

# Alice's Online Bank CTF 2025 – Write-Up

Team: LAC (Tushig and Mughees)

Total Flags Submitted: 20

## Approach & Methodology

Our team used a mix of browser inspection, command-line tools, and web analysis techniques to find the hidden flags throughout Alice's Online Bank. The flags were hidden in many formats including plaintext, base64, and image metadata.

Key tools and techniques used:

- curl, wget — to crawl and download site resources
- exif, exiftool — to extract image metadata
- strings – to extract regular text file
- file, mv — to crawl into the file's data and move the file one to another
- echo — prints its arguments to the terminal, adding a newline by default.
- xxd -r -p — converts the hex stream back into raw bytes
- base64 — to decode encoded strings
- Browser DevTools — to inspect cookies, console logs, network requests, and local storage

## Flags Found

Each flag entry includes the flag, the location, and the method used to find it. Screenshots are also provided as requested.

1. **flag{cc54f1d3a59bc705dac3eafc372b3eb8b689dbfb5f61d40e98ab4efd8417ef70}**

*Location:* favicon link in HTML (<link rel="icon">)

*Method:* Crawled site with wget, inspected downloaded HTML



```
flag{
cc54f1d3a59bc705
dac3eafc372b3eb8
b689dbfb5f61d40e
98ab4efd8417ef70
}
```

2. **flag{e188f6aa6b006a3179a67e12205931cf3828a31b6b5aced30ac465230e37c17c}**

*Location:* main HTML body

*Method:* Viewed page source, found plaintext flag

```
<div class="has-text-centered">
  <div class="marquee">
    <span>
      flag{e188f6aa6b006a3179a67e12205931cf3828a31b6b5aced30ac465230e37c17c}
    </span> == $0
  </div>
  
</div>
</main>
</script>
```

3. **flag{2d1cc8bbe18c2648034e12f015924be0b0c1644974aa037cfb793e1b28a13cc1}**

*Location:* <meta name="description"> tag

*Method:* Inspected page <head> section

```
html lang="en">
<head>
  <style>
  </style>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta name="description" content="flag{2d1cc8bbe18c2648034e12f015924be0b0c164
4974aa037cfb793e1b28a13cc1}"> == $0
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bulma@1.0.2/css/bul
ma.min.css">
  <link rel="stylesheet" href="https://bulma.io/vendor/fontawesome-free-6.5.2-w
eb/css/all.min.css">
  <link rel="stylesheet" href="/static/style.css">
```

4. **flag{075e8b1a7a886c35c8e40e72fb7b1002459a83313378c08f3dd70b3f6d5992a1}**

*Location:* Browser cookies

*Method:* Inspected cookies using DevTools → Application tab

Name	Value	D...	Pa...	Ex...	Size	Ht...	Se...	Sa...	Pa...	Cr...
clicked	3	ali...	/	Se...	8					
flag	flag{075e8b1a7a886c35...	ali...	/	Se...	74					
session	eyJfZnJlc2giOmZhbnNlL...	ali...	/	Se...	138	✓				

**Cookie Value** ☐ Show URL-decoded  
flag{075e8b1a7a886c35c8e40e72fb7b1002459a83313378c08f3dd70b3f6d5992a1}

5. **flag{a4b4a0504fe7f3964d3b80880ed476bf6a655fb695d8f2130c84a8ed8048287d}**

*Location:* Alice's profile console output / HTML comment

*Method:* Opened browser console on profile page

```
</div>
▼ <div class="cell has-text-centered">
  ▶ <p>...</p>
  <!--
    flag{a4b4a0504fe7f3964d3b80880ed476bf6a655fb695d8f2130c84a8ed8048287d}
    -- remove before deployment!--> == $0
  </div>
  ▶ <div class="cell has-text-right">...</div>
</div>
```

6. **flag{08c3f4385bdc89e23c50c1248d1fa8621859c41cd465e70c06cd5cb41fb2de60}**

*Location:* Alice's Report 1

*Method:* Inspected report contents, used strings tool in bash

```
</div>
▼ <div class="cell has-text-centered">
  ▶ <p>...</p>
  <!--
    flag{a4b4a0504fe7f3964d3b80880ed476bf6a655fb695d8f2130c84a8ed8048287d}
    -- remove before deployment!--> == $0
  </div>
  ▶ <div class="cell has-text-right">...</div>
</div>
```

7. **flag{a90d4b57520e9078912adb829c5298a1d3c4f44f8d5f000742d5034cdcae83f7}**

*Location:* Alice's Report 2

*Method:* Joined ASCII fragments, then base64-decoded them

```
pipe> | base64 -d
Downloads awk '{ for(i=2; i<=9; i++) printf $i } END{print ""}' report2 \
| xxd -r -p \
| base64 -d
flag{a90d4b57520e9078912adb829c5298a1d3c4f44f8d5f000742d5034cdcae83f7}
Downloads
```

8. **flag{e2e823cb13094791323df44cc99a8af4776844032e51973340d858b38a47fdb8}**

*Location:* Alice's Report 3 (PDF)

*Method:* Opened and read using PDF viewer / extracted text, then base64-decoded

```
Downloads echo 'ZmxhZ3tIMmU4MjNjYjEzMDk0NzIxZGY0NGNjOTlhOGFmNDc3Njg0NDZm
mU1MTk3MzM0MGQ4NThiMzhhNDdmZGI4fQo=' \
| base64 -d
flag{e2e823cb13094791323df44cc99a8af4776844032e51973340d858b38a47fdb8}
```

9. **flag{c179387830d8cb1a1bf7dc190f4c28e6560041368c55b1a5d6d582fd85a8dbcc}**

*Location:* Alice's Report 4 (report4.bin)

*Method:* Renamed to .pdf, opened and extracted text (flag was in white color)



10. **flag{b11af07fe76d435b24c6673361489cebddb0262cd1a2669d1b477ce95fa904a4}**

*Location:* Profile picture of everyone, we can see it from the html

*Method:* console, and reverse

```
<div class="container">
  <div class="grid has-2-cols">
    <div class="container grid">
      <div class="cell">
         == $0
      </div>
    <div class="cell">⋮</div>
    <div class="cell"></div>
  </div>
</div>
```

11. **flag{522f0b8d2b1d82d44320b1311aba8da04e6906681b929425ec910a6fe1cabb31}**

*Location:* Bob's Report 5 (.hex file)

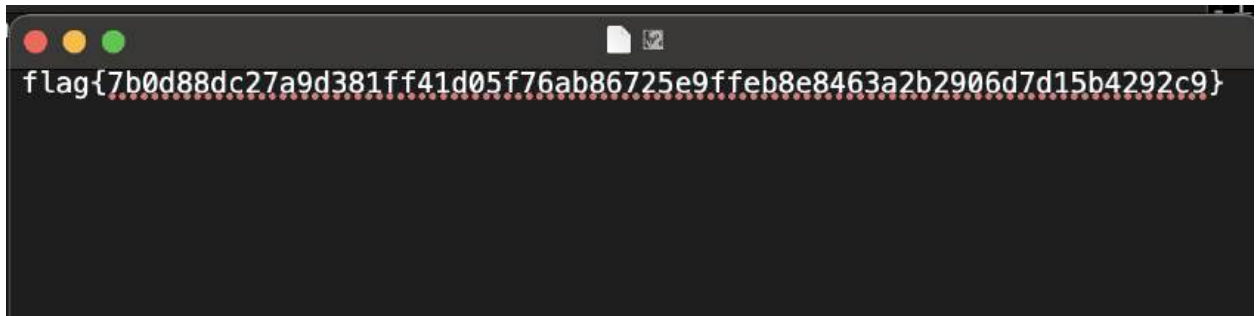
*Method:* Decoded hex with xxd / strings

```
decoded.txt — Edited
flag{522f0b8d2b1d82d44320b1311aba8da04e6906681b929425ec910a6fe1cabb31}
```

12. **flag{7b0d88dc27a9d381ff41d05f76ab86725e9ffeb8e8463a2b2906d7d15b4292c9}**

*Location:* Bob's Report 6

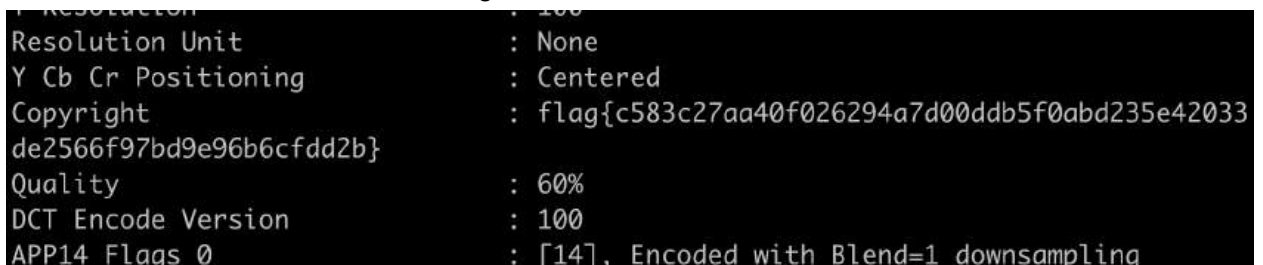
*Method:* Inspected report file directly



13. **flag{c583c27aa40f026294a7d00ddb5f0abd235e42033de2566f97bd9e96b6cfdd2b}**

*Location:* Bob's picture

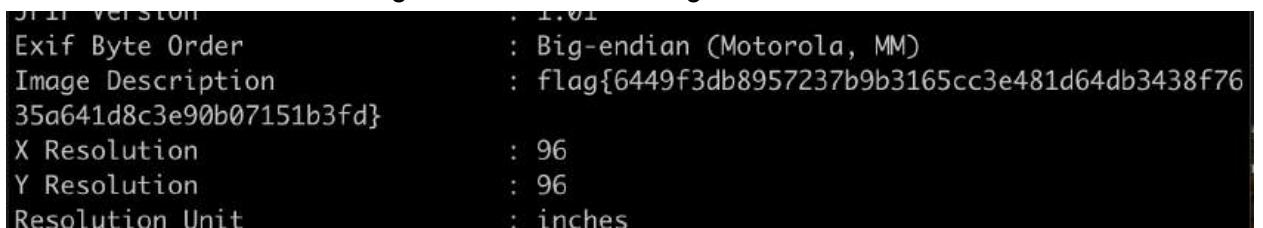
*Method:* Used exiftool to extract image metadata



14. **flag{6449f3db8957237b9b3165cc3e481d64db3438f7635a641d8c3e90b07151b3fd}**

*Location:* logo1.jpg

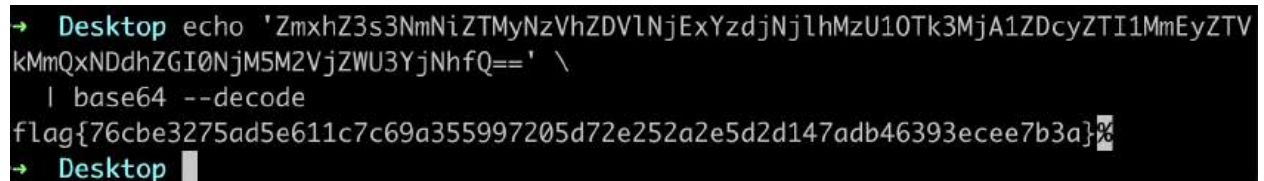
*Method:* Used exiftool or strings to extract hidden flag



15. **flag{76cbe3275ad5e611c7c69a355997205d72e252a2e5d2d147adb46393ecee7b3a}**

*Location:* Sign up button

*Method:* Clicked signup button multiple times; debug message revealed  
base64-encoded flag

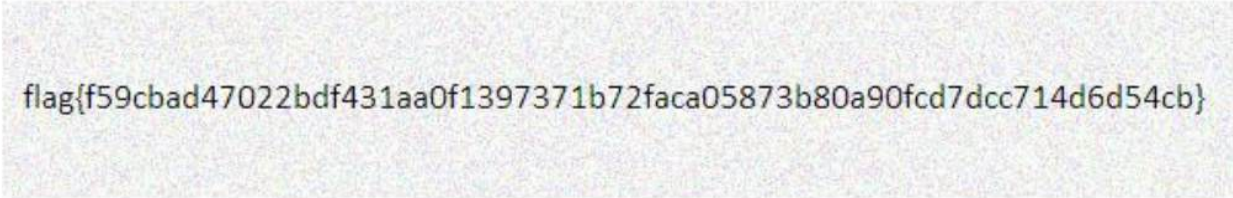




16. **flag{f59cbad47022bdf431aa0f1397371b72faca05873b80a90fcd7dcc714d6d54cb}**

*Location:* Trudy's Report 7

*Method:* Extracted the report and found flag in document body

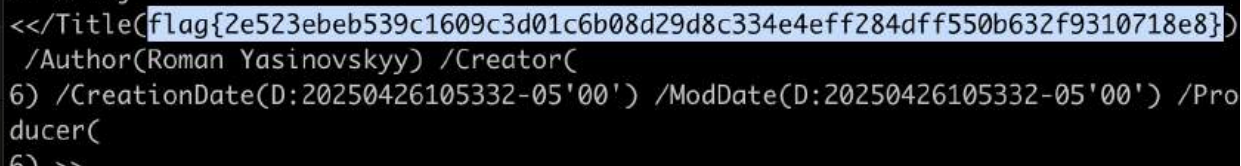


```
flag{f59cbad47022bdf431aa0f1397371b72faca05873b80a90fcd7dcc714d6d54cb}
```

17. **flag{2e523eb539c1609c3d01c6b08d29d8c334e4eff284dff550b632f9310718e8}**

*Location:* Trudy's Report 7 (second flag)

*Method:* Same file, found a second embedded flag, mv to pdf then you strings tool to find



```
<</Title(flag{2e523eb539c1609c3d01c6b08d29d8c334e4eff284dff550b632f9310718e8})  
/Author(Roman Yasinovskyy) /Creator(  
6) /CreationDate(D:20250426105332-05'00') /ModDate(D:20250426105332-05'00') /Pro  
ducer(  
6) >>
```

18. **flag{b28d0c42cd78e3d998942d0b77a07b365beeaecd8f28032478b489b9a57fe79b}**

*Location:* Trudy's secret

*Method:* When we log into trudy's profile, this flag will flash on the screen, and we also can find from the console

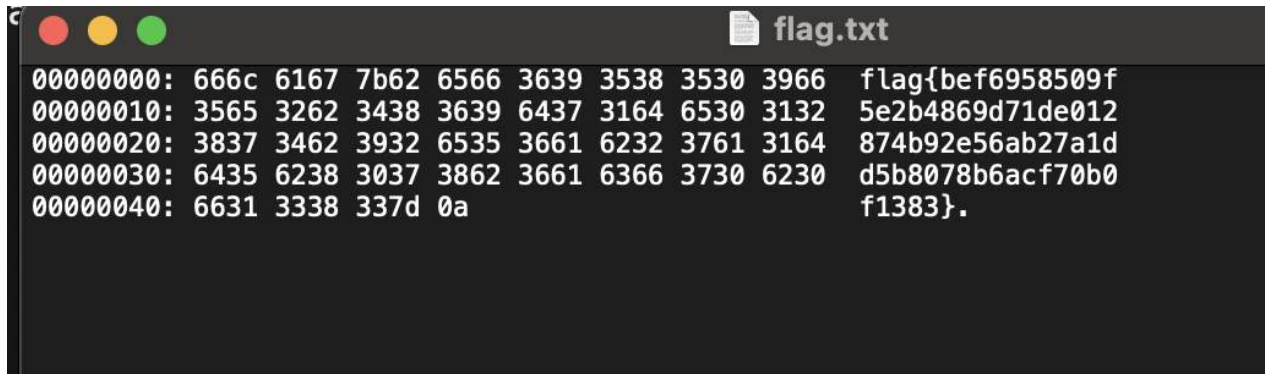


```
class= container >  
:t">flag{b28d0c42cd78e3d998942d0b77a07b365beeaecd8f28032478b
```

19. **flag{bef6958509f5e2b4869d71de012874b92e56ab27a1dd5b8078b6acf70b0f1383}**

*Location:* /admin → flag.bin

*Method:* Downloaded .bin file, mv the file into txt file and will find the flag



```
00000000: 666c 6167 7b62 6566 3639 3538 3530 3966 flag{bef6958509f
00000010: 3565 3262 3438 3639 6437 3164 6530 3132 5e2b4869d71de012
00000020: 3837 3462 3932 6535 3661 6232 3761 3164 874b92e56ab27a1d
00000030: 6435 6238 3037 3862 3661 6366 3730 6230 d5b8078b6acf70b0
00000040: 6631 3338 337d 0a f1383}.
```

20. **Flag{}** (forgot to document)

*Location:*

*Method:*