אתגר סייבר – מעבדת התקפה

סמסטר א שנה ג

# פרטי המגישים

|  |  |  |
| --- | --- | --- |
| מגישים | דואר אלקטרוני | תעודת זהות |
| **עוז לוי** | [ozmaatuk@gmail.com](mailto:ozmaatuk@gmail.com) | 305181158 |
| **אבישלום ג'אן** | [avishalom14@gmail.com](mailto:avishalom14@gmail.com) | 308481423 |

# תיאור האתגר

## נקודת פתיחה

* כתובת DNS/IP לאתר אינטרנט. Logforkey.com

## מטרת האתגר

* המטרה היא להתחבר לשרת עם גישת קריאה/כתיבה לקבציי ה-admin ולהגיע לקובץ סודי (secret).

## מהלך האתגר

* למשתמש מופיע אתר אינטרנט המציג דף התחברות, עבור משתשמשים טריוויאלים.
* **נתיב א':**
  + - ההתחברות ע"י שם וסיסמא, למשתמש יועבר לדף שיאמת את נתוניו ויעביר לדף מתאים אם ההתחברות נכשלה או הצליחה.
  + רמזים בהסטוריית המחשב או בשם של מפתח האתגר
* **נתיב ב':**
  + מעבר ישיר ע"י גילוי כתובת דף היעד (אשר מופיע לאחר התחברות מאומתת)
  + רמזים בשמות הדפים
* **שלב SQLi (weby - ניתן לדלג באמצעות ניחוש משתמש וסיסמא ל-SSH)**
  + הפרצה ל sql injection תהיה בדף שיופיע לאחר התחברות מוצלחת לאתר.
  + לאחר ביצוע sql injection מוצלח למשתמש יהיה הרשאות מלאות ע"י סיסמת ה admin שהשיג, ובזה נגמר האתגר.
* **שלב – System (התחברות ב-SSH)**
  + במערכת רץ שירות שסוגר את ה SSH, (משתמש רגיל כעבור 5 שניות, משתמש ניהולי -15)  
    ניתן להתגבר על השירות ע"י מחיקת הסקריפט או שינוי קובץ crontab.
  + חיבור עם משתמש אדמין (סיסמא שהושגה בשלב ה-SQLi).
  + חיבור עם משתמש רגיל שנוחש בחלק הראשון
    - הbash- יהיה הרוס. (פקודת CD והשלמה אוטו' לא עובדים) – ניתן להחליף את ה-SHELL או למצוא דרך גישה אחרת.
    - דף המעבר (LOADING.HTML) יכיל רשימת משתמשים לכניסה לאתר, כאשר רק אחד מהם הוא סודו והסיסמא שלו קשה לפיצוח.

## שלב סיום

## חיפוש קובץ מוחבא (מוסתר) בשם secret ולסיים את האתגר.