

findme

Medium Web Exploitation picoCTF 2023

AUTHOR: GEOFFREY NJOGU

Description

Help us test the form by submitting the username as `test` and password as `test`!

The website running [here](#).

debug info: [u:834257 e: p: c:349 i:294958]

23,331 users solved

This challenge launches an instance on demand.

Its current status is: **RUNNING**

Instance Time Remaining: **13:21**

Restart Instance

Hints ?

1

68% Liked

Submit Flag

picoCTF{FLAG}

masukkan user test dan password test!

Help us test this form

username:test and password:test.

Username

test

Password

.....

test

tekan tombol back

Setelah submit form, kamu diminta:

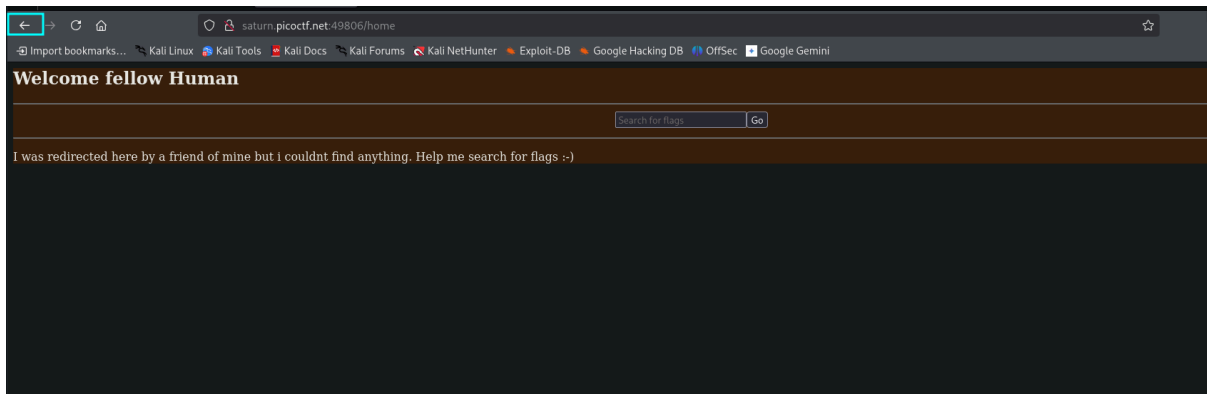
“Tekan tombol back”

Ini trik umum di CTF: redirect cepat menyembunyikan sesuatu, tapi jika kamu kembali (via tombol back), kamu bisa melihat halaman sebelumnya yang mungkin memuat informasi rahasia, contohnya:

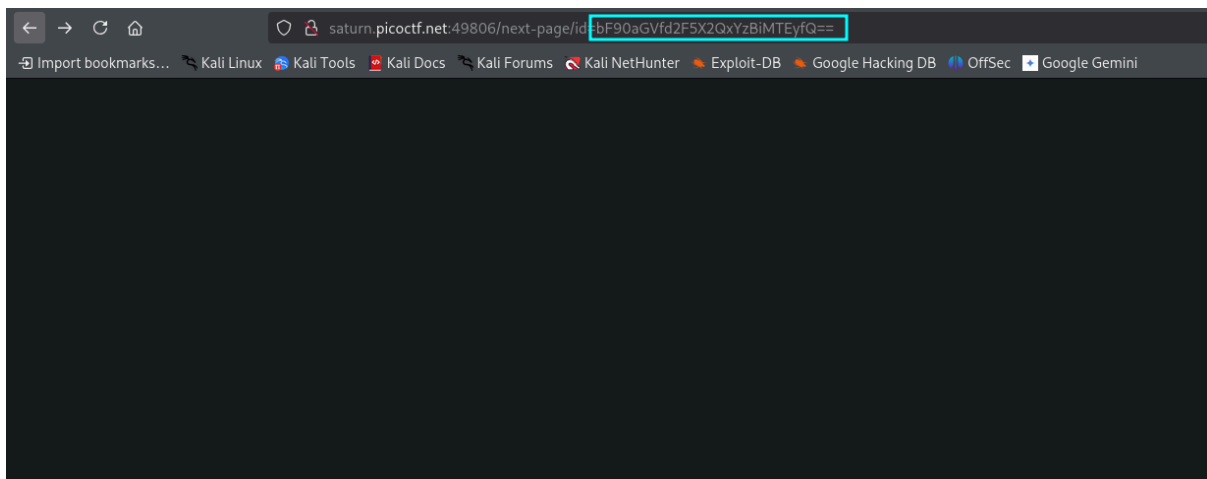
Kode Base64

JavaScript injection

HTML comment (<!-- secret here -->)



dan ada kode base64 dan kita akan coba terjemahkan



ini adalah potongan flagnya

Decode from Base64 format
Simply enter your data then push the decode button.

bF90aGVfd2F5X2QxYzBiMTEyfQ==

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

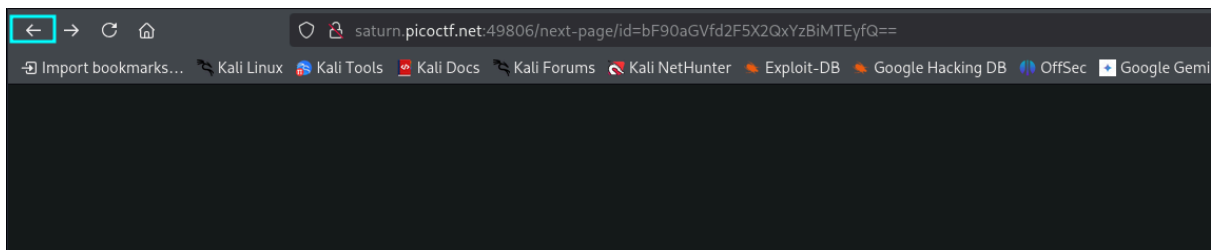
☒ Decode each line separately (useful for when you have multiple entries).

☐ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

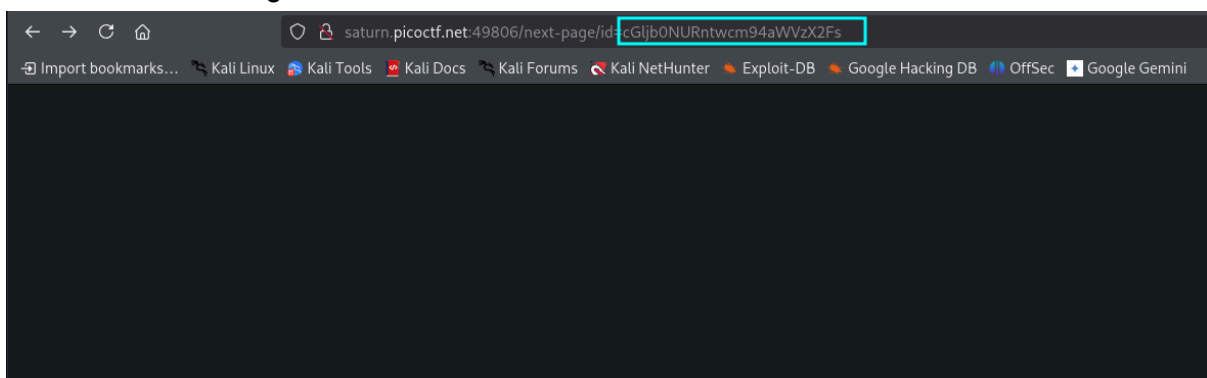
< DECODE > Decodes your data into the area below.

I_the_way_d1c0b112}

lalu kita kembali di tab tadi dan tekan tombol back sekali lagi



ada kode base 64 lagi




gabungkan dengan kode tadi

Decode from Base64 format


Simply enter your data then push the decode button.



```
cGljb0NURntwcm94aWVzX2FsbF90aGVfd2F5X2QxYzBiMTEyfQ==
```

 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8  Source character set.

☒ Decode each line separately (useful for when you have multiple entries).

 Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

 **DECODE**  Decodes your data into the area below.

```
picoCTF{proxies_all_the_way_d1c0b112}
```

Explanation:

Teknik	Penjelasan
Redirection	Halaman mengarahkan user langsung ke tempat lain, menyembunyikan data
"Back Trick"	Gunakan tombol back browser untuk melihat halaman sebelum redirect
Base64 Encoding	Teknik menyembunyikan data agar terlihat seperti acak (tapi mudah didecode)
Form Injection Biasa	Tidak ada login sebenarnya — cuma trigger redirect/script saja