

## Introduction

Roboto Sans

Medium Web Exploitation picoCTF 2022

AUTHOR: MUBARAK MIKAIL

Description

The flag is somewhere on this web application not necessarily on the website. Find it.  
Check [this](#) out.

debug info: {u:834257 e: p: c:291 i:296097}

This challenge launches an instance on demand.  
Its current status is: **RUNNING**  
Instance Time Remaining: **14 : 25**  

Restart Instance

Hints ?  
(None)

23,588 users solved

48% Liked

picoCTF{FLAG}

Submit Flag

ini adalah tampilan web di challenge kali ini

← → ↺ ↻

saturn: picotf.net 63702

☆

Import bookmarks... Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Google Gemini

✉ Email : demo@gmail.com

**Flexed**

📞 Contact : +71 71234567

Home About Yoga Pricing Yoga Online Contact us

Gather  
New Body Energy

CONTACT US

saya mencoba mencari flagnya di page source dan ternyata tidak ada

```

38 <!-- class="app" -->
39 <!-- end loader -->
40
41 <div id="content">
42 <!-- header -->
43 <header>
44 <!-- header inner -->
45 <div class="head-top">
46 <div class="container">
47
48 <div class="row">
49 <div class="col-xl-4 col-lg-4 col-md-4 col-sm-4">
50 <div class="email">
51 <a href="#"> Email : demo@gmail.com/</a>
52 </div>
53 </div>
54 <div class="col-xl-4 col-lg-4 col-md-4 col-sm-4">
55 <div class="logo">
56 <a href="index.html"></a>
57 </div>
58 </div>
59 <div class="col-xl-4 col-lg-4 col-md-4 col-sm-4">
60 <div class="contact_nu">
61 <a href="#"> Contact : +71 71234567</a>
62 </div>
63 </div>
64 </div>
65 </div>
66 </div>
67 <div class="bg">
68 <div class="container">
69 <nav class="navigation navbar-expand-md navbar-dark">
70
71 <button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarsExample04" aria-controls="navbarsExample04" aria-expanded="false" aria-label="Toggle navigation">
72 <span class="navbar-toggler-icon"></span>
73 </button>
74
75 <div class="collapse navbar-collapse" id="navbarsExample04">
76 <ul class="navbar-nav mr-auto">
77 <li class="nav-item active">
78 <a class="nav-link" href="index.html">Home <span class="sr-only">(current)</span></a>
79 </li>
80 <li class="nav-item">
81 <a class="nav-link" href="#about">About </a>
82 </li>
83 <li class="nav-item">
84 <a class="nav-link" href="#yoga">Yoga</a>
85 </li>
86 <li class="nav-item">
87 <a class="nav-link" href="#pricing">Pricing</a>
88 </li>
89 <li class="nav-item">
90 <a class="nav-link" href="#online">Yoga Online</a>
91 </li>
92 <li class="nav-item">
93 <a class="nav-link" href="#contact">Contact us</a>
94 </li>
95 </ul>

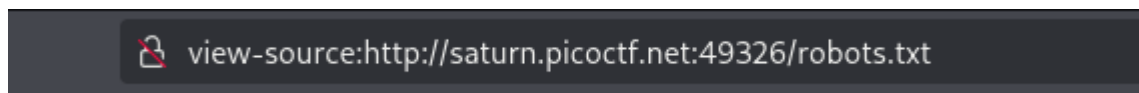
```

dan saya membuka direktori /robots.txt

Apa itu robots.txt?

robots.txt adalah **file teks sederhana** yang digunakan untuk memberi tahu **web crawler** (seperti Googlebot, Bingbot, dll) **bagian mana dari website yang boleh atau tidak boleh mereka indeks**.

Letaknya biasanya di **root direktori** sebuah website:

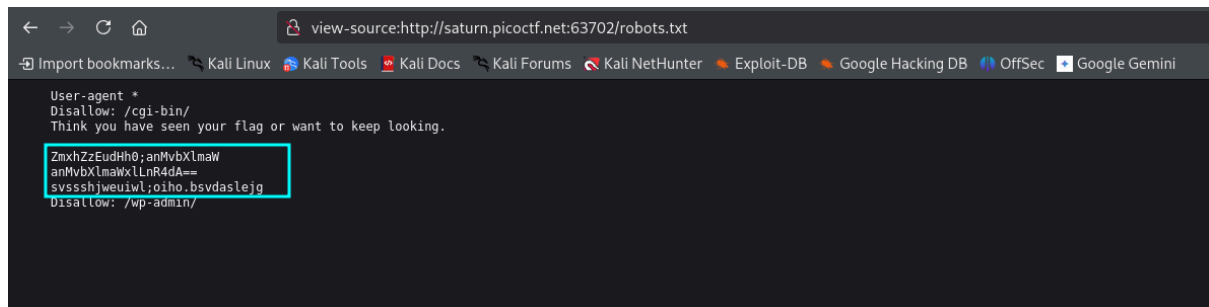


**Fungsinya untuk Apa?**

File ini **bukan untuk keamanan**, tapi hanya **panduan etika** bagi crawler/search engine.

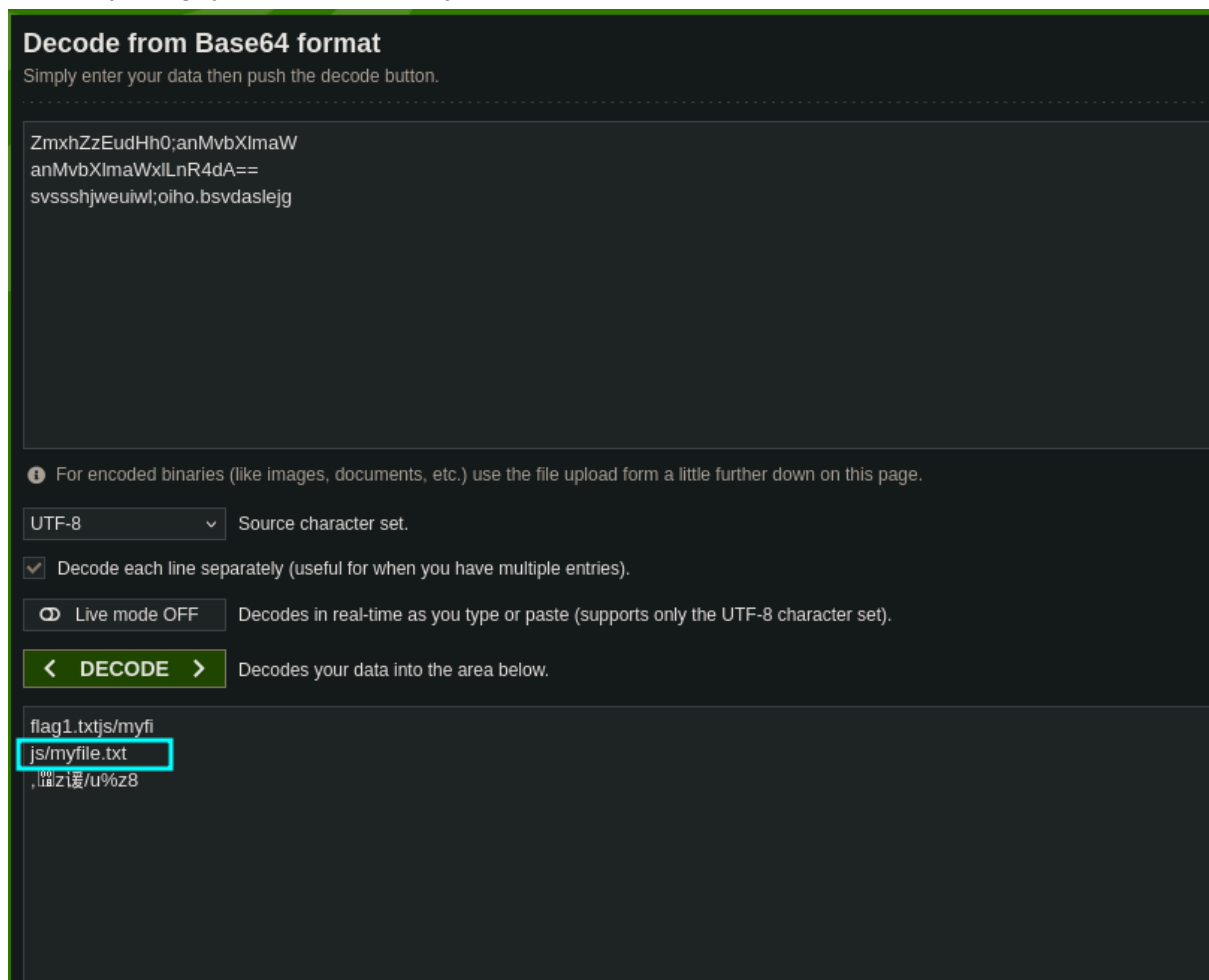
ini bukan direktori tersembunyi. Tapi robots.txt sering dipakai untuk "menyembunyikan" direktori sensitif dari search engine — sayangnya ini bisa menjadi petunjuk emas bagi attacker

Dan di direktori /robots.txt di challenge kali ini ada petunjuk berupa base64



```
view-source:http://saturn.picoctf.net:63702/robots.txt
User-agent *
Disallow: /cgi-bin/
Think you have seen your flag or want to keep looking.
ZmxhZzEudHh0;anMvbXlmaW
anMvbXlmaWxlnR4dA==
svssshjweuiwl;oiho.bsvdaslejg
Disallow: /wp-admin/
```

saya coba decodedan menemukan petunjuk direktori mencurigakan yaitu js/myfile.txt yang sepertinya flagnya berada disana yaitu



### Decode from Base64 format

Simply enter your data then push the decode button.

ZmxhZzEudHh0;anMvbXlmaW  
anMvbXlmaWxlnR4dA==  
svssshjweuiwl;oiho.bsvdaslejg

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.

flag1.txtjs/myfi  
js/myfile.txt  
,.z8

ketika saya akses ternyata benar flagnya berada disana

