



הפקולטה למדעי המחשב

מבחן בתכנות מאובטח – 236491

סמסטר חורף, תשפ"ב
מועד א', 14.02.22

מרצה: פרופ' אליא ביהם
מתרגל: טל נהרון

משך המבחן : שלוש שעות.

במבחן 4 שאלות, ענו על כלן בטופס המבחן.

במבחן זה 13 עמודים, כולל עמוד זה + 2 עמודי דף עוזר.

חומר סגור. מותר לשימוש רק בדף העזר המצורף.

הקדישו את 10 הדקות הראשונות לקריאת כל השאלות והבנתן.

ענו תשובה ברורות ככל האפשר. **נמקו את כל תשובה תיכם.**

כתבו בצורה מסודרת ונקייה ובכתב ברור. **תשובה לא ברורה לא תיבדקנה.**

במידה שנייתן לענות על שאלה במספר דרכים, ניקוד מלא יינתן לפתרונות קצרים ופשוטים.

בהצלחה!



שאלה 1 (28 נק')

היא הקוד הבא של לוגין למערכת בסיס נתונים.

במערכת זו קיימת טבלת users בה יש חמישה עמודות: username, firstname, lastname, email, password. הסיסמה משומם מה שומרה בכתב גלווי (כלומר, בינווד למקובל, שומרה הסיסמא עצמה ולא תמצית שלה).

```
char username[1000];
char sqlc[10000];
int rows;
gets(username);
// ***
sprintf(sqlc, "select 1 from users where username='%s';", username);
rows=sql_numrows(sqlc); // Returns the number of rows that satisfy the sql query
if(rows!=1) {
    printf("No such user\n");
    exit(0);
}
char password[1000];
gets(password);
sprintf(sqlc, "select 1 from users where username='%s' and password='%s';",
        username, password);
rows=sql_numrows(sqlc); // Returns the number of rows that satisfy the sql query
if(rows!=1) {
    printf("Wrong password\n");
    exit(0);
}
```

לצורך שאלה זו הניחו שהתוקף איןנו מבצע חריגה מוחצת.

בנוסף, שימו לב שאף אחת משאלות ה-SQL אינה מחייבת שום מידע על תוכן הרשומות, פרט לידעיה על קיומן של רשותות העומדות בתנאי השאלה.

בשאלה זו מותר לכם להשתמש (בין השאר) באופרטורים והפונקציות הבאים:

- אופרטור like מהצורה 'a%column like %a' שבודק אם הערך של column תואם לביטוי הרגולרי '%a'. הסימן % הוא wildcard שמסמן כל מהירות שתיה (מקביל -* ב-shell) ונitin לשים אותו בכל מיקום בביטוי (למשל השאילטה 'Ben%' ; select * from users where firstname like 'Ben%'). ניתן לשים אותו גם יותר מפעם אחת (למשל 'C%b%').
- פונקציה substring(column,loc,len) שמחזירה את len התווים של הערך column החל מהຫוו במיקום loc (למשל השאילטה select substring(asdfg,2,2);).
- פונקציה sleep(t) שממתינה t שניות. תמיד מחזירה 0 לאחר שסיימה את החמתנה. בהקשר של השאילטה היא מופעלת על כל רשותה בנפרד (כמו שלמשל substring מופעלת על כל רשותה בנפרד).
- שימוש לב סכמו בשפת C הייצוג של True-False 1,0 בהתחאה (למשל הביטוי 2=2 מבהיר 1).
- ענו על הסעיפים הבאים. **בכל הסעיפים הסבירו בפירוט את תשובתכם, כולל האלגוריתם והקלטים הנדרשים לפתרונכם, ובנה השאילות שתבצעו. על כל התפקידות להסתמיכם בזמן סביר (מוגבל ביחס אחד).**
- א. האם תוכלו לתקן מערכת זו כדי להשיג את הסיסמא של משתמש admin? אם לא, האם תוכלו לפחות להשיג את התו הראשון של הסיסמא? הסבירו.

האם גנטא אין צאן גנדי גודזון:

8/8

: Username admin' and substring(password,1,1) = ' {placeholder for guessed char}'

Or je האם גנטא אין צאן גנדי גודזון לא יכולו לא'

admin' or 'No such user' הלא נ



האם עכשו תוכנו לתקן כדי להציג את הסיסמה של admin? הסבירו.

admin' and substring(password, 2, 1) = '{next symbol to guess}'

האם עכשו תוכנו לתקן כדי להציג את הסיסמה של admin? הסבירו.

(Wrong Password) (Correct Password)

~~בשיטות שבסיסם sleep()~~

בטעיפים הבאים הינו שמיין הקריאה במקלדת מוקלקל, כך שבמוקם השורות { (1!=1 מופיע) if(rows!=1) {

ב. האם עכשו תוכנו לתקן כדי להציג את הסיסמה של admin? הסבירו.

admin' and sleep(1) --> (Wrong Password) (Correct Password)

האם עכשו תוכנו לתקן כדי להציג את הסיסמה של admin? הסבירו.

8/8

admin' and sleep(substring(password, 1, 1)) = '{guess}'

No such user 'No such user'

האם עכשו תוכנו לתקן כדי להציג את הסיסמה של admin? הסבירו.

admin' and sleep(1) --> (Wrong Password) (Correct Password)

(C) or (B) --> (Wrong Password) (Correct Password)

האם עכשו תוכנו לתקן כדי לקבל את מספר המשתמשים שהתו השלישי בסיסמה שלהם הוא

האות 'A'? הסבירו.

or (A) > (Wrong Password)

' or 1=1 and sleep(substring(password, 3, 1)) = 'A')

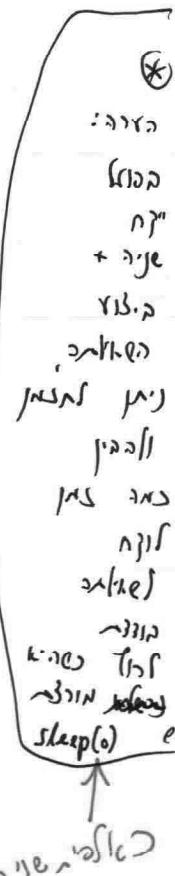
No such user if 1=1 or sleep(1) --> (Wrong Password)

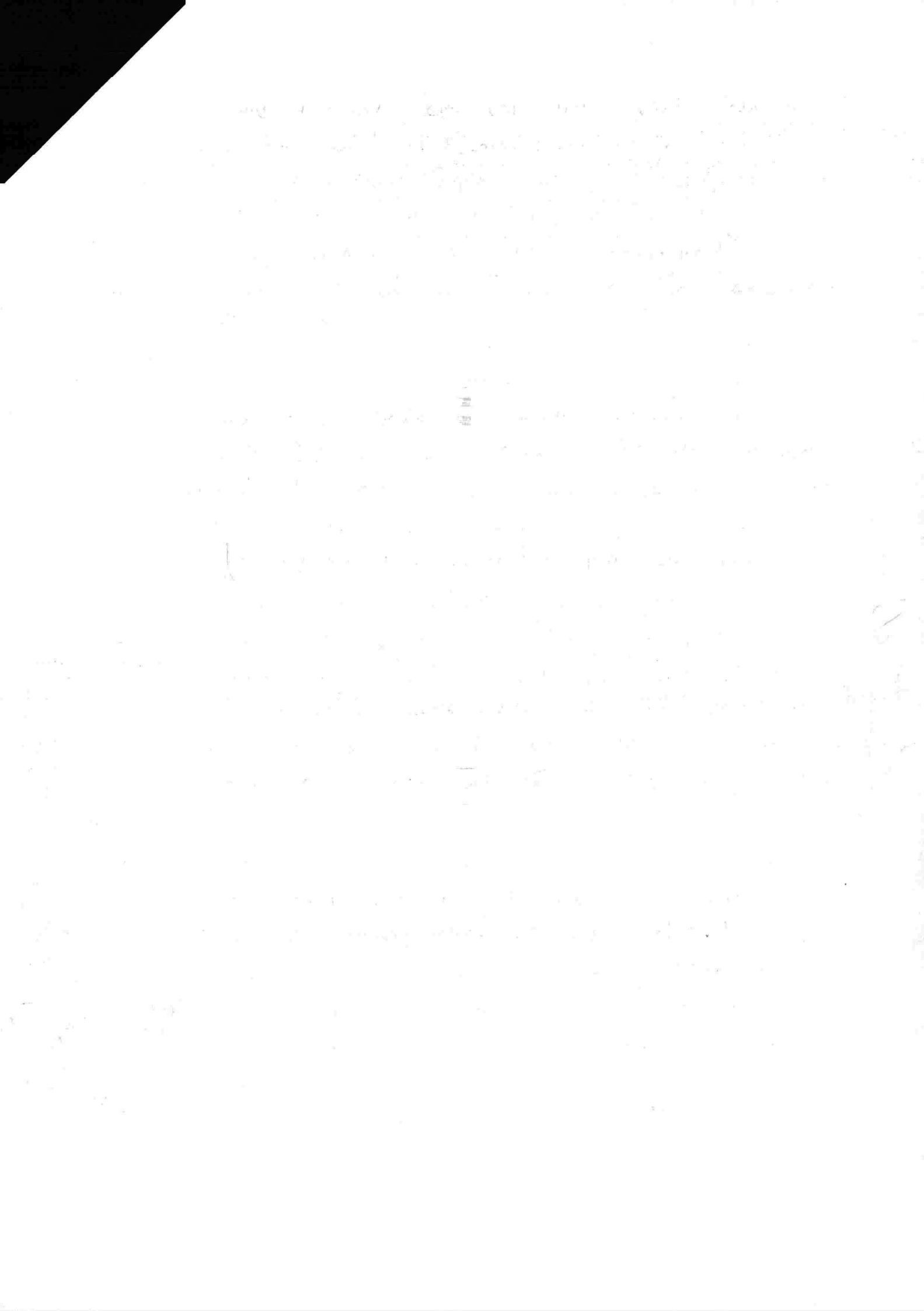
(A) > (Wrong Password)

or (B) > (Wrong Password)

and (C) > (Wrong Password)

sleep(0) || sleep(1) > (Wrong Password)





ד. האם תוכל לתקן כדי לקבל את מספר המשתמשים שיש להם את האות 'Z' במקומות כלשהו בסיסמא? הסבירו.

ד. מילון ?�ן גּוֹן
' or 1=1 and sleep(password like '%Z%') --
אנו נזיר גּוֹן גּוֹן גּוֹן גּוֹן גּוֹן
וגם המאובן דב' .
ולא מ' sleep(1) א' גּוֹן גּוֹן גּוֹן גּוֹן
ל' sleep(0) -
4/4

ה. סטודנט מאוניברסיטת שוטרגט הציע הגנה שמיסירה את כל המופעים של המחרוזות "=" ו- "like" מהחרוזות `username`. לצורך כך הוא הציע להחליף את ההצעה המסומנת ב-*** בשתי שורות הקוד הבאות:

```
removeSubstring(username, " like ");  
removeSubstring(username, "=");
```

בקוד זה הפונקציה `removeSubstring` מוחקת את כל מופעי המחרוזות שבפרמטר השני מתוך המחרוזת שבפרמטר הראשון ומשאירת את התוצאה בפרמטר הראשון.

אם ההצעה מונעת את ההתקפות שהצעתם בסעיפים ג' ו- ד' הסבירו.

ד. מילון ?�ן גּוֹן גּוֹן גּוֹן גּוֹן גּוֹן
: ז Fro
4/4

' and sleep(password like '%Z%') ; --
ג' יחו' גּוֹן גּוֹן גּוֹן גּוֹן
: ז Fro

' and sleep(password like '%Z%')
substring((password,3,1) like 'A') ; --
ל' יחו' גּוֹן גּוֹן גּוֹן
: ז Fro
4/4

' and sleep(substring(password,3,1) like 'A'))
sleep(1) א' יחו' גּוֹן גּוֹן גּוֹן
ל' יחו' גּוֹן גּוֹן גּוֹן
: ז Fro
4/4

' or substr('a',1,1) like 'A' -> ק-הס, יחו' גּוֹן גּוֹן
down, true -> true
4/4

the first time in the history of the world, the people of the United States have been called upon to make a choice between two opposite ways of life, between two different philosophies of government—between anarchy and law.

The choice is made. We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

We have decided to live by the rule of law, and not by anarchy.

שאלה 2 (32 נק')
נתונה התוכנית הבאה:

```
// The address of g is 0x13111010
void g() {
    printf("The Magic Words are Squeamish Ossifrage\n");
    exit(0);
}

// The address of f is 0x13111198
void f(int flag) {
    // The address of str is 0x61626364
    char str[1024];
    ...

    // The address of the code here is 0x13111217
    gets(str);
    printf(str); // This printf

    // The address of the code here is 0x13111246
    if (flag) {
        gets(str);
        printf(str);
    }
}

// The address of main is 0x13111288
int main() {
    f(1);
    // The address of the code here is 0x131114a4
    exit(0);
}
```

בשאלה זו: הקלדתתו שאמינו נמצא על המקלדת מאופשרת ב-Windows ע"י לחיצה על ALT ואז כשהוא לחוץ להקליד את המספר העשרוני שמייצג את התו ב-numerical keypad. אם יש צורך לכתוב קלט כזה ממקלדת, סמן ואות בתשובותיכם ע"י המספר בעיגול (אפשר גם בהקסדצימלי בעיגול עם קידומת אפס). למשל $A = \boxed{65} = \boxed{0x41}$.

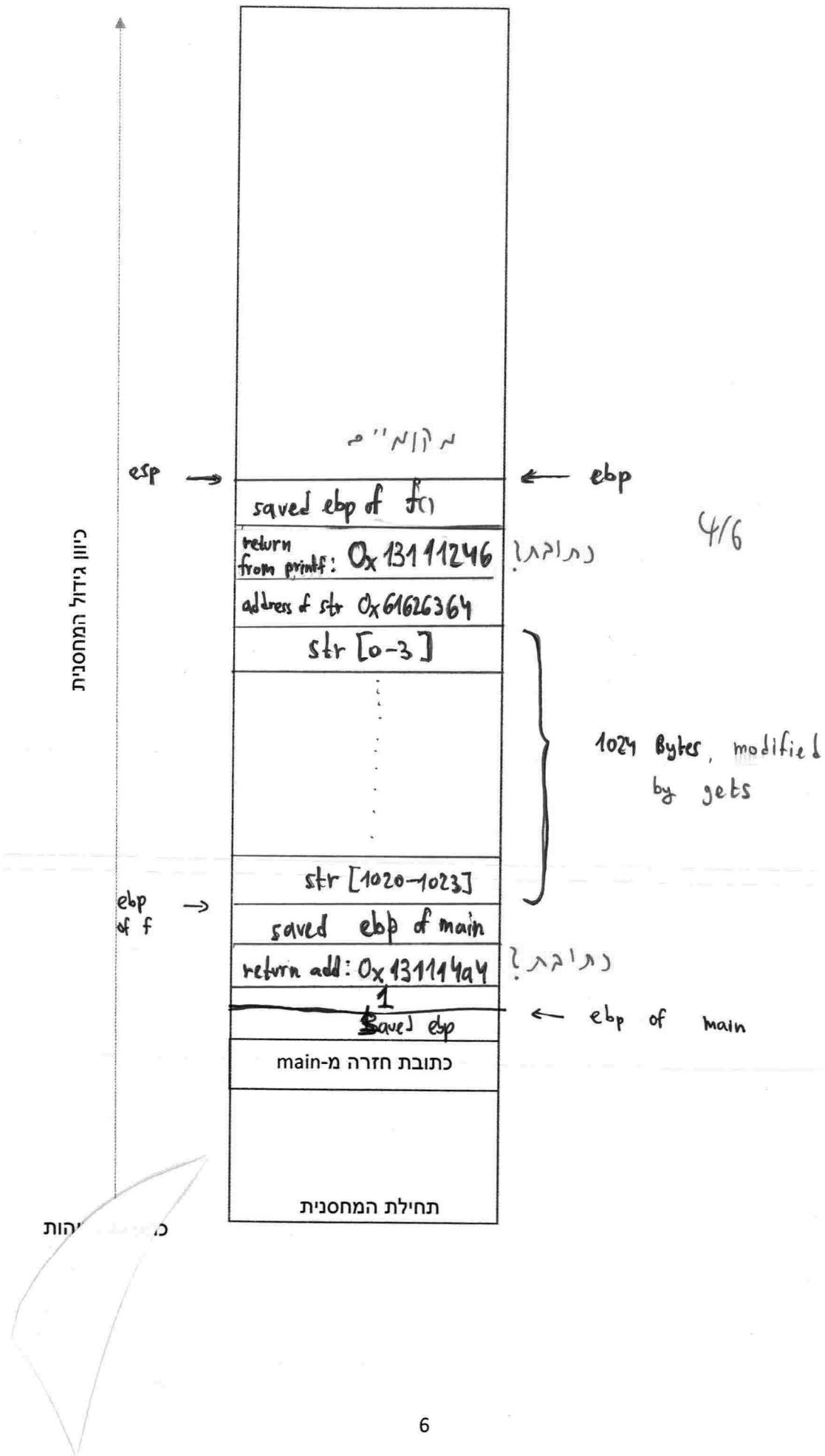
ענו על הסעיפים הבאים:

א. ציררו את המחסניתה בתחילת ריצת הפונקציה `f()` בקריאה הראשונית שלה (זו עם החערה `This`) במהלך ריצה **חוקית** של התוכנית (לצורך סעיף זה, תחילת ריצת התוכנית הינה לאחר הקצתה המשתנים המקומיים על המחסנית ולפניהם ביצוע פקודות מכונה נוספים).

אל תשחחו לרשום בה את כל הפונקציות שנמצאות במחסנית, כולל המשתנים, הפרמטרים, וכו'. בנוסך רשמו את הכתובות על המחסנית בהן נמצאות כתובות החזרה `-m` ו-`-f`, ואת הערכיהם של כתובות החזרה והפרמטרים, אם הם ידועים לכם או שביכולתכם לחשב אותם.

לנוחותכם צירפנו ציור בסיסי של מחסנית בעמוד הבא.









(3) תוקף מעוניין לגרום להפעלת הפונקציה g. תארו התקפה שתוקף יכול להפעיל לצורך קפיצה ל-g. הסבירו.

3/3 ✓

(~~gets~~) ~~gets~~: ~~gets~~ - f . C_f

~~gets~~ - f . ~~gets~~ ~~gets~~ flag = 1 - f . ~~gets~~
~~A~~_x 102~~8~~ + ~~canary~~ ~~Ox10~~ ~~Ox10~~ ~~Ox11~~ ~~Ox13~~ : ~~gets~~
~~Cf~~ ~~gets~~, ~~gets~~

~~f~~ - f . ~~gets~~ - f . ~~gets~~ - f . ~~gets~~ - f . ~~gets~~ - f . ~~gets~~

g - f . ~~gets~~ - f . ~~gets~~

gets - f . ~~gets~~ - f . ~~gets~~

(~~Ox13111010~~ - f . ~~gets~~)

~~gets~~ - f . ~~gets~~

~~Ox~~ x 256 + ~~000~~ + ~~%X~~

xx

gets - f . ~~gets~~ - f . ~~gets~~

gets - f . ~~gets~~ - f . ~~gets~~

האם ווגכלו לבצע ארבע הפעולות write-what-where שונות במהלך הרצת התוכנית? ומה עם מהה? ואלף? איך? פרטו והסבירו.

4)

רץ ג'ק א "מי" - printf כב עוזן נגלו אונ גט!

gets - f . ~~gets~~ - f . ~~gets~~

רץ ג'ק א

WWW - f . ~~gets~~ - f . ~~gets~~

רץ ג'ק א

PR 3 f . ~~gets~~ - f . ~~gets~~

רץ ג'ק א

WWW - f . ~~gets~~ - f . ~~gets~~

רץ ג'ק א

0x13111211 - f . ~~gets~~ - f . ~~gets~~

רץ ג'ק א

הקס: f . ~~gets~~ - f . ~~gets~~

רץ ג'ק א

+1

~~Ox17~~ ~~Ox12~~ ~~Ox11~~ ~~Ox13~~

WWW - f . ~~gets~~ - f . ~~gets~~ - f . ~~gets~~ - f . ~~gets~~ - f . ~~gets~~

the \mathcal{L} -operator is given by

$$\mathcal{L} = \frac{\partial}{\partial t} + \frac{\partial^2}{\partial x^2} - \frac{\partial^2}{\partial y^2} - \frac{\partial^2}{\partial z^2} + \frac{\partial^2}{\partial w^2}.$$

Let $\psi(x, y, z, w)$ be a solution to the differential equation $\mathcal{L}\psi = 0$. Then we have

$$\begin{aligned} \frac{\partial \psi}{\partial t} &= -\frac{\partial^2 \psi}{\partial x^2} - \frac{\partial^2 \psi}{\partial y^2} - \frac{\partial^2 \psi}{\partial z^2} + \frac{\partial^2 \psi}{\partial w^2}, \\ \frac{\partial^2 \psi}{\partial x^2} &= -\frac{\partial \psi}{\partial t} - \frac{\partial^2 \psi}{\partial y^2} - \frac{\partial^2 \psi}{\partial z^2} + \frac{\partial^2 \psi}{\partial w^2}, \\ \frac{\partial^2 \psi}{\partial y^2} &= -\frac{\partial \psi}{\partial t} - \frac{\partial^2 \psi}{\partial x^2} - \frac{\partial^2 \psi}{\partial z^2} + \frac{\partial^2 \psi}{\partial w^2}, \\ \frac{\partial^2 \psi}{\partial z^2} &= -\frac{\partial \psi}{\partial t} - \frac{\partial^2 \psi}{\partial x^2} - \frac{\partial^2 \psi}{\partial y^2} + \frac{\partial^2 \psi}{\partial w^2}, \\ \frac{\partial^2 \psi}{\partial w^2} &= -\frac{\partial \psi}{\partial t} - \frac{\partial^2 \psi}{\partial x^2} - \frac{\partial^2 \psi}{\partial y^2} - \frac{\partial^2 \psi}{\partial z^2}. \end{aligned}$$

Substituting these into the original equation $\mathcal{L}\psi = 0$, we get

$$\begin{aligned} \frac{\partial \psi}{\partial t} &= -\left(-\frac{\partial^2 \psi}{\partial x^2} - \frac{\partial^2 \psi}{\partial y^2} - \frac{\partial^2 \psi}{\partial z^2} + \frac{\partial^2 \psi}{\partial w^2}\right) - \left(-\frac{\partial^2 \psi}{\partial x^2} - \frac{\partial^2 \psi}{\partial y^2} - \frac{\partial^2 \psi}{\partial z^2} + \frac{\partial^2 \psi}{\partial w^2}\right) \\ &\quad - \left(-\frac{\partial^2 \psi}{\partial x^2} - \frac{\partial^2 \psi}{\partial y^2} - \frac{\partial^2 \psi}{\partial z^2} + \frac{\partial^2 \psi}{\partial w^2}\right) + \left(-\frac{\partial^2 \psi}{\partial x^2} - \frac{\partial^2 \psi}{\partial y^2} - \frac{\partial^2 \psi}{\partial z^2} + \frac{\partial^2 \psi}{\partial w^2}\right) \\ &= 0. \end{aligned}$$

ד. בסעיף זה לא מופעלות הגנות בכלל, כולל לא עיי' קנריות. תוקפת מעוניינת לגרום להפעלת הפונקציה g. תארו התקפה שונה מזו שהצעתם בסעיף ג.(ושמשתמשה בחולשה אחרת) שהתקפת תוכל להפעיל לצורך קפיצה ל-g. הסבירו.

main ebp ret main

0x13111010 ak * (ebp - 8)

-printf -1 gets : (ה↙ן ה↙ן

6/6 ✓

התרבר לתוכניתית ש-f תמיד נקראת מקום בווד בקוד, ככלומר כתובות החזרה ממנה תמיד זהה. התוכניתית היחילית לבדוק שכותבות החזרה של f על המחסנית אכן זהה למצופה רגע לפני ביצוע ret, והכניסה בדיקה שימושה את כתובות החזרה לערך המצופה (ואם לא מתקיים שווין התוכניתית מבצעת exit(0)). היא טעונה שלא ניתן יותר לבצע קפיצה ל-g עיי' שניי כתובות חזרה. האם היא צודק? אם כן, הסבירו מדוע. אם לא, תארו התקפה שפועלת גם במקרה זה.

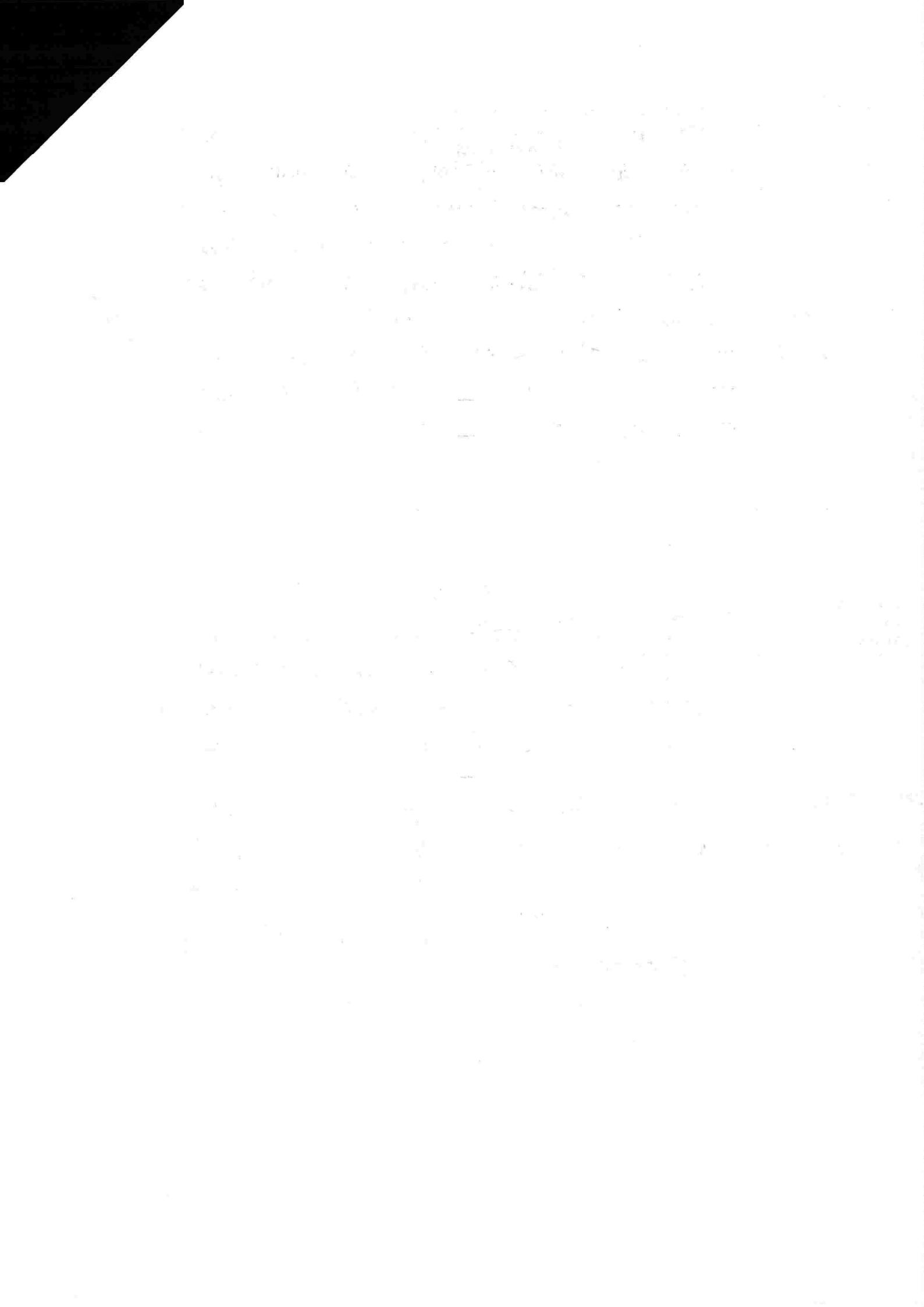
ה↙ן ה↙ן ה↙ן ה↙ן ה↙ן ה↙ן

return hard coded

0/3

(ה↙ן)

printf -r ret main



שאלה 3 (26 נק')

א. הסבירו ממי חולשת XSS ומה ההבדל בין XSS לStored XSS

web server sees our message
(XSS) (client sends request to server)
the browser parses HTML from server
the user sees the message "Hello World" 4/4
the user's browser sends a POST request to the server.
function URL contains a parameter (name=) - Reflected XSS

ב. הסבירו מהי מדיניות Same Origin Policy. מהי המטרה של המדיניות זו?
origin : host:port → Origin header contains the same host and port as the request
origin → same origin policy applies to cookies and session tokens.
origin → facebook cookies are shared across different domains. 2/2

ה. הסבירו כיצד חולשת XSS מאפשרת לעקוף את המדיניות זו.
XSS, attack from malicious JS code
if, the malicious JS runs in the browser and can access the victim's browser
but malicious JS can't access other domains.
so (using attack via JavaScript in the victim's browser) 2/2

בטעוף הבא ניתן לדף `https://www.example.com/showtext?text`, כאשר `text` הוא פרמטר. הדף המתקבל יכול את התוכן הבא:

`<HTML>...<BODY>[text] ...</BODY></HTML>`

כאשר `[text]` מצין את תוכן הפרמטר ב-URL.

ד. הציעו ערך של `text` שייגרום להופעת המחרוזת `"alert"` בחלון קופץ (`Secure Programming`) כאשר טוענים את הדף.

`<script> alert ('Secure Programming'); </script>`
HTML → `<js> tag` generates the payload. 6/6
the payload contains the command to run the script.

10
the payload is injected into the browser by the victim (user).
and the user runs the script. 3/3



סְקָרֶרֶת (JS) פְּרָגָמִינְגַּ (פְּרָגָמִינְגַּ)

לְעֵגָלָה (פְּרָגָמִינְגַּ) גְּזָרָה (פְּרָגָמִינְגַּ) example.com

.alert

cut נתייחס לכך https://www.example.com/showimage:image המכיל את התוכן הבא:

<HTML>...<BODY></BODY></HTML>

בסעיף זה ידוע שהשרת מבצע בדיקת קלט שלא מאפשרת את התווים '<' ו'-''. הצביעו ערך של image שיגרום להופעת המחרוזת "Secure Programming" (alert) כאשר טוענים את הדף.

" onerror = alert ('Secure programming') alt = "Hi"

 ← הטענה

הטענה מושפעת מ- src (הטענה) ← הטענה

הטענה מושפעת מ- alt (הטענה) ← הטענה

. IMG tag ← הטענה מושפעת מ- alt attribute

1. בסעיף זה ידוע שהשרת מבצע בדיקת קלט שלא מאפשרת את התו '='. הצביעו ערך של image שיגרום להופעת המחרוזת "Secure Programming" (alert) כאשר טוענים את הדף.

"> <Script> alert ('Secure Programming') </script> <script> alert... </script> <">

הטענה מושפעת מ- src (הטענה) ← הטענה

. IMG tag ← הטענה מושפעת מ- src attribute

the same time, the δ -function is not zero at $x = 0$, so the solution is not zero at $x = 0$. This is a contradiction.

Therefore, δ is a non-zero function that satisfies the equation $\delta''(x) + \lambda^2 \delta(x) = 0$ for all $x \neq 0$. This contradicts the fact that δ is a non-zero function that satisfies the equation $\delta''(x) + \lambda^2 \delta(x) = 0$ for all $x \in \mathbb{R}$.

Therefore, there is no non-zero function δ that satisfies the equation $\delta''(x) + \lambda^2 \delta(x) = 0$ for all $x \in \mathbb{R}$.



setuid (3)

uid -> ut user linux -> setuid (1)
ה杆菌 מודם (טב) גורם uid מודם
(רין צה)

2/2

uid root הפוך מהן שולחן בדרכו uid root (2)
ה杆菌 מודם (טב) גורם uid מודם

Zero day (4)

לפוף מודם (טב) גורם uid מודם (patch) הפוך
uid root הפוך גורם uid root (patch). הפוך (טב)

2/2

Downgrade attack (5)

לפוף מודם (טב) גורם uid מודם (patch) הפוך
uid root הפוך גורם uid root (patch) הפוך (טב)
uid root הפוך גורם uid root (patch) הפוך (טב)
uid root הפוך גורם uid root (patch) הפוך (טב)

2/2

