Technologic Papers

שימוש במזהה חד חד ערכי לאיתור מאגרי מידע פרוצים

מאת: אמיתי דן

הקדמה

גיגול עצמי ("Self Googling" או "Egosurfing") יכול להעלות לפעמים תוצאות מעניינות. בעבר יצא לי לחפש על עצמי בגוגל, ולמצוא נתונים מעניינים על אנשים עם שמות דומים. האמת היא שמציאת מידע על אנשים דרך האינטרנט זה לא תחום שנולד היום, וישנם אתרים רבים המתמחים בו, ישנם מנועי חיפוש שכל תפקידם הוא לתת שירות שיאפשר לבסוף קבלת פלט מהיר על האדם שאותו מחפשים, כדוגמת מנועי החיפוש: pipl.com ו-123people.com.

חשוב לציין כי התחום, המכונה People Search, נחשב לאחד התחומים הלוהטים ברשת האינטרנט כבר מעל 5 שנים. בשקט בשקט, זו אחת התעשיות המוכרות יותר לאנשי שיווק באינטרנט, וכמות האנשים המחפשים פרטים על אנשים אחרים היא עצומה ורק מתגברת כל הזמן.

מבחינת דרכי חיפוש באתרים אלה - הנתונים שאנו נדרשים לספק לרוב הינם שמות משתמש, שם פרטי ושם משפחה, מיקום מגורים, ואם אפשר אז גם מספר טלפון. כאשר מתקבל הפלט, ניתן להבין בבירור כי הנתונים הללו, המשמשים לאיתור פריטים שאדם עלול להשאיר בשטח האינטרנטי, אלו הנתונים שבדרך כלל אותו אדם סיפק. איסוף הנתונים שהאדם עצמו סיפק זאת נקודת התחלה לא רעה, אבל בדרך כלל (ומי שהתנסה, יכול להעיד כי קיימים מקרים מפתיעים מאוד...) נתונים אלו יהיו נתונים שטחיים.

כשניגשתי לנושא, הנחת המוצא שלי הייתה שאדם סביר לא ישאיר באינטרנט נתונים האישיים, כמו הקוד הסודי לבנקאי שלו, ולחלופין תעודת הזהות שלו שהינה כלי חשוב להזדהות מול מקומות רבים. כשצללתי וחקרתי את הנושא הבנתי שאם מישהו השאיר את תעודת הזהות שלו גלויה באתר כזה או אחר, כנראה שהתרחש פרסום לא מכוון מצידו. למשל - יתכן שהוא מילא עצומה, פרסם קורות חיים או פעולה דומה בסגנון ללא הבנה כי מידע זה יהיה ציבורי. מהצד שני - במקרים אחרים נראה שקרה משהו אחר - מישהו, ברשלנות, חשף את הפרטים של אנשים שמסרו פרטים.

אלפי פרטים אישיים בקליק אחד

אחרי אבחנות אלה החלטתי לנסות ליישם על עצמי, ולראות האם מישהו הפר את הפרטיות שלי ופרסם את תעודת הזהות שלי בפומבי. לצערי צדקתי - מבלי להיכנס לפרטי האתר הספציפי התברר לי לבסוף שלא רק שהזהות שלי הופקרה ונחשפו בפומבי פרטים אישיים שלי, אלא שלקוחות רבים של החברה היו חשופים אף הם וגם החברה התברר, חשפה את עצמה. לאחר שהתרעתי לבעל החברה על הנושא (שאכן תוקן) הבנתי שניתן לקחת את הנושא צעד קדימה ככלי למציאת פרצות אבטחה באתרים ומערכות מידע

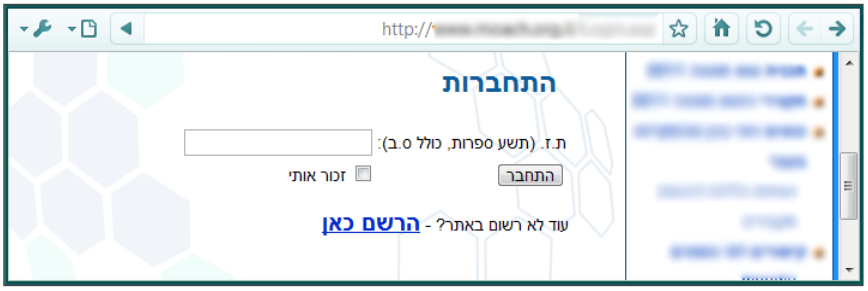
רבות. מספר טלפון הנו נתון שלעיתים קרובות מפורסם בפומבי ולכן איתור שלו לא יחשוף בפנינו בהכרח רשומות חסויות (למרות שגם כאן אתם צפויים להפתעות), לעומתו מספר תעודת הזהות, שהוא פריט נדיר יותר, ושימוש בו ככלי חיפוש יחשוף בפומבי את האזרח שאליו הוא מוצמד.

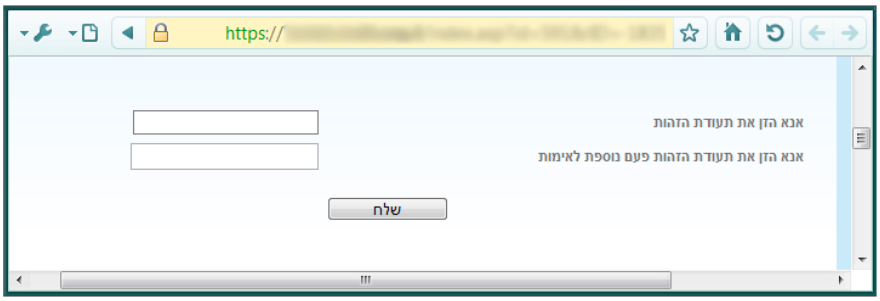
וכאן נכנס השלב השיטתי: כדוגמא ראשונית וקלה ליישום סטודנטים לעיתים מקבלים את נתוני תוצאות הבחינות בשיטה של תעודות זהות גלויות ללא שם (דבר שבעייתי בעיני כי הוא חושף אותם לבעיות זהות אחרות). אם נחפש בגוגל את מספרי התעודות ייתכן מאוד שנמצא מאגרי מידע פרוצים ואף גישה ליכולות ניהול לא צורך בהזנת סמת מנהל.

[חיפוש אחד - מאות תעודות זהות]

בשלב מתקדם יותר ניתן לנצל מאגרי מידע פרוצים עם מספרי תעודות זהות כגון אגרון בישראל (או Social Number) ולהגדיר את החיפוש לפי מדינת המוצא של המאגר. במהלך המחקר מצאתי גם טופס התעניינות למכללה שפורסם באופן לא חוקי בפומבי, יחד עם פרטי המתעניינים שבו נכלל רקע לימודי, תחום לימודים מבוקש מקום מגורים ופרטים נוספים. גם מקרה זה נפתר לאחר שלחצתי על המכללה הספציפית לפתור את הנושא.

מלבד הפרטיות הנחשפת עקב נתונים אלו, קיימות מערכות (שחלקן מנוהלות על ידי גופים פורמליים או עובדות בשיתוף פעולה עם גופים אלו) שתפקידן הוא לספק שירותים (כדוגמת דרכים להרשמה להטבות כאלה או אחרות) למגזר ספציפי. מבדיקות נראה כי במספר טפסי הזדהות ישנו הצורך להכניס את תעודת הזהות של העובד בלבד.





אם ניקח לדוגמא, את המגזר העסקי-מדיני, ישנן מערכות באינטרנט המאפשרות לעובדי מדינה להירשם להטבות כאלה או אחרות המוצעות כמסלול הניתן מחברות אזרחיות. אותן החברות מפרסמות פורטלים שלמים למגזר ספציפי (בדרך כלל מדובר במערכת אחת, עם מספר ממשקים המשוכפלים לכל מגזר בפני עצמו). לאחר שמצאנו את ממשק ההזדהות לאותו הפורטל וזיהינו את המגזר אליו הוא מופנה, נוכל לחפש רשימות המכילות את אותו מזהה ודרכן לשלוף את פרטי המידע שיעזרו לנו להיכנס לאותן מערכות.

כמו שניתן, על ידי שאילתת חיפוש אחת בגוגל למצוא תעודות זהות של סטודנטים רבים, ניתן להסב את החיפוש ולמצוא רשימות ארוכות הכוללות רשימות תעודות זהות של עובדי מדינה. מכאן ועד לפגיעה אישית באותו עובד או אפילו איסוף נתונים על עובדי משרדים כאלה ואחרים - הדרך קצרה מאוד.

סיכום

עקב הפשטות של השיטה מומלץ לכל אחד מאיתנו לבדוק האם חברה או גוף שאיתו הוא עמד בקשר בעבר פירסם את הנתונים האישיים שלו. לרוב כשחברה כזאת פירסמה אותך היא מפרסמת נתונים שיזיקו לה באופן ישיר ולכן הטיפול בבעיות אלו יהיה לרוב מהיר. ככלי לבדיקה עצמית הייתי ממליץ לחברות אלו לסרוק באופן אקראי את האתרים של עצמן ולבדוק האם המאגרים שלהם חשופים. מהניסיון שלי, לעיתים קרובות ישנו שער נעול אבל החומה עצמה חסרה, ולכן ניתן יהיה לנסות לפרוץ את השער אך בקלות רבה יותר להיכנס מהצד ללא הפעלת כח רב.

כלי מעניין בנושא זה הוא Google Dorks - זוהי דרך שבה כל אחד מאיתנו יכול לבדוק כיצד להגן על עצמו, על הזהות שלו ולבדוק אם היא נפגעה במהלך הדרך הדיגיטלית שלו, וזאת בדומה לכלי הבדיקה שיוצרו לבדיקה לאחר פריצת מאגרי המידע עם כרטיסי האשראי.

גם במקרה זה וגם בשני, מדובר על חברות שמחזיקות מאגרי מידע בצורה לא מוגנת ולכן חובה עלינו כאזרחים לבדוק האם נפגענו. ברור לי שניתן לנצל זאת גם ככלי לתקיפה של אתרי אינטרנט אקראיים אך לכן יש להזהיר על היתכנות זו.

קישורים

- **http://www.google.com**
- http://www.123people.com
- http://www.pipl.com
- http://www.yoname.com
- http://www.zoominfo.com
- http://www.zabasearch.com