

Introduction

Secrets

MediumWeb ExploitationpicoCTF 2022

AUTHOR: GEOFFREY NJOGU

Description

We have several pages hidden. Can you find the one with the flag?
The website is running [here](#).

debug info: {u:834257 e: p: c:296 l:296105}

This challenge launches an instance on demand.
Its current status is: **RUNNING**
Instance Time Remaining: **14:27**

Restart Instance

Hints

1

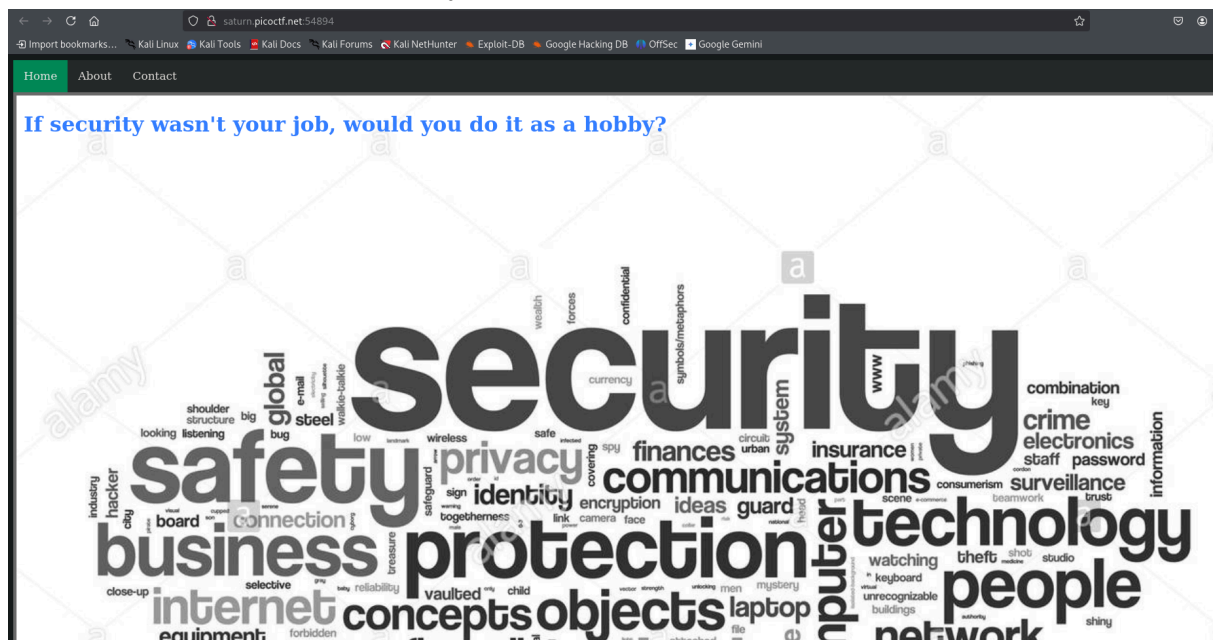
25,367 users solved

👍75% Liked👍

🚩picoCTF{FLAG}

Submit Flag

ini adalah tampilan halaman webnya



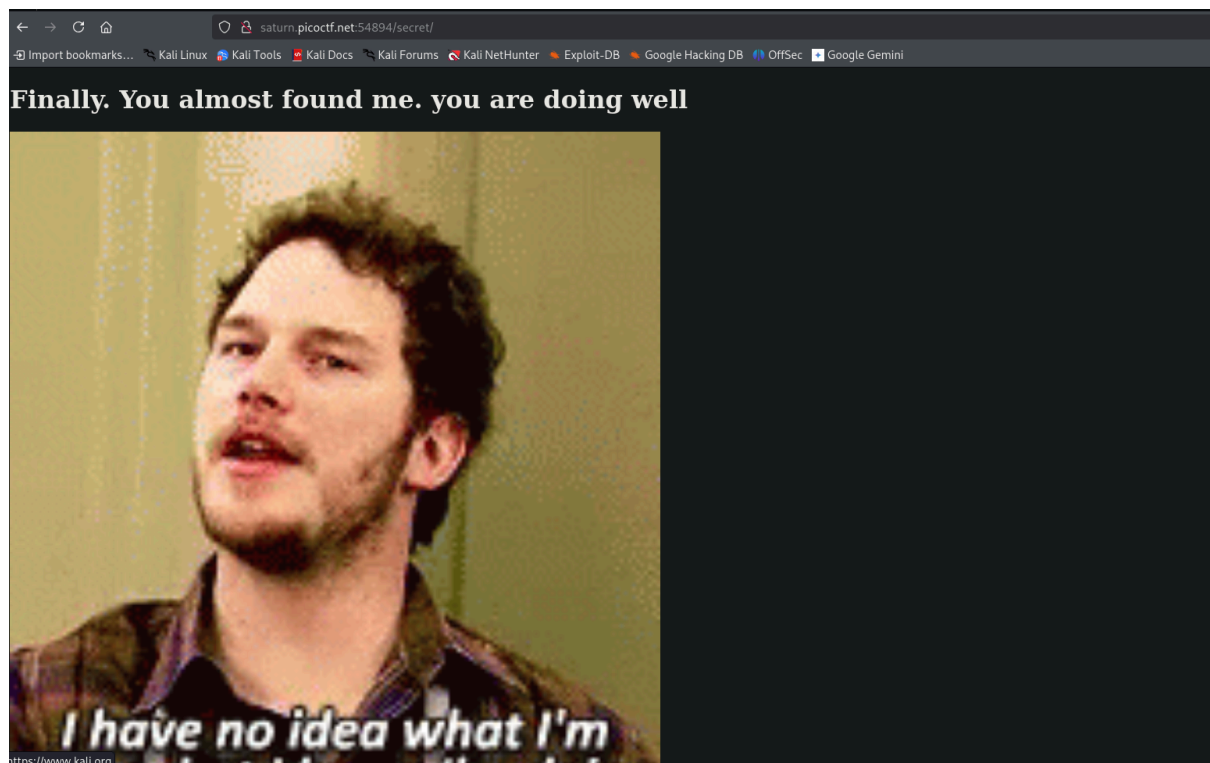
saya mencoba melihat page sourcenya dengan menekan ctrl u dan saya menemukan direktori mencurigakan bernama secret

```

1 <!DOCTYPE html>
2 <html>
3   <head>
4     <meta charset="UTF-8" />
5     <meta
6       name="viewport"
7       content="width=device-width, initial-scale=1, shrink-to-fit=no"
8     />
9     <meta name="description" content="" />
10    <!-- Bootstrap core CSS -->
11    <link href="vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet" />
12    <!-- title -->
13    <title>home</title>
14    <!-- CSS -->
15    <link href="secret/assets/index.css" rel="stylesheet" />
16  </head>
17  <body>
18    <!-- ***** Header Area Start ***** -->
19    <div class="topnav">
20      <a class="active" href="#home">Home</a>
21      <a href="about.html">About</a>
22      <a href="contact.html">Contact</a>
23    </div>
24
25    <div class="imgcontainer">
26      
31      <div class="top-left">
32        <h1>If security wasn't your job, would you do it as a hobby?</h1>
33      </div>
34    </div>
35  </body>
36 </html>
37

```

ini tampilan dari direktori secret



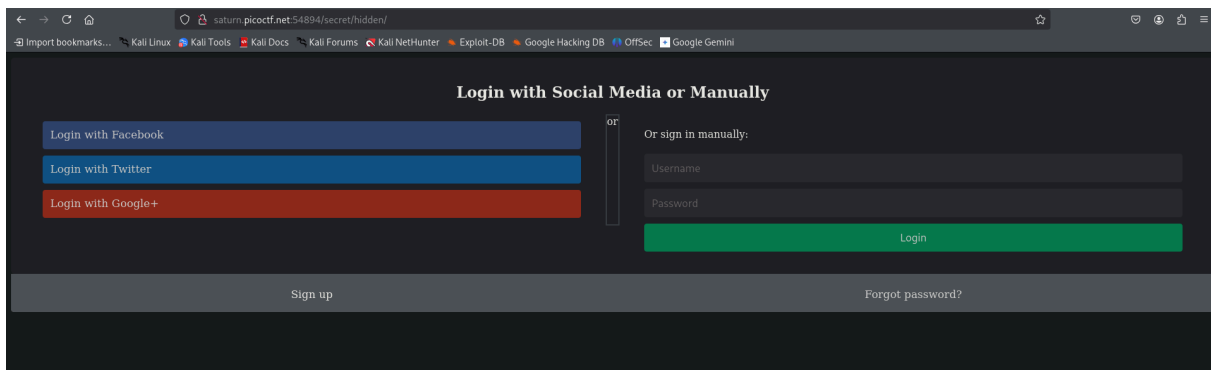
saya mencoba melihat source kodenya lagi dan menemukan direktori mencurigakan lagi yaitu hidden

```

1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title></title>
5 <link rel="stylesheet" href="hidden/file.css" />
6 </head>
7
8 <body>
9 <h1>Finally, You almost found me. you are doing well</h1>
10 
11 </body>
12 </html>
13

```

ini isi dari direktori hidden



ctrl u

dan saya menemukan direktori superhidden

```

1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>LOGIN</title>
5 <!-- css -->
6 <link href="superhidden/login.css" rel="stylesheet" />
7 </head>
8 <body>
9 <form>
10 <div class="container">
11 <form method="" action="/secret/assets/popup.js">
12 <div class="row">
13 <h2 style="text-align: center;">
14 Login with Social Media or Manually
15 </h2>
16 <div class="vl">
17 <span class="vl-innertext">or</span>
18 </div>
19
20 <div class="col">
21 <a href="#" class="fb btn">
22 <i class="fa fa-facebook fa-fw"></i> Login with Facebook
23 </a>
24 <a href="#" class="twitter btn">
25 <i class="fa fa-twitter fa-fw"></i> Login with Twitter
26 </a>
27 <a href="#" class="google btn">
28 <i class="fa fa-google fa-fw"></i> Login with Google+
29 </a>
30 </div>
31
32 <div class="col">
33 <div class="hide-md-lg">
34 <p>Or sign in manually:</p>
35 </div>
36
37 <input
38 type="text"
39 name="username"
40 placeholder="Username"
41 required
42 />
43 <input
44 type="password"
45 name="password"
46 placeholder="Password"
47 required
48 />
49 <input type="hidden" name="db" value="superhidden/xdfgwd.html" />
50
51 <input
52 type="submit"
53 value="Login"
54 onclick="alert('Thank you for the attempt but oops! try harder. better luck next time!')"
55 />
56 </div>
57 </div>
58 </form>
59 </div>
60

```

berhasil dapat flagnya

