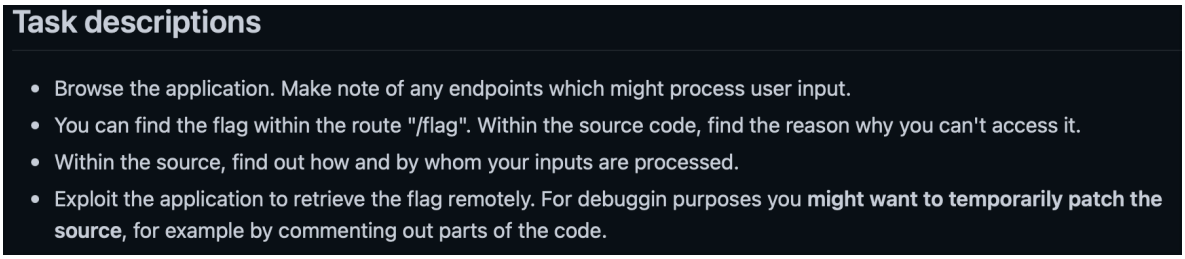
Memo-rap-check

Main page of Memo rap, the first thing we notice is the dude sure is stoned :)



The first thing we do is obviously nmap -sV

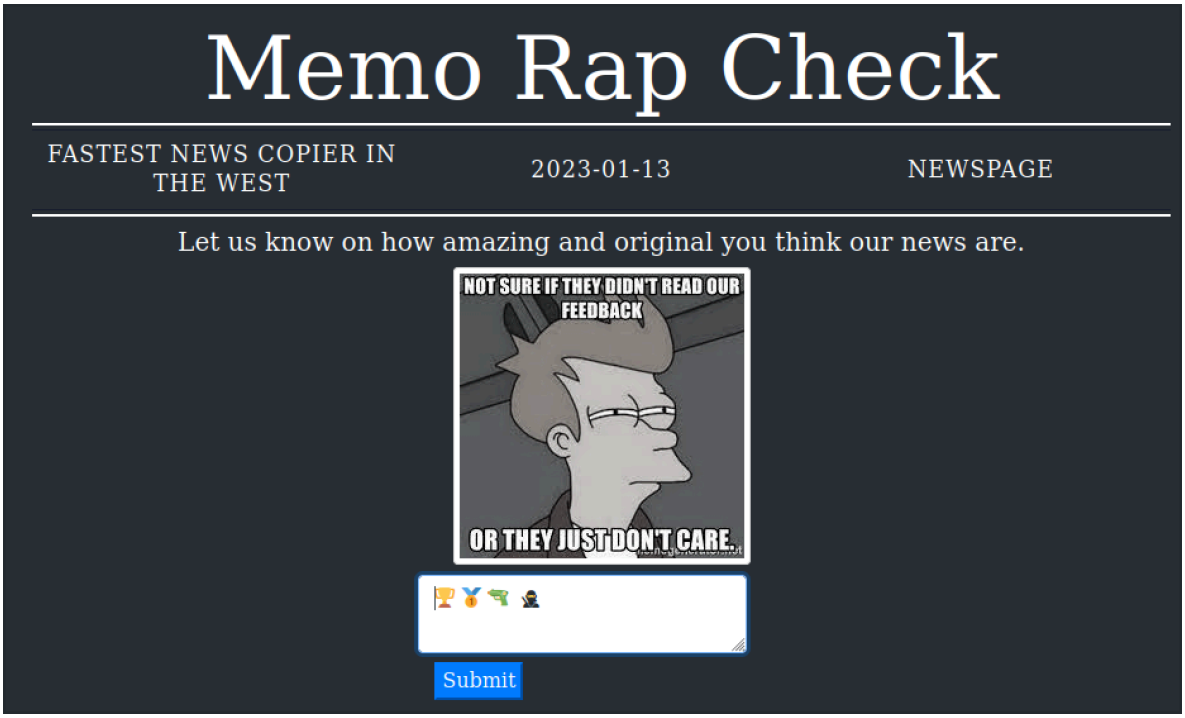
```
└─$ sudo nmap -sV 172.17.0.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-13 10:56 CET
Nmap scan report for 172.17.0.2
Host is up (0.0000040s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http
1 service unrecognized despite returning data. If you know the service/version,
ollowing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.93%I=7%D=1/13%Time=63C12AE6%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,E81,"HTTP/1\.1\x20200\x20OK\r\nX-DNS-Prefetch-Control:\x20off\r\
SF:nExpect-CT:\x20max-age=0\r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Tr
SF:ansport-Security:\x20max-age=15552000;\x20includeSubDomains\r\nX-Downlo
SF:ad-Options:\x20noopen\r\nX-Content-Type-Options:\x20nosniff\r\nX-Permit
SF:ted-Cross-Domain-Policies:\x20none\r\nReferrer-Policy:\x20no-referrer\r
SF:\nX-XSS-Protection:\x200\r\ncontent-type:\x20text/html\r\ncontent-lengt
SF:h:\x203294\r\nDate:\x20Fri,\x2013\x20Jan\x202023\x2009:56:54\x20GMT\r\n
SF:Connection:\x20close\r\n\r\n<html\x20lang=\"en\">\n\x20\x20\x20<head>\n
SF:\x20\x20\x20\x20\x20\x20<meta\x20charset=\"UTF-8\">\n\x20\x20\x20\x20\x
SF:20\x20<title>Memo\x20Rap\x20Check</title>\n\x20\x20\x20\x20\x20\x20<met
SF:a\x20name=\"viewport\"\x20content=\"width=device-width,\x20initial-scal
SF:e=1,\x20user-scalable=no\">\n\x20\x20\x20\x20\x20\x20<link\x20rel=\"ico
SF:n\"\x20href=\"/static/images/favicon\.png\">\n\x20\x20\x20\x20\x20\x20<
SF:link\x20rel=\"stylesheet\"\x20href=\"/static/css/bootstrap\.min\.css\">
SF:\n\x20\x20\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"/static
SF:/css/main\.css\">\n\x20\x20\x20</head>\n\x20\x20\x20<body>\n\x20\x20\x2
SF:0\x20\x20\x20<div\x20class='clouds'>\n\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20<div\x20class=\"main__wrapper\">\n\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20<main>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20")%r(HTTPOpti
SF:ons,20A,"HTTP/1\.1\x20404\x20Not\x20Found\r\nX-DNS-Prefetch-Control:\x2
SF:0off\r\nExpect-CT:\x20max-age=0\r\nX-Frame-Options:\x20SAMEORIGIN\r\nSt
SF:rict-Transport-Security:\x20max-age=15552000;\x20includeSubDomains\r\nX
SF:-Download-Options:\x20noopen\r\nX-Content-Type-Options:\x20nosniff\r\nX
SF:-Permitted-Cross-Domain-Policies:\x20none\r\nReferrer-Policy:\x20no-ref
SF:errer\r\nX-XSS-Protection:\x200\r\ncontent-type:\x20application/json;\x
```

we see there is a http server running on port 80, which is common, and the other output, which is uncommon

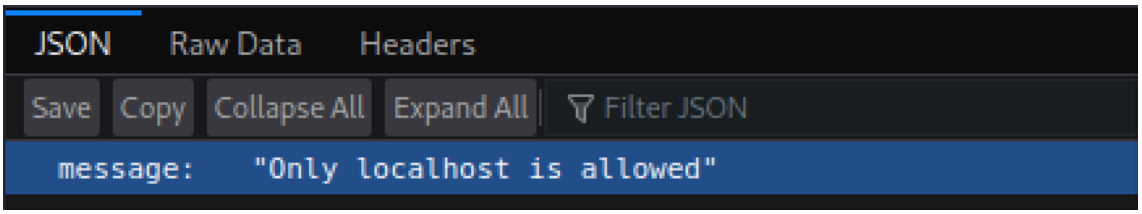
now let's try to dirb it, maybe we find something interesting

```
---- Scanning URL: http://172.17.0.2/ ----
+ http://172.17.0.2/feedback (CODE:200|SIZE:2690)
+ http://172.17.0.2/flag (CODE:401|SIZE:39)
+ http://172.17.0.2/list (CODE:401|SIZE:39)
```

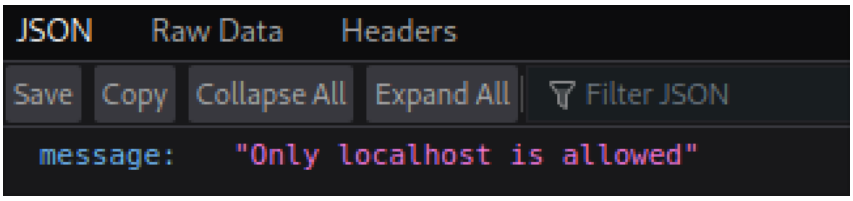
we see 3 direcotries, 1 of them has to contain the flag



Feedback directory: the text field might be exploitable, but let's check other directories first

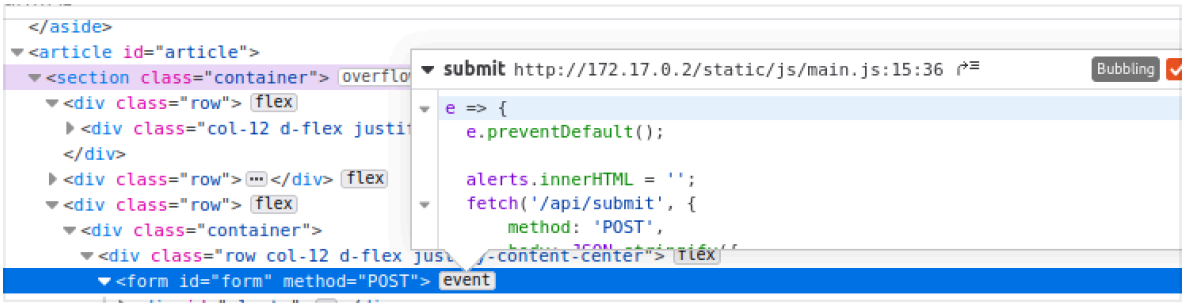


The list directory is only allowed to be accessed with localhost, so only if I am the one who runs the server

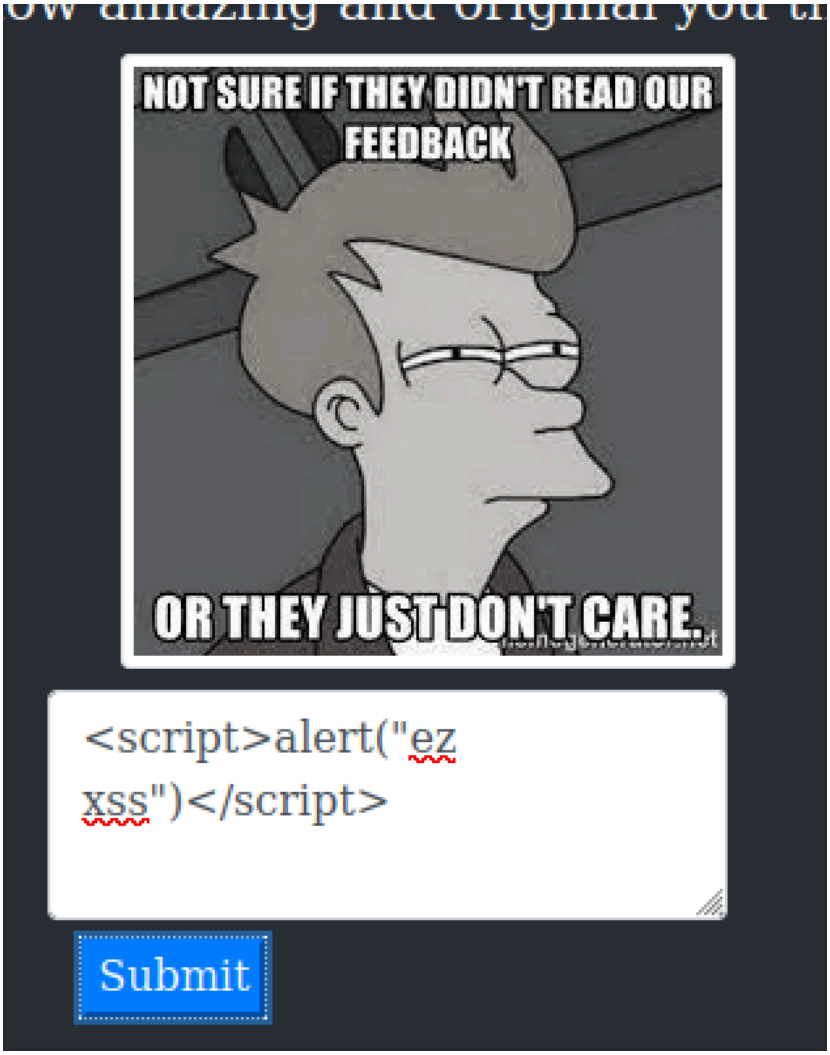


Same thing with /flag directory

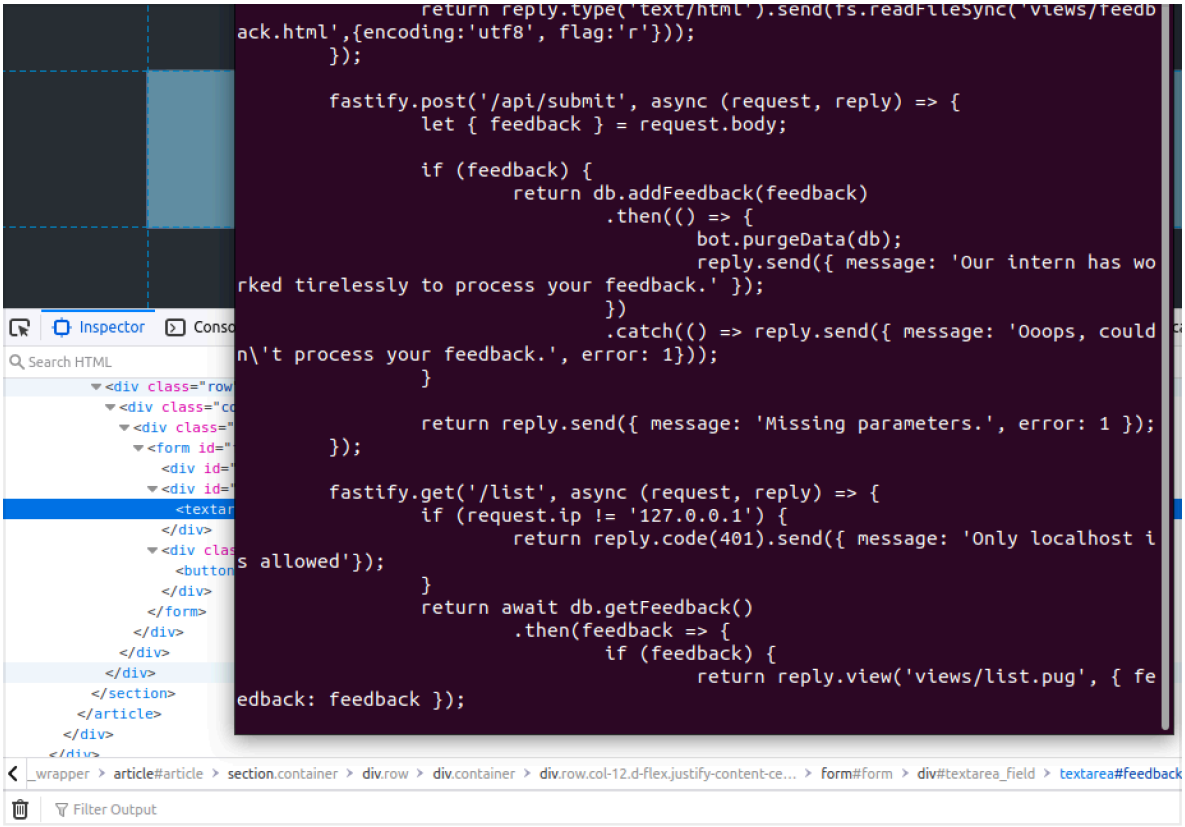
Let's get back to our /feedback page and see if we can inject some code in that chat box



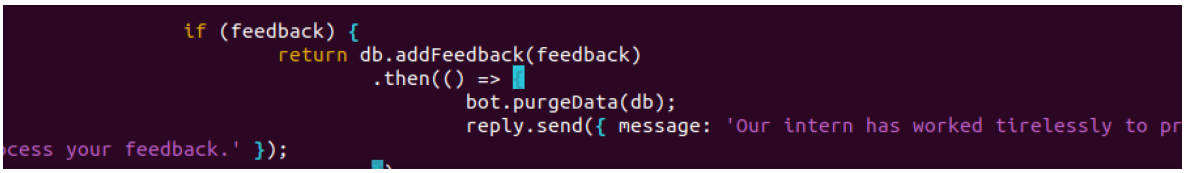
from what I see the submit button creates POST request



First thing that comes to mind is to try and exploit the comment box, which didn't work :(



In the container we can encounter the source code



We can notice what addFeedback() function is called when we press the button

```
fastify.get('/flag', async (request, reply) => {
        if (request.ip != '127.0.0.1') {
                return reply.code(401).send({ message: 'Only localhost is allowed'});
        }
        return reply.send({ message: 'flag_you_w0uldnt_copy_paste_content_Would_u?'})
});
```

We could have commented out the function and check /list in the browser, but for what if we already got the flag:
flag_you_w0uldn’t_copy_paste_content_Would_u?