

###Memo-rap-check CTF Writeup

Task descriptions

- Browse the application. Make note of any endpoints which might process user input.
- You can find the flag within the route "/flag". Within the source code, find the reason why you can't access it.
- Within the source, find out how and by whom your inputs are processed.
- Exploit the application to retrieve the flag remotely. For debuggin purposes you might want to temporarily patch the source, for example by commenting out parts of the code.


As always we go to the main page of the application and act as an innocent user

Haters delight

Due to some risky Bitcoin "investments" the network of rapper 50 Cent is once again higher then 50 cent. After a recent bankruptcy case the rapper managed to come back full swing.


According to a recent interview the rapper plans to invest the money into the community by funding supplying crack dealers with the latest and newest scales.

Lorem ipsum dolor sit amet, et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea



Rapper 50 cent back on track..

Hot this month



BREAKING NEWS

Tekashi69 sues Takeshi's Castle for copyright infringement.

Rapper allegedly states: I'm clearly in *heavy mubmling* and therefore this is a clear and shut case.

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

Let's not judge the funny guy and nmap the application

```

$ 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,
following 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\nncontent-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=\x20en\x20>\n\x20\x20\x20<head>\n
SF:\x20\x20\x20\x20\x20\x20\x20<meta\x20charset=\x20UTF-8\x20>\n\x20\x20\x20\x20\x20
SF:20\x20<title>Memo\x20Rap\x20Check</title>\n\x20\x20\x20\x20\x20\x20\x20<met
SF:a\x20name=\x20viewport\x20\x20content=\x20width=device-width,\x20initial-scal
SF:e=1,\x20user-scalable=no\x20>\n\x20\x20\x20\x20\x20\x20\x20<link\x20rel=\x20ico
SF:n\x20\x20href=\x20/static/images/favicon.png\x20>\n\x20\x20\x20\x20\x20\x20\x20<
SF:link\x20rel=\x20stylesheet\x20\x20href=\x20/static/css/bootstrap.min.css\x20>
SF:\n\x20\x20\x20\x20\x20\x20\x20<link\x20rel=\x20stylesheet\x20\x20href=\x20/static
SF:/css/main.css\x20>\n\x20\x20\x20\x20</head>\n\x20\x20\x20\x20<body>\n\x20\x20\x20\x20
SF:0\x20\x20\x20<div\x20class=\x20clouds\x20>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:x20<div\x20class=\x20main__wrapper\x20>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:20\x20\x20\x20<main>\n\x20\x20\x20\x20\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:riict-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:error\r\nX-XSS-Protection:\x200\r\nncontent-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 to find hidden directories, 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

Memo Rap Check

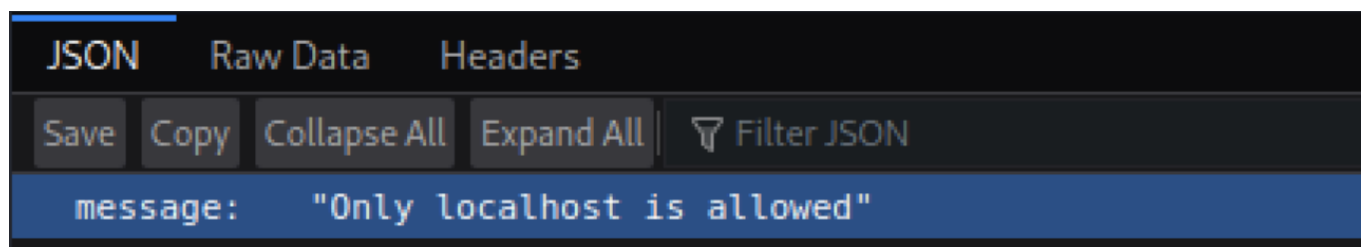
FASTEST NEWS COPIER IN THE WEST 2023-01-13 NEWSPAGE

Let us know on how amazing and original you think our news are.

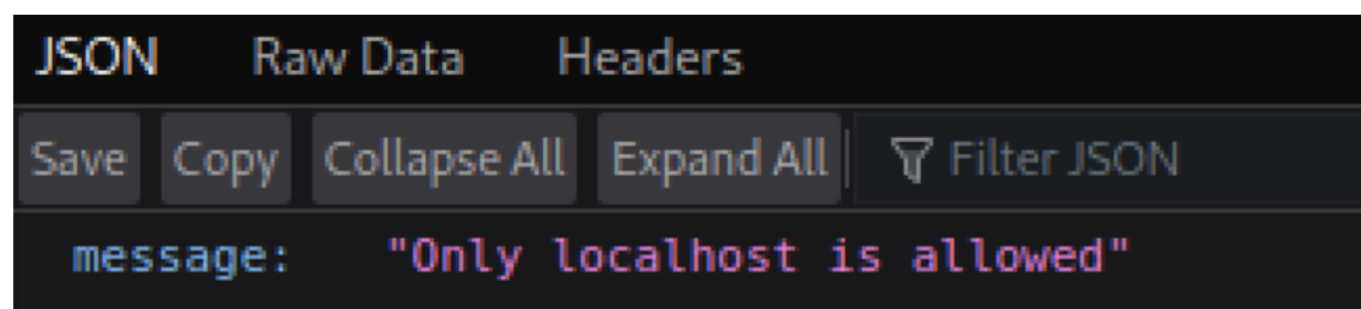




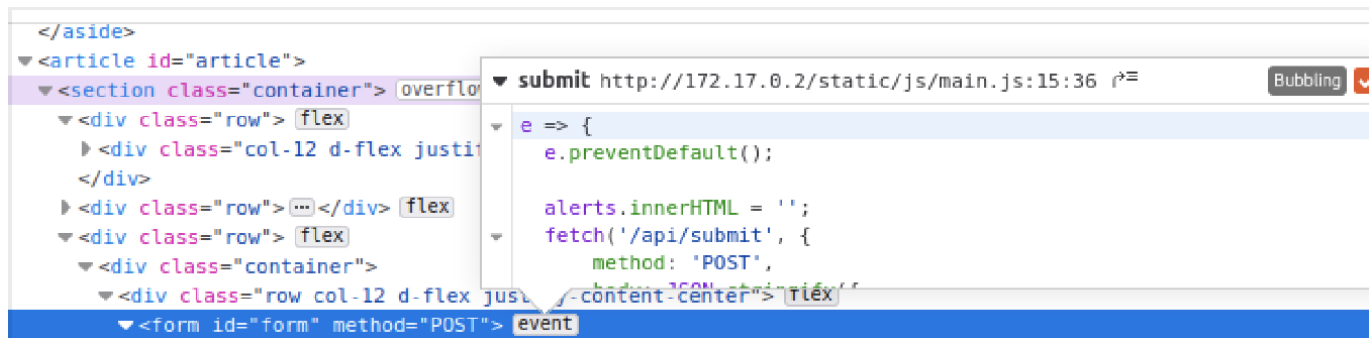
Feedback directory: the text field might be exploitable, but let's check other directories first



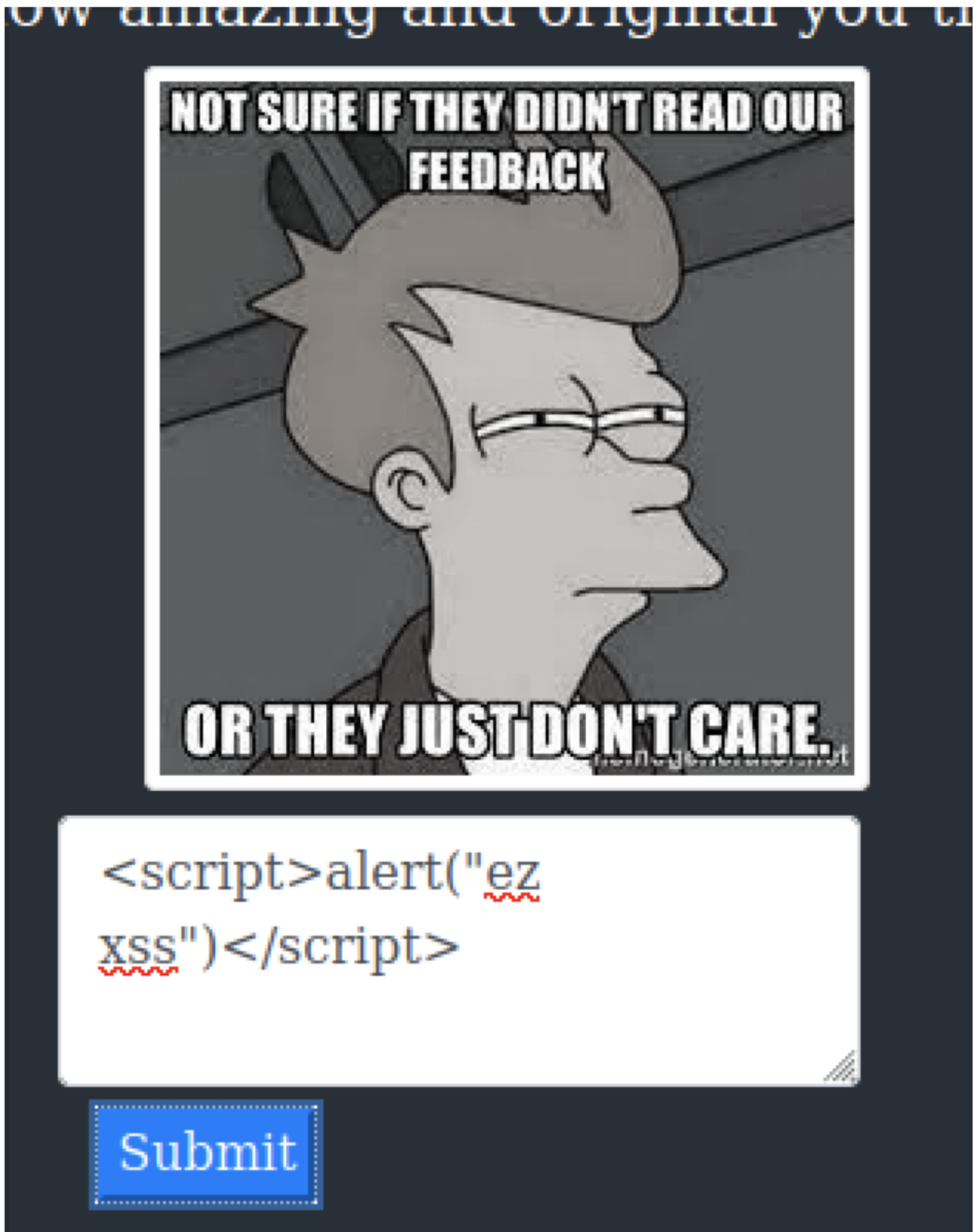
The list directory is only allowed to be accessed with localhost, so only if I am the one who runs the server



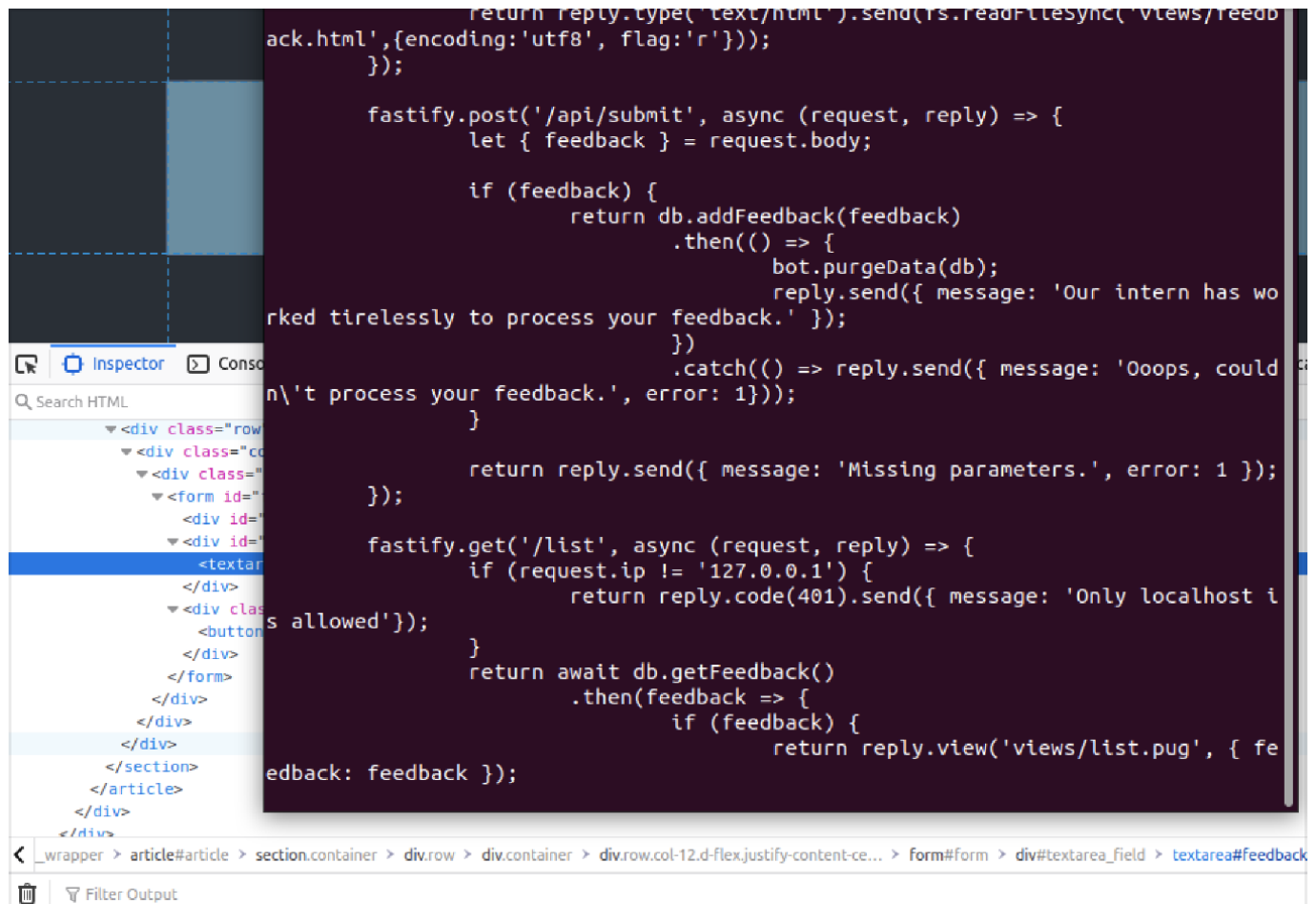
Same thing with /flag directory Let's get back to our /feedback page and see if we can inject some code in that chat box



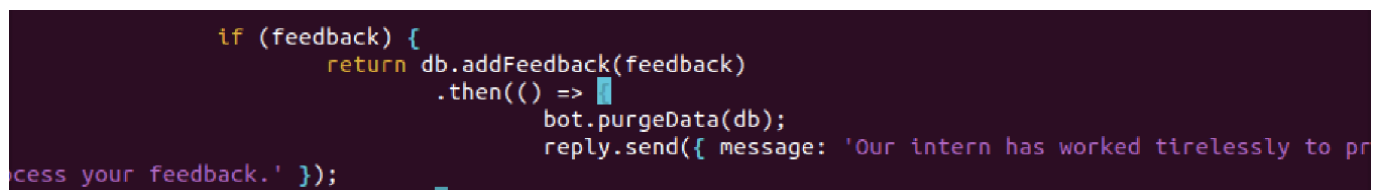
from what I see the submit button creates POST request



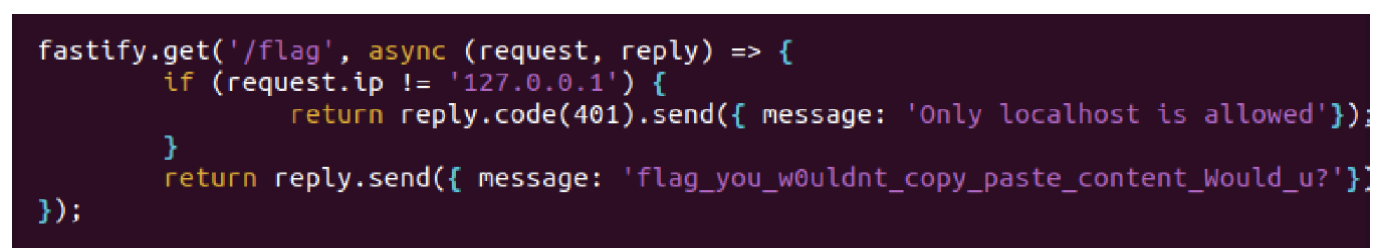
First thing that comes to mind is to try and easily exploit the comment box with XSS to output an alert on the site, which didn't work 😞



In the container we can encounter the source code



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



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