Guilherme Alt Chagas Merklein

PicoCTF 2024 - Web Exploitation

flag: picoCTF{p@g3_turn3r_1d1ba7e0}

26/03/2024

Bookmarklet

This one was very straightforward. I just clicked on the URL provided by picoCTF and went to a webpage that displayed some javascript code in the middle. The code had a *encryptedFlag* variable which was pretty self-explanatory, and it also had the function to decrypt the flag and display it via an alert. I made a quick webpage to run that javascript code using a html script tag, here's the photo of the page source.

```
<!DOCTYPE html>

<html>

    <body>

        <h1>My First Heading</h1>
        <p>My first paragraph.</p>

    </body>


    <script>
        var encryptedFlag = "àÒÆÞ¦È¬ëÙ£ÖÐÓÚåÛÑ¢ÕÓÐÓÇ¡Ð¥Ìí";
        var key = "picoctf";
        var decryptedFlag = "";
        for (var i = 0; i < encryptedFlag.length; i++) {
            decryptedFlag += String.fromCharCode((encryptedFlag.charCodeAt(i) - key.charCodeAt(i % key.length) + 256) % 256);
        }
        alert(decryptedFlag);
    </script>

</html>
```

Image 1: index.html.

Saved this and opened it on my browser. As expected, it revealed the flag.

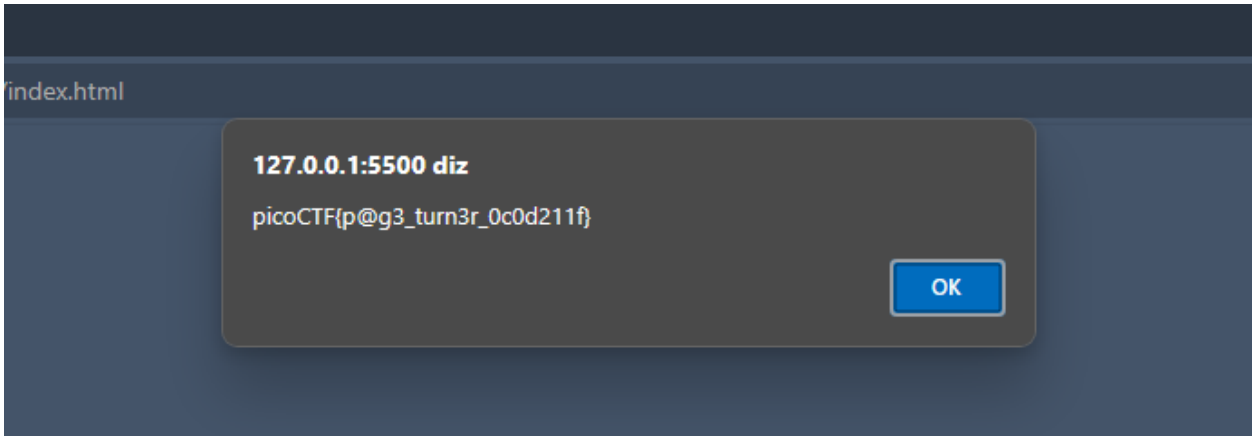

Image 2: flag.