XSS

מבוא:

בתרגיל זה נתרגל את ההתקפה "Cross Site Scripting (XSS)". התקפה זו מאפשרת לתוקף לבצע קוד בשם משתמש אחר.

בתרגיל זה:

1. נוסיף רשומה זדונית לפורום
2. נמתין להתחברותת של משתמש admin ונייירט את ה-session id שלו
3. נשתמש ב-session id כדי לשנות את הסיסמא שלו
4. נתחבר לאתר באמצעות הסיסמא החדשה

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 אשר תשלח את ה-Cookies באופן סמוי ל-
http://localhost/cgi-bin/logit.pl
5. לחצו על Sign Guestbook
6. בצעו logout

שאלה א': מה כתבתם בשדה Message?

צפייה ברשומה

7. היכנסו ל-DVWA עם שם משתמש admin, סיסמא password ועברו לעמוד XSS (Stored)
8. הכניסה לעמוד גרמה להרצאת הסקריפט logit.pl וכתיבת ערכי ה-cookies לקובץ לוג:
/var/www/logdir/log.txt

שאלה ב': מה הם השמות והערכים של שני ה-cookies שנשמרו בקובץ?

9. עברו לעמוד CSRF, שתפקידו לשנות את סיסמת המשתמש הנוכחי, וענו על השאלות הבאות

שאלה ג': מה הוא סוג הטופס שמופיע בעמוד (POST או GET)?

שאלה ד': מה הם שמות השדות שבטופס?

שינוי סיסמא

10. כדי לשנות סיסמא של המשתמש admin, נשלח את הטופס שבעמוד CSRF עם ה-cookies של המשתמש admin שיירטנו. לצורך כך נריץ פקודה שנראית כך:

```
curl -b "cookie1=value1;cookie2=value2;cookie3=value3"
 --location "http://localhost/DVWA/vulnerabilities/csrf/?
field1=value1&field2=value2&field3=value3"
```

כאשר cookieX הוא שם ה-cookie אותו נרצה לשלוח ו-valueX הוא הערך שלו

ובאופן דומה fieldX הוא שם השדה בטופס ו-valueX הוא הערך שלו

11. שנו את הסיסמא של המשתמש admin ל-1234.

שאלה ה': מה היא הפקודה שהרצתם?

הוראות הגשה

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

בהצלחה!