פתרון ה- CTF

- קריאת מכתב הפתיחה והוצאת מידע חשוב:
  - הארגון – Eclipse
  - האקר – bob
  - הסנפת Wireshark של הארגון – מהיומיים האחרונים

- <u>הוצאת מידע מההסנפה:</u>

שימוש בפילטר **frame contains "bob"**

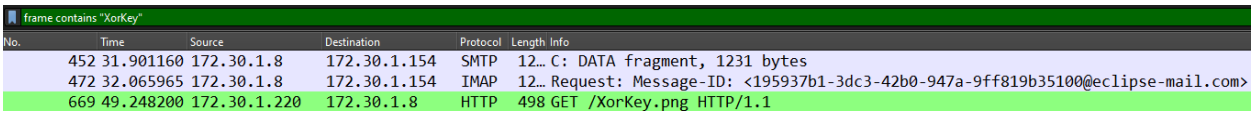
frame contains "bob"

No.	Time	Source	Destination	Protocol	Length	Info
448	31.886295	172.30.1.8	172.30.1.154	SMTP	86	C: RCPT TO:<bob@eclipse-mail.com>
452	31.901160	172.30.1.8	172.30.1.154	SMTP	12…	C: DATA fragment, 1231 bytes
472	32.065965	172.30.1.8	172.30.1.154	IMAP	12…	Request: Message-ID: <195937b1-3dc3-42b0-947a-9ff819b35100@eclipse-mail.com>
532	38.487905	172.30.1.8	172.30.1.154	SMTP	605	C: DATA fragment, 551 bytes
569	38.675069	172.30.1.8	172.30.1.154	IMAP	605	Request: Message-ID: <c17fad60-c39a-48a4-be27-7c85456616f0@eclipse-mail.com>
600	38.900988	172.30.1.154	172.30.1.162	IMA…	795	from: mike <mike@eclipse-mail.com>, subject: I'm So Sorry!, (text/plain)
604	38.977909	172.30.1.154	172.30.1.162	IMA…	369	(text/plain)
635	43.651966	172.30.1.154	172.30.1.8	IMA…	337	from: bob <bob@eclipse-mail.com>, subject: The Message -> reply, (text/plain)
640	43.746089	172.30.1.154	172.30.1.8	IMA…	661	from: bob <bob@eclipse-mail.com>, subject: The Message -> reply, (text/plain)

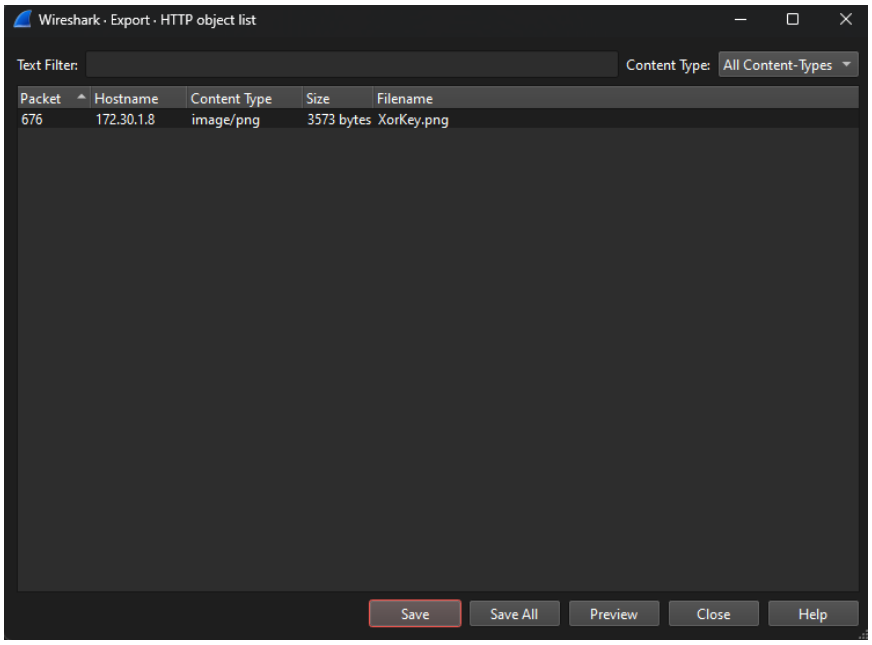
ביצוע **Follw TCP Stream** על החבילה הראשונה

```
220 DESKTOP-0DG3LQ7 ESMTP
EHLO [172.30.1.8]
250-DESKTOP-0DG3LQ7
250-SIZE 20480000
250-AUTH LOGIN
250 HELP
AUTH LOGIN
334 VXNlcm5hbWU6
bWlrZUBlY2xpcHNlLW1hawwuY29t
334 UGFzc3dvcmQ6
bWlrZTE5OTY=
235 authenticated.
MAIL FROM:<mike@eclipse-mail.com> SIZE=1231
250 OK
RCPT TO:<bob@eclipse-mail.com>
250 OK
DATA
354 OK, send.
Message-ID: <195937b1-3dc3-42b0-947a-9ff819b35100@eclipse-mail.com>
Date: Sun, 18 Aug 2024 05:15:41 +0300
MIME-Version: 1.0
User-Agent: Mozilla Thunderbird
Content-Language: en-US
To: bob@eclipse-mail.com
From: mike <mike@eclipse-mail.com>
Subject: The Message
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit

It was great doing business with you.

Here is the secret message you asked me to send you:

0001011110001011000010111000111100001100110001010101000
0
1101000000011011100011010001011010001001000110101101000
1
0001100010010000000100001001100000010011100110100101000
1
1001110000010000100100100101000010011011000011011001011
0
0000100110011010010100001001100100010000100100110001101
1
1001101000001101100011000101000011001110000100111010100
1
0011010110001011001101101100101100010000101101000001000
1
1011101000100000101111100001010111001110000110001010101
1
0011011111001001001110101010101000110010100011000011110
1
1011011000011011100011000101000101110110001000110110101
0
0010111010010011010000001000101000001100100011110100001
0
1000110000010111100111100000110110010110000100011001100
0


To decrypt the message you need to use the XorKey from my HTTP server.

.
250 Queued (0.140 seconds)
QUIT
221 goodbye
```

אם נקרא את ההודעה (שמגיעה אחרי 354 OK, send.) נבין ש- Mike שולח מסר מוצפן בביטים ל- bob.
אפשר לראות שבסוף ההודעה Mike מציין איך לפענח את ההודעה – בעזרת XorKey.
נבצע סינון **frame contains XorKey** ונקבל חבילות HTTP,



נוכל לראות שזאת בקשת HTTP לתמונה.
נבצע **HTTP → Export Objects → File** נבחר בתמונה ונשמור אותה באמצעות **save**.



נפתח את התמונה ששמרנו, במקום ששמרנו, ונוכל לגלות את המספר **32767**

התמונה נקרת בשם XorKey. נעשה אחד ועוד אחד...
פיענוח המסר על ידי במספר (= המפתח) בעזרת שיטת Xor, כמו בתרגיל בית 6 למי שזוכר ומי שלא בעיה שלו! סתם. אפשר לעשות חיפוש בגוגל ולראות איך זה עובד.

- <u>פיענוח המספר:</u>

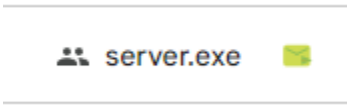
נעתיק את המסר והמפתח וניצר את הקוד הבא

```
def symmetric_encryption(input_data, key):
    # Determine chunk and key size based on length of data (even or odd)
    if len(input_data) % 2 == 0:
        chunk_size = 16
        # Using the all bits of key
        key_in_bits = format(key, '016b')
    else:
        chunk_size = 8
        # Using the last 8 bits of the key
        key_in_bits = format(key, '016b')[-8:]

    # Split data into chunks of appropriate size
    chunks = [input_data[i:i + chunk_size] for i in range(0, len(input_data),
chunk_size)]

    # Perform XOR operation on each chunk with the key
    result = ""
    for chunk in chunks:
        for bit, key_bit in zip(chunk, key_in_bits):
            result += '1' if bit != key_bit else '0'

    return result


Encrypted_message =
'0001011110001011000010111000111100001100110001010101000011010000000110111000
1101000101101000100100011010110100010001100010010000000100001001100000010011 1
0011010010100011001110000010000100100100101000010011011000011011001011000001 0
0110011010010100001001100100010000100100110001101110011010000011011000110001 0
1000011001110000100111010100100110101100010110011011011001011000100001011010 0
0001000110111010001000001011111000010101110011100001100010101011001101111100 1
0010011101010101010001100101000110000111101101101100001101110001110001010001 0
1110110001000110110101001011101001001101000000100010100000110010001111010000 1
0100011000001011110011110000011011001011000010001100110 00'

XorKey = 32767

Decoded_message = symmetric_encryption(Encrypted_message, XorKey)

message = ''.join(chr(int(Decoded_message[i:i + 8], 2)) for i in range(0,
len(Decoded_message), 8))

print(message)
```

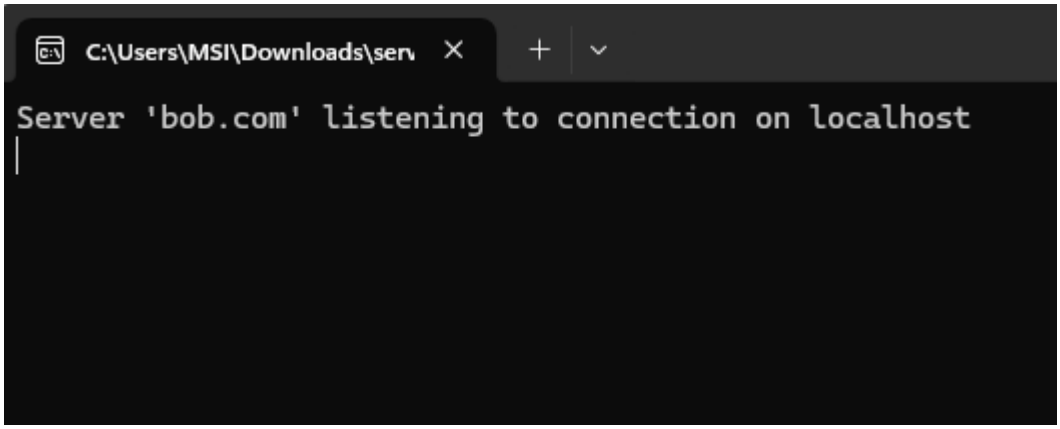
נריץ ונקבל את קישור הבא

```
"C:\Users\MSI\Desktop\NETWORK\Final Exercise\step B - message decoding\.venv\Scripts\pyth
https://drive.google.com/drive/folders/1lVJtI4oKnE_Aj1qTH6EUMsBIdqWDnJQl?usp=sharing

Process finished with exit code 0
```

- <u>הרצת השרת:</u>



נוריד את השרת ונריץ אותו



השרת רץ. אנחנו מספיק חכמים ויודעים שעלינו להתחבר לשרת בעזרת קוד לקוח. אך יש בעיה!
אנחנו לא יודעים מה הפורט שהשרת משתמש.
לכן נריץ את פקודת Nmap וככה נמצא את הפורט

```
C:\Users\MSI>nmap -p- 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-26 03:03 Jerusalem Daylight Time
Nmap scan report for kubernetes.docker.internal (127.0.0.1)
Host is up (0.00022s latency).
Not shown: 65511 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
445/tcp   open     microsoft-ds
1536/tcp  open     ampr-inter
1537/tcp  open     sdsc-lm
1538/tcp  open     3ds-lm
1539/tcp  open     intellistor-lm
1540/tcp  open     rds
1543/tcp  open     simba-cs
2179/tcp  open     vmrdp
5040/tcp  open     unknown
5357/tcp  open     wsdapi
5939/tcp  open     unknown
6463/tcp  open     unknown
7680/tcp  open     pando-pub
9010/tcp  open     sdr
9080/tcp  open     glrpc
9100/tcp  open     jetdirect
9180/tcp  open     unknown
15924/tcp open     unknown
45600/tcp open     unknown
45654/tcp open     unknown
46285/tcp open     unknown
65333/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 2.65 seconds
```

עכשיו שקיבלנו את כל האפשרויות האלו, ננסה אחד אחד. נכון שקיבלנו יחסית הרבה תוצאות אבל זה עדיף מאשר לבדוק את כל ה- 65,535 פורטים הקיימים.
נכתוב קוד שרק מתחבר לשרת וננסה כל פעם פורט שונה. ספוילר, הפורט הוא 46,285.
כמובן ש- אנחנו חכמים, ולכן הדבר הראשון שנחשוב לעשות הוא לבקש **עמוד בררת מחדל '/'**.
נתכנת את שאר קוד הלקוח שנשלח מספר הודעות עד שנשלח את ההודעה המתאימה.
כמובן שהשרת מתקן ומכוון עבור גל טעות. קוד הלקוח המתקבל

```
import socket

IP = '127.0.0.1'
PORT = 46285

def main():
    client_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    client_socket.connect((IP, PORT))

    request = (
        "GET bob/website/link HTTP/1.0\r\n"
        "Host: bob.com\r\n"
        "\r\n"
    )
    client_socket.send(request.encode())

    response = client_socket.recv(1024).decode()
    print("Server response:")
    print(response)

    client_socket.close()


if __name__ == '__main__':
    main()
```

עבור קוד לקוח זה, נקבל הודעת תגובה 200 ok מהשרת עם תוכן. התוכן ההודעה קישור לאתר

```
"C:\Users\MSI\Desktop\NETWORK\Final Exercise\HTTP Se
Server response:
HTTP/1.0 200 OK
Content-Length: 0

https://bobbase.vercel.app

Process finished with exit code 0
```

- <u>כניסה לאתר:</u>

כאשר נכנס לאתר נתקל בבקשת התחברות!

לעבור את השלב הזה בלי מעט ידע על כלי סייבר – בלתי אפשרי!

המטרה היא למצוא אתרים נתיבים מוסתרים אך קיימים שיכולים להדליף לנו מידע.

כדי למצוא את אותם נתיבים, נשתמש ב- Gobaster המשתמש ב- brute force למציאת הנתיבים.

לרוב האנשים אין את הפקודה במחשב ולכן נוריד אותה (הוראות אפשר למצוא בגוגל).

נריץ את הפקודה על כתובת האתר

```
C:\Users\MSI>gobuster dir -u https://bobbase.vercel.app -w C:\Users\MSI\go\bin\common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://bobbase.vercel.app
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                C:\Users\MSI\go\bin\common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/Downloads            (Status: 301) [Size: 185] [--> /Downloads/]
/backup               (Status: 301) [Size: 179] [--> /backup/]
/security             (Status: 301) [Size: 183] [--> /security/]
/uploads              (Status: 301) [Size: 181] [--> /uploads/]
Progress: 1942 / 1942 (100.00%)
===============================================================
Finished
===============================================================
```

קיבלנו 4 תוצאות. נחקור כל אחת ונוכל למצוא עוד המשכי נתיבים. אך נוכל למצוא דברים מעניינים רק בנתיבים הבאים:

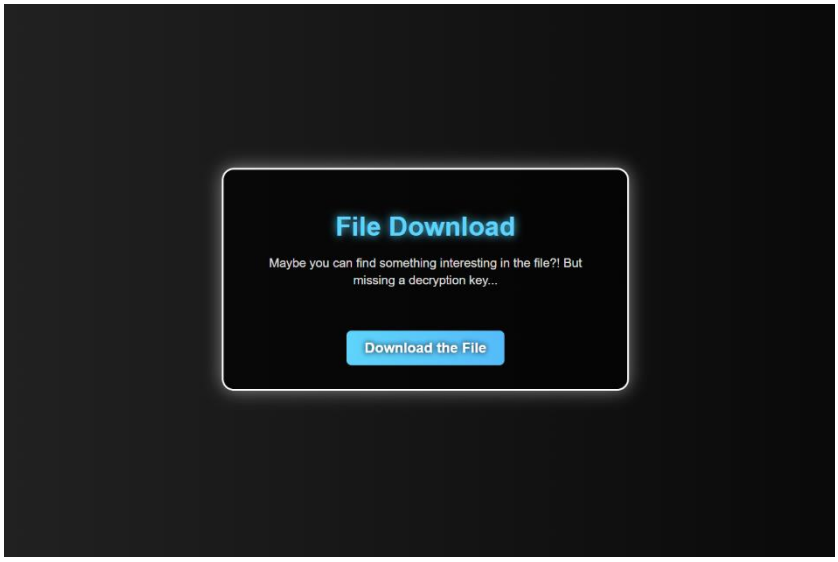
Downloads/network/

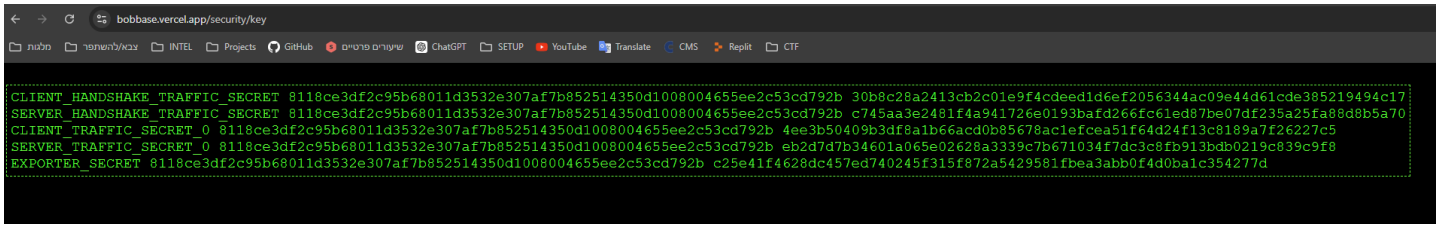
```
C:\Users\MSI>gobuster dir -u https://bobbase.vercel.app/Downloads -w C:\Users\MSI\go\bin\common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://bobbase.vercel.app/Downloads
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                C:\Users\MSI\go\bin\common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/network  <-          (Status: 200) [Size: 2473]
/passwords            (Status: 200) [Size: 1748]
Progress: 1942 / 1942 (100.00%)
===============================================================
Finished
===============================================================
```

security/key/

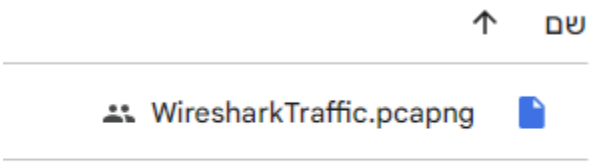
```
C:\Users\MSI>gobuster dir -u https://bobbase.vercel.app/security -w C:\Users\MSI\go\bin\common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://bobbase.vercel.app/security
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                C:\Users\MSI\go\bin\common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/Admin                (Status: 200) [Size: 1129]
/Logs                 (Status: 200) [Size: 1378]
/admin                (Status: 200) [Size: 1129]
/key  <-              (Status: 200) [Size: 1689]
/logs                 (Status: 200) [Size: 1378]
Progress: 1942 / 1942 (100.00%)
===============================================================
Finished
===============================================================
```

נציב את הנתיבים ל- URL של האתר ונקבל את העמודים האלו



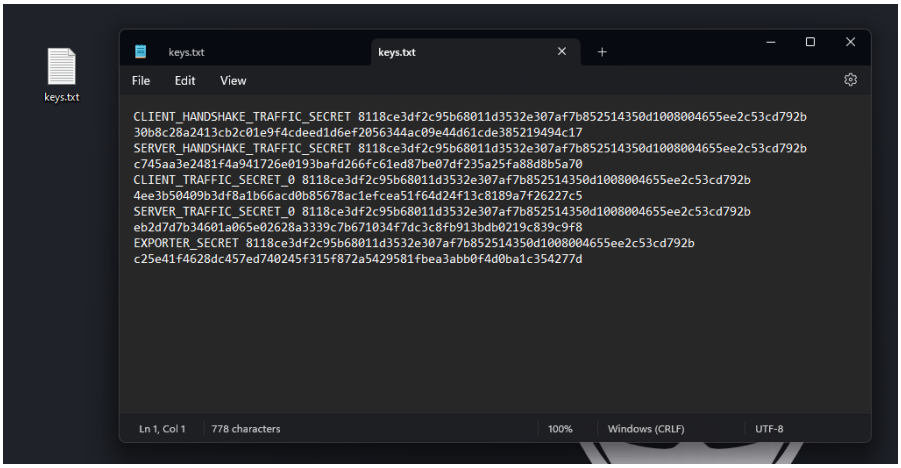


העמוד הראשון מכיל כפתור. אם נלחץ עליו, נגש ל- Google Drive עם קובץ הסנפה.
העמוד השני מכיל מפתחות ו- Client Random.

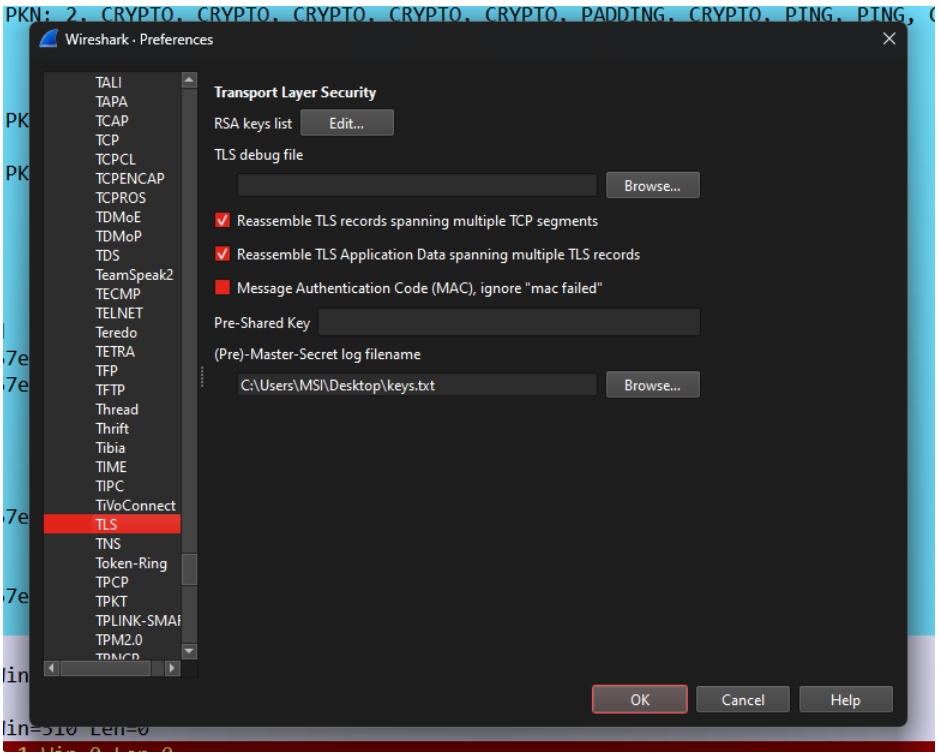


- <u>פתיחה ופיענוח ההסנפה:</u>

נבצע שוב פעם אחד ועוד אחד...
נשתמש במפתחות כדי לפענח את ההסנפה!
ניצור קובץ txt ונשמור בו את המפתחות



נפתח את ההסנפה נפעיל את הפיענוח
Edit → Preferences → Protocols → TLS
נכניס את הנתיב בו שמרנו את קובץ המפתחות



נבצע את הפילטר **http2** ונראה את כל החבילות הצהובות שפוענחו

http2

No.	Time	Source	Destination	Protocol	Length	Info
216	17.424910	172.30.1.220	76.76.21.142	HTTP2	146	Magic, SETTINGS[0], WINDOW_UPDATE[0]
217	17.425022	172.30.1.220	76.76.21.142	HTTP2	668	HEADERS[1]: GET /
219	17.493432	76.76.21.142	172.30.1.220	HTTP2	115	SETTINGS[0]
220	17.493838	172.30.1.220	76.76.21.142	HTTP2	85	SETTINGS[0]
221	17.494074	76.76.21.142	172.30.1.220	HTTP2	120	SETTINGS[0]
251	18.166964	76.76.21.142	172.30.1.220	HTTP2	212	HEADERS[1]: 304 Not Modified
252	18.167177	172.30.1.220	76.76.21.142	HTTP2	89	RST_STREAM[1]
253	18.167414	76.76.21.142	172.30.1.220	HTTP2	85	DATA[1]
258	18.176027	172.30.1.220	76.76.21.142	HTTP2	198	HEADERS[3]: GET /styles.css
259	18.179396	172.30.1.220	76.76.21.142	HTTP2	148	HEADERS[5]: GET /script.js
290	18.358552	76.76.21.142	172.30.1.220	HTTP2	142	HEADERS[5]: 304 Not Modified
291	18.359156	172.30.1.220	76.76.21.142	HTTP2	89	RST_STREAM[5]
292	18.359275	76.76.21.142	172.30.1.220	HTTP2	85	DATA[5]
293	18.368232	76.76.21.142	172.30.1.220	HTTP2	143	HEADERS[3]: 304 Not Modified
295	18.368625	76.76.21.142	172.30.1.220	HTTP2	85	DATA[3]
459	36.819630	172.30.1.220	76.76.21.142	HTTP2	175	HEADERS[7]: POST /login
460	36.819693	172.30.1.220	76.76.21.142	HTTP2	93	PING[0]
461	36.819707	172.30.1.220	76.76.21.142	HTT…	138	DATA[7], JSON (application/json)
464	36.884569	76.76.21.142	172.30.1.220	HTTP2	93	PING[0]
466	37.051276	76.76.21.142	172.30.1.220	HTTP2	381	HEADERS[7]: 200 OK
467	37.051692	76.76.21.142	172.30.1.220	HTTP2	101	DATA[7]
468	37.051692	76.76.21.142	172.30.1.220	HTT…	85	DATA[7], JSON (application/json)
470	37.052007	172.30.1.220	76.76.21.142	HTTP2	89	WINDOW_UPDATE[0]
473	37.059233	172.30.1.220	76.76.21.142	HTTP2	229	HEADERS[9]: GET /protected/login_success.html
504	37.241961	76.76.21.142	172.30.1.220	HTTP2	174	DATA[9]

אפשר לראות שיש חבילה המבצעת פעולת **POST /login** ולכן היא הופכת לחבילה למאוד מעניינת.
נבצע עליה **Follow HTTP/2 Stream** ונקבל את החלונית הבאה

```
:method: POST
:authority: bobbase.vercel.app
:scheme: https
:path: /login
content-length: 53
sec-ch-ua: "Not)A;Brand";v="99", "Google Chrome";v="127", "Chromium";v="127"
content-type: application/json
sec-ch-ua-mobile: ?0
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36
sec-ch-ua-platform: "Windows"
accept: */*
origin: https://bobbase.vercel.app
sec-fetch-site: same-origin
sec-fetch-mode: cors
sec-fetch-dest: empty
referer: https://bobbase.vercel.app/
accept-encoding: gzip, deflate, br, zstd
accept-language: en,he-IL;q=0.9,he;q=0.8
cookie: connect.sid=s%3AcZ2RjGPA4I_lTP_L0LZGdB2VYYf6JVer.S2vkFkfXaZ2aD2VKwRGeHKBSwlar%2F8OKdDHxxSzwiTE
priority: u=1, i

{"username":"BobAdmin","password":"Y0uG0tMe#Unlock!"}:status: 200
cache-control: public, max-age=0, must-revalidate
content-type: application/json; charset=utf-8
date: Sun, 25 Aug 2024 17:07:37 GMT
etag: W/"10-oV4hJxRVSENxc/wX8+mA4/Pe4tA"
server: Vercel
set-cookie: connect.sid=s%3AYWH_wjGq2sRyeLffNdFTUinnFqXSWui6.m7iDAr%2FmnqpD8MRSTfjOX5Udu%2FTZtHEr%2BGCUArayQ%2B8; Path=/; HttpOnly
strict-transport-security: max-age=63072000; includeSubDomains; preload
x-powered-by: Express
x-vercel-cache: MISS
x-vercel-id: cdg1::iad1::bsqjw-1724605657229-d8f7856102b6
content-length: 16

{"success":true}
```

וכך מצאנו את שם המשתמש והסיסמא שהוסנפו כאשר bob לא שם לב והתחבר לאתר, ולכן כך יכולנו למצוא אותם.

התחבר בעזרת שם המשתמש והסיסמא ונקבל את עמוד ההתחברות עם כפתור להורדת הקובץ הגנוב!