הזרקת SQL

מבוא:

בתרגיל זה נתרגל את ההתקפה "הזרקת SQL". התקפה זו מאפשרת לתוקף להכניס לבסיס נתונים מידע משובש (שלא עבר אימות של התוכנה שרצה בשרת) או לשלוף ממנו מידע רגיש.

בתרגיל זה:

1. נבדוק האם דף להוספת הודעות טקסט מכיל חולשה שמאפשרת לבצע הזרקת SQL
2. נוסיף הודעת טקסט עם תאריך שגוי
3. נשתמש בהודעת השגיאה בדף כדי לראות את סימסת המשתמש admin

הוראות:

[] הוספת הודעה:

1. היכנסו לכתובת:

http://localhost/mutillidae/index.php?page=add-to-your-blog.php

2. נסו להכניס הודעה רגילה וודאו שהיא מופיעה בתחתית הדף
3. בדקו האם הדף מכיל חולשה שמאפשרת לבצע הזרקת SQL באמצעות הכנסת ' במקום ההודעה
4. נסו לדלות מידע מהודעת השגיאה:
    1. כמה ערכים מוכנסים לטבלה בכל הוספת הודעה
    2. על איזה מהערכים אנחנו יכולים להשפיע?
    3. באיזה תאריך מפורסמת כל הודעה חדשה?
    4. כיצד נוכל לשנות את תאריך הפרסום ל-14/05/1948 בשעה 16:00?
5. הוסיפו הודעה בתאריך שמופיע מעלה עם שמות חברי הקבוצה (שמרו צילום מסך)

[] אחזור סיסמת המשתמש admin. אילו היינו יכולים להשפיע בשאילתא על שדה מסוג טקסט, היינו יכולים לכתוב לתוכו את תת-השאילתא הבאה:

(select password from accounts where username='admin')

לצערנו אנו יכולים להשפיע רק על שדה מסוג תאריך. ניסיון לכתוב לשדה זה מחרוזת, גורמת לשגיאה. לכן, כדי לאחזר את סיסמת המשתמש admin יש לבצע

1. בצעו הזרקת SQL, בה לשדה התאריך נכתבת המחרוזת שמוחזרת ע"י תת-השאילתא שמופיעה מעלה
2. נתחו את הודעת השגיאה שמופיעה על המסך ומצאו בה את הסיסמא (שמרו צילום מסך)

הוראות הגשה

1. יש להגיש שני צילומי מסך (תמונת JPG/PNG)
    1. צילום מסך עם תאריך משובש ושמות חברי הקבוצה
    2. צילום מסך בו סיסמת המשתמש admin מוקפת במלבן שחור
2. כל אחד מחברי הקבוצה צריך להגיש.
3. שם הקובץ צריך לכלול את מספרי ת.ז. של כל חברי הקבוצה.

בהצלחה!