CSRF

מבוא:

בתרגיל זה נתרגל את ההתקפה "Cross-site request forgery (CSRF)". התקפה זו מאפשרת לתוקף לבצע פעולות בשם משתמש אחר.

בתרגיל זה:

1. נוסיף רשומה זדונית לספר האורחים שתגרום לשינוי הסיסמא של מי שמעביר מעליה את העכבר
2. נמתין שהמשתמש admin יעביר מעל הרשומה את העכבר
3. נתחבר עם שם המשתמש admin והסיסמא החדשה שבחרנו

הוראות:

הוספת רשומה

1. היכנסו ל-DVWA עם שם משתמש 1337, סיסמא charley ועברו לעמוד XSS (Stored)
2. שנו את הגודל של השדה Message ל-500 תווים
3. כתבו בשדה Name את שמות התלמידים בקבוצה
4. כתבו בשדה Message הודעה כך שכאשר מעבירים מעליה את מבוצע מעבר לכתובת אחרת
   1. הפקודה ששמנה את הכתובת של עמוד הנוכחי היא:
      window.location.href=
   2. הכתובת שאליה נרצה לעבור היא כתובת שגורמת לשינוי הסיסמא. הסיסמא הרצויה היא pass.
      היכנסו לעמוד CSRF שבתפריט השמאלי ונסו לשנות את הסיסמא כדי להבין כיצד נראית הכתובת הרצויה. שאלה א': האם המידע נשלח לשרת בצורת GET או בצורת POST?
5. לחצו על Sign Guestbook
6. בצעו logout

   שאלה ב': מה כתבתם בשדה Message?

צפייה ברשומה

7. היכנסו ל-DVWA עם שם משתמש admin, סיסמא password ועברו לעמוד XSS (Stored)
8. העבירו את העכבר מעל הרשומה שהוספתם
9. דבר זה גרם לשינוי הסיסמא של המשתמש admin
10. בצעו logout
11. התחברו שוב כמשתמש admin עם הסיסמא החדשה (pass).

הוראות הגשה

1. יש להגיש קובץ PDF שמכיל תשובות לשאלות א'-ב'.
2. שם הקובץ צריך לכלול את מספרי ת.ז. של כל חברי הקבוצה.

בהצלחה!