd= and click the **"Add §"** button. This marks the username and password as the two positions for your payloads.
6. Set the **"Attack type"** dropdown menu to **Cluster Bomb**. This type is used to test different combinations from two separate lists (one for usernames, one for passwords).

---

5. Set the Payloads

Here you will provide the lists of usernames and passwords for Intruder to test.

1. Go to the **Intruder → Payloads** tab.
2. Under **Payload Sets**, ensure **Payload set** is set to **1**. This corresponds to the username (log) field.
3. Under **Payload Options**, choose **"Simple list"**.
4. In the text box below, enter a list of usernames to try. For this test, you could enter:
5. admin
6. user
7. guest
8. Now, change the **Payload set** to **2**. This corresponds to the password (pwd) field.
9. In the same text box, enter a list of passwords to try. Include the correct one to ensure a successful result:
10. password
11. 123456
12. pranavkd

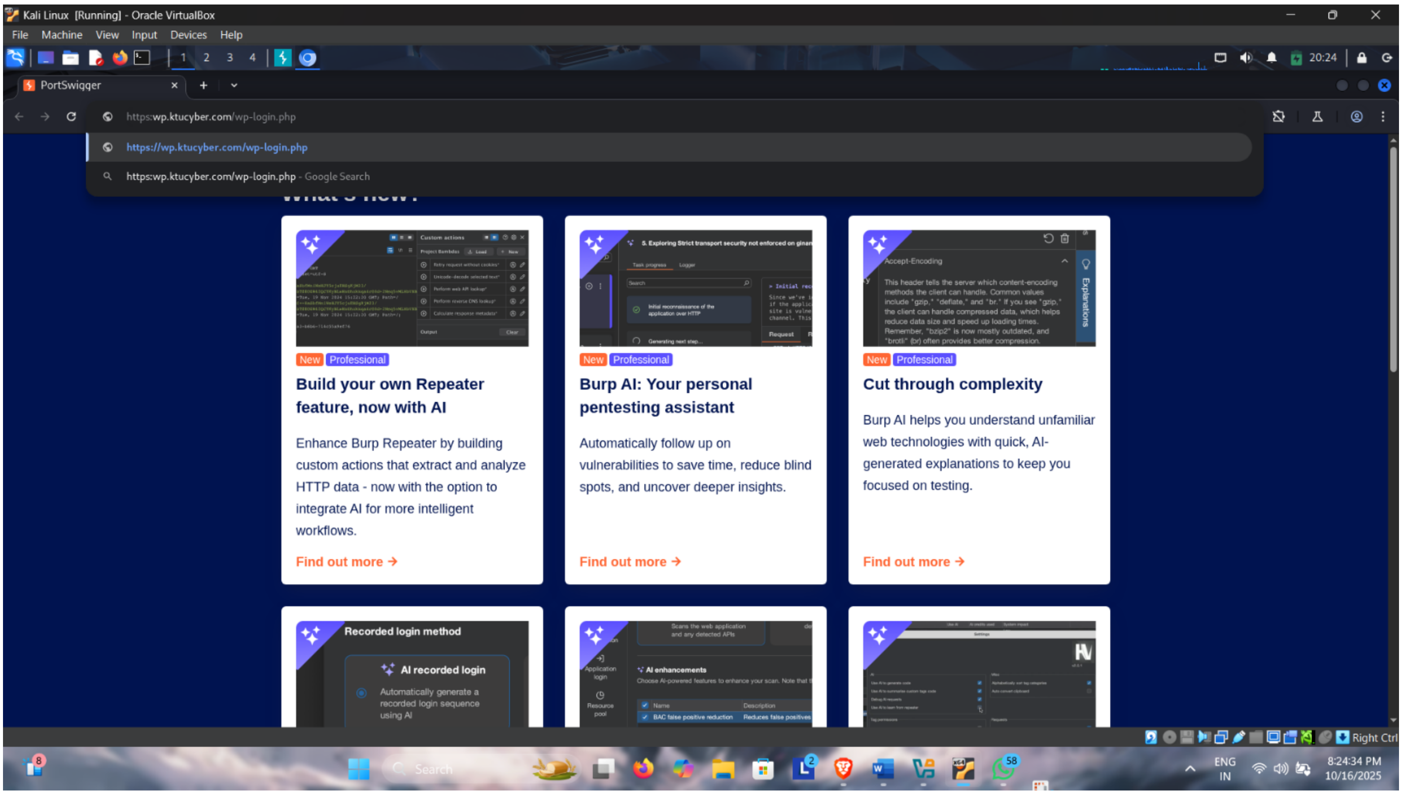
---

6. Start and Analyze the Attack

You are now ready to launch the attack and review the results.

1. Click the **"Start attack"** button in the top right corner. A new "Intruder attack" window will appear.
2. In the attack window, Intruder will test every combination of username and password.
3. To find the successful login, **click on the "Length" column header to sort the results**. A successful login to WordPress typically results in a redirect, which will have a significantly different response length than all the failed attempts. You can also sort by the "Status" column and look for a 302 Found response, which indicates a successful redirect after login.
4. The request that shows this different length or status is the one with the correct credentials: admin and pranavkd.

This procedure allows you to methodically test multiple login combinations to discover valid credentials, which is a fundamental technique in web application security testing.



Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
20:24
PortSwigger
https:wp.ktucyber.com/wp-login.php
https://wp.ktucyber.com/wp-login.php
https:wp.ktucyber.com/wp-login.php - Google Search
8:24:34 PM
10/16/2025

New Professional

Build your own Repeater feature, now with AI

Enhance Burp Repeater by building custom actions that extract and analyze HTTP data - now with the option to integrate AI for more intelligent workflows.

Find out more →

New Professional

Burp AI: Your personal pentesting assistant

Automatically follow up on vulnerabilities to save time, reduce blind spots, and uncover deeper insights.

Find out more →

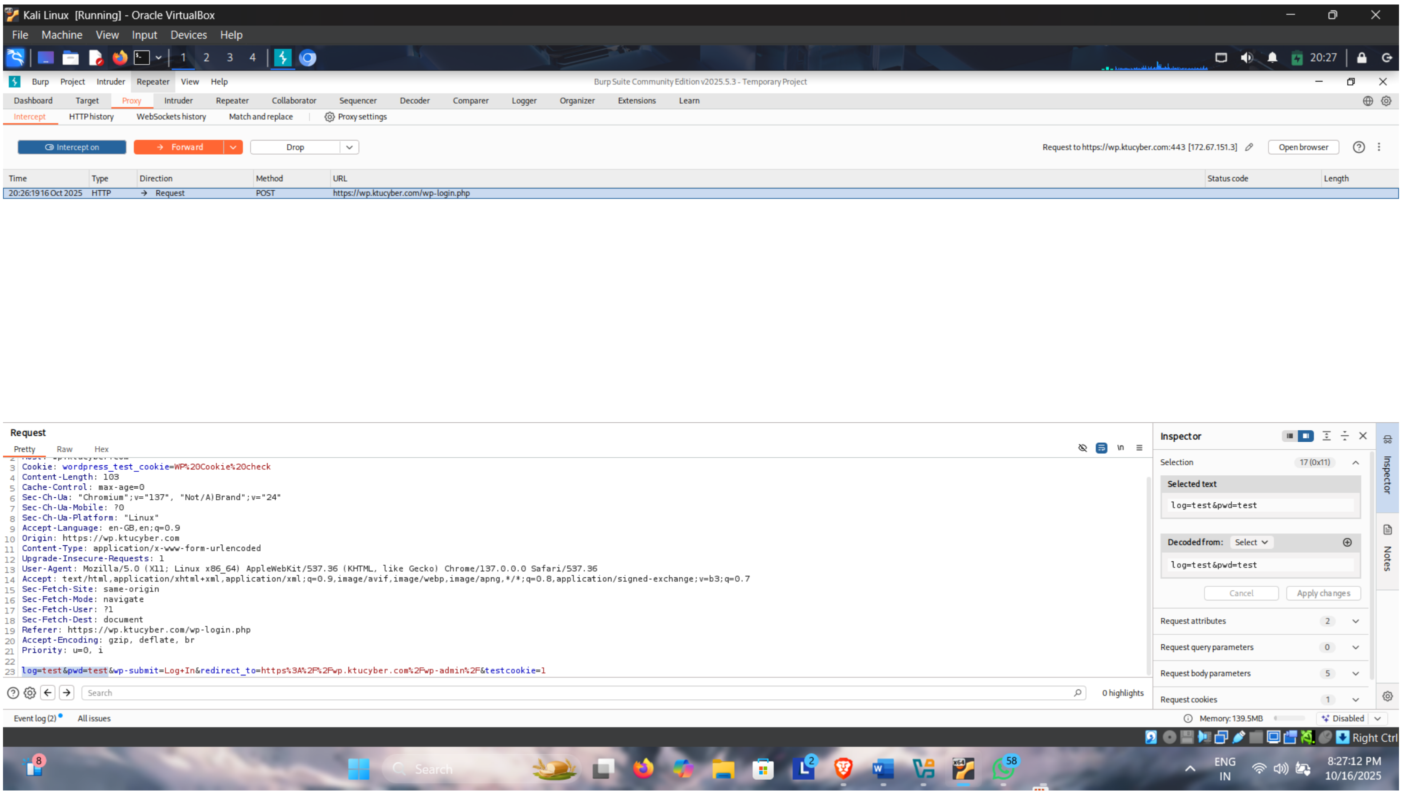
New Professional

Cut through complexity

Burp AI helps you understand unfamiliar web technologies with quick, AI-generated explanations to keep you focused on testing.

Find out more →

Recorded login method
AI recorded login
Automatically generate a recorded login sequence using AI
AI enhancements



Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
20:27
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to https://wp.ktucyber.com:443 [172.67.151.3]
Open browser
Request
Pretty Raw Hex
Search
0 highlights
Event log (2) All issues
Inspector
Selection 17 (0x11)
Selected text
Decoded from: Select
Cancel Apply changes
Request attributes 2
Request query parameters 0
Request body parameters 5
Request cookies 1
Memory: 139.5MB
Disabled
8:27:12 PM
10/16/2025

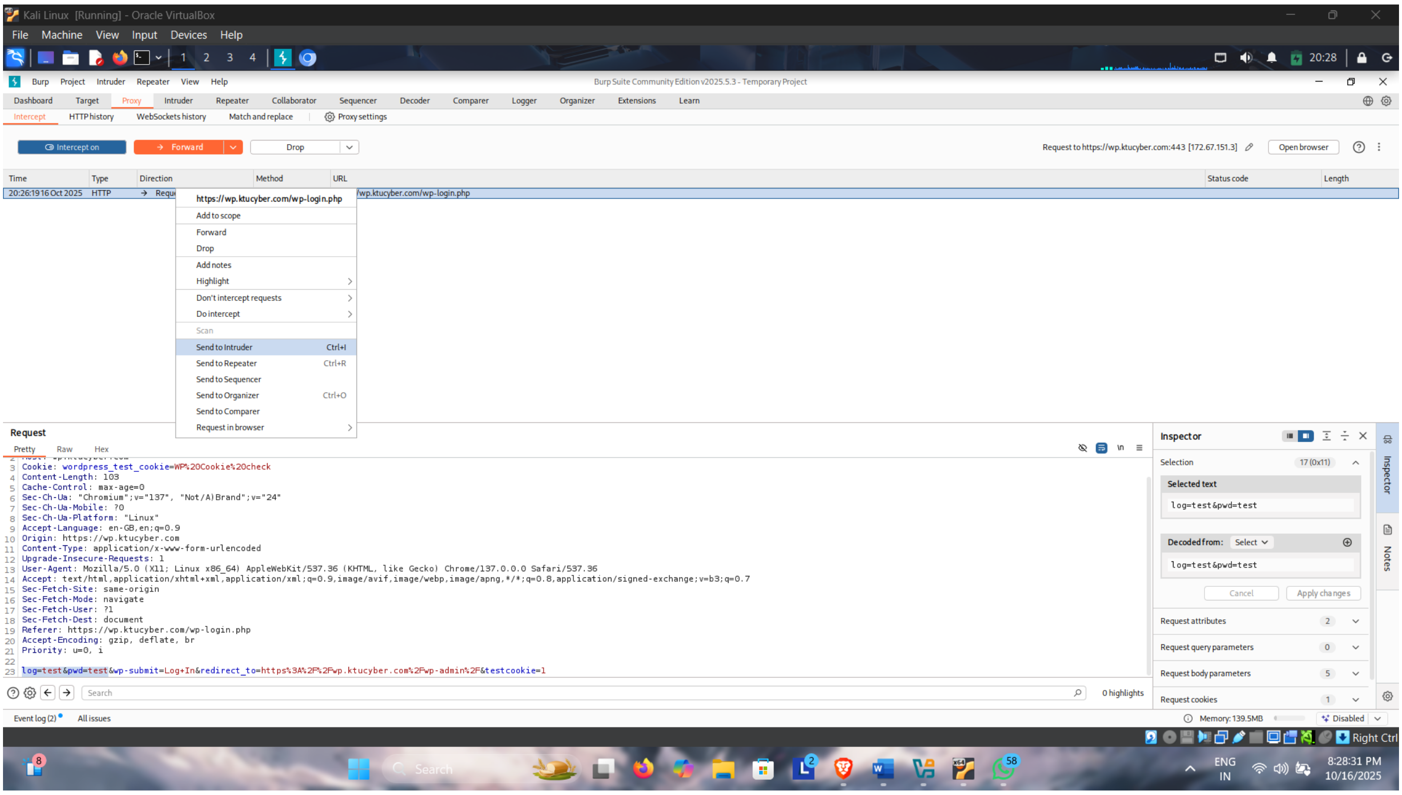
Time	Type	Direction	Method	URL	Status code	Length
20:26:19 16 Oct 2025	HTTP	→ Request	POST	https://wp.ktucyber.com/wp-login.php		

```
Cookie: wordpress_test_cookie=WP%20Cookie%20check
Content-Length: 103
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="137", "Not/A)Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-GB,en;q=0.9
Origin: https://wp.ktucyber.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://wp.ktucyber.com/wp-login.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

log=test&pwd=test&wp-submit=Log+In&redirect_to=https%3A%2F%2Fwp.ktucyber.com%2Fwp-admin%2F&testcookie=1
```

Selected text: log=test&pwd=test

log=test&pwd=test


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to https://wp.ktucyber.com:443 [172.67.151.3]
Open browser
https://wp.ktucyber.com/wp-login.php
Add to scope
Forward
Drop
Add notes
Highlight
Don't intercept requests
Do intercept
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Organizer Ctrl+O
Send to Comparer
Request in browser
Request
Pretty Raw Hex
Search
0 highlights
Event log (2)
All issues
Memory: 139.5MB
Disabled
Right Ctrl
20:28
ENG IN
8:28:31 PM
10/16/2025

Time	Type	Direction	Method	URL	Status code	Length
20:26:19 16 Oct 2025	HTTP	→ Requ		/wp.ktucyber.com/wp-login.php		

```
Cookie: wordpress_test_cookie=WP%20Cookie%20check
Content-Length: 103
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="137", "Not/A)Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-GB,en;q=0.9
Origin: https://wp.ktucyber.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://wp.ktucyber.com/wp-login.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

log=test&pwd=test&wp-submit=Log+In&redirect_to=https%3A%2F%2Fwp.ktucyber.com%2Fwp-admin%2F&testcookie=1
```

Inspector

Selection 17 (0x11)

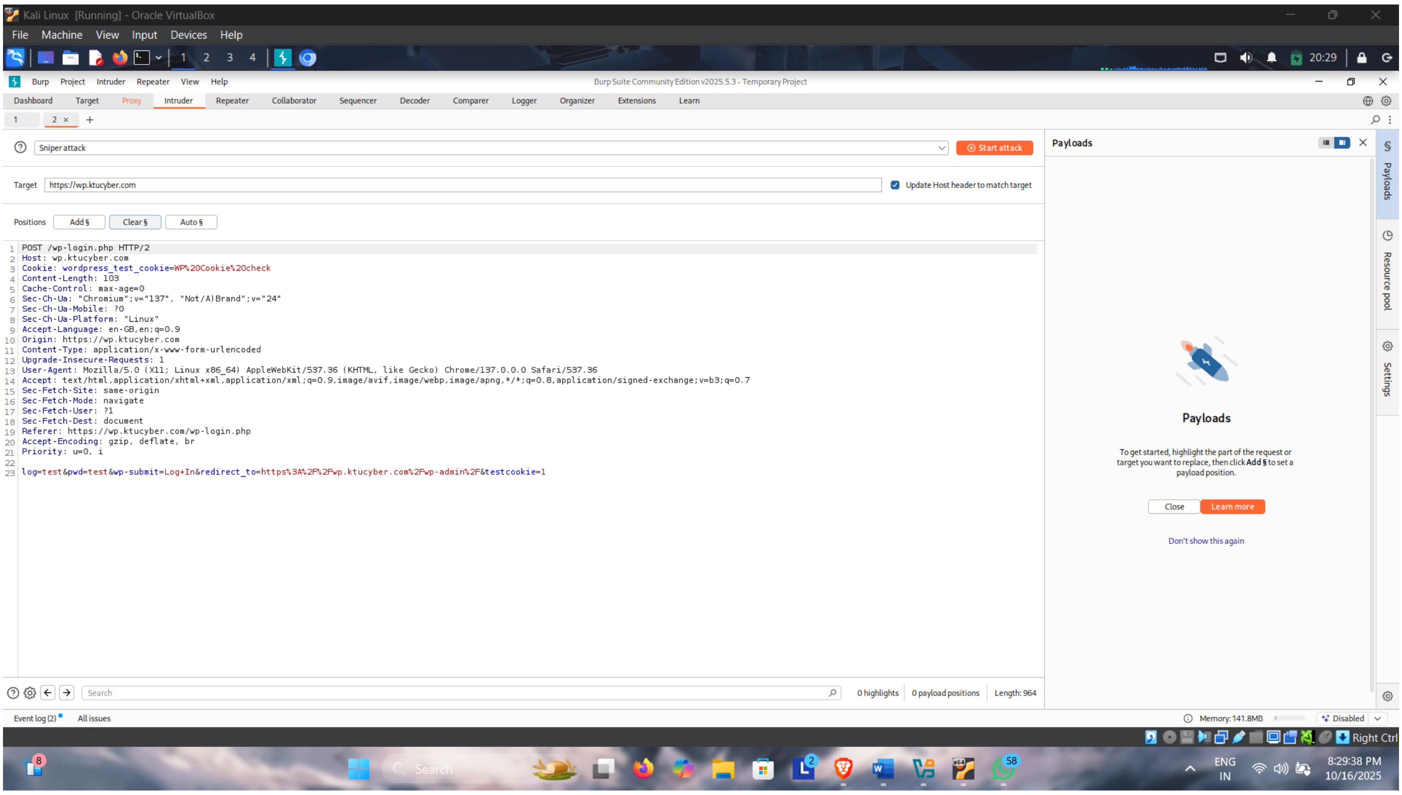
Selected text: log=test&pwd=test

Decoded from: Select

log=test&pwd=test

Cancel Apply changes

Request attributes	2
Request query parameters	0
Request body parameters	5
Request cookies	1


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 2 × +
Start attack
Positions
Add §
Clear §
Auto §
Payloads
Resource pool
Settings
Payloads
Close
Learn more
Don't show this again
Search
Event log (2)
All issues
Memory: 141.8MB
Disabled
Right Ctrl
20:29
ENG IN
8:29:38 PM
10/16/2025

Sniper attack

Target: https://wp.ktucyber.com

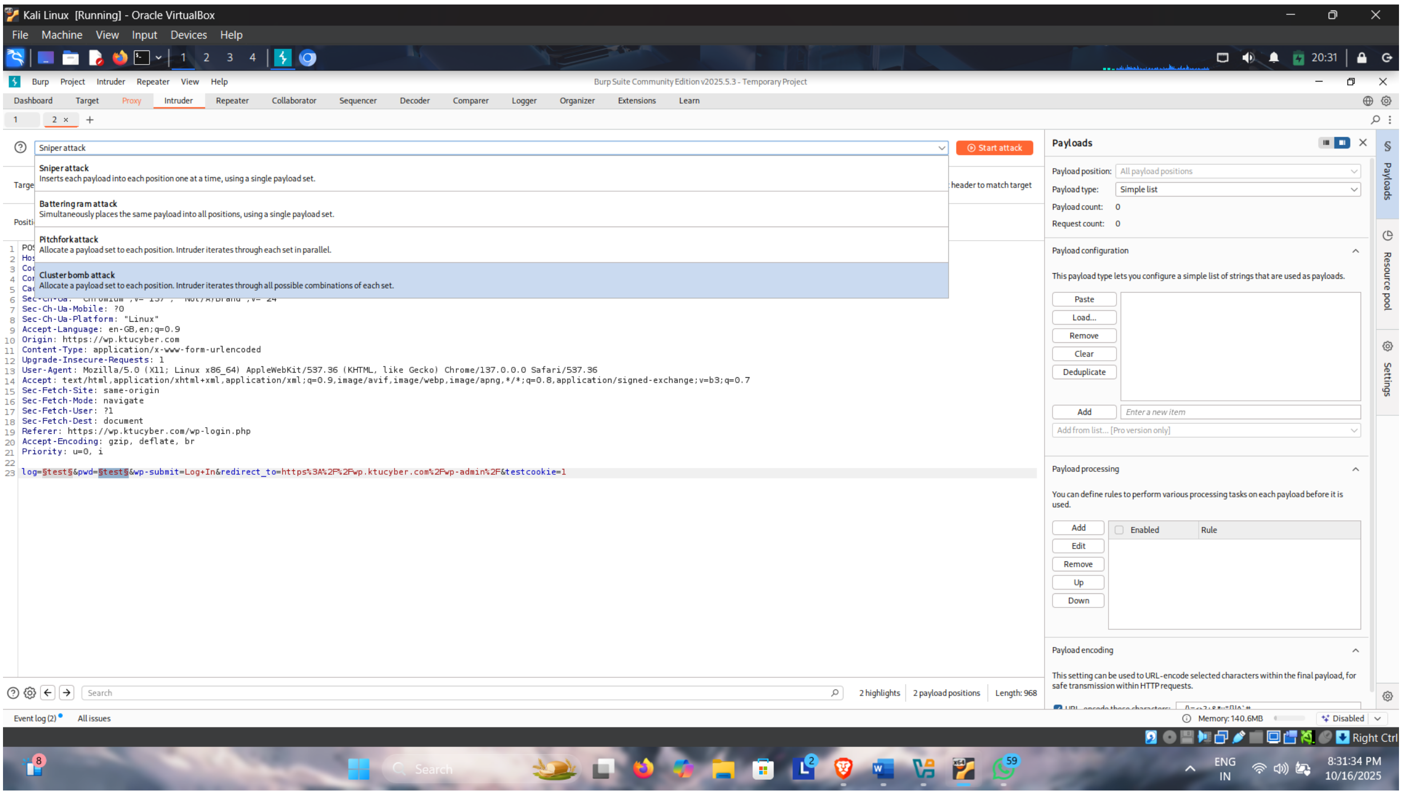
☑ Update Host header to match target

```
POST /wp-login.php HTTP/2
Host: wp.ktucyber.com
Cookie: wordpress_test_cookie=WP%20Cookie%20check
Content-Length: 103
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="137", "Not/A)Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-GB,en;q=0.9
Origin: https://wp.ktucyber.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://wp.ktucyber.com/wp-login.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

log=test&pwd=test&wp-submit=Log+In&redirect_to=https%3A%2F%2Fwp.ktucyber.com%2Fwp-admin%2F&testcookie=1
```

To get started, highlight the part of the request or target you want to replace, then click **Add §** to set a payload position.

0 highlights | 0 payload positions | Length: 964


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Start attack
Payloads
Resource pool
Settings
Event log (2) All issues
20:31
8:31:34 PM
10/16/2025

Sniper attack

Sniper attack
Inserts each payload into each position one at a time, using a single payload set.

Battering ram attack
Simultaneously places the same payload into all positions, using a single payload set.

Pitchfork attack
Allocate a payload set to each position. Intruder iterates through each set in parallel.

Cluster bomb attack
Allocate a payload set to each position. Intruder iterates through all possible combinations of each set.

```
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-GB,en;q=0.9
Origin: https://wp.ktucyber.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://wp.ktucyber.com/wp-login.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

log=§test§&pwd=§test§&wp-submit=Log+In&redirect_to=https%3A%2F%2Fwp.ktucyber.com%2Fwp-admin%2F&testcookie=1
```

2 highlights 2 payload positions Length: 968

Payload position: All payload positions
Payload type: Simple list
Payload count: 0
Request count: 0

Payload configuration

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

Paste Load... Remove Clear Deduplicate Add Enter a new item
Add from list... [Pro version only]

Payload processing

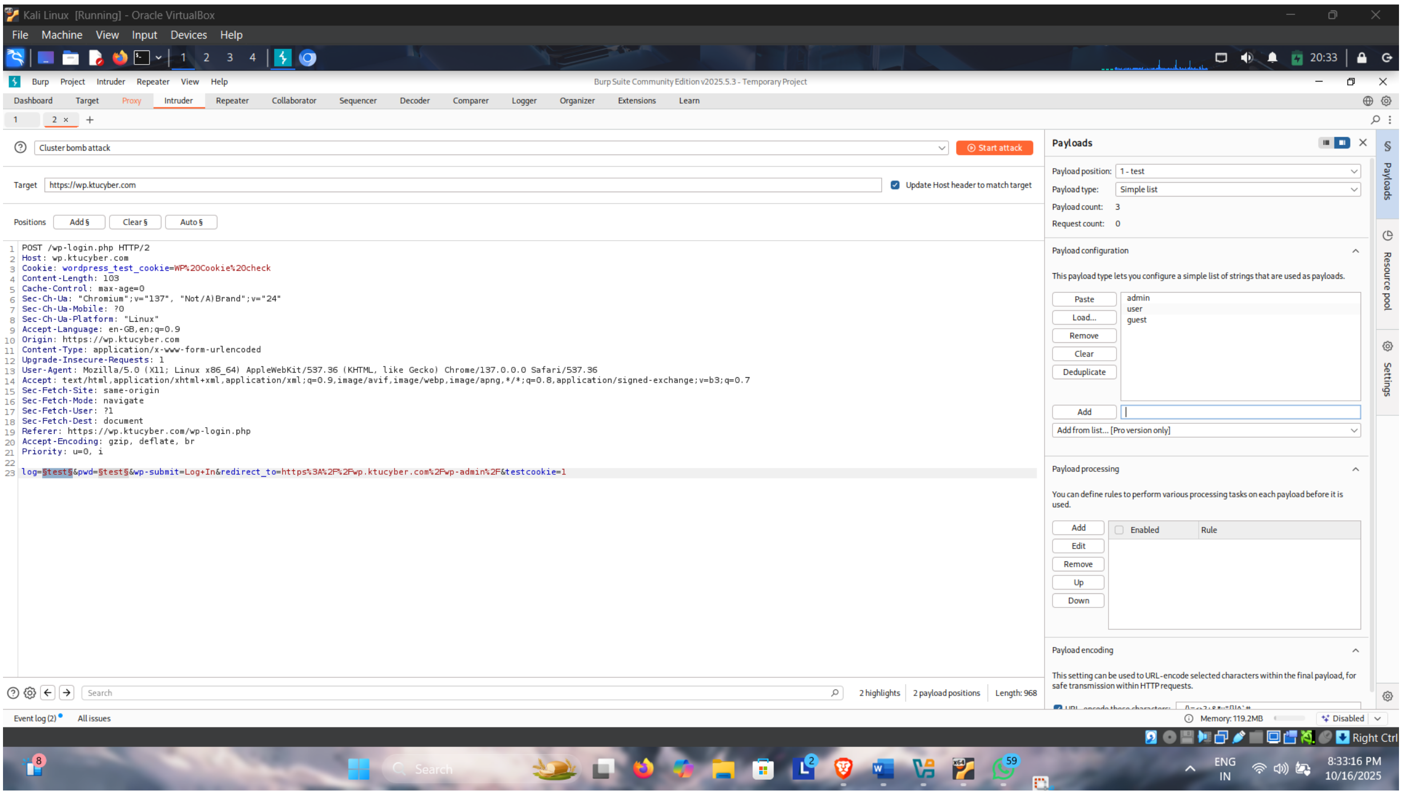
You can define rules to perform various processing tasks on each payload before it is used.

Add Edit Remove Up Down | ☐ Enabled | Rule

Payload encoding

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

Memory: 140.6MB Disabled


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Start attack
Payloads
Resource pool
Settings
Event log (2) All issues
20:33
8:33:16 PM
10/16/2025

Cluster bomb attack

Target https://wp.ktucyber.com ☑ Update Host header to match target

Positions Add § Clear § Auto §

```
POST /wp-login.php HTTP/2
Host: wp.ktucyber.com
Cookie: wordpress_test_cookie=WP%20Cookie%20check
Content-Length: 103
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="137", "Not/A)Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-GB,en;q=0.9
Origin: https://wp.ktucyber.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://wp.ktucyber.com/wp-login.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

log=§test§&pwd=§test§&wp-submit=Log+In&redirect_to=https%3A%2F%2Fwp.ktucyber.com%2Fwp-admin%2F&testcookie=1
```

2 highlights 2 payload positions Length: 968

Payload position: 1 - test
Payload type: Simple list
Payload count: 3
Request count: 0

Payload configuration

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

Paste Load... Remove Clear Deduplicate

```
admin
user
guest
```

Add
Add from list... [Pro version only]

Payload processing

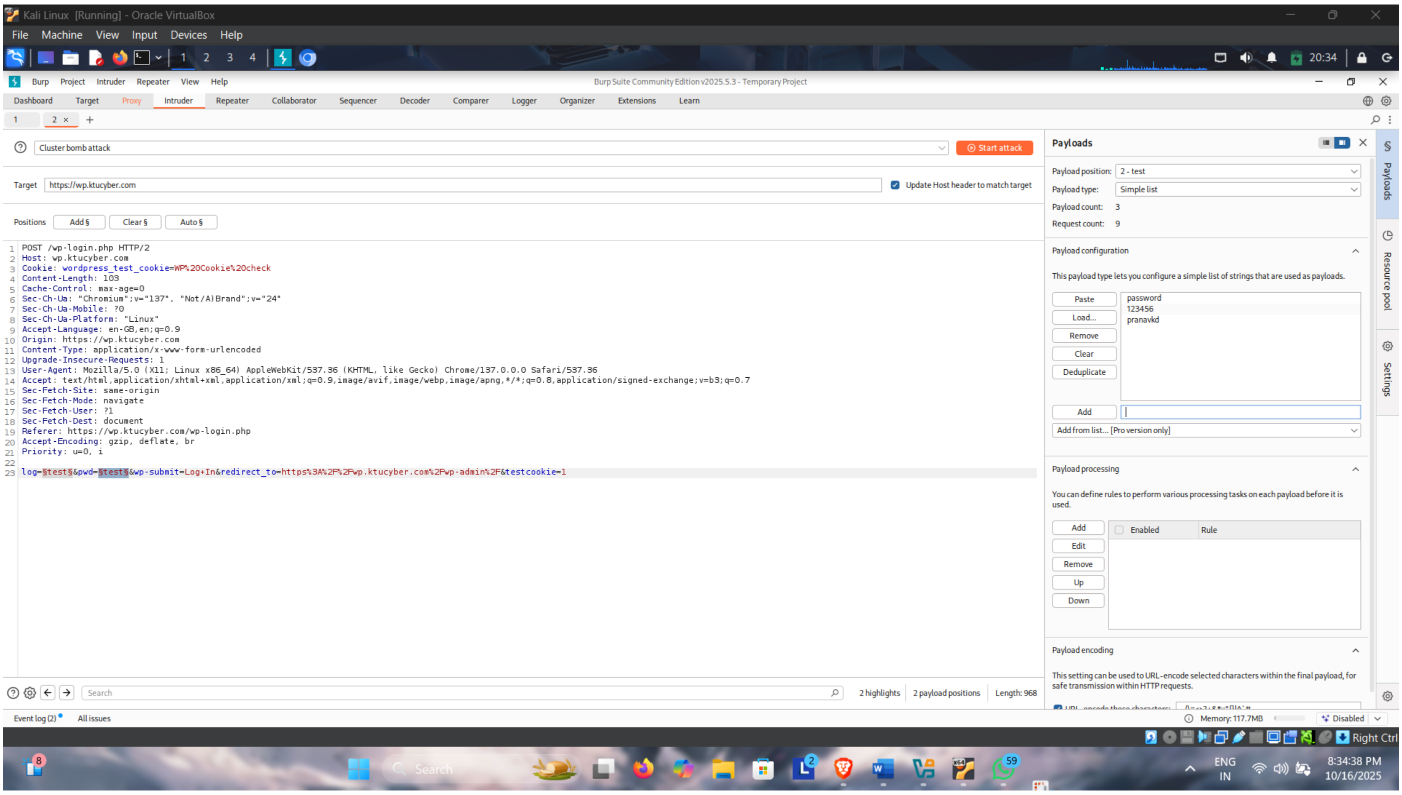
You can define rules to perform various processing tasks on each payload before it is used.

Add Edit Remove Up Down | ☐ Enabled | Rule

Payload encoding

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

Memory: 119.2MB Disabled



Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2025.5.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Start attack
Positions Add § Clear § Auto §

Cluster bomb attack

Target: https://wp.ktucyber.com ☑ Update Host header to match target

```
POST /wp-login.php HTTP/2
Host: wp.ktucyber.com
Cookie: wordpress_test_cookie=WP%20Cookie%20check
Content-Length: 103
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="137", "Not/A)Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-GB,en;q=0.9
Origin: https://wp.ktucyber.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://wp.ktucyber.com/wp-login.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

log=§test§&pwd=§test§&wp-submit=Log+In&redirect_to=https%3A%2F%2Fwp.ktucyber.com%2Fwp-admin%2F&testcookie=1
```

2 highlights 2 payload positions Length: 968

Payloads

Payload position: 2 - test
Payload type: Simple list
Payload count: 3
Request count: 9

Payload configuration

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

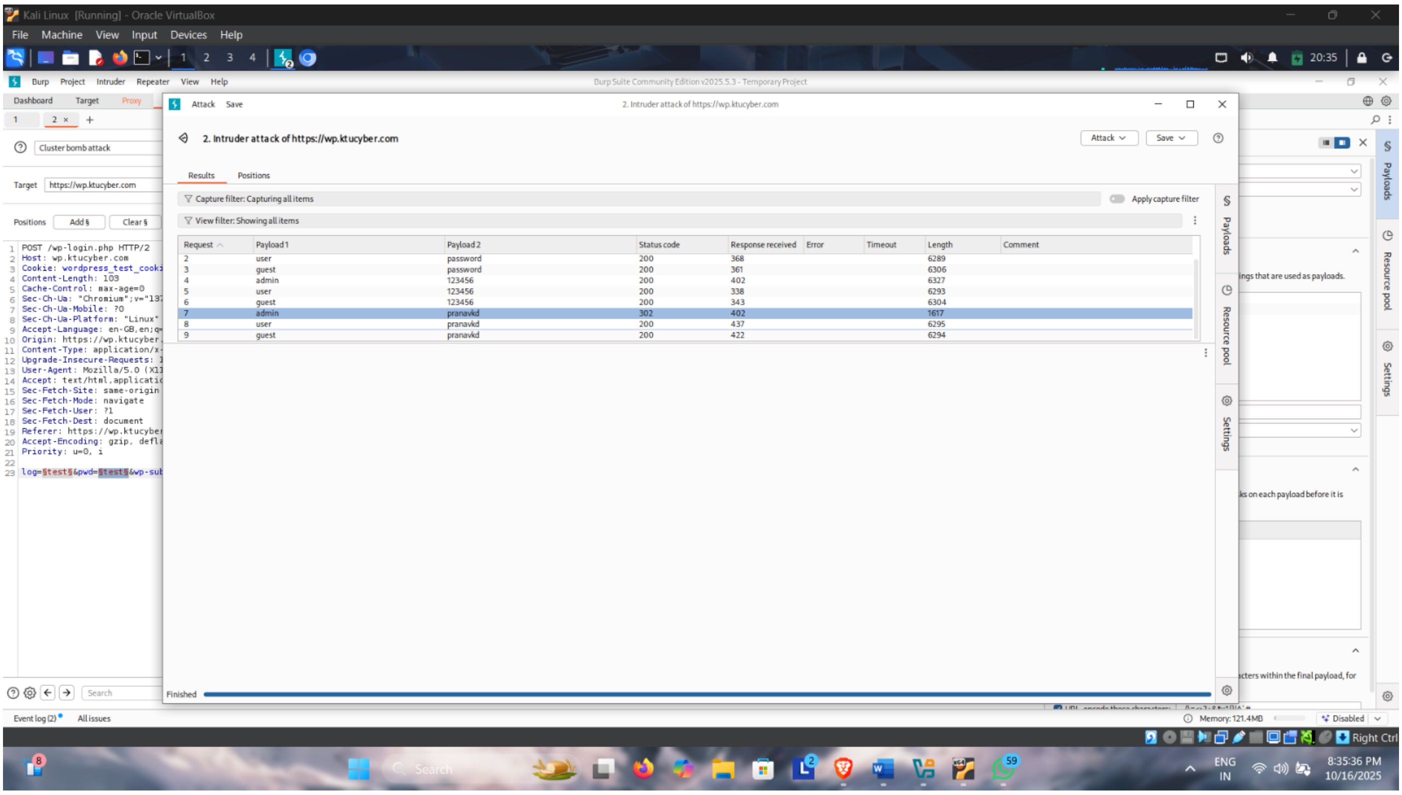
password
123456
pranavkd

Payload processing

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

Payload encoding

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



Kali Linux [Running] - Oracle VirtualBox
Attack Save
2. Intruder attack of https://wp.ktucyber.com
Attack Save
Results Positions
Apply capture filter

2. Intruder attack of https://wp.ktucyber.com

Capture filter: Capturing all items

View filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
2	user	password	200	368			6289	
3	guest	password	200	361			6306	
4	admin	123456	200	402			6327	
5	user	123456	200	338			6293	
6	guest	123456	200	343			6304	
7	admin	pranavkd	302	402			1617	
8	user	pranavkd	200	437			6295	
9	guest	pranavkd	200	422			6294	

Finished