

---

## על כשלונות ותובנות - הגישה שלי לאתגרים

מאת דניאל איסקוב

---

### הקדמה

המאמר הזה התבשל אצלי לאחרונה, החלטתי לכתוב אחרי תקופה ארוכה שלא כתבתי כלום. האמת שפשוט לא התחשק לי. כמובן בגלל הטבח הנוראי והמלחמה אבל לא רק, גם בגלל הפאן התחרותי. אני מרגיש שהייתי גרוע בכמעט כל תחרות CTF שהשתתפתי בה. הצלחתי לפתור מעט מאוד אתגרים.

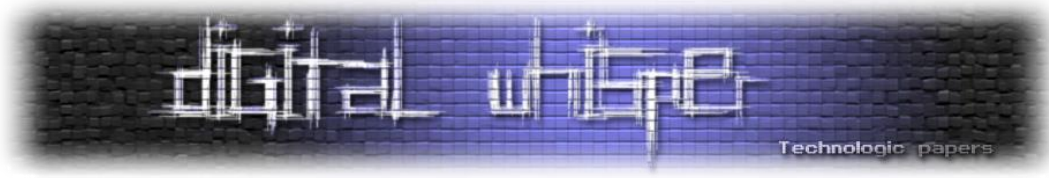
נקודת השפל הייתה כשעשיתי את תחרות Flare-On 2023 (או לפחות: כשניסיתי לעשות), הצלחתי רק את ארבעת השלבים הראשונים! בייחוד בהתחשב בעובדה ששנה שעברה כן הצלחתי לפתור את כל האתגרים (ואפילו כתבתי [מאמר](#) במגזין, המאגד את כל הפתרונות...). הרגשתי כמו מתחזה. הקול בראש אמר לי: "יש ילדים בני 17 שפתרו את זה, איך אתה לא פותרת?" "אולי עדיף שתפרוש מתחרויות" "אולי התחום הזה בכלל לא בשבילך" "6 שנים אתה פותר אתגרים ולא השתפרת?!"

האמת שלא רק שנכשלתי בלפתור, אלא גם פרשתי באמצע במחשבה שאת השלב החמישי כבר לא אצליח לפתור. בעיקר כי הרגשתי תסכול רב מכל הניסיונות הכושלים שלי. בסופו של דבר החלטתי לכתוב על זה.

אפיק, העורך המדהים של המגזין הזה, אמר לי שלכתוב באופן כללי זה קצת כמו תרפיה והוא צודק. אוסיף גם שכשמעלים את הנקודות הקשות על הנייר, זה עוזר לארגן את המחשבות ולהוריד מאיתנו מעט את העול הרגשי שהן גובות.

מסיבות אלה מאמר זה נולד, המאמר הזה יעזור לי באתגרים עתידיים וכולי תקווה שיעזור גם לכם לכשתתקלו באתגרים, ולא דווקא בתחרויות, ולא דווקא בכלל בתחום! לעניות דעתי, חלק מהתובנות יכולות אפילו להועיל לפתרון בעיות באופן כללי בחיים...

אם טרם הבנתם, המאמר הולך להיות מאוד תיאורטי ולא יגע באף תחום ספציפי באבטחת מידע, הוא הולך להתמקד בפאן המנטלי ולחשוף מעט מנבכי נפשי בעת פתירת אתגרים. אם אתם פחות מתחברים, אל תגידו שלא הזהרתני מראש 😊



## הכוח המתסכל של אתגרים קשים והשיעור החשוב לחיים

לאורך הדרך שלי כחובב אתגרים מושבע, נתקלתי בלא מעט אתגרים קשים במיוחד. בייחוד זכורים לי האתגרים הקשים (והמוזרים) ביותר של צ'קפוינט לאורך השנים באתגרי ה-CSA שלהם.

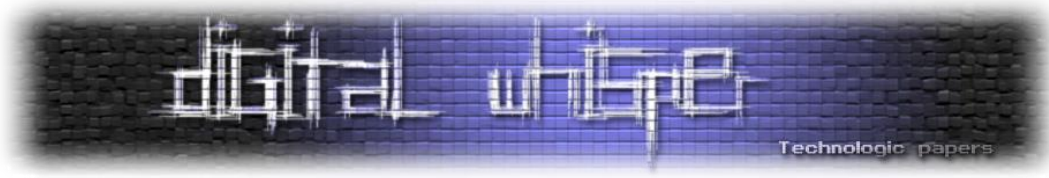
כהערה צדדית, זה לא העיקר ובטח לא פרסומת לצ'קפוינט: למי מכם שלא יודע, עד לא מזמן חברת צ'קפוינט הוציאה שורת אתגרים (למעשה, CTF שלם). ואלה שפותרים סף מסוים של אתגרים, מקבלים זימון לתוכנית ה-CSA שלהם: תוכנית שבה משלמים לך תוך כדי הכשרה אינטנסיבית שמעניקים לך, על מנת שבסוף תתקבל לעבוד בחברה. כך על פי צ'קפוינט עצמה ועדויות ממקור ראשון.

בכל מקרה, האתגרים הקשים ב-CTF שמוביל לתוכנית הזאת הם ממש קשים, מתישים ובעיקר - מתסכלים. ברמה הטכנית, בין אם פתרתי או שהסתכלתי על הפתרון ברגע שהתפרסם, אף פעם לא למדתי מהם משהו טכני חדש, לפחות לא משהו שיכולתי להגדיר כמעניין (מרחק לוינשטיין אתם מכירים?).

אבל לא לשווא סבלתי! כי בזכות האתגרים האלה, למדתי שיעור חשוב: לא לעשות את האתגרים המפגרים האלה מלכתחילה. אבל אם אתם תחרותיים כמוני ובכל זאת רוצים לנסות ולפתור אז קודם כל, אתם צריכים להבין ולהתכונן לעובדה שזה הולך להיות מאוד קשה. שנית, ברגע שהבנתם את זה, השלב הבא זה לקחת כמה צעדים אחורה מכל מה שניסיתם עד כה, לנוח מעט, לחזור עם ראש רענן ולחשוב על הדברים הבאים:

1. מה אני רוצה להשיג? (במקרה שלנו זה דגל)
2. איזה מידע נתון לי? בדרך כלל ניתן קובץ או מספר קבצים ושם ותיאור של האתגר, לפעמים השם והתיאור מהווים רמז.
3. איך מה שאני רוצה להשיג מיוצג במידע הנתון? זאת שאלה קריטית ביותר. ברור שלא תמיד ניתן לענות עלייה, אבל השערות טובות יקרבו אותך לדגל בצורה משמעותית (ולהשערות גרועות האפקט ההפוך). בסופו של דבר זה עניין של זיהוי דפוסים מורכבים מאוד. פעם חשבתי שהטריק הוא להצליח לחשוב על כמה שיותר כיוונים, אבל זה נכון רק חלקית, החלק שפחות חושבים עליו אבל לא פחות חשוב, הוא לדעת לפסול כיוונים שמתסברים כלא נכונים, ובמהירות.

כשאני מסתכל על זה בדיעבד, עיקר הסבל שלי נגרם בגלל שנעלתי על כיוון שכל הסימנים מראים לי שהוא לא נכון ואני ממשיך ללכת בו. הדבר שקול ללנסות לחבר חלק בפאזל במקום שהוא לא מתאים. אפילו ילד בן שש יודע שזה לא מעשה נבון. אגב איכשהו בסוף תמיד קיבלתי אימייל מצ'קפוינט שהזמין אותי למיונים אם ארצה בכך, אז אולי בכל זאת אני לא כזה גרוע...



## כל הפעמים שחשבתי והתנהגתי כמו קוף

הורדתי אתגר הנדסה לאחור מאחדי האתרים המוכרים והנפוצים. ישבתי ועמלתי עליו, כשלפתע קרה משהו ששבר לי לחלוטין את כל הציפיות. ואני בשלי, דופק את הראש בקיר. לא משנה את צורת החשיבה שלי. תקוע בקונספציה שגויה מיסודה. זכרו את האתגר הזה עוד נחזור אליו כמה פעמים בהמשך המאמר.

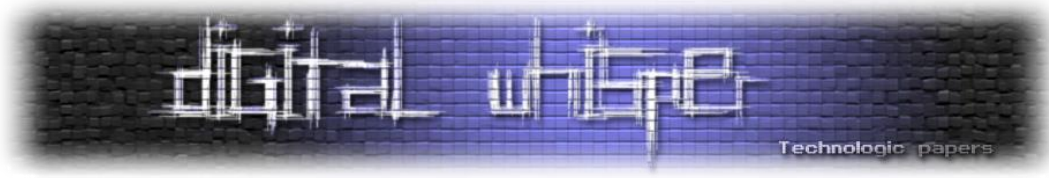
לא נעים להודות, אבל האמת שיותר מדי פעמים חשבתי והתנהגתי כמו קוף במהלך פתירת אתגרים (יש שיטענו שלא רק במהלך פתירת אתגרים ©). הכוונה שיותר מדי פעמים לא בדקתי את ההיגיון שלי, ברגע שהייתה לי השערה או הנחה - פשוט הלכתי עליה בכל הכוח! ואם זה לא עבד, אז ביצעתי שינוי זעיר וניסיתי שוב. האמת שבתוך תוכי ידעתי שהשינוי הזה לא יוביל לפתרון, אבל מנקודה מסוימת בתהליך הפסקתי לחשוב בהיגיון.

בשיא הכנות, אני לא יכול להגיד בוודאות מה קורה לי ברמה הפסיכולוגית שגורם לי להפסיק לחשוב בהיגיון. אבל יש לי שתי השערות:

1. [אפקט העלות השקועה](#) - על פי ויקיפדיה, היא הטייה קוגניטיבית הגורמת לנו להמשיך להשקיע במשימה גם כשהסיכויים לא לטובתי, כשמאחורי ההחלטה עומד ההיגיון הפגום שאם כבר השקעתי אז כדאי ללכת עד הסוף ולהשקיע עוד כדי לא להפסיד את הרווח שכביכול אמור לצאת מההשקעה. בנוסף לכך, קשה לנו כבני אדם להודות בטעות ובהפסד. זה כואב. כואב מאוד. באופן מעשי, כשאני נתקע באתגר ואני תקוע בדפוס מחשבה מסוים, קשה לי מאוד עד כמעט בלתי אפשרי לשחרר את מה שאני חושב ולחשוב על כיוון אחר. זה מצטרף למה שכתבתי בעמוד הקודם - על החשיבות של לדעת לפסול כיוונים שמסתברים כלא נכונים ומסביר למה זה כל כך קשה. אין לי פתרון שיעלים את ההטייה הזאת, הדבר היחיד שאני יכול לעשות הוא להעלות את המודעות לעצם קיומה.

2. [יוהרה](#) - כן, אחרי שפתרתי כל כך הרבה אתגרים, אז ברור שבאתגר העשרת אלפים אני אהיה הרבה יותר בטוח בעצמי ואשים הרבה יותר סימני קריאה מסימני שאלה. אני חושב שזו בסך הכל היוריסטיקה שנועדה לקצר תהליכים. הבעיה שלא תמיד ההנחות שלי נכונות. אתן דוגמה קצרה: באותו אתגר הנדסה לאחור, שמת' Break Point בנקודה מסוימת בקוד. ולא משנה מה ניסיתי לעשות, לא הגעתי אליה לעולם. למרות שכל האינדיקציות הראו שאני אמור להגיע אליה או לפחות ככה חשבתי, בשל הנחה שגויה שלי.

חטא היוהרה הוא חטא עתיק יומין, הוא מוזכר בתנ"ך בסיפור [כיבוש העי](#), בני ישראל חשו ביטחון יתר עקב הצלחת כיבוש יריחו, דבר שהוביל למחשבה שלא צריך להשקיע כוחות רבים בניסיון כיבוש העי ונגמר בתבוסה לבני ישראל בקרב הראשון. חטא היוהרה מוזכר גם כאחד הגורמים לנפילתו של נפוליאון אחרי פלישתו הכושלת לרוסיה. אך מדוע לנו להפליג לעבר הרחוק, היוהרה קיימת ובעטת גם בישראל המודרנית ולאחרונה כולנו היינו עדים לה. על מה אפשר לעשות נגד היוהרה (הטבעית יש לומר) ארחיב בהמשך המאמר, אך עצם המודעות מהווה כבר חצי מהדרך.



## כבר עשיתי את זה אינספור פעמים

כשאני עושה אתגר אני רוצה להיות הכי חד שאפשר על מנת שחלילה לא אפספס פרט או דפוס מעניין. אך לא תמיד הדבר מתאפשר, לפעמים תחושת העייפות הקוגניטיבית חזקה מדי. כשהתחושה מכה, אני לא במיטבי לקבל החלטות, ואני הרבה יותר רגיש לעיוותים מחשבתיים או הטיות קוגניטיביות. לכן, אני נוהג לייעל ולהפוך לאוטומטי כל תהליך שרק ניתן בתהליך הכולל של פתירת אתגר, כך שאצטרך להשקיע מאמץ מינימלי בכל הדברים הבנאליים ומאמץ מירבי בדברים החשובים באמת.

זה מתחיל בדברים הפשוטים:

- הגדרת תיקיית הורדות נוחה כברירת מחדל, כדי לא לבזבז זמן בלנווט בין תיקיות שמורידים קבצי אתגר.
  - יצירת קיצורי דרך נוחים לכל התוכנות שאני יודע שאשתמש בהם.
  - שמירת קוד boilerplate שימושי
- וממשיך בדברים יותר מתקדמים, כמו כתיבת סקריפטים מותאמים אישית לייעול תהליך ניסוי וטעייה. למשל, כשאני נתקל באתגר בו צריך לבצע מספר צעדים כדי להגיע לחולשה ואז להזין קלט מסוים (שלא ידוע לי) כדי לנצל את החולשה, אז יהיה חכם מצדי להכין סקריפט שמבצע את כל הצעדים כדי להגיע לחולשה, על מנת שלבסוף אוכל לשחק עם הקלט בקלות מבלי דאגה יתרה לפשל. הרי כשיש סקריפט אפשר לבצע מחדש את הצעדים באופן מיידי.
- כמובן שיש גם טיפים בצד המנטלי שעזרו לי והם ישמעו ברורים מאליו ובכל זאת שווה לחזור עליהם כי כל כך קל לנו לשכוח אותם בעת מאמץ:
- מנוחה, שינה אם אפשרי.
  - שתייה מספקת - אני לא יכול להדגיש כמה פעמים ההתרכזות שלי באתגר הייתה כל כך קיצונית ששכחתי לשתות מים והתייבשתי קלות. המדע יודע להגיד לנו היום שגם ההתייבשות הקלה ביותר פוגעת בביצועים שלנו.
  - יציאה לטבע - האירוניה מתה אם הגעתי למצב שאני זה שממליץ על יציאה לטבע. אבל זה פשוט עובד.
  - תנועה - הפיתוחים הטכנולוגיים בעת המודרנית כמעט כופים עלינו חיים שלא דורשים תנועה רבה, אך האבולוציה לא מתקדמת בקצב כל כך מהיר. אנחנו לא בנויים בשום צורה שהיא לשיבה ממושכת. כשאנחנו בתנועה אנחנו פשוט חדים יותר. מומלץ על הליכה, אבל גם תנועות קטנות כמו משחק עם הידיים או תזוזות קלות של הגוף עוזרות באופן לא מבוטל.
- באופן כללי, ככל שתהיו פחות עייפים, פיזית, נפשית, קוגניטיבית, ככה תהיו יותר חדים. עייפות מסוג אחד תורמת לאחרת, סוגי העייפות קשורים זה בזה.

## חשיבה מעקרונית ראשוניים - המזור ליוהרה?

מוקדם יותר במאמר דיברתי על יוהרה. אני חושב שחשיבה מעקרונית ראשוניים יכולה להוות מזור ליוהרה. לפי ויקיפדיה, עקרון ראשוני הוא טענה בסיסית שלא ניתן להסיק על ידי טענה או הנחה אחרת. כשחושבים מעקרונית ראשוניים למעשה אנחנו חוזרים לבסיס, לשורשים, לאקסיומות ומשם מתחילים לבנות את הטיעון הכולל שלנו בצורה לוגית כל הדרך אל המטרה. טענה הגיונית נשקלת וטענה שסותרת את ההיגיון נפסלת. צורת החשיבה הזאת עובדת גם בכיוון ההפוך, זאת אומרת כשיש כבר טיעון כולל שמתברר שהוביל למסקנה שגויה, אפשר לחזור לבסיס ולבחון כל הנחה שביצענו במהלך הדרך, על מנת לאשש או להפריך אותה.

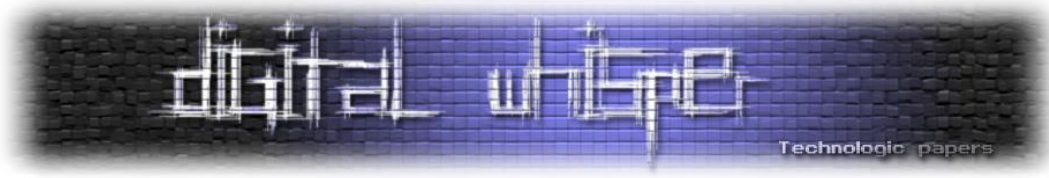
לצורך הדוגמה אחזור לאתגר ההנדסה לאחור שצינתי קודם במאמר, באתגר ניתן קובץ שהוא קובץ הרצה (מעתה אקרא לו - הבינארי), רוגלה מדומה. הבינארי מחפש תהליך של הדפדפן Firefox (בגרסה מסוימת) ומזריק לו קוד. אז כמובן שהשלב הבא הוא להבין את מהות הקוד המוזרק. עשיתי את דרכי דרך הקוד, התחלתי לקבל תמונה ברורה של מה הקוד עושה עד שכאמור קרה משהו ששבר לי את הציפיות. במהלך הקוד היה תנאי, אם מזוהה בקשת POST מהדפדפן, אז ה-flow מגיע לקוד שנראה סופר מעניין שיגרום לתעבורת נתונים לא אופיינית. שמתי נקודת עצירה בדיבאגר והמשכתי לרוץ ונכנסתי לאתרים שברור לי שייצרו את הבקשה המיוחלת. הבעיה שאף פעם לא הגעתי לנקודת העצירה! לא משנה כמה שיחקתי עם תוכן הבקשה הנשלחת.

למה? שאלתי את עצמי בעודי מנסה את אותו דבר שוב ושוב כמו קוף. כאילו בפעם המאה זה פתאום יעבוד. התשובה האמיתית היא שאחת מההנחות שלי שגויה. הייתי יהיר מדי, אבל עוד לא הבנתי את זה. ישבתי על האתגר לסירוגין במשך כשלושה שבועות, עד שנתקלתי מחדש ברעיון של חשיבה מעקרונית ראשוניים המוזכר לעיל.

חזרתי לדיבאגר, התחלתי להטיל ספק בכל הנחה שלי, אז הפעם גם פתחתי wireshark וראיתי דבר מוזר. התעבורת רשת שלכאורה אמורה להתרחש ברגע שנשלחת בקשה, באמת מתרחשת! אבל הדיבאגר לא עוצר בנקודת העצירה, למרות שהיא מופיעה מיד אחרי התנאי שבודק אם מדובר בבקשת POST.

בשלב הזה כבר עמדתי לאבד את זה אבל התעשתתי וחשבתי לעצמי - "איזה הנחה אני מניח שיכול להיות שהיא שגויה והיא משבשת לי את כל התפיסה?". לאחר קצת חשיבה הגעתי למסקנה היחידה שהייתה לי הגיונית: יכול להיות שאותו התנאי והפרוצדורה שאחריו, מופיעים בעוד מקומות בקוד המוזרק ואני ננעלתי על מקום אחד? חיפשתי את התנאי בקוד ומצאתי עוד ארבעה קטעי קוד זהים לחלוטין לקוד שיש לי בו נקודת עצירה, שמחתי, ידעתי שמפה הדרך לניצחון קצרה ובאמת זמן קצר לאחר מכן פתרתי את האתגר.

התפנית התרחשה ברגע ששיניתי גישה והתחלתי לפקפק בכל ההנחות שלי עד שאני מאמת (או מפריך) אותן. כמה בעיות יש לכם שאתם לא מצליחים לפתור? אולי אתם פשוט מניחים הנחות לא נכונות.



## לא נכשלתי - מעדתי

ועכשיו לנקודת השבר שציינתי בהקדמה, האתגר החמישי בתחרות Flare-On 2023. האתגר התחיל ככל אתגר אחר. קובץ הרצה שבהתחלה ניתחתי סטטית, מהר מאוד הבנתי שאחד הקשיים של האתגר הזה הוא שיש Control-Flow obfuscation אז מאוד קשה לעקוב אחרי מה שקורה. עברתי לניתוח דינמי עם Time-travel debugging. אפילו הצלחתי להגיע לרמז שזורק קצה חוט לגבי הכיוון הבא. אבל לא משנה כמה ניסיתי להתחקות אחר הכיוון הזה, וניסיתי ימים על גבי ימים, בסוף לא הצלחתי להגיע לדגל.

הייתי מתוסכל, עשיתי את כל הטעויות שהזכרתי לאורך המאמר הזה:

- ניסיתי את אותו דבר שוב ושוב ושוב כמו קוף למרות שידעתי שזה לא יעבוד.
- לא נחתי מספיק וכשנחתי הייתי דבוק לחדשות בעקבות הטבח.
- לא ניסיתי לחשוב מעקרונות ראשונים בכלל.
- לא בניתי סקריפטים שיקצרו לי את העבודה, עשיתי המון עבודת נמלים.
- בכל התקופה שהובילה לתחרות, חשבתי שהניצחון כבר בכיס שלי אחרי שהצלחתי בשנה שעברה וכתוצאה מכך לא השתפרתי מספיק בכל הקשור להנדסה לאחור ב-Windows. הייתי יהיר והטעות הגרועה מכל: ויתרתי טרם תם הזמן. אני לא זוכר בדיוק את היום שבו ויתרתי, אבל אני מעריך שנשאר לי כשבועיים עד שהתחרות הסתיימה ואני פשוט ויתרתי, הפסקתי לנסות. התסכול הכריע אותי. במשך השבוע שלאחר מכן, אני ממש התביישתי בעצמי. חשבתי לעצמי - "איך יכולת להיכשל בזה?" "אתה כזה אפס!". אבל בשלב מסוים הבנתי שזה לא עוזר. עשיתי מה שיכולתי בהתאם למה שידעתי באותו זמן נתון.

במקום להתמקד בכישלון עצמו, עדיף להתמקד בדברים הפרקטיים, במה אני יכול להשתפר להבא וזאת אחת הסיבות המרכזיות שאני כותב את המילים האלו: **כדי שפעם הבאה אהיה טוב יותר, חכם יותר, מבין יותר.**

מישהו לא מזמן אמר לי: "אין בושה בלנסות ולהיכשל, הבושה טמונה בלא לנסות כלל" וזה נגע בי. אני אמור לדעת את זה, כשהתחלתי לפתור אתגרים נכשלתי אינספור פעמים, אם הייתי מוותר בכל פעם בכלל לא הייתי מגיע למצב שאני עושה את Flare-On. אבל האמת היא שזה פשוט לא הוגן וגם לא נכון לקרוא לזה כישלון. משול הדבר למעידה. נפילה זמנית שקמים ממנה מיד אחר כך, ירידה לצורך עלייה!

שמעתי פעם על מחקר שבו שאלו אנשים קשישים לקראת סוף חייהם אם יש דברים שהם מתחרטים עליהם ומתברר שרובם מתחרטים על דברים שרצו לעשות ולא עשו. אם יש משהו שאני רוצה שניקח מהמאמר הזה, זה שאם אתם רוצים להשיג משהו, תפעלו כדי להשיג אותו. רוב הסיכויים שלא תצליחו בניסיון הראשון ותמעדו בדרך, אבל מעידה איננה כישלון ועם כל מעידה מגיע גם שיפור ואם תתמידו בסוף אתם תהיו הכי טובים שיש!



## סוף דבר

במאמר הזה הצפתי מספר נקודות שברור לי שאי-אפשר לסגל ביום אחד ורק מסתם קריאה של מאמר, הרצון לשינוי לא יכול לבוא ממקור חיצוני, הוא צריך לבוא מכם. אך קריאת המאמר הזה היא הזמנה לביצוע עצירה של כמה דקות וניתוק מכל מה שמסביב, והזמנה לחשוב עליכם, אם התחברתם לחלק ממה שנכתב כאן - יכול להיות ששווה לכם לנסות לאמץ את אחד הרעיונות, זה כמובן לא שינוי שיגיע במהרה, והתהליך יארך תקופה, אך ברור לי שאם תתמידו - בסופו של דבר תצאו מהצד השני טובים, חזקים ומוכנים יותר לקראת תחרות ה-CTF הבאה שבה תתמודדו.

המאמר הזה היה הקשה ביותר שכתבתי עד כה, נתתי לכם מבט לנבכי נפשי לצורך למידה ושיפור של כולנו. אין לי מושג כמה ערך יש למאמר כזה, אם בכלל. אך עזרתי לפחות לאדם אחד - לעצמי. אם עזרתי לעוד מישהו אז לדעתי המאמר הזה עשה את שלו.

בהצלחה!

## קצת על עצמי

שמי [דניאל איסקוב](#), אני בן 25, שחקן CTF-ים ותיק ומושבע שאוהב במיוחד אתגרי Mobile-i Reversing.

אהבתם את המאמר? שנאתם את המאמר? חשבתם שהוא משעמם עד מוות? אשמח לשמוע את דעתכם!

כתבו לי בקישור! 😊