Topics

- Reverse Engineering - Binary Exploitation

Linux Interactive Exploit Develoment with GDB and PEDA

Challenges

Links

File (16)	Category	LINK
Floppy	ReverseEngineering	https://github.com/VoidHack/write-ups/tree/master/Square%20CTF%202017/reverse/floppy
Behind The Scenes	ReverseEngineering	https://app.hackthebox.com/challenges/Behind%2520the%2520Scenes
Box Cutters	ReverseEngineering	-
Loot Stash	ReverseEngineering	Apocalypse 2024
Reykjavik	ReverseEngineering	https://ctflearn.com/challenge/990
FactCheck	ReverseEngineering	https://play.picoctf.org/events/73/challenges/challenge/416?category=3&page=1&user_solved=1
GDB Test Drive	ReverseEngineering	https://play.picoctf.org/practice/challenge/273?category=3&page=1&solved=1
Don't Bump Your Head(er)	Web	https://ctflearn.com/challenge/109
My Blog	Web	https://ctflearn.com/challenge/979
Post Practice	Web	https://ctflearn.com/challenge/114
Cookies	Web	https://play.picoctf.org/practice/challenge/173
Get aHEAD	Web	https://play.picoctf.org/practice/challenge/132?category=1&page=1&search=
Insp3ct0r	Web	https://play.picoctf.org/practice/challenge/18?category=1&page=1
Intro to Burp picoCTF 2024	Web	https://play.picoctf.org/events/73/challenges/challenge/419?category=1&page=1&user_solved=1
Local Authority	Web	https://play.picoctf.org/practice/challenge/278?category=1&page=2
picobrowser	Web	https://play.picoctf.org/practice/challenge/9?category=1&page=3

Web

1. My Blog
2. Cookies
3. Insp3ct0r
4. Local Authority
5. Get aHEAD
6. Don't Bump Your Head(er)
7. Post Practice
8. picobrowser
9. Intro to Burp picoCTF 2024

RevEng

1. Loot Stash
2. Box Cutters
3. FactCheck
4. GDB Test Drive
5. Behind The Scenes
6. Reykjavik
7. Floppy

Resources

- TryHackMe room
- Medium Walkthrough
- https://tryhackme.com/r/room/compiled

yt Cryptocat

Binary Exploitation

> meeting-05

Writeups

Web

My Blog

My Blog

- Description
- Steps
- Flag

Description

Summary

Hi, I'm Noxtal! I have hidden a flag somewhere in my Cyberworld (AKA blog)... you may find a good **application** for your **memory**. ;)

Note: This is my real website (thus no deadly bug to exploit here). You might want to read some of my content (writeups, tutorials, and cheatsheets). I would be glad to receive any kind of feedback.

Click here to access it, have fun checking my blog out! Cheers!

Hint: replace the flag{} part with CTFlearn{}.

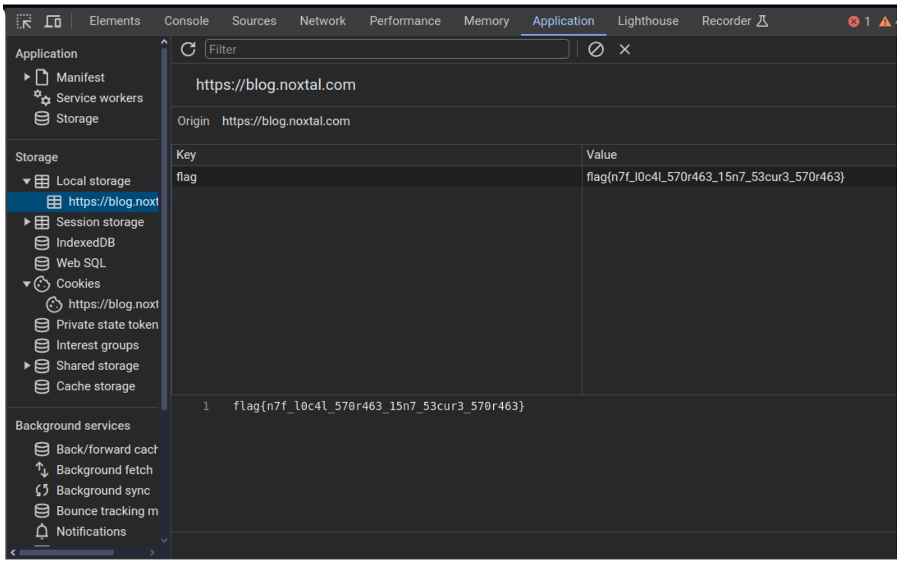
Steps

We open the site :

Go to inspection

And follow the blog url

then go to application/local storage/ https://blog.noxtal.com



https://blog.noxtal.com

Origin https://blog.noxtal.com

Key	Value
flag	flag{n7f_l0c4l_570r463_15n7_53cur3_570r463}

```
flag{n7f_l0c4l_570r463_15n7_53cur3_570r463}
```

flag{n7f_l0c4l_570r463_15n7_53cur3_570r463}

Flag

`ctflearn{n7f_l0c4l_57`

✓ **flag**

ctflearn{n7f_l0c4l_570r463_15n7_53cur3_570r463}

Cookies

Cookies

- Description
- Steps
- Flag

Description

Summary

Who doesn't love cookies? Try to figure out the best one. http://mercury.picoctf.net:64944/

Steps

We go to the website
Open burpsuite

Intercept a request at "flag"

then right click and send to repeater

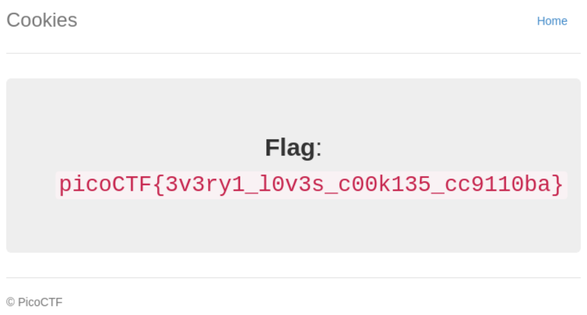
You see that it has a filed name: Cookie; name=

So we try 1, ..., till 18

We accept follow redirection since that is the response

And then we go to the tab : (Pretty, Raw, Hex, Render) Render

And we see the result



Cookies

Home

Flag:
`picoCTF{3v3ry1_l0v3s_c00k135_cc9110ba}`

© PicoCTF

picoCTF{3v3ry1_l0v3s_c00k135_cc9110ba}

Flag

`picoCTF{3v3ry1_l0v3s_c`

✓ **flag**

picoCTF{3v3ry1_l0v3s_c00k135_cc9110ba}

Insp3ct0r

Insp3ct0r

- Description
- Steps
- Flag

Description

Summary

Kishor Balan tipped us off that the following code may need inspection: `https://jupiter.challenges.picoctf.org/problem/9670/` (link) or http://jupiter.challenges.picoctf.org:9670

Steps

We open inspection

and open all the folded until we find this comment

```
<!-- Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3 -->
```

This is the first

Then we go to sources :

and to mycss.css

```
/* You need CSS to make pretty pages. Here's part 2/3 of the flag: t3ct1ve_0r_ju5t */
```

Lastly we go to myjs.js

```
/* Javascript sure is neat. Anyways part 3/3 of the flag: _lucky?2e7b23e3} */
```

Flag

`picoCTF{tru3_d3t3ct1ve`

✓ **flag**

picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?2e7b23e3}

Local Authority

Local Authority

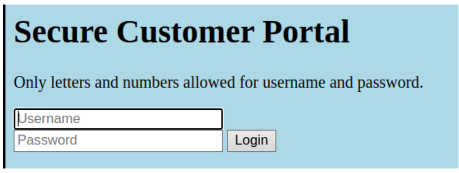
- Description
- Steps
- Flag

Description

Summary

Can you get the flag?
Go to this website and see what you can discover.

Steps



Secure Customer Portal

Only letters and numbers allowed for username and password.

Open burpsuite

And try admin & flag in the browser and send to repeater

```
username=admin&password=flag&login=
```

The following script is inside the result of the request

```
<script src="secure.js"></script>
```

Since it is a local js file we go to inspection and sources and open it

```



function checkPassword(username, password)
{
  if( username === 'admin' && password === 'strongPassword098765' )
  {
    return true;
  }
  else
  {
    return false;
  }
}

```

So we try the passwords and get the result that it is successful

```
picoCTF{j5_15_7r4n5p4r3n7_05df90c8}
```

Flag

`picoCTF{j5_15_7r4n5p4r`

> ✓ **flag**
>
> picoCTF{j5_15_7r4n5p4r3n7_05df90c8}

Get aHEAD

Get aHEAD

- Description
- Steps
- Flag

Description

> **Summary**
>
> Find the flag being held on this server to get ahead of the competition http://mercury.picoctf.net:28916/

Steps

Open Burpsuite

Open the browser, press red and intercept the request

Send it to the repeater and change the POST to HEAD

And send it

```
HEAD /index.php? HTTP/1.1
Host: mercury.picoctf.net:28916
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.110 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://mercury.picoctf.net:28916/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response :

```
HTTP/1.1 200 OK
flag: picoCTF{r3j3ct_th3_du4l1ty_70bc61c4}
Content-type: text/html; charset=UTF-8
```

Flag

```
flag: picoCTF{r3j3ct_t
```

> ✓ **flag**
>
> flag: picoCTF{r3j3ct_th3_du4l1ty_70bc61c4}

Don't Bump Your Head(er)

Don't Bump Your Head(er)

- Description
- Steps
- Flag

Description

> **Summary**
>
> Try to bypass my security measure on this site! http://165.227.106.113/header.php

---

Steps

Go to the site :

```
Sorry, it seems as if your user agent is not correct, in order to access this website. The one you supplied is: Mozilla/5.0
(X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 OPR/107.0.0.0
```

So we open burpsuite and send it to the repeater

Request :

```
GET /header.php HTTP/1.1
Host: 165.227.106.113
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 OPR/107.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Tue, 05 Mar 2024 21:36:47 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 255

Sorry, it seems as if your user agent is not correct, in order to access this website. The one you supplied is: Mozilla/5.0
(X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 OPR/107.0.0.0
<!-- Sup3rS3cr3tAg3nt  -->
```

Request:

```
GET /header.php HTTP/1.1
Host: 165.227.106.113
Upgrade-Insecure-Requests: 1
User-Agent: Sup3rS3cr3tAg3nt
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Tue, 05 Mar 2024 21:37:40 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 106

Sorry, it seems as if you did not just come from the site, "awesomesauce.com".
<!-- Sup3rS3cr3tAg3nt  -->
```

Request:

```
GET /header.php HTTP/1.1
Host: 165.227.106.113
Upgrade-Insecure-Requests: 1
User-Agent: Sup3rS3cr3tAg3nt
Referer: awesomesauce.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Tue, 05 Mar 2024 21:39:32 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 81

Here is your flag: flag{did_this_m3ss_with_y0ur_h34d}
<!-- Sup3rS3cr3tAg3nt  -->
```

Flag

`flag{did_this_m3ss_wit`

✓ **flag**

flag{did_this_m3ss_with_y0ur_h34d}

Post Practice

Post Practice

- Description
- Steps
- Flag

Description

Summary

This website requires authentication, via POST. However, it seems as if someone has defaced our site. Maybe there is still some way to authenticate? http://165.227.106.113/post.php

---

Steps

Using burpsuite

you do one request and it says that the website takes POST data that have not been submitted

Change the GET request to POST and get this result

```
POST /post.php HTTP/1.1
Host: 165.227.106.113
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.110
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Tue, 05 Mar 2024 19:02:49 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 118

<h1>This site takes POST data that you have not submitted!</h1><!-- username: admin | password: 71urlkufpsdnlkadsf -->
```

online walkthrough

```
python -c "print(len('username=admin&password=71urlkufpsdnlkadsf'))"
```

We send this post: It needed the correct number of spaces between the data and the Content-Length

```
POST /post.php HTTP/1.1
Host: 165.227.106.113
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 42

username=admin&password=71urlkufpsdnlkadsf
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Tue, 05 Mar 2024 21:28:58 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Content-Length: 32

<h1>flag{p0st_d4t4_4ll_d4y}</h1>
```

Flag

`flag{p0st_d4t4_4ll_d4y`

✓ **flag**

flag{p0st_d4t4_4ll_d4y}

picobrowser

picobrowser

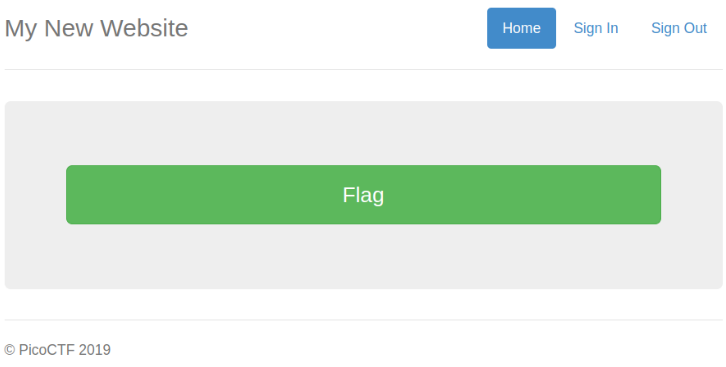
- Description
- Steps
- Flag

Description

Summary

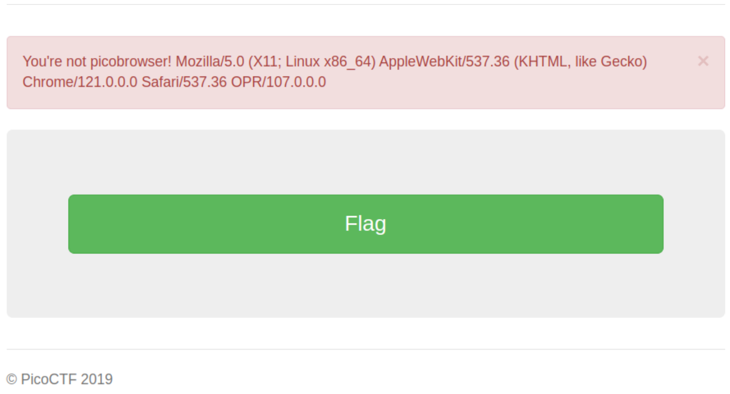
This website can be rendered only by **picobrowser**, go and catch the flag! `https://jupiter.challenges.picoctf.org/problem/28921/` (link) or http://jupiter.challenges.picoctf.org:28921

Steps



There is a catch with the rendering picobrowser

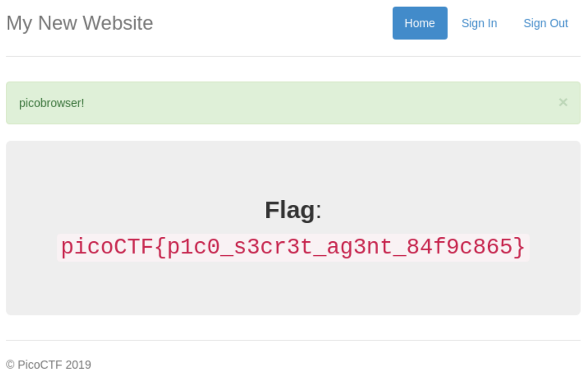
Press flag



You're not picobrowser! Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 OPR/107.0.0.0

Open burpsuite and in the request change the User-Agent :

```
GET /flag HTTP/1.1
Host: jupiter.challenges.picoctf.org:28921
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: picobrowser
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```



picobrowser!

Flag: picoCTF{p1c0_s3cr3t_ag3nt_84f9c865}

Flag

`picoCTF{p1c0_s3cr3t_ag`

✓ **flag**

picoCTF{p1c0_s3cr3t_ag3nt_84f9c865}

Intro to Burp picoCTF 2024

Intro to Burp picoCTF 2024

- Description
  - Hint
- Steps
  - Analyzing the first register
- Flag

Description

Summary

Additional details will be available after launching your challenge instance.
Try here to find the flag

Hint

> Try mangling the request, maybe their server-side code doesn't handle malformed requests very well.

Steps

Launch instance

Open burpsuite, try a registration, intercept the packet and send it to repeater

```
POST / HTTP/1.1
Host: titan.picoctf.net:61159
Content-Length: 190
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://titan.picoctf.net:61159
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.110
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Referer: http://titan.picoctf.net:61159/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=eyJjc3JmX3Rva2VuIjoiOGQ2MTk3MmMyZDhkZDA2ZWY2ZjIxZDViNzEzYWZjODA4YzMwMTVhNCJ9.ZfYhOQ.xT5p1x72GxB4j6segBTIk1-5ZME
Connection: close

csrf_token=IjhkNjE5NzJjMmQ4ZGQwNmVmNmYyMWQ1YjcxM2FmYzgwOGMzMDE1YTQi.ZfYhOQ.prA0wwqp47dRetEdsW9v-
RbyinE&full_name=admin&username=admin&phone_number=12828&city=cy&password=test&submit=Register
```

Analyzing the first register

```
csrf_token=IjhkNjE5NzJjMmQ4ZGQwNmVmNmYyMWQ1YjcxM2FmYzgwOGMzMDE1YTQi.ZfYhOQ.prA0wwqp47dRetEdsW9v-
RbyinE&full_name=admin&username=admin&phone_number=12828&city=cy&password=test&submit=Register
```

```
b64 IjhkNjE5NzJjMmQ4ZGQwNmVmNmYyMWQ1YjcxM2FmYzgwOGMzMDE1YTQi
```

```
"8d61972c2d8dd06ef6f21d5b713afc808c3015a4"
```

From the cookie session :

```
b64 eyJjc3JmX3Rva2VuIjoiOGQ2MTk3MmMyZDhkZDA2ZWY2ZjIxZDViNzEzYWZjODA4YzMwMTVhNCJ9
```

```
{"csrf_token":"8d61972c2d8dd06ef6f21d5b713afc808c3015a4"}
```

```
POST /dashboard HTTP/1.1
Host: titan.picoctf.net:61159
Content-Length: 4
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://titan.picoctf.net:61159
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.110
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Referer: http://titan.picoctf.net:61159/dashboard
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=.eJxVzEsOgyAUheG9MO6Al4jdDEHuJTUVMDxiTNO99zrs8HzJ-
T8sbP1iTxYu9mCh1eh6eWMmsWDEMssgwQJwg9FEKWBaZ6F8DJbboLiYvKZfHPvusk9INw9py2SlH3dEL0oLmodv7SwVyDq2fsurZHR5pBUrqZBWWuLRsP6lvj_rCjHw
.ZfYh9w.XrFCKH7cbVO3EOvePx_XGyLpwlg
Connection: close

otp=
```

Flag

Text

✓ **flag**

RevEng

Loot Stash

Loot Stash

- Description
- Steps
- Flag

Description

Summary

A giant stash of powerful weapons and gear have been dropped into the arena - but there's one item you have in mind. Can you filter through the stack to get to the one thing you really need?

Steps

```
strings stash | grep "HTB"
HTB{n33dl3_1n_a_l00t_stack}
```

Flag

`HTB{n33dl3_1n_a_l00t_s`

✓ flag

HTB{n33dl3_1n_a_l00t_stack}

Box Cutters

Box Cutters

- Description
- Steps
- Flag

Description

Summary

You've received a supply of valuable food and medicine from a generous sponsor. There's just one problem - the box is made of solid steel! Luckily, there's a dumb automated defense robot which you may be able to trick into opening the box for you - it's programmed to only attack things with the correct label.

Steps

```
ltrace ./cutter
open("HTB{tr4c1ng_th3_c4ll5}", 0, 00)                                                                      = -1
puts("[X] Error: Box Not Found"[X] Error: Box Not Found
)                                                                           = 25
+++ exited (status 0) +++
```

Flag

`HTB{tr4c1ng_th3_c4ll5}`

✓ flag

HTB{tr4c1ng_th3_c4ll5}

FactCheck

FactCheck

- Description

Description

📋 **Summary**

This binary is putting together some important piece of information... Can you uncover that information?Examine this file. Do you understand its inner workings?

Steps

```
file bin
```

```
bin: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2,
BuildID[sha1]=ba87dd5805704ffe3d15a1e136c290a83fe95dba, for GNU/Linux 3.2.0, not stripped
```

```
strings bin
```

```
GLIBC_2.4
GLIBC_2.2.5
u+UH
[]A\A]A^A_
picoCTF{wELF_d0N3_mate_
Hello
```

```
ida64 bin
```

```
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "picoCTF{wELF_d0N3_mate_", v3);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v23, "0", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "0", v4);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v24, "5", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "5", v5);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v25, "d", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "d", v6);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v26, "3", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "3", v7);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v27, "2", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "2", v8);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v28, "a", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "a", v9);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v29, "a", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "a", v10);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v30, "e", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "e", v11);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v31, "e", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "e", v12);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v32, "d", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "d", v13);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v33, "b", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "b", v14);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v34, "e", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "e", v15);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v35, "6", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "6", v16);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v36, "c", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "c", v17);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v37, "9", &v21);
  std::allocator<char>::~allocator(&v21);
  std::allocator<char>::allocator(&v21, "9", v18);
  std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(v38, "8", &v21);
```

```
05d32aaeedbe6c9
```

Converting to python

```
vim bin.py
```

```
def main():
    v22 = "picoCTF{wELF_d0N3_mate_"
    v23 = "0"
    v24 = "5"
    v25 = "d"
    v26 = "3"
    v27 = "2"
    v28 = "a"
    v29 = "a"
    v30 = "e"
    v31 = "e"
    v32 = "d"
    v33 = "b"
    v34 = "e"
    v35 = "6"
    v36 = "c"
    v37 = "9"
    v38 = "8"

    if ord(v24[0]) <= 65:
        v22 += v34
    if ord(v35[0]) != 65:
        v22 += v37
    if "Hello" == "World":  # This will always be False
        v22 += v25
    if ord(v26[0]) - ord(v30[0]) == 3:
        v22 += v26

    v22 += v25
    v22 += v28

    if ord(v29[0]) == 71:
        v22 += v29

    v22 += v27
    v22 += v36
    v22 += v23
    v22 += v31
    v22 += "}"

    print(v22)

if __name__ == "__main__":
    main()
```

```
picoCTF{wELF_d0N3_mate_e9da2c0e}
```

Flag

`picoCTF{wELF_d0N3_mate`

✓ **flag**

picoCTF{wELF_d0N3_mate_e9da2c0e}

GDB Test Drive

GDB Test Drive

- Description
- Steps
- Flag

Description

📋 **Summary**

Can you get the flag?Download this binary.Here's the test drive instructions:

- `$ chmod +x gdbme`
- `$ gdb gdbme`
- `(gdb) layout asm`
- `(gdb) break *(main+99)`
- `(gdb) run`
- `(gdb) jump *(main+104)`

Steps

```
0000| 0x7fffffffdb00 --> 0x7fffffffdc68 --> 0x7fffffffe032 ("/home/figaro/CTF/picoCTF/ReverseEngineering/GDB_Test_Drive/gdbme")
0008| 0x7fffffffdb08 --> 0x100000000
0016| 0x7fffffffdb10 --> 0x0
0024| 0x7fffffffdb18 --> 0x0
0032| 0x7fffffffdb20 ("A:4@r%uL5b3F88bC05C`Gb0fa35gbddN")
0040| 0x7fffffffdb28 ("5b3F88bC05C`Gb0fa35gbddN")
0048| 0x7fffffffdb30 ("05C`Gb0fa35gbddN")
0056| 0x7fffffffdb38 ("a35gbddN")
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
```

```
gdb-peda$ jump *(main+104)
Continuing at 0x55555555532f.
picoCTF{d3bugg3r_dr1v3_72bd8355}
[Inferior 1 (process 319338) exited normally]
Warning: not running
```

Flag

`picoCTF{d3bugg3r_dr1v3`

✓ **flag**

picoCTF{d3bugg3r_dr1v3_72bd8355}

Behind The Scenes

Behind The Scenes

- Description
- Steps
  - Explanation
- Flag

Description

📋 **Summary**

After struggling to secure our secret strings for a long time, we finally figured out the solution to our problem: Make decompilation harder. It should now be impossible to figure out how our programs work!

Steps

```
strings behindthescenes
```

```
/lib64/ld-linux-x86-64.so.2
libc.so.6
strncmp
puts
__stack_chk_fail
printf
strlen
```

```
sigemptyset
memset
sigaction
__cxa_finalize
__libc_start_main
GLIBC_2.4
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
./challenge <password>
> HTB{%s}
:*3$"
GCC: (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0
```

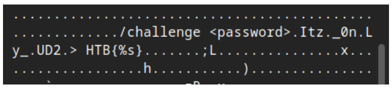
we can find what it wants us to pass

```
ltrace ./behindthescenes
```

```
--- SIGILL (Illegal instruction) ---
--- SIGILL (Illegal instruction) ---
./challenge <password>
--- SIGILL (Illegal instruction) ---
+++ exited (status 1) +++
```

We receive a SIGILL, which is a signal that the program tried to execute an illegal instruction. I'd like to see the program in hexeditor to reveal more information.

```
ghex behindthescenes
```



```
...........................................
............./challenge <password>.Itz._0n.L
y_.UD2.> HTB{%s}.......;L..............x...
...............h...........)..............
```

```
and the answer is after <password>
Itz_0nLy_UD2
```

```
./challenge <password>
```

Hacking/Tools/readelf

```
readelf -x .rodata ./behindthescenes
```

```
Hex dump of section '.rodata':
  0x00002000 01000200 2e2f6368 616c6c65 6e676520 ...../challenge
  0x00002010 3c706173 73776f72 643e0049 747a005f <password>.Itz._
  0x00002020 306e004c 795f0055 4432003e 20485442 0n.Ly_.UD2.> HTB
  0x00002030 7b25737d 0a00                       {%s}..
```

Explanation

ⓘ Info

-x <number or name>
--hex-dump=<\number or name>
Displays the contents of the indicated section as a
hexadecimal bytes. A number identifies a particular section
by index in the section table; any other string identifies
all sections with that name in the object file.

Flag

`HTB{Itz_0nLy_UD2}`

✓ flag

HTB{Itz_0nLy_UD2}

Reykjavik

Reykjavik

Description

Summary

Good beginning Reversing challenge - jump into gdb and start looking for the flag!

Steps

```
ls
```

```
Reykjavik      sources.zip.enc
Reykjavik.zip  readme
```

so we install gdb-peda

and then run it :

```
gdb --args Reykjavik CTFlearn{test}
```

```
gdb-peda$ start
gdb-peda$ disas
```

find the pointer of the memory that does the strcmp and break there

```
0x0000555555555168 <+200>:      call   0x555555555080 <strcmp@plt>
```

```
gdb-peda$ b *0x0000555555555168
Breakpoint 2 at 0x555555555168
```

```
gdb-peda$ r
```

```
Starting program: /home/figaro/CTF/ctflearn_com/Reverse_Engineering/Reykjavik/Reykjavik CTFlearn\{test\}
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Welcome to the CTFlearn Reversing Challenge Reykjavik v2: CTFlearn{test}
Compile Options: ${CMAKE_CXX_FLAGS} -O0 -fno-stack-protector -mno-sse


[----------------------------------registers-----------------------------------]
RAX: 0xffffff7d
RBX: 0x7fffffffdc78 --> 0x7fffffffe032 ("/home/figaro/CTF/ctflearn_com/Reverse_Engineering/Reykjavik/Reykjavik")
RCX: 0x16
RDX: 0x76304c5f6579457b ('{Eye_L0v')
RSI: 0x7fffffffe078 ("CTFlearn{test}")
RDI: 0x7fffffffdb30 ("CTFlearn{Eye_L0ve_Iceland_}")
RBP: 0x7fffffffe078 ("CTFlearn{test}")
RSP: 0x7fffffffdb30 ("CTFlearn{Eye_L0ve_Iceland_}")
RIP: 0x555555555168 (<main+200>:        call   0x555555555080 <strcmp@plt>)
R8 : 0x55555557a000
R9 : 0x73 ('s')
R10: 0x0
R11: 0x202
R12: 0x0
R13: 0x7fffffffdb30 ("CTFlearn{Eye_L0ve_Iceland_}")
R14: 0x0
R15: 0x7ffff7ffd020 --> 0x7ffff7ffe2f0 --> 0x555555554000 --> 0x10102464c457f
EFLAGS: 0x286 (carry PARITY adjust zero SIGN trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x55555555515a <main+186>:   movzx  eax,BYTE PTR [rip+0x2ec9]        # 0x55555555802a <data+26>
   0x555555555161 <main+193>:   xor    eax,0xffffffab
   0x555555555164 <main+196>:   mov    BYTE PTR [rsp+0x1a],al
=> 0x555555555168 <main+200>:   call   0x555555555080 <strcmp@plt>
   0x55555555516d <main+205>:   mov    r12d,eax
   0x555555555170 <main+208>:   test   eax,eax
   0x555555555172 <main+210>:   jne    0x555555555197 <main+247>
   0x555555555174 <main+212>:   mov    rdx,r13
No argument
[------------------------------------stack-------------------------------------]
0000| 0x7fffffffdb30 ("CTFlearn{Eye_L0ve_Iceland_}")
0008| 0x7fffffffdb38 ("{Eye_L0ve_Iceland_}")
0016| 0x7fffffffdb40 ("e_Iceland_}")
0024| 0x7fffffffdb48 --> 0x7fff007d5f64
0032| 0x7fffffffdb50 --> 0x2
0040| 0x7fffffffdb58 --> 0x0
0048| 0x7fffffffdb60 --> 0x7fffffffdc90 --> 0x7fffffffe087 ("SHELL=/usr/bin/bash")
0056| 0x7fffffffdb68 --> 0x7ffff7de124a (<__libc_start_call_main+122>:  mov    edi,eax)
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value

Breakpoint 2, 0x0000555555555168 in main ()
```

flag : CTFlearn{Eye*L0ve_Iceland*}

```
./Reykjavik CTFlearn{Eye_L0ve_Iceland_}
```

```
Welcome to the CTFlearn Reversing Challenge Reykjavik v2: CTFlearn{Eye_L0ve_Iceland_}
Compile Options: ${CMAKE_CXX_FLAGS} -O0 -fno-stack-protector -mno-sse

Congratulations, you found the flag!!: 'CTFlearn{Eye_L0ve_Iceland_}'
```

Alternative software

Cutter : for disassembly
But the libraries in parrot where fried so it couldn't work

yt source

Flag

`CTFlearn{Eye_L0ve_Icel`

✓ **flag**

CTFlearn{Eye_L0ve_Iceland_}