New issue

Jump to bottom

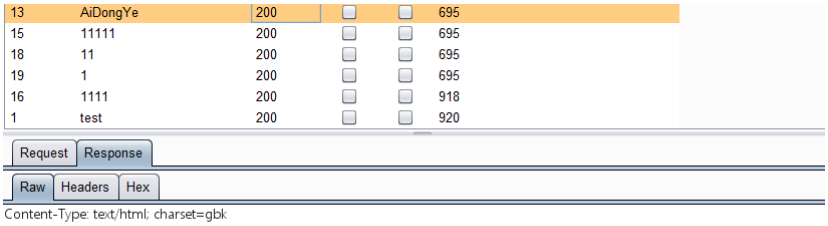
cscms demourl:http://demo.chshcms.com/ login have UserTraversal-Vulnerability #5

Open **wind-cyber** opened this issue on Nov 14, 2019 · 0 comments

wind-cyber commented on Nov 14, 2019

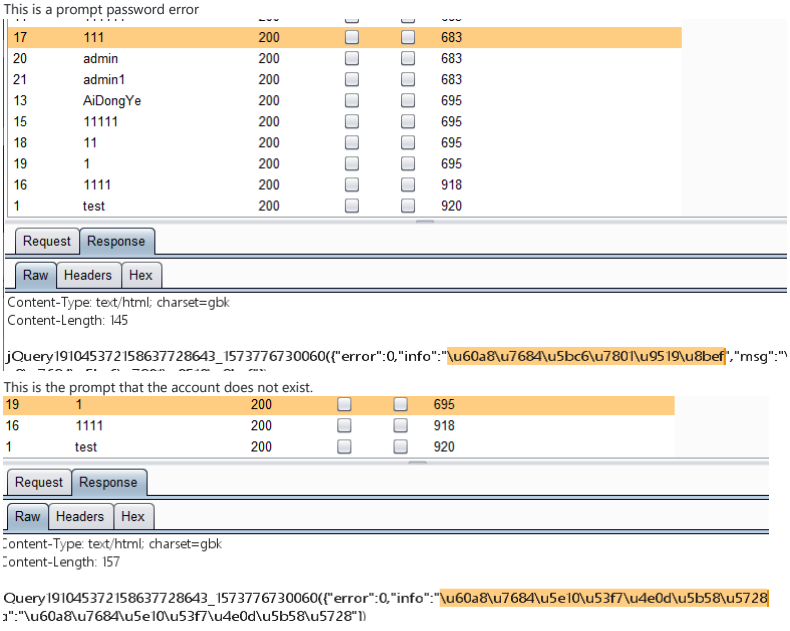
cscmsV4.0-4.1 demourl:http://demo.chshcms.com/
In the user login box Sign in now without a verification code and prompt that the user does not exist， which makes it easier for remote attackers to hijack accounts via a brute-force approach.

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



Successful login account

This is a prompt password error



This is the prompt that the account does not exist.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant