New issue

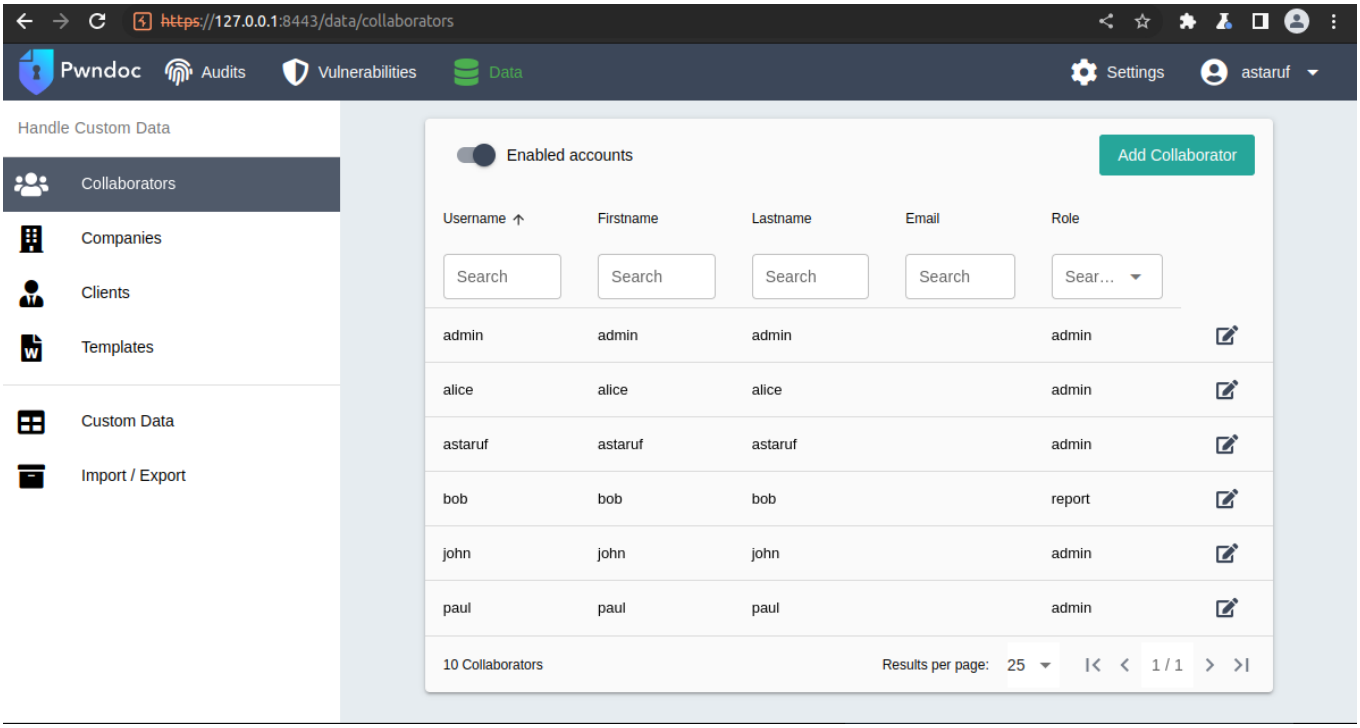
Jump to bottom

# (Vulnerability) Username enumeration via response timing #381

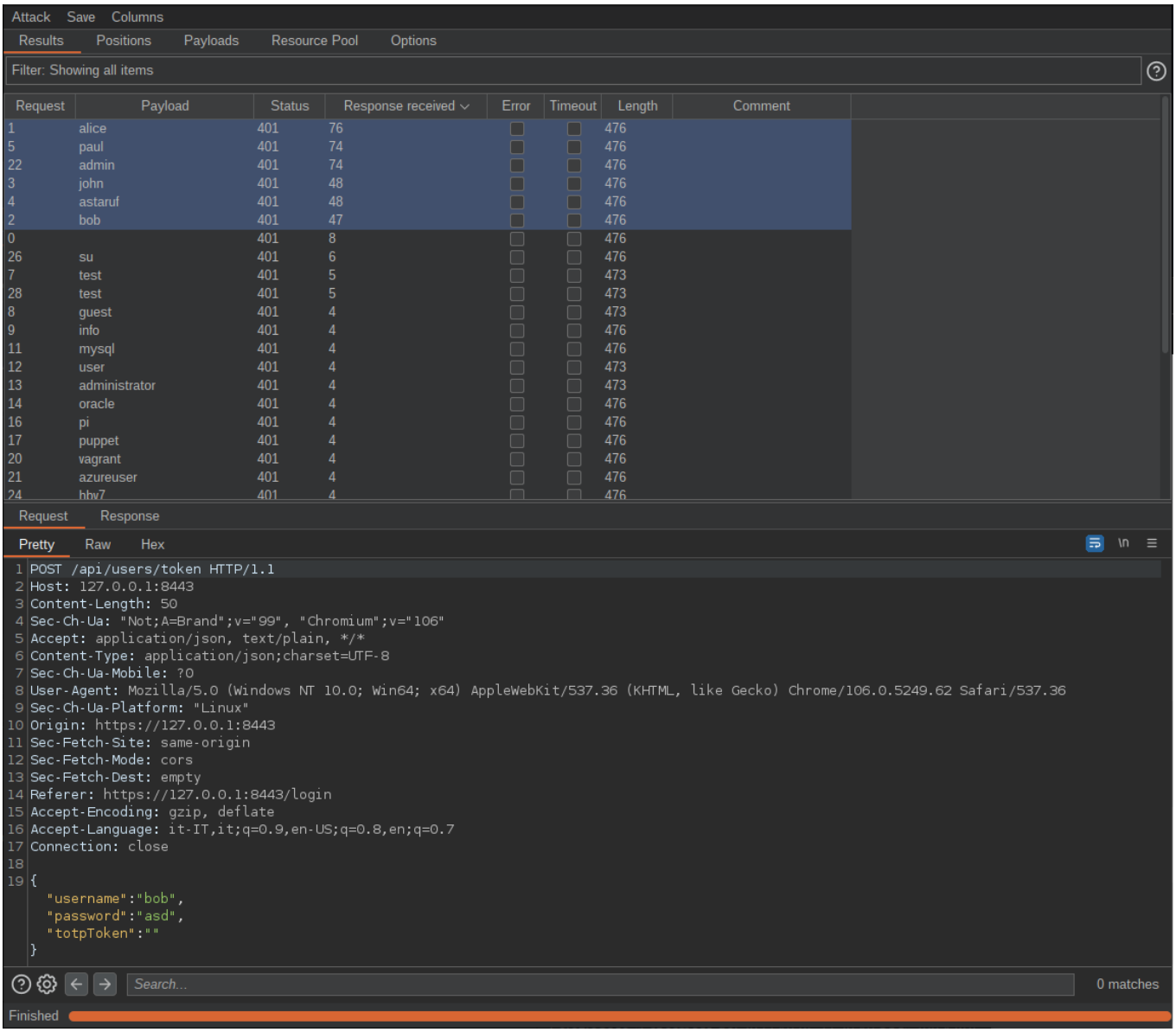
Open **Astaruf** opened this issue on Oct 24 · 1 comment

**Astaruf** commented on Oct 24 • edited

It is possible to enumerate users registered in PwnDoc (tested on 0.5.3 - 2022-07-19 and previous versions) observing the web server response timing.
For example, let's suppose these users were registered on PwnDoc:




By performing a brute force dictionary attack, a defined list of users can be provided via login POST request to detect the server's response time.




All the valid users can be discovered by a potential attacker checking if the response time to the login request is long. For not-existing users we can see a shorter response time.

The attack success depends higly on the stability of the server and the Internet connection between hosts. In any case, in order to apply a remediation, it is advisable to add a timing delay to balance the response timing for each login request.

Let me know if I can help you in any way so, once fixed I would like to get a CVE from mtre.org

**Astaruf** changed the title ~~Username enumeration via response timing~~ **(Vulnerability) Username enumeration via response timing** last month

**Astaruf** commented 26 days ago — Author

A CVE-ID has been reserved by Mitre.org for this vulnerability CVE-2022-44022.

🚀 1

**Assignees**

No one assigned

**Labels**

None yet

**Projects**

None yet

**Milestone**

No milestone

**Development**

No branches or pull requests

**1 participant**