New issue

Jump to bottom

koa2-blog v1.0.0 sql injection vulnerability #40

Closed jiguangsdf opened this issue on Nov 28, 2019 · 0 comments

jiguangsdf commented on Nov 28, 2019 • edited

A sql injection was discovered in koa2-blog 1.0.0 .There is a sql injection vulnerability which allows remote attackers to Injecting a malicious SQL statement into a server via:

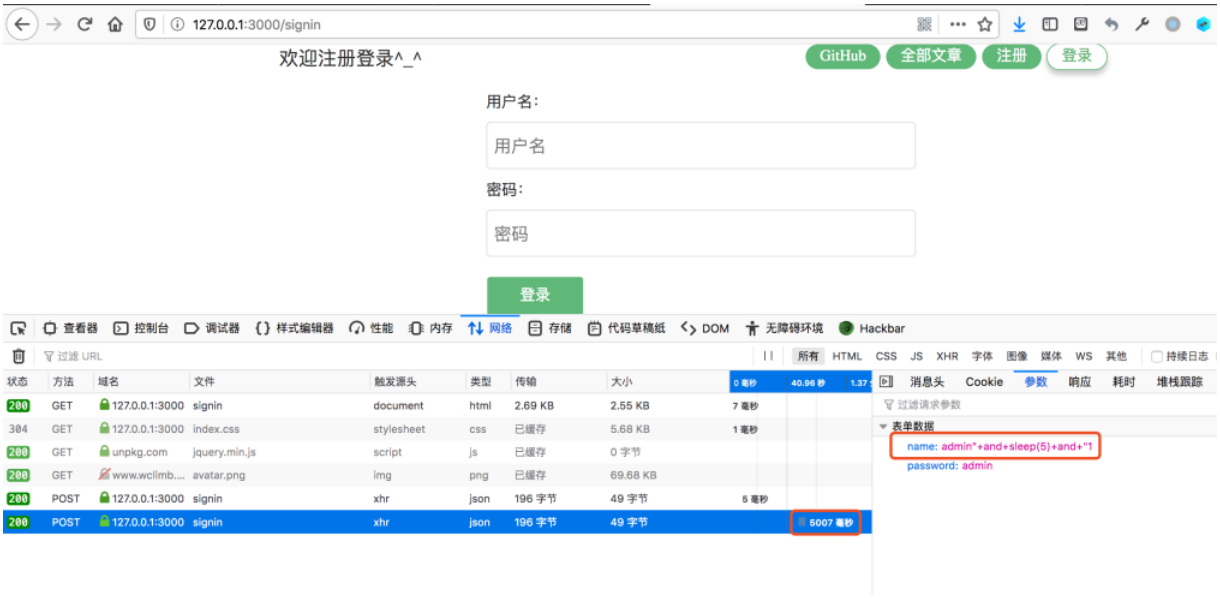
```
post http://127.0.0.1:3000/signin
```

Vulnerability code

```
// 通过名字查找用户
exports.findDataByName =  ( name ) => {
  let _sql = `select * from users where name="${name}";`
  return query( _sql)
}
```

POC

Trigger SQL injection vulnerability by signin,we can see that the injected statement executed successfully and the page response timed out for 5S



wclimb closed this as completed on Nov 30, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants