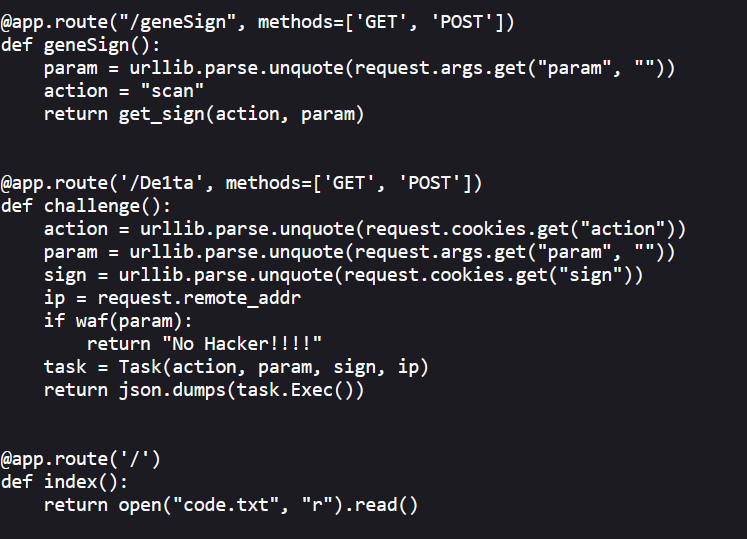
# ISCC2024 WriteUp

### AB\_C 刘子博 3627634696@qq.com

### 练武题

### 解题思路

1.阅读源码发现三个路由



/路由是让我们读取到该源码的

/geneSign：为给定的参数生成签名。

/De1ta：主要端点，根据 cookies 和参数处理任务。

Exec函数执行逻辑

如果 action 包含 "scan"：

调用 scan 函数，传入 param，获取扫描结果。

如果扫描结果为 "Connection Timeout"，将其设置为 result 的 data，并设置状态码为 200。

如果 action 包含 "read"：

调用 read\_from\_file 方法，读取文件内容。

设置 result 的 data 为读取到的文件内容，并设置状态码为 200。

如果 action 既不包含 "scan" 也不包含 "read"：

设置 result 的 data 为 "Action Error"。

scan这个方法，访问param并将其内容的前50个字母返回回来，我们构造param

但是/geneSign路由规定了action=scan，Exec方法中action必须有read和scan构造传入param=flag.txtread

得到sign值: 3d561e076ab1d02b00272eab7723e793利用scan方法来读取flag.txt的内容。

def get\_sign(action, param):  
 return hashlib.md5(secret\_key + param.encode('latin1') + action.encode('latin1')).hexdigest()

所以param=flag.txtreadscan

访问/De1ta

