

# CTF Report: Extracting the Flag via Bookmarklet Execution

Ayoub Goubraim

September 9, 2025

## Abstract

This report presents the solution to the picoCTF challenge **Bookmarklet**. The challenge demonstrates how JavaScript bookmarklets can be used to obfuscate and later reveal sensitive information. By inspecting the code, copying it to the console, and executing it, we successfully retrieve the hidden flag.

## 1 Challenge Overview

The challenge introduces a bookmarklet that supposedly prints the flag when executed.

The screenshot shows the interface for the 'Bookmarklet' challenge on the picoCTF platform. At the top, the challenge title 'Bookmarklet' is displayed with a bookmark icon. Below the title, there are several tags: 'Easy', 'Web Exploitation', 'picoCTF 2024', 'obfuscation', 'browser\_webshell\_solvable', and 'browser'. The page is divided into two main sections. The left section, titled 'Description', contains the text: 'AUTHOR: JEFFERY JOHN', 'Why search for the flag when I can make a bookmarklet to print it for me?', and 'Additional details will be available after launching your challenge instance.' The right section contains the text: 'This challenge launches an instance on demand.', 'Its current status is: NOT\_RUNNING', and a 'Launch Instance' button. Below the description, there is a 'Hints' section with a question mark icon and three hint buttons labeled '1', '2', and '3'. At the bottom of the page, there is a '50,468 users solved' badge, a '93% Liked' badge, and a 'Submit Flag' button. A text input field at the bottom left contains the placeholder text 'picoCTF{FLAG}'.

Bookmarklet

Easy Web Exploitation picoCTF 2024 obfuscation browser\_webshell\_solvable browser

AUTHOR: JEFFERY JOHN

Description

Why search for the flag when I can make a bookmarklet to print it for me?

Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.

Its current status is: NOT\_RUNNING

Launch Instance

Hints ?

1 2 3

50,468 users solved

93% Liked

Submit Flag

picoCTF{FLAG}

Figure 1: Challenge statement for *Bookmarklet*.

## 2 Environment & Tools

- **OS:** Kali Linux
- **Browser:** Firefox Developer Tools

### 3 Reconnaissance

The website displays a simple page titled *flag distribution website*, containing a bookmarklet with obfuscated JavaScript code.

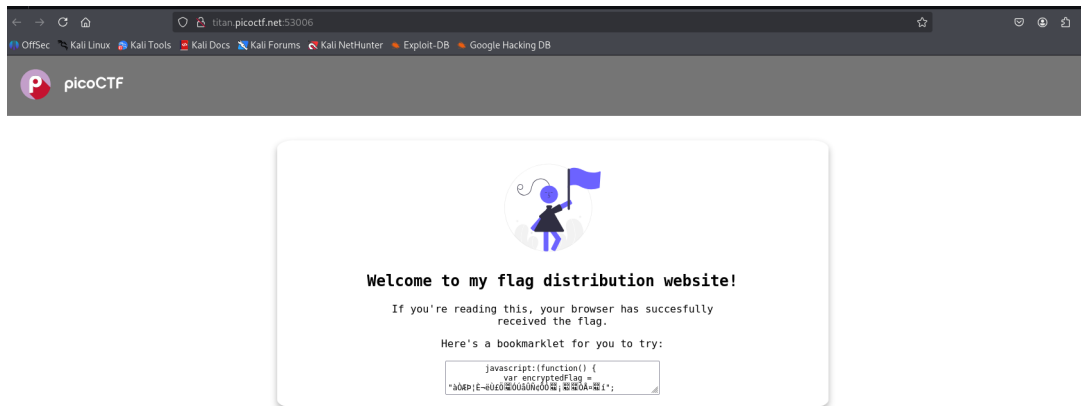


Figure 2: Homepage displaying the bookmarklet JavaScript code.

## 4 Inspecting the Bookmarklet Code

The HTML source contains a `textarea` with the bookmarklet code. This script defines an `encryptedFlag`, applies a simple cipher using the key “picocftf”, and finally alerts the decrypted flag.

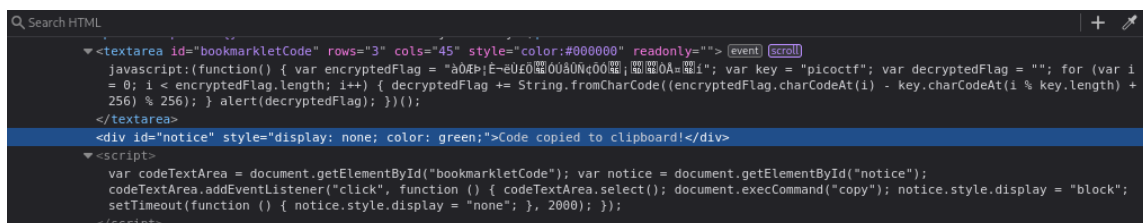


Figure 3: The obfuscated bookmarklet code found in the page source.

## 5 Executing the Code

Copying the bookmarklet code into the browser console and executing it runs the decryption loop and displays the flag.

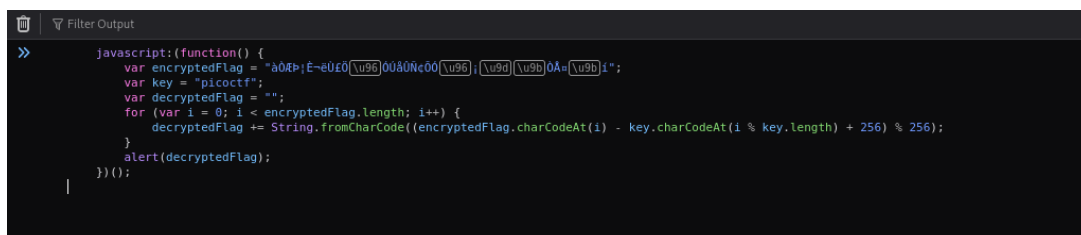


Figure 4: Executing the bookmarklet code in the browser console.

## 6 Results

The code execution triggers a JavaScript alert box displaying the flag.

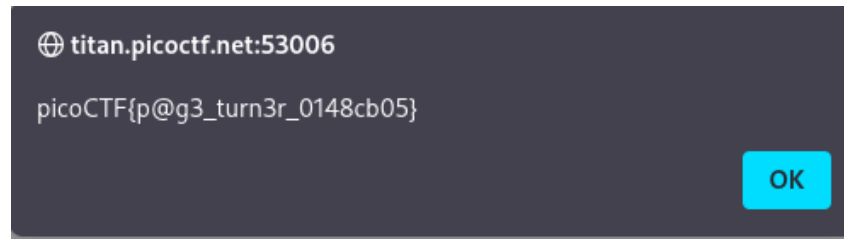


Figure 5: The decrypted flag displayed via alert.

The final flag is:

`picoCTF{p@g3_turn3r_0148cb05}`

## 7 Discussion & Takeaways

This challenge highlights:

- Bookmarklets can hide logic using obfuscation.
- Viewing and running JavaScript in the browser console is a useful inspection technique.
- Obfuscation is not encryption — client-side code should never contain sensitive secrets.

## 8 Conclusion

By analyzing and executing the provided bookmarklet, we successfully decrypted the hidden flag, completing the *Bookmarklet* challenge.