הזרקת SQL מתקדמת

מבוא:

בתרגיל זה נתרגל הזרקת SQL מתקדמת.

בתרגיל זה נשתמש בהזרת SQL על מנת:

1. למצוא את שמות כל הטבלאות של בסיס הנתונים המותקף ובפרט את טבלת המשתמשים
2. למצוא את שמות כל העמודות של טבלת המשתמשים
3. למצוא את שמות כל המשתמשים וה-HASH-ים של הסיסמאות שלהם
4. לאחר מכן נשתמש בהתקפת מילון כדי לשחזר סיסמא מ-HASH

הוראות:

היכנסו לעמוד http://localhost/DVWA/vulnerabilities/sqli.

שם המשתמש הוא admin והסיסמא היא 12

לפני תחילת העבודה שנו את הגדרות האבטחה של האפליקציה

1. בתפריט שבצד שמאל לחצו על DVWA Security
2. ברשימה הנפתחת שליד הכפתור Submit בחרו Low
3. לחצו על הכפתור Submit
4. חזרו לעמוד http://localhost/DVWA/vulnerabilities/sqli

בדקו האם העמוד מכיל חולשה שמאפשרת להזריק SQL. (א) באמצעות איזו שאילתא בדקתם?

השתמשו בהזרקת UNION SELECT כדי למצוא את מספר העמודות בפלט השאילתא. (ב) לאור הממצאים שלכם, כמה עמודות יש בפלט השאילתא?

הזריקו שאילתא שמאפשרת למצוא את שמות כל הטבלאות בבסיס הנתונים dvwa. (ג) מהי השאילתא ומהם שמות הטלבאות?

הזריקו שאילתא שמאפשרת למצוא את שמות העמודות בטבלת המשתמשים. (ד) מהי השאילתא ומהם שמות העמודות?

הזריקו שאילתא שמאפשרת למצוא את כל הזוגות (שם משתמש, סיסמא). (ה) מהי השאילתא ומהם שמות המשתמשים? שימו לב שהסיסמא היא למעשה ה-MD5 HASH של הסיסמא האמיתית.

צרו קובץ שמכיל את שם המשתמש admin ואת ה-MD5 HASH של הסיסמא שלו מופרדים ב- : .

הפעילו את

```
/snap/bin/john --format=raw-MD5 hash.txt
```

וודאו שאתם מקבלים את הסיסמא 12

הוראות הגשה

1. יש להגיש קובץ PDF עם תשובות לשאלות (א)-(ה) וצילום מסך בו נראית הסיסמא שנמצאה ע"י John the Ripper
2. כל אחד מחברי מהקבוצה צריך להגיש.
3. שם הקובץ צריך לכלול את מספרי ת.ז. של כל חברי הקבוצה.

בהצלחה!