

**פרוייקט במעבדה מתקדמת
באבטחת רשתות תקשורת מחשבים
מרצה: מר וולך נדב**

מגישים:

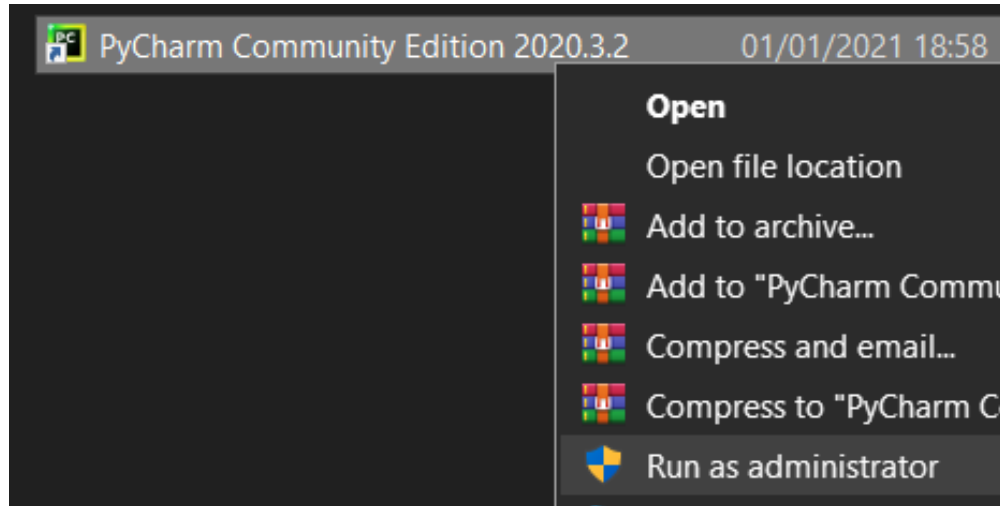
**שם מלא: מוסקוביץ אורי
ת"ז: 312483977**

**שם מלא: בן אהרון דניאל
ת"ז: 206282519**

**שם מלא: ספקטור שקד
ת"ז: 308132281**

**שם מלא: מועלם ג'ון
ת"ז: 315837872**

הערות:



הרצת Pycharm צריכה להתבצע **בהרשאת Administrator**, כיוון שבמתודת DDOS, אנחנו מבצעים ניקיון של Socket-ים דרך CMD, כך שתתאפשר הרצה מחודשת עבור Port זהה לזה שהחזן בהרצה הראשונה, אחרת Port נותר לא זמין אף על פי שהחיבור סגור, למיטב הבנתנו הדבר נגרם מסוג Socket בעת האתחול, אך גם בשינוי ההגדרות, עדיין התקבלה שגיאה כי Port עדיין בשימוש.

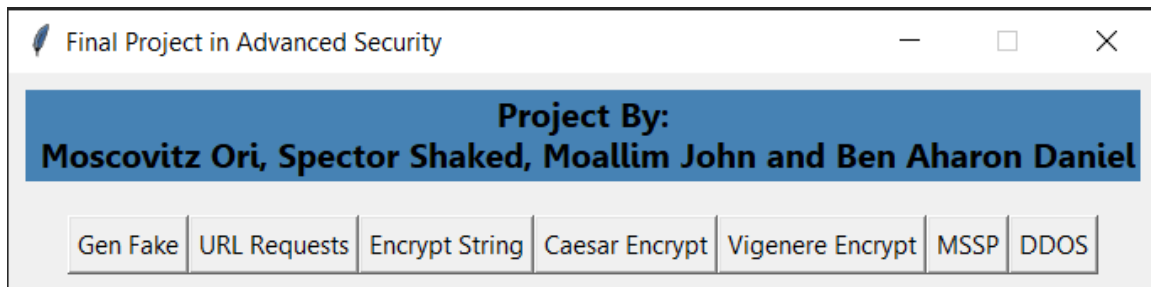
בפתיחה רגילה של Pycharm, הכל יעבוד תקין אך בחלון מתקפת DDOS, בעת לחיצה על Restart תוצג הודעה:

The requested operation requires elevation (Run as administrator).

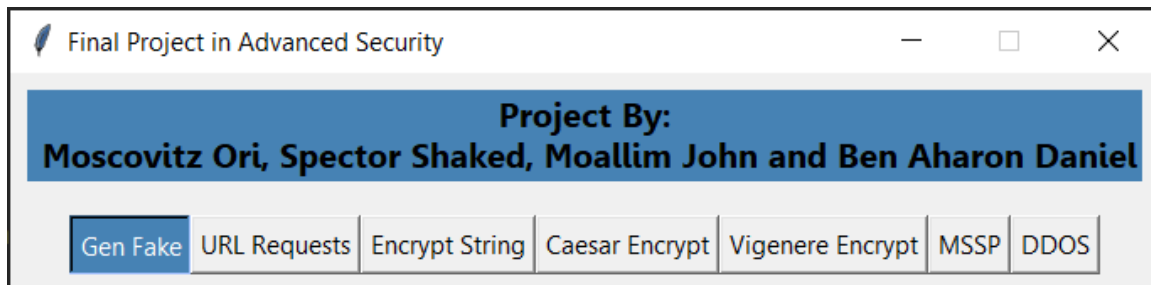
רקע:

הפרויקט בנוי מ-GUI ראשי, בו נמצאות כל האפשרויות אותן התבקשנו לממש. האיתחול ל-GUI הראשי מתבצע על ידי הפונקציה InitMainWin, המאתחלת את החלון ומוסיפה אליו את הכפתורים בקריאה ל-AddMainButtons.

```
# initialize main window
def InitMainWin(root):
    ClearFrame(root)
    root.resizable(0, 0)
    root.eval('tk::PlaceWindow . center')
    mainFrame = Frame(root, bd=10)
    mainFrame.grid()
    upperFrame = Frame(root, bd=10)
    upperFrame.grid(row=0, column=0)
    # Label of project collaborators
    Label(upperFrame, text=names, font=("Gisha bold", 12), bg='steelblue').grid(row=0, column=0)
    lowerFrame = Frame(root, bd=10)
    lowerFrame.grid(row=1, column=0)
    # Adding all options to menu
    AddMainButtons(lowerFrame)
    root.title('Final Project in Advanced Security')
    root.mainloop()
```



כמו גם, דאגנו לחיווי בעת לחיצה:



מחלון זה, ניתן לגשת לכל פונקציה וכן לחזור לחלון הראשי בכל עת, כעת נתבונן בכל אחת מן הפונקציות.

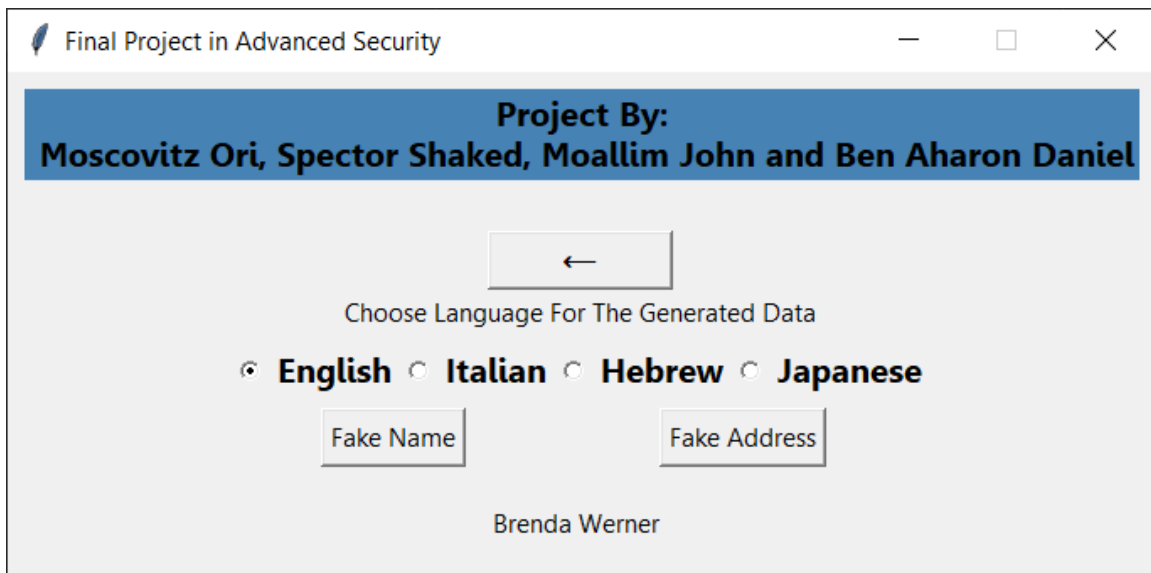
יצירת נתונים מזויפים:

בבחירת שפה כלשהי (כאשר אנגלית מוגדרת כברירת המחדל), ולחיצה על אחד מהכפתורים, תוצג המחרוזת המזויפת המתאימה.



The screenshot shows a window titled "Final Project in Advanced Security". At the top, a blue banner reads "Project By: Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel". Below this is a button with a left arrow. Underneath is the text "Choose Language For The Generated Data". There are four radio buttons: "English" (selected), "Italian", "Hebrew", and "Japanese". Below the radio buttons are two input fields labeled "Fake Name" and "Fake Address".

דוגמה לשם מזויף באנגלית:



This screenshot is identical to the previous one, but with the text "Brenda Werner" displayed at the bottom of the window, below the "Fake Name" and "Fake Address" fields.

דוגמה לכתובת מזויפת באנגלית:

Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

←

Choose Language For The Generated Data

☒ English ☐ Italian ☐ Hebrew ☐ Japanese

Fake Name Fake Address

Unit 5587 Box 8905
DPO AP 36649

ובאופן זה ניתן לראות את התוצאה עבור כל שפה ואפשרות

Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

←

Choose Language For The Generated Data

☐ English ☐ Italian ☒ Hebrew ☐ Japanese

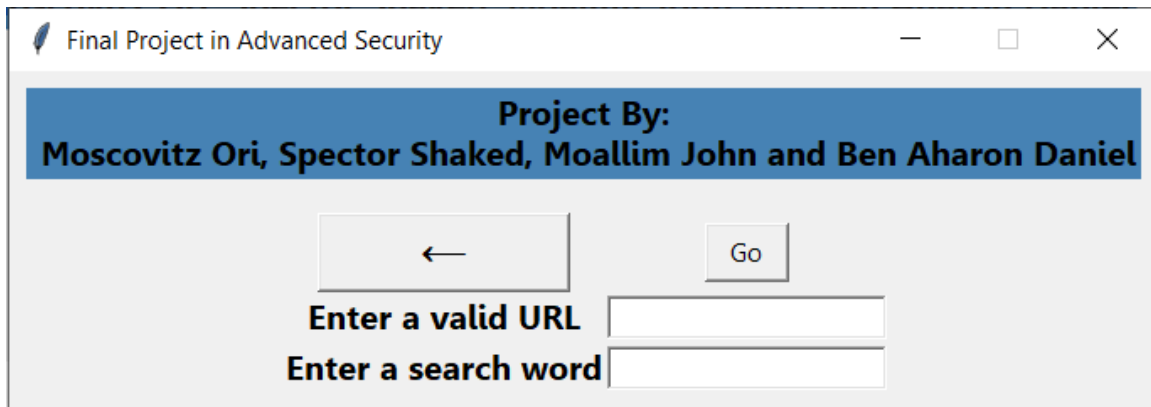
Fake Name Fake Address

פרופ' בירק יהודית 61, אודם, 3020742

כעת נחזור לתפריט הראשי ע"י לחיצה על החץ העליון.

הדפסת קוד מקור ומיקומי מילת חיפוש:

בבחירת URL Requests מן התפריט הראשי נגיע לחלון הבא:



Final Project in Advanced Security

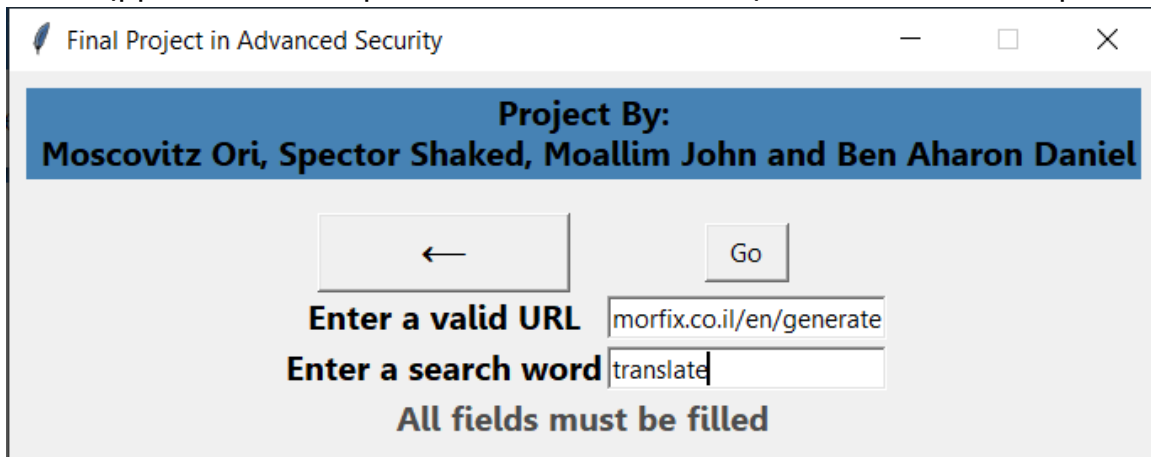
Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

← Go

Enter a valid URL

Enter a search word

בהינתן כתובת URL ומילה (ולאחר וולידציה שאינם ריקים ושהURL תקין):



Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

← Go

Enter a valid URL

Enter a search word

All fields must be filled

נגיע למסך הנ"ל, אשר מציג את טקסט המקור (כך שניתן לגלול לאורכו) וכמובן מציג את המילה ואת המיקומים בה היא נמצאה.

Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

Back

"translate" has been found in position:
6229,352166,357114,
<Scroll for viewing>

```
<!DOCTYPE html>
<html itemscope itemtype="http://schema.org/Thing">
<head>
  <!-- Facebook Pixel Code -->
  <script>
    !function (f, b, e, v, n, t, s) {
      if (f.fbq) return; n = f.fbq = function
() {
        n.callMethod ?
          n.callMethod.apply(n, arguments)
        : n.queue.push(arguments)
      };
      if (!f._fbq) f._fbq = n; n.push = n; n.l
oaded = !0; n.version = '2.0';
      n.queue = []; t = b.createElement(e); t.
async = !0;
      t.src = v; s = b.getElementsByTagName(e)
[0];
      s.parentNode.insertBefore(t, s)
    }(window, document, 'script',
      'https://connect.facebook.net/en_US/fbev
ents.js');
      fbq('init', '543147059155097');
```

במידה והמילה לא קיימת, תוצג הודעה מתאימה:

Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

Back

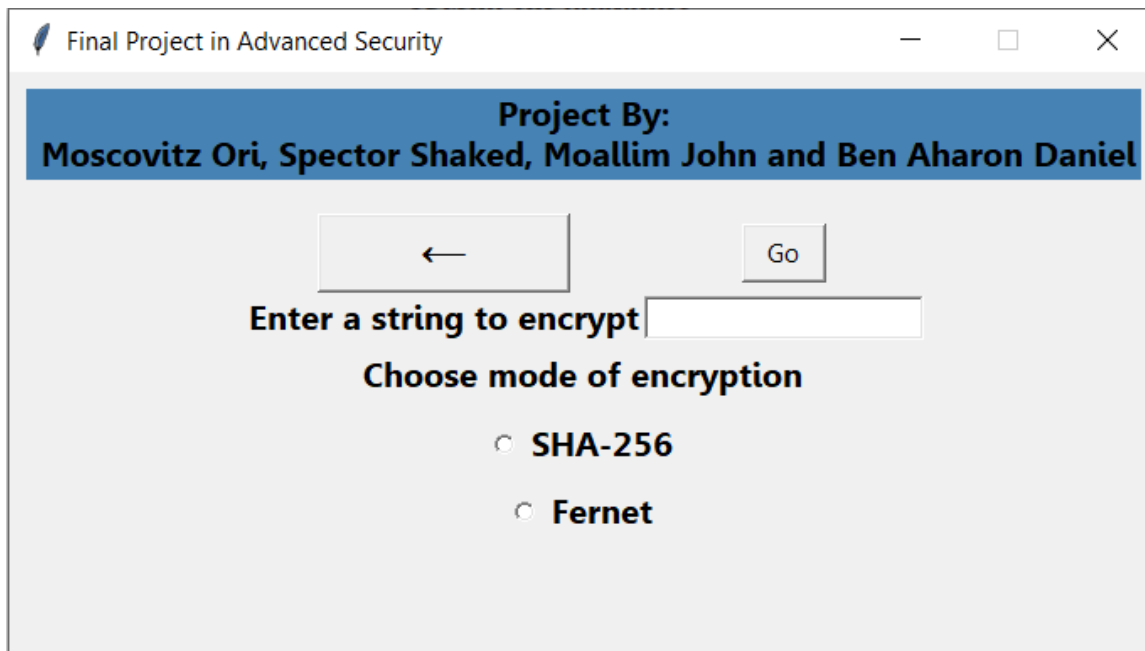
"NOTHINGGG" has not been found in doc.

<Scroll for viewing>

```
<!DOCTYPE html>
<html itemscope itemtype="http://schema.org/Thing">
<head>
  <!-- Facebook Pixel Code -->
  <script>
    !function (f, b, e, v, n, t, s) {
      if (f.fbq) return; n = f.fbq = function
    () {
      n.callMethod ?
        n.callMethod.apply(n, arguments)
      : n.queue.push(arguments)
    };
    if (!f._fbq) f._fbq = n; n.push = n; n.l
loaded = !0; n.version = '2.0';
    n.queue = []; t = b.createElement(e); t.
async = !0;
    t.src = v; s = b.getElementsByTagName(e)
[0];
    s.parentNode.insertBefore(t, s)
  }(window, document, 'script',
    'https://connect.facebook.net/en_US/fbev
ents.js');
    fbq('init', '543147059155097');
```

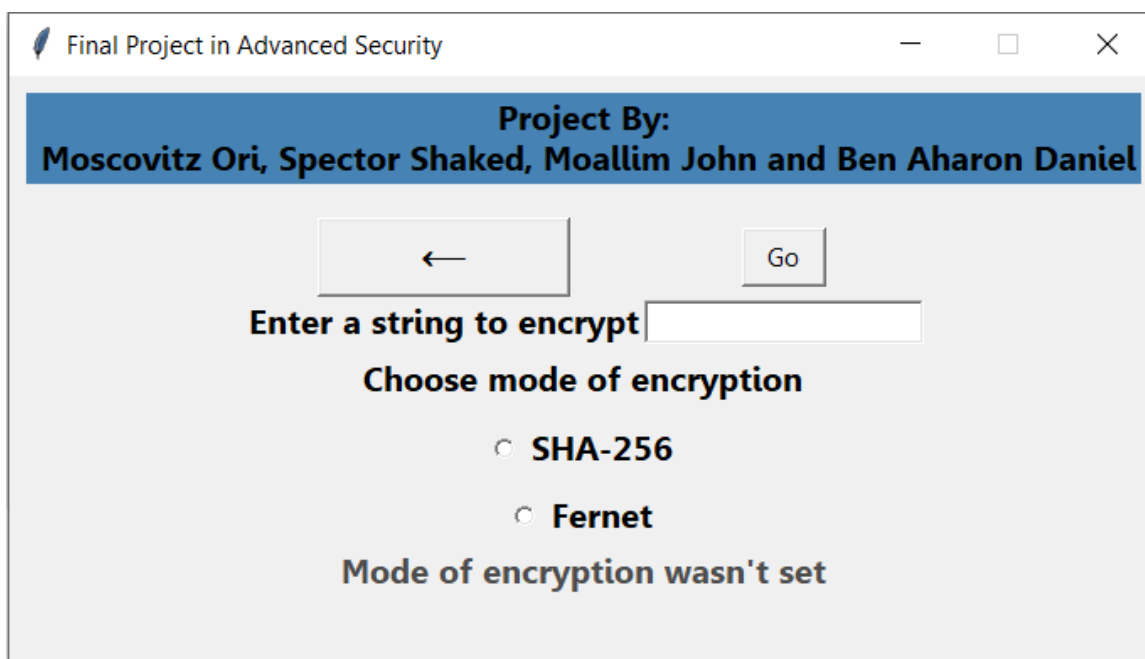

הצפנת מחרוזת עם פונקצית גיבוב (Encrypt String):

גם כאן, ביצענו וולידציות כך שלא ניתן להצפין מילה ללא קביעת סוג ההצפנה והכנסת המילה.



The screenshot shows a web application window titled "Final Project in Advanced Security". At the top, a blue banner displays "Project By: Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel". Below this, there is a navigation bar with a left arrow button and a "Go" button. The main content area contains the text "Enter a string to encrypt" followed by an input field. Below the input field, it says "Choose mode of encryption" with two radio button options: "SHA-256" and "Fernet".

ניסיון להצפנה ללא קביעת סוג ההצפנה:



This screenshot shows the same application window as the previous one, but with an error message displayed at the bottom: "Mode of encryption wasn't set". The "SHA-256" radio button is selected, and the "Fernet" option is unselected. The input field for the string to encrypt is empty.

ניסיון להצפנה ללא הכנסת מחרוזת:

Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

← Go

Enter a string to encrypt

Choose mode of encryption

☒ SHA-256

☐ Fernet

No text was entered

בהינתן נתונים תקינים תוצג התוצאה:

Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

← Go

Enter a string to encrypt HerelsMyString

Choose mode of encryption

☒ SHA-256

☐ Fernet

The encrypted text:
854393eea898240dae0c7878053ac3
8e344c95b7d8b56bd52f379f6f12e9
7fd1

ניתן להישאר בחלון זה ולנסות הצפנות שונות, עבור מילים ו-MODEים שונים,
או לחזור לתפריט הראשי.

Final Project in Advanced Security

Project By:

Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

←

Go

Enter a string to encrypt

HereIsMyString

Choose mode of encryption

☐ SHA-256

☒ Fernet

The encrypted text:

b'gAAAAABiyaPU-V4agzGcCLSJxM_rXX'

b'eeGUHcQTtt2aluzl1Krk7X9gp6WW1B'

b'Do8iAaVlk2dyt1XWswlnm24d56qMEP'

b'lzL7Hesw=='

התקפה על צופן קיסר:

ראשית המשתמש ייבחר מילת הצפנה ומפתח (Int) להצפנה:



Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

← Go

Enter a string to encrypt

Enter a key for encryption

גם כאן בוצעו ווילדציות כך שהמשתמש חייב למלא את השדות ולהשתמש במפתח אינטג'רי.

Final Project in Advanced Security

←

Go

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

Enter a string to encrypt

str

Enter a key for encryption

1

Key must be numeric

Final Project in Advanced Security

←

Go

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

Enter a string to encrypt

str

Enter a key for encryption

1

The encrypted text:

tus

Show Offset Table

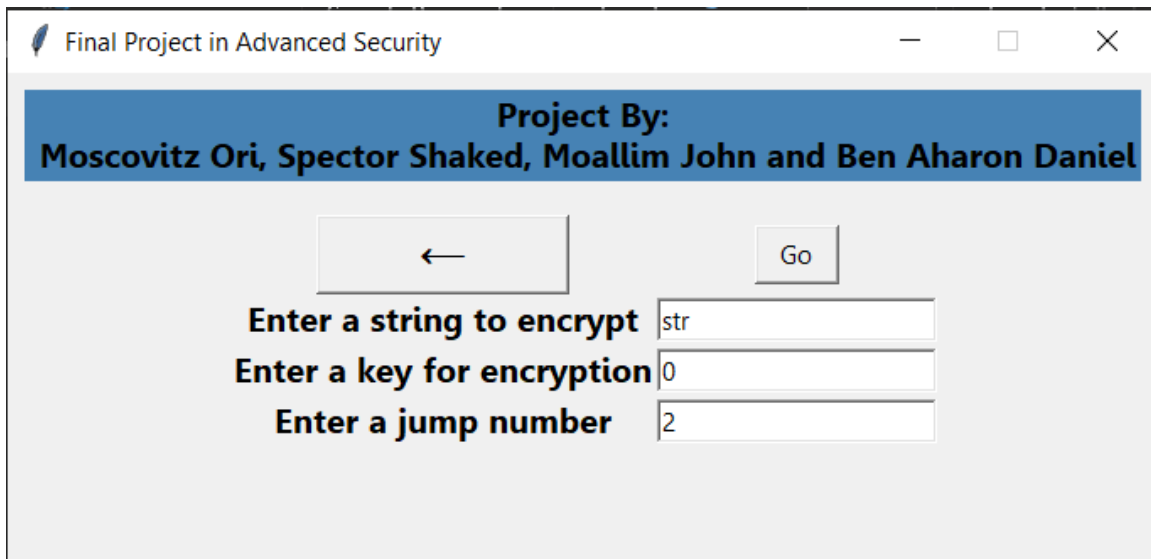
וכעת ניתן לקבל את טבלת Offset-ים:

ואכן עבור מפתח 1 כפי שבחרנו, מופיעה המחרוזת אותה הצפנו:

Final Project in Advanced Security	
Project By: Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel	
←	
Text	Offset
tus	0
str	1
rsq	2
qrp	3
pqo	4
opn	5
nom	6
mnl	7
lmk	8
klj	9
jki	10
ijh	11
hig	12
ghf	13
fge	14
efd	15
dec	16
cdb	17
bca	18
abz	19
zay	20
yzx	21
xyw	22
wxv	23
vwu	24
uvt	25

הצפנת ויז'נר:

ביצענו וולידציות עבור הקלטים, ובהינתן קלט תקין:



Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

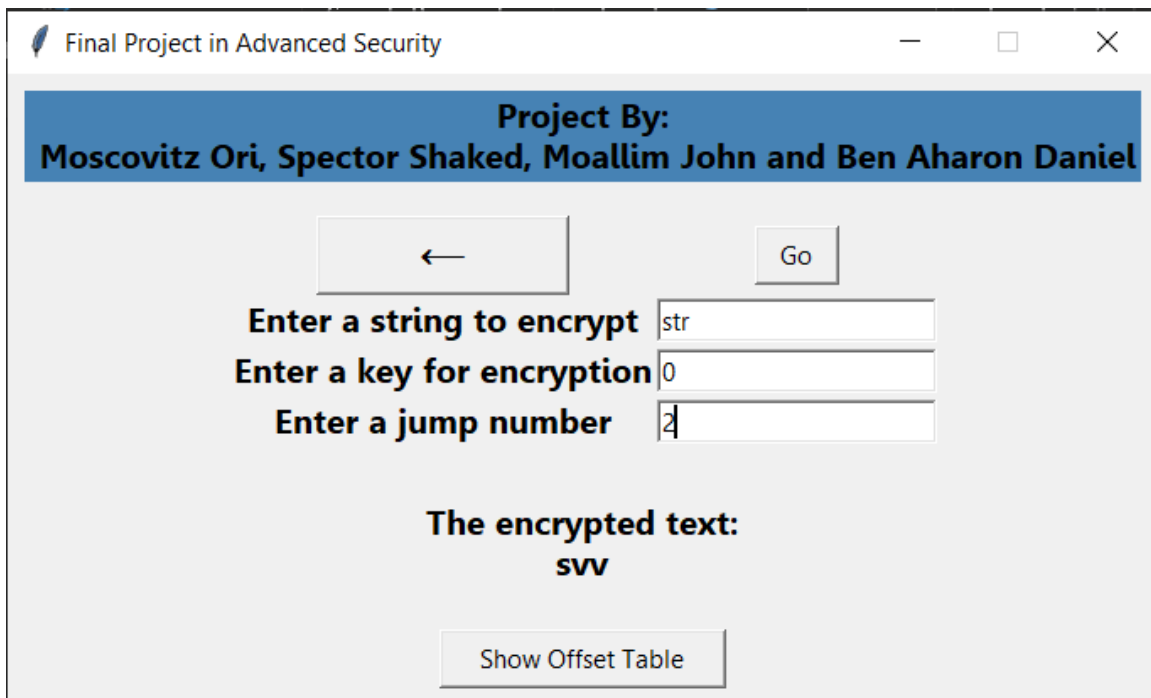
← Go

Enter a string to encrypt str

Enter a key for encryption 0

Enter a jump number 2

לאחר לחיצה על 'Go' תוצג המחרוזת המוצפנת:



Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

← Go

Enter a string to encrypt str

Enter a key for encryption 0

Enter a jump number 2

The encrypted text:
svv

Show Offset Table

כעת ניתן לראות את טבלת ההיסטים פר קפיצה:

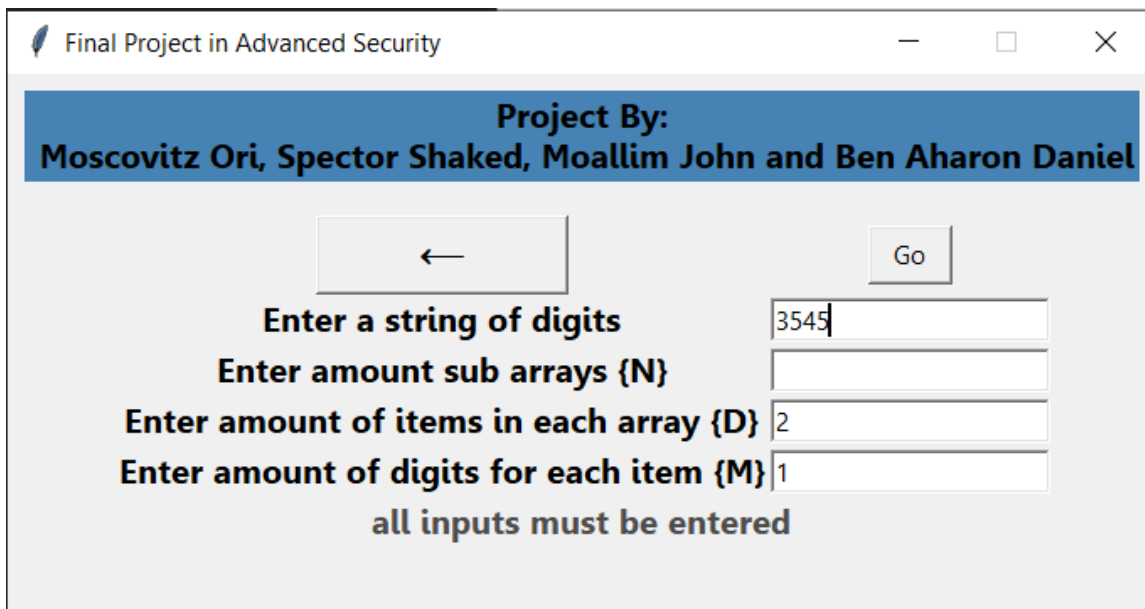
Final Project in Advanced Security			—	□	×
Project By:					
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel					
			←		
Text	Offset	Jump			
svv	0	0			
sut	0	1			
str	0	2			
ssp	0	3			
srn	0	4			
sql	0	5			
spj	0	6			
soh	0	7			
snf	0	8			
smd	0	9			
slb	0	10			
skz	0	11			
sjx	0	12			
siv	0	13			
sht	0	14			
sgr	0	15			
sfp	0	16			
sen	0	17			
sdl	0	18			
scj	0	19			
sbh	0	20			
saf	0	21			
szd	0	22			

ואכן עבור היסט 0 וקפיצה של 2, ניתן לראות את הטקסט המקורי (משמע פריצת ההצפנה תקינה).

הצפנה עם MSSP:

ראשית ביצענו וולידציה עבור הנתונים המוכנסים על ידי המשתמש.

עבור נתונים חסרים:



Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

← Go

Enter a string of digits 3545

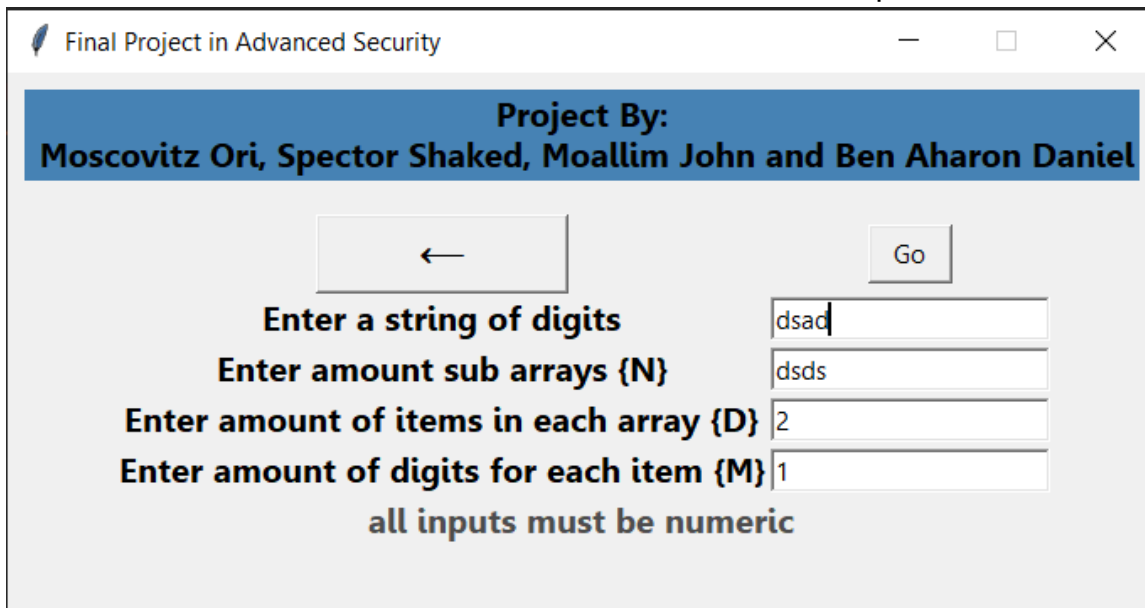
Enter amount sub arrays {N}

Enter amount of items in each array {D} 2

Enter amount of digits for each item {M} 1

all inputs must be entered

עבור נתונים לא תקינים:



Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

← Go

Enter a string of digits dsad

Enter amount sub arrays {N} dsds

Enter amount of items in each array {D} 2

Enter amount of digits for each item {M} 1

all inputs must be numeric

בהכנסת פרמטרים תקינים, תוצג התוצאה (במידה וקיימת).

עבור דוגמת ההרצה מן הדוגמה בהרצאה:

Input: "55495458205016966826278532461565"

Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

← Go

Enter a string of digits 16966826278532461565

Enter amount sub arrays {N} 4

Enter amount of items in each array {D} 2

Enter amount of digits for each item {M} 1

Result is: 112

במידה ועבור הקלט הנוכחי **לא קיים פתרון**, תוצג הודעה מתאימה גם כן:

Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

← Go

Enter a string of digits 11115678

Enter amount sub arrays {N} 4

Enter amount of items in each array {D} 2

Enter amount of digits for each item {M} 1

Cannot compute result from parameters

התקפת DDOS:

באופן דומה יש וולידציה על הנתונים:

Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

←

Connect Server

Enter an ip address or 'localhost'

Enter a port number

Enter a message to send

Enter amount of threads

Enter how many times to run threads

all inputs must be entered, port must be numeric

<Scroll for viewing>

בהזנת נתונים תקינים, ניתן לראות הודעת התחברות מצד השרת:

Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

←

Connect Server

Enter an ip address or 'localhost'

localhost

Enter a port number

86

Enter a message to send

Hello World!

Enter amount of threads

4

Enter how many times to run threads

5

all inputs must be entered, port must be numeric

<Scroll for viewing>

```
{<_io.TextIOWrapper name='<stderr>' mode='w' encoding='utf-8'>} {starting up on localhost port 86} {
```

Attack

בעת נוכל לתקוף את השרת, ונקבל תצוגה של כל הודעות הלקוח:

Final Project in Advanced Security

Project By:
Moscovitz Ori, Spector Shaked, Moallim John and Ben Aharon Daniel

←

Connect Server

localhost

86

Hello World!

4

5

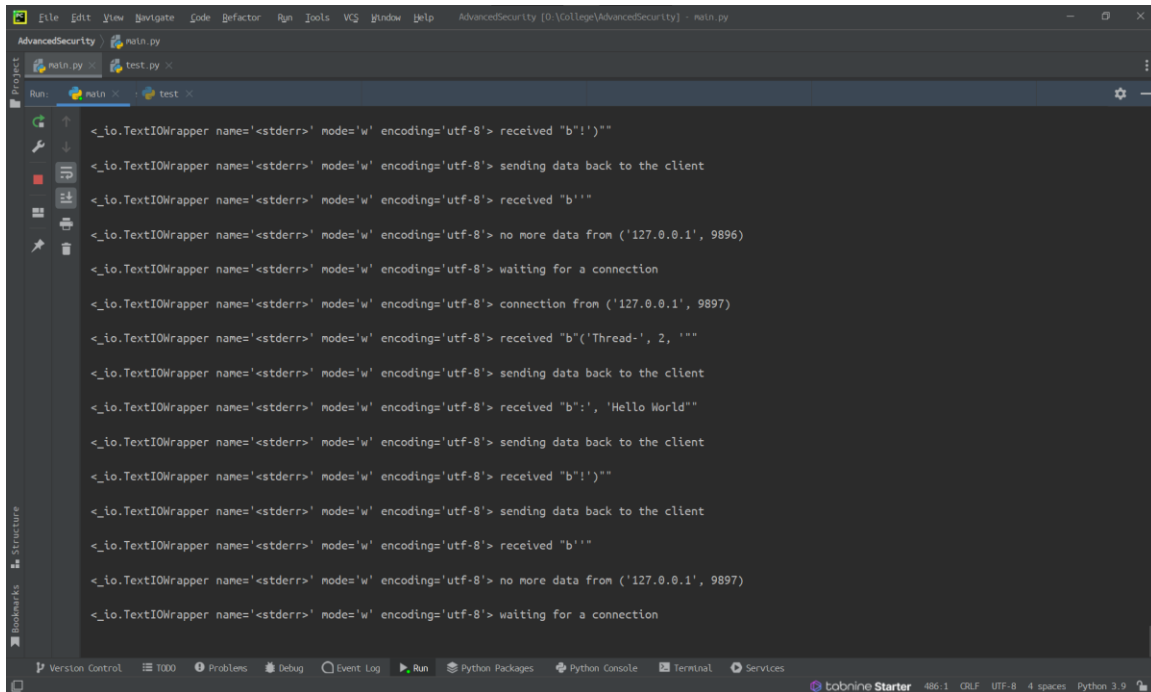
all inputs must be entered, port must be numeric

<Scroll for viewing>

```
{<_io.TextIOWrapper name='<stderr>' mode='w' encoding='utf-8'
'>} {starting up on localhost port 86} {
}Starting Thread-0
<_io.TextIOWrapper name='<stderr>' mode='w' encoding='utf-8'
> connecting to localhost port 86
Starting Thread-1
Starting Thread-2
Starting Thread-3
Starting Thread-0
<_io.TextIOWrapper name='<stderr>' mode='w' encoding='utf-8'
> connecting to localhost port 86
<_io.TextIOWrapper name='<stderr>' mode='w' encoding='utf-8'
> connecting to localhost port 86
<_io.TextIOWrapper name='<stderr>' mode='w' encoding='utf-8'
> connecting to localhost port 86
<_io.TextIOWrapper name='<stderr>' mode='w' encoding='utf-8'
> connecting to localhost port 86
{<_io.TextIOWrapper name='<stderr>' mode='w' encoding='utf-8'
'>} thread- 0 {sending "b"('Thread-', 0, ':', 'Hello World!'
)""} {
```

Restart

את הודעות השרת ניתן לראות בחלון ההרצה של Pycharm, כיוון שלמיטב הבנתנו, לא קיימת דרך להדפיס באופן אינסופי לתוך אובייקט Textn של Tkinter.



```
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> received "b'!'"
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> sending data back to the client
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> received "b'"
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> no more data from ('127.0.0.1', 9896)
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> waiting for a connection
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> connection from ('127.0.0.1', 9897)
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> received "b'('Thread-', 2, '"
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> sending data back to the client
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> received "b':', 'Hello World'"
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> sending data back to the client
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> received "b'!'"
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> sending data back to the client
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> received "b'"
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> no more data from ('127.0.0.1', 9897)
<_io.TextIOWrapper names='stderr' mode='w' encoding='utf-8'> waiting for a connection
```