Technologic Papers

# אם תמונה שווה אלף מילים, כמה מילים שווה חולשה באינסטגרם?

מאת עדן אלון

## הקדמה

בזמן האחרון מספר לא מובטל של חברות וארגונים גדולים מאמצים שיטה חדשה בתחום המחקר ואבטחת המידע הנקראת - Bug Bounty. התוכנית מאפשרת לכל חוקר אבטחה לנסות למצוא פגיעות בשירותי החברה ובתמורה לכל דיווח אמין שייבדק וימצא נכון - יתוגמל החוקר בתשלום בהתאם לסוג חולשה שדווח. בזמני הפנוי אני חוקר לא מעט מערכות ושירותים נפוצים במטרה למצוא פגיעות ולדווח עליהם.

לאחר הרבה מחקרים מוצלחים, החלטתי להתקדם קצת ולנצל את ניסיוני עם שירותים יותר גדולים - פייסבוק, גיימייל, וואלה ועוד... את המאמר על וואלה נשמור ליום שבו וואלה יחליטו לתקן את בעיות האבטחה שלהם ☺

המחקר שלי התחיל בחיפוש אחר XSS באינסטגרם והתפתח בסופו לחולשה לוגית קריטית המאפשרת שינוי סיסמה עבור כל חשבון אינסטגרם.

לאינסטגרם עבר לא רע בתוכנית ה-Bug Bounty, כאשר ב-7 במאי ב-2013 מצא חוקר אבטחת מידע בשם Sebastián Guerrero חולשה יפה ופשוטה מאוד שמאפשרת לצפות בתמונות של כל משתמש, כולל משתמשים פרטיים.

סבסטיאן מצא בשירות המפות של אינסטגרם באג ב-API שעוקף את ה-API הפומבי ומאפשר לגשת לכל תמונה בבקשת GET פשוטה. שירות המפות עצמו נזקק לאפשרות הזו על מנת לטעון את התמונות של משתמשים ולהציג אותם על המפה בהתאם למיקום שלהם.
בשירות ה-API שהמפות עבדו איתו, (לא הפומבי) אינסטגרם לא חשבו על מקרה של משתמשים המוגדרים כ-Private ולכן כל בקשת תמונה החזירה תמונה עבור כל משתמש. לקריאה מורחבת על החולשה של סבסטיאן:

https://www.nowsecure.com/blog/2013/06/28/how-i-hacked-your-instagram-account/

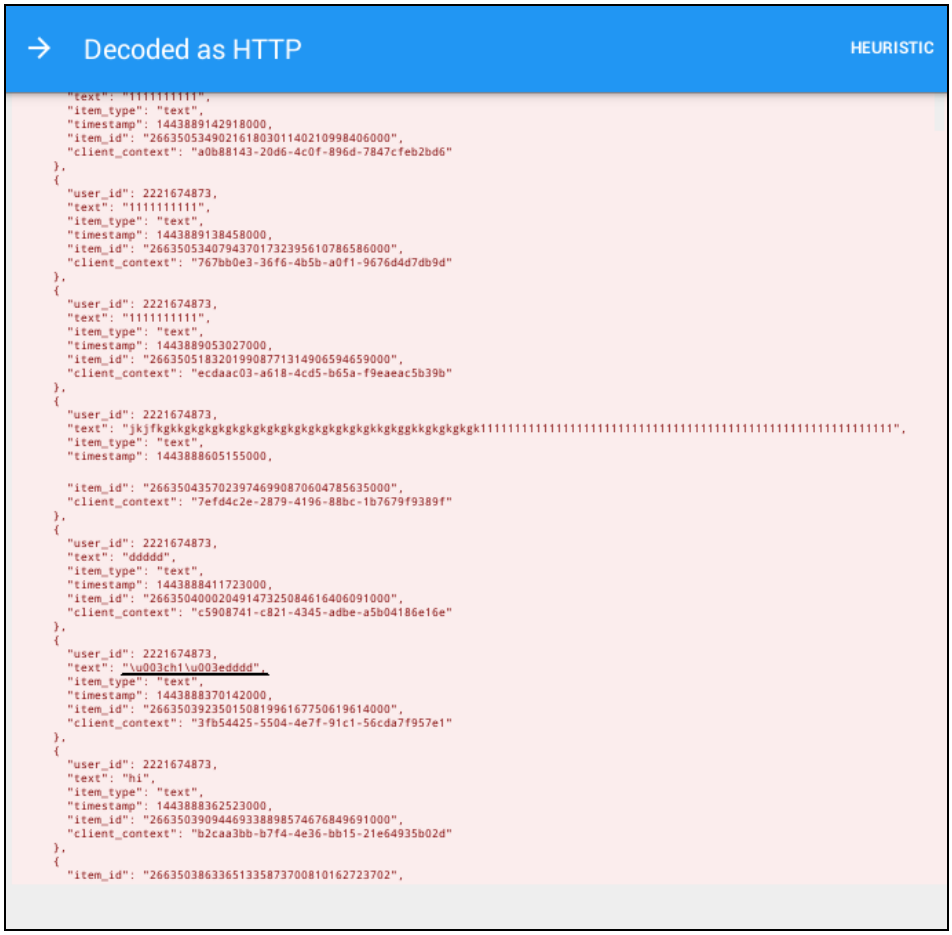
## אז... איך אינסטגרם עובד?

כיום אינסטגרם מתבססת בעיקר על האפליקציה שלה בפלטפורמת המובייל ולאחרונה השיקה אתר מותאם שמאפשרת שימוש גם מהדסקטופ וגם מהנייד.

האתר מוגבל מאוד מבחינת הפונקציות שבו לעומת האפליקציה ולכן התחלתי לחקור אותו. בכל זאת, כדאי להתחיל מקטן ולהתקדם לאט. הכיוון הראשון שהתחלתי בחיפושים אחריו היה פגיעות XSS. הפגיעה מאוד נפוצה ופשוטה לניצול לעומת שאר הפגיעות (RCE,SQLI ועוד).

לאחר כמה שעות שלא מצאתי דברים מעניינים\פגיעים באתר עצמו החלטתי לעבור למחקר של האפליקציה שמכילה הרבה יותר פונקציות ומגוון רחב יותר של פעולות. בחקירת האפליקציה של פלטפורמת המובייל (שתתואר בהמשך) החלטתי ללכת על כיוון של שליחת הודעות פרטיות מסוג Direct. הפונקציה חדשה באינסטגרם ואולי יש בה חורים שטרם נסגרו.

השיטה בה אינסטגרם משתמשת כדי למנוע הרצה של קוד ברמת הדפדפן ידועה ונפוצה - תווים מיוחדים יומרו וישלחו בקידוד מסוג Unicode והאפליקציה תמיר אותם בהצגה בלבד.
כך נראות הפקטות:



יש לא מעט כיוונים שטרם חקרתי כמו יצירת מיקום במפה עם שם\תיאור הכוללים XSS, חיפוש (באפליקציה), XSS בתגובה כאשר מקבל ההתראה יפתח את דף ההתראות וירוץ שם XSS (לא בתצוגת התגובה עצמה) ועוד...

על מנת להבין ולקבל קצת רקע על האפליקציה ואיך היא עובדת השתמשתי במגוון כלים לביצוע Decompile לקובץ ה-APK של האפליקציה.

כיום יש עשרות כלים באינטרנט על מנת להמיר APK לקוד JAVA. בין היתר השתמשתי ב:

- http://forum.xda-developers.com/showthread.php?t=1910873 - **[TOOL] APK to Java RC2**
- http://www.neshkov.com/ac_decompiler.html - **AndroChef Java Decompiler**
- http://bytecodeviewer.com/ - **Bytecode Viewer - Java & Android APK Reverse**

הכלים הללו נתנו לי קצת רקע בסיסי להבין איך האפליקציה עובדת, עם מי היא מדברת, ופרטים אודות בקשות ה-POST שהיא מוציאה בכל פעולת משתמש.

השלב הבא הוא להקליט את הפקטות, להבין את התקשורת וה API אותו האפליקציה מממשת. מכיוון שהאפליקציה מתקשרת SSL - נהיה חייבים להשתמש במכשיר פרוץ (Rooted) או לחילופין להתקין תעודת SSL משלנו שבעזרתה נוכל לקרוא ולפענח את ההצפנה.

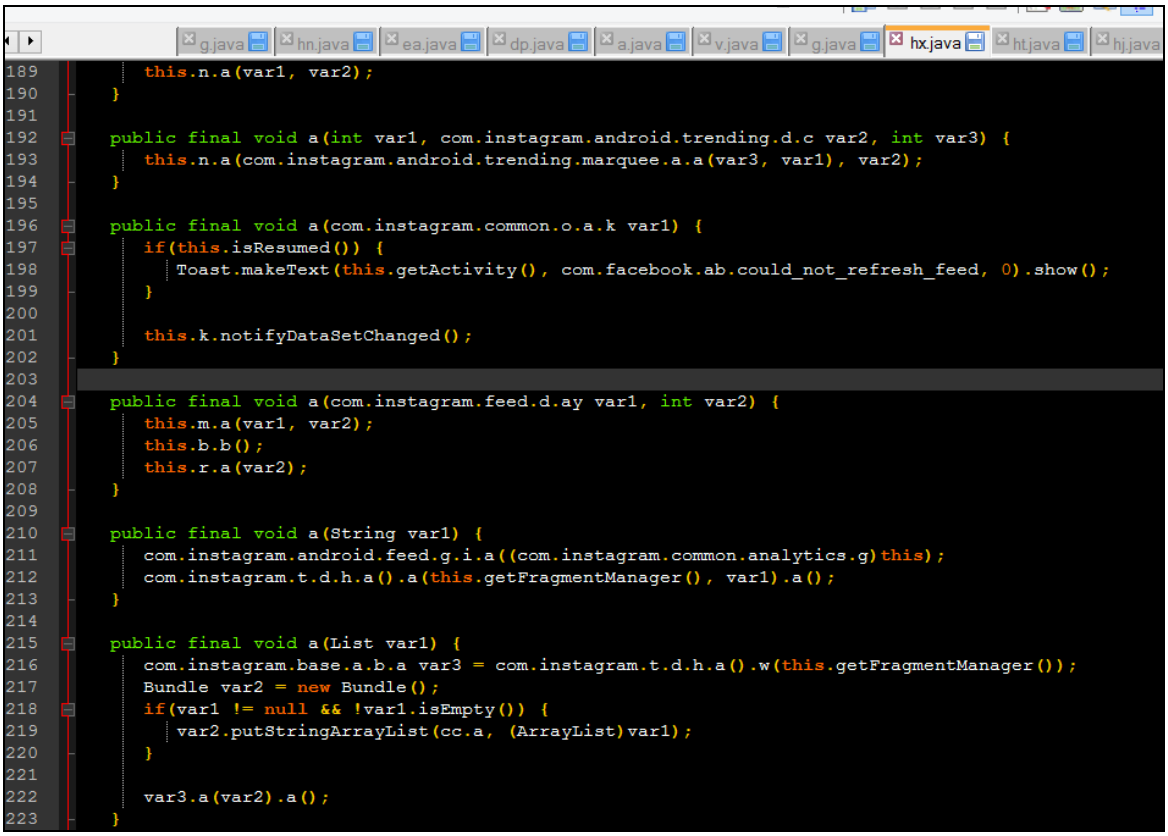
שלל ניסיונות עם Fiddler ו-Burp נכשלו תחת ההודעה "No internet connection" (רק באפליקציה הזו). ולבסוף האפליקציה שהשתמשתי על מנת להתמודד עם הבעיה נקראת "Packet Capture":

- https://play.google.com/store/apps/details?id=app.greyshirts.sslcapture

האפליקציה יוצרת חיבור VPN דרכו תצא התעבורה של כל האפליקציות במכשיר, מקליטה את כל התעבורה ושומרת בצורה נוחה המאפשרת קריאה ישירה מתוך האפליקציה או לחילופין לקובץ pcap רגיל לחלוטין עם תעבורה לא מוצפנת.

בטעות (או שלא) - כאשר האפליקציה מזהה VPN, היא לא מוציאה בקשות ומחזירה שגיאה למשתמש שיש בעיה באינטרנט (כמו קודם - "No internet connection").

קצת מחקר של הקוד יכול להוביל ל-Flow מאוד גדול וארוך (בכל זאת, השימוש בכלי Decompiler אמור לתת רקע ולא קוד מושלם ויפה):




מבחינת המחקר - הגעתי לנקודה בעייתית, לאחר מעט מחשבה והסתכלות על מחקרים קודמים שעשיתי - החלטתי לתת צ'אנס גם הפעם ולחפש אחר גרסה ישנה שעדיין כוללת את רוב הפונקציות שיש כיום.

לאחר חיפוש קצר בגוגל אחר Instagram APK ראיתי גרסאות ישנות מאוד כמו 3.7 ועד לגרסה אחרונה 7.6.1 (נכון לכתיבת שורות אלו). לאחר בדיקה קצרה של גרסאות 4,5 ו-6 החלטתי ללכת על גרסה 5.0.0 שעובדת נהדר עם Packet Capture ומצד שני עדיין כללת לא מעט אפשרויות, וכמובן - ניתן לראות תעבורה לא מוצפנת. ניתן להשיג את הגרסא איתה עבדתי בקישור הבא:

https://www.androidfilehost.com/?fid=23252070760975436

## המעבר מ-XSS לחולשה לוגית - המימוש

כדי שיהיה נוח ונקי - התקנתי אימולטור של אנדרואיד למחשב בשם **Andy** (http://www.andyroid.net) שמאוד נוח ומהיר לעומת המתחרים. (BlueStacks, GenyMotion, Droid4X וכו...). בכניסה הראשונית לאינסטגרם שכחתי את הסיסמה והשם משתמש שלי (גם אני רגיל להתחבר באמצעות הפייסבוק/גוגל למגוון שירותים) ובחרתי ב"שכחתי סיסמה". בשלב זה אינסטגרם הציע לי 3 אופציות לאיפוס הסיסמה:

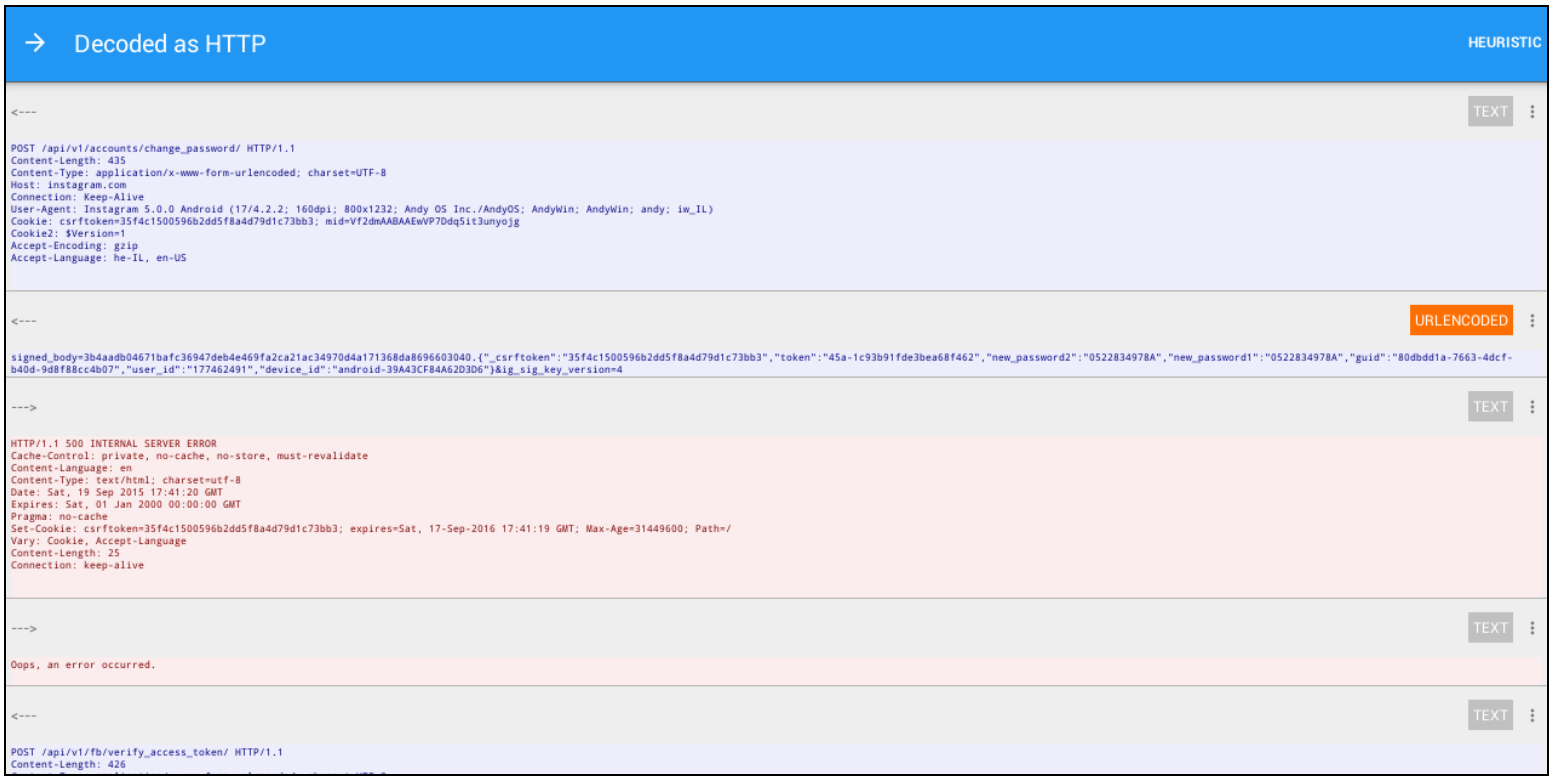
- איפוס באמצעות הודעת סמס.
- איפוס באמצעות אימייל.
- איפוס באמצעות חשבון פייסבוק.

האופציה האחרונה משכה את תשומת ליבי - התהליך מתאפשר רק למי שחשבון הפייסבוק שלו מקושר עם חשבון האינסטגרם (כך רוב המשתמשים).

מרגע זה החלטתי לעצור את הכיוון של XSS ולשנות כיוון למחקר על תהליך איפוס הסיסמה. (אגב, מחקר ה-XSS לא ננטש ובסוף לאחר החולשה הלוגית המשכתי בו ללא הצלחה מרובה...), השלב הבא הוא לבחון את הקוד JAVA שקבלתי בשלב הראשון בשילוב עם הסנפת התעבורה ולהבין היטב כיצד עובד התהליך. דוגמה לפקטות:

**לפני פתיחת ההצפנה:**

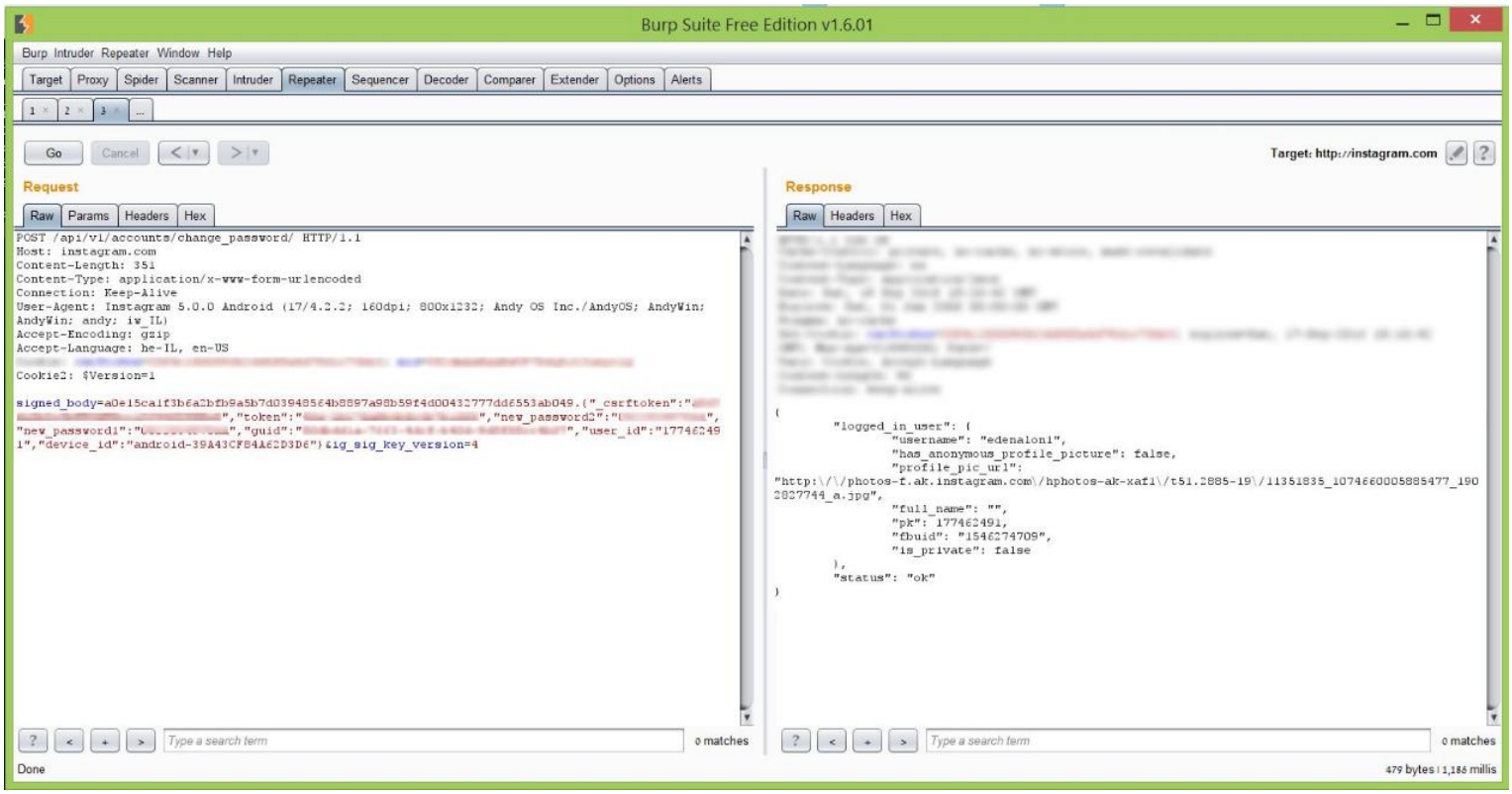
**לאחר פתיחת ההצפנה:**




תהליך איפוס הסיסמה מתחלק ל-2 שלבים:

- **שלב ראשון:** תהליך האימות (Authentication) מול חשבון הפייסבוק - מתבצע באמצעות חיבור לאפליקציית פייסבוק לקבלת token של חשבון הפייסבוק וקישור שלו ל-ID של משתמש אינסטגרם.
- **שלב שני:** שלב איפוס הסיסמה עבור ה-ID שהתקבל מפייסבוק עם נתוני הפייסבוק שהתקבלו. שלב זה מתבסס על כך שכבר נעשה קישור ואימות מול המשתמש ואינו מבצע אימות נוסף בתהליך איפוס הסיסמה עצמו. כלומר - בשלב זה במידה ואערוך את הפרמטר של ה-ID של חשבון האינסטגרם שהתקבל לחשבון אחר ואבצע שינוי איפוס לסיסמה החדשה, הסיסמה עבור חשבון המשויך ל-ID המבוקש.

להלן דוגמה לתשובה מהשרת לאחר שליחת בקשה לאיפוס סיסמה עבור ID מסוים:




בכך השגנו אפשרות לשינוי סיסמה לכל חשבון אינסטגרם. מדובר בחולשה לוגית בשלבי אימות האפליקציה מול המשתמש. במקרה או לא, באחד מאתרי הסחר הנפוצים בחולשות - 1337 (כיום - 0day.today) ישנה חולשה דומה מאוד שנמכרת בסכום לא מבוטל : (רמת האמון שלי באתר לא גבוהה אבל בכל זאת מעניין...)

http://0day.today/exploit/description/23926

## התמודדות מול הגנות באפליקציות

כיום לא מעט חברות ואפליקציות מתחילות להבין ולהפנים שהתחום הולך וגודל וכך גם הסכנות ותחום הסייבר נכנס חזק ומהר מאוד. מבלי להיכנס יותר מידי לתחום הרברסינג במובייל, ישנם לא מעט אפליקציות (חלק ציינתי כאן) שמאפשרות להגיע לקוד JAVA קריא יחסית, אך השאלה הגדולה כיצד ניתן באופן פשוט להתמודד עם קטעי קוד לא רצויים עבורנו בתור חוקרים. ישנה תוכנה לא רעה שעושה עבודה יפה בתחום - Virtuous Ten Studio.

התוכנה מאוד נוחה ומאפשרת לערוך את הקוד של האפליקציות החל מעריכה בסיסית ועד לעריכה מתקדמת מאוד עם שלל כלים ואפשרויות.

היתרון המשמעותי הוא היכולת לערוך ולקמפל חזרה ל-APK חדש היישר מה APK המקורי ללא צורך במספר כלים נוספים. מומלצת בחום לכל חוקר מובייל.

## חולשות לוגיות - סיכום

הכיוון לחקור ולחשוב על כיוונים פשוטים אך מתוחכמים שככל הנראה לא חשבו עליהם נובע מהמקום של החשיבה הפשוטה - Keep It Simple. החולשות הלוגיות נובעות בעיקר מטעויות אנוש בהם המפתחים לא דאגו מספיק טוב לאותנטיקציה מלאה בכל השלבים, ממשקי ניהול חשופים ועוד...

לא מזמן נחשפנו אודות חולשה לוגית ביוטיוב, כאשר נשלחת בקשה למחיקת סרטון באמצעות משתמש מחובר (מאומת ותקין) לא מתבצעת ולידציה האם הסרטון המבוקש למחיקה אכן משויך לאותו חשבון ובכך התאפשר לכל משתמש למחוק כל סרטון באתר. לפרטים נוספים על הפגיעה ניתן לקרוא כאן:
http://thehackernews.com/2015/04/hack-delete-youtube-video.html

מאמר נוסף על חולשה בפייסבוק המאפשרת למחוק כל תמונה:
http://thehackernews.com/2015/02/hacking-facebook-photo-album.html

בקרוב מאוד מקווה לפרסם מאמר נוסף המאפשר לשנות את פרטי החשבון באינסטגרם ובכך להוביל ב-Flow ספיציפי לאיפוס\שינוי סיסמה. ☺ (פרומו: זה עובד!)

## אודות

עדן אלון: תעקבו באינסטגרם - edenalon1 ;)
אם יש שאלות או הצעות אשמח לענות - adming4f@gmail.com.