

New issue

[Jump to bottom](#)

cscms demourl:http://demo.chshcms.com/ login have UserTraversal-Vulnerability #5

[Open](#) wind-cyber opened this issue on Nov 14, 2019 · 0 comments

wind-cyber commented on Nov 14, 2019

cscmsV4.0-4.1 demourl:<http://demo.chshcms.com/>

In the user login box Sign in now without a verification code and prompt that the user does not exist , which makes it easier for remote attackers to hijack accounts via a brute-force approach.

Capture the packet in burp to truncate the current request the current data packet sent to the intruder module, identification "username" used to traverse account information; Select the dictionary for the account name to open the attack

13	AiDongYe	200	<input type="checkbox"/>	<input type="checkbox"/>	695
15	11111	200	<input type="checkbox"/>	<input type="checkbox"/>	695
18	11	200	<input type="checkbox"/>	<input type="checkbox"/>	695
19	1	200	<input type="checkbox"/>	<input type="checkbox"/>	695
16	1111	200	<input type="checkbox"/>	<input type="checkbox"/>	918
1	test	200	<input type="checkbox"/>	<input type="checkbox"/>	920

Request Response

Raw Headers Hex

Content-Type: text/html; charset=gbk
Content-Length: 157

```
jQuery191045372158637728643_1573776730060({"error":0,"info":":\u60a8\u7684\u5e10\u53f7\u4e0d\u5b58\u5728","msg":":\u60a8\u7684\u5e10\u53f7\u4e0d\u5b58\u5728"})
```

Successful login account

1111 Lv. 1 ♂[签到领金币](#)

1	74	1
关注	人气	粉丝

会员类型: 普通会员 会员级别: 注册会员 [升级](#)剩余金币: 0 个 [充值](#) 剩余金钱: 0.00 元 [兑换](#)空间地址: <http://demo.chshcms.com/1111/home>当前经验: 96.25%

综合管理

最新动态

我的说说

我的消息

我的留言

粉丝关注

发布说说

发一条说说, 让大家知道你在做什么...

140

表情

[发布](#)

全站动态

我的动态

好友动态

This is a prompt password error

17	111	200	<input type="checkbox"/>	<input type="checkbox"/>	683
20	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	683
21	admin1	200	<input type="checkbox"/>	<input type="checkbox"/>	683
13	AiDongYe	200	<input type="checkbox"/>	<input type="checkbox"/>	695
15	11111	200	<input type="checkbox"/>	<input type="checkbox"/>	695
18	11	200	<input type="checkbox"/>	<input type="checkbox"/>	695
19	1	200	<input type="checkbox"/>	<input type="checkbox"/>	695
16	1111	200	<input type="checkbox"/>	<input type="checkbox"/>	918
1	test	200	<input type="checkbox"/>	<input type="checkbox"/>	920

RequestResponse

RawHeadersHex

Content-Type: text/html; charset=gbk
Content-Length: 145

jQuery191045372158637728643_1573776730060({"error":0,"info":"\u60a8\u7684\u5bc6\u7801\u9519\u8bef","msg":"

This is the prompt that the account does not exist.

19	1	200	<input type="checkbox"/>	<input type="checkbox"/>	695
16	1111	200	<input type="checkbox"/>	<input type="checkbox"/>	918
1	test	200	<input type="checkbox"/>	<input type="checkbox"/>	920

RequestResponse

RawHeadersHex

Content-Type: text/html; charset=gbk
Content-Length: 157

jQuery191045372158637728643_1573776730060({"error":0,"info":"\u60a8\u7684\u5e10\u53f7\u4e0d\u5b58\u5728\u7cf5\u60a8\u7684\u5e10\u53f7\u4e0d\u5b58\u5728"})

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

