תיאור מפורט כיצד הקמתם את הפרויקט ואת המכונה )כל

פקודה ופקודה או שלב שבצעתם כדי להגיע למכונה עובדת(.

שימו לב שבקובץ זה יש לציין קישורים בהם נעזרתם - מידע נוסף תחת "אתיקה" – באם אין קישורים כאלו יש

לציין במקום בולט בתחילת הקובץ "אין קישורים שנעזרנו בהם"

הרעיון:

את הרעיונות קיבלנו משוטטות באינטרנט ואחרי שראינו כל אחד הרבה רעיונות כל אחד תרם את חלקו.

חלק ראשון:

את החלק הזה אני לא זוכר איפה ראיתי אבל ראיתי איזה רעיון של לעשות api שישאר פתוח הכתובת של הרישום אך בפרונט יהיה כתוב שההרשמה נסגרה והקוד יהיה ב comment out.

מכיוון שחלקנו מתעסק בפיתוח ווב, לקחנו איזה תבנית בסיס מהקישור הנ"ל:

<https://medium.com/swlh/jwt-authentication-authorization-in-nodejs-express-mongodb-rest-apis-2019-ad14ec818122>

ועליה עבדנו.

הנ"ל הינו api בסיס שמריץ שרת node js.

הוספנו כתובות ל api, שינינו את צורת הקריאה של האובייקט כך שיתאים ל axios (החבילה שעושה את ה post), שינינו את שיטת ה hashing של הסיסמה, שינינו טיפה את הצורה של היוזר' הוספנו שרת web שרץ כפרונט כאשר צד הפרונט נכתב from scratch.

להן הוראות להקמת המערכת:

1. Install ubuntu desktop 18.04 image on the vm
2. Install node js by this manual:  
   <https://www.digitalocean.com/community/tutorials/how-to-install-noade-js-on-ubuntu-18-04>
3. Download and unzip from:  
   <https://medium.com/swlh/jwt-authentication-authorization-in-nodejs-express-mongodb-rest-apis-2019-ad14ec818122>
4. Run ‘npm install’ in the main folder (all the dependencies will be installed)
5. כאן הוספנו קוד, שינינו קוד, הוספנו שרת ווב שרץ על הנוד - הכל נמצא בתיקיה של הקבצים
6. רץ שרת בקאנד בכתובת:  
   127.0.0.1:3000
7. רץ שרת הפרונט בכתובת:  
   127.0.0.1:8080
8. ה db רץ ב atlas mongodb על יוזר וסיסמה פרטיים שלי (אם נחוץ, אתן אותם, למרות שניתן למשוך את כל ה data שזה היוזרים דרך הפירצה שצריכים לגלות).
9. הגדרת יוזרים

user : [aidenpearce@mail.com](mailto:aidenpearce@mail.com) pass : windycity

User : [damian@mail.com](mailto:damian@mail.com) pass : evillaugh

* **הפיכת app.js לservice שרץ ברקע**

ליצור קובץ

/etc/systemd/system/ctos.service

עם התוכן

[Unit]

Description=Node.js ctOS Http Server

[Service]

PIDFile=/tmp/ctOS-99.pid

User=ctos

Group=root

Restart=always

StartLimitIntervalSec=5

KillSignal=SIGQUIT

WorkingDirectory=/home/ctos/user-registration-api/src

ExecStart=/usr/local/bin/node /home/ctos/user-registration-api/src/app.js

[Install]

WantedBy=multi-user.target

כדי לאפשר את הservice

systemctl daemon-reload

systemctl enable myapp

systemctl restart myapp

* **התקנת vsftpd**

[**https://www.howtoforge.com/tutorial/ubuntu-vsftpd/**](https://www.howtoforge.com/tutorial/ubuntu-vsftpd/)

sudo apt-get install vsftpd

# systemctl start vsftpd

# systemctl enable vsftpd

sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig

sudo nano /etc/vsftpd.conf

בקובץ /etc/vsftpd.conf צריך להוסיף

# Allow anonymous FTP? (Disabled by default).

anonymous\_enable=YES

#

# Point users at the directory we created earlier.

anon\_root=/var/ftp/

#

# Stop prompting for a password on the command line.

no\_anon\_password=YES

#

# Show the user and group as ftp:ftp, regardless of the owner.

hide\_ids=YES

#

# Limit the range of ports that can be used for passive FTP

pasv\_min\_port=40000

pasv\_max\_port=50000

לאחר מכן

sudo systemctl restart vsftpd

$ sudo useradd -m -c "damian" -s /bin/bash damian

$ sudo passwd damian

ולהקיש evillaugh פעמיים לקביעת סיסמה

ליצור תיקייה

/home/damian/ftp

ליצור בתוכה קובץ flag.txt עם התוכן

Flag\_no\_2\_########

להוריד קובץ dictionary מהאתר <https://thehacktoday.com/password-cracking-dictionarys-download-for-free/>

ולשתול בו את הסיסמה supercalifragilisticexpialidocious. לשמור בשם ctos בתיקיית ftpשל damian

* **התקנת SSH**

[**https://linuxize.com/post/how-to-enable-ssh-on-ubuntu-18-04/**](https://linuxize.com/post/how-to-enable-ssh-on-ubuntu-18-04/)

sudo apt install openssh-server

sudo cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.original

sudo chmod a-w /etc/ssh/sshd\_config.original

sudo systemctl restart sshd.service

התחברות כroot באמצעות היוזר ctos והסיסמא supercalifragilisticexpialidocious

יצירת תיקייה

/root/almostthere

ובתוכה קובץ congrats.txt עם התוכן

Flag\_no\_3\_b7BJX56Lahw2z3Wj

* **שינוי שם המכונה בקבצים**

sudo nano /etc/hostname

sudo nano /etc/hosts

לשם ctOS

* **ביטול GUI**

sudo systemctl set-default multi-user.target

* **ולסיום**

reboot