


## Picobrowser picoCTF

picobrowser 

Tags: picoCTF 2019 Web Exploitation



AUTHOR: ARCHIT

### Description


This website can be rendered only by **picobrowser**, go and catch the flag!  
<https://jupiter.challenges.picoctf.org/problem/28921/> ([link](#)) or  
<http://jupiter.challenges.picoctf.org:28921>

---

24,797 solves / 25,931 users attempted (96%)

 89% Liked 

Submit Flag

Hints 

1

You don't need to download a new web browser

To begin I opened the link provided and saw this page.

## My New Website

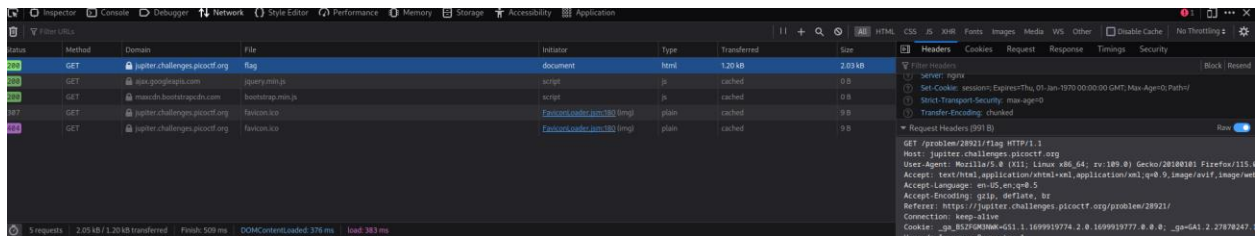
[Home](#)[Sign In](#)[Sign Out](#)

Flag

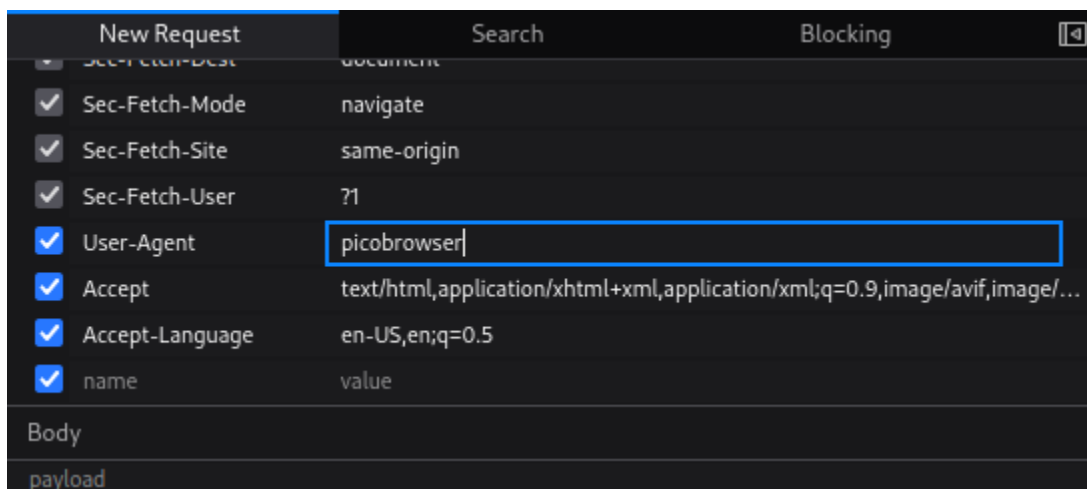
After clicking the flag button I triggered this message.



This caused me to inspect the page and view how the requests were being sent. I saw the get request for the flag and saw that the useragent was specified for other browsers instead of picobrowser.



I proceeded to edit the header to get to the User-Agent and change it to picobrowser.



I then sent the request and viewed the response which gave me the flag.

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

New Request Search Blocking

Sec: Fetch-Mode: navigate  
Sec: Fetch-Site: same-origin  
Sec: Fetch-User: n  
User-Agent: picobrowser  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/...  
Accept-Language: en-US,en;q=0.5  
Name: value

Body: payload

Clear Send

6 requests · 4.17 kB / 2.43 kB transferred · Fresh 3.55 ms · DOMContentLoaded 376 ms

St...	M...	Domain	File	Initiator	Type	Transferred	Size
200	GET	jupyter...	flag	document	html	1.20 kB	2...
200	GET	static...	jquery.min.js	script	js	cached	0.0
200	GET	static...	bootstrap.min.js	script	js	cached	0.0
307	GET	jupyter...	favicon.ico	favicon	plain	cached	0.0
200	GET	jupyter...	favicon.ico	favicon	plain	cached	0.0
200	GET	jupyter...	flag	document	html	1.23 kB	2.1...

Headers Cookies Request Response Timings Stack Trace Security

Response: picoctf{p1c0\_s3cr3t\_ag3nt\_84f9c865}

Flag:  
picoCTF{p1c0\_s3cr3t\_ag3nt\_84f9c865}