בס"ד

הצעת פיתוח – אבישי גונן

בתרגיל זה נעשה שימוש ב-6 נושאים שונים: שימוש ב wireshark, גישה לשרת שנוצר לצורך הפרוייקט, פרוטוקול HTTP, פרוטוקול DNS, הצפנה, scraping מיוטיוב בקטנה?

שלב א – רשתות

בשלב הראשון המשתמש יקבל איזשהו סיפור כיסוי שמספר על "יוסי" (שם בדוי)[1], המשתמש יקבל איזשהו סיפור שיכלול הסנפה, שתכיל בתוכה בקשת NSLookup לאתר שלי, וככה מה ה domain של האתר שלי. (חלק מהשם של האתר שלי זה "ctf", ככה הוא ידע איך לחפש אותו..)

התוצר של השלב הזה הוא שהמשתמש יודע לאיזה domain לגשת.

שלב ב – הצפנה

המשתמש יופנה לדף הפתיחה, ששמה תהיה תמונה מגניבה, ולמטה יהיה איזשהו מפתח 16byte, וכן IV 16byte.

על המשתמש יוטל להצפין את התמונה ב AES-CBC עם המפתח וה IV שהוא קיבל.

באותו דף פתיחה יהיה גם אופציה ללחוץ על כפתור "enter_password", שיעביר אותו לדף אחר באותו אתר, ששם יהיה רשום סיפור קורע לב על אותו "יוסי" ששכח את הסיסמא שלו, וישמח אם מישהו יוכל לעזור לו למצוא אותה. באותו דף גם יהיה תיבת הכנסה לשם משתמש וסיסמא.

בשלב הזה המשתמש עוד לא יודע מה הסיסמא, אבל בהמשך הוא יגלה.

התוצר של השלב הזה זו איזשהיא תמונה חדשה שהמשתמש יקבל, שתכיל בתוכה קישור לסרטון יוטיוב, ובנוסף, כיתוב שרשום בו כך: "hint: comments"

שלב ג - scarping

בסרטון היוטיוב הזה אותו "יוסי"[2], ישאיר איזשהו מפתח בנוסף ל comment הנורמלי שהוא מפרסם. באותה תגובה יהיה רשום משהו בסגנון של "remember to backup my password: check"

התוצר של השלב הזה כך שהמשתמש יודע מה הסיסמא ל user "יוסי" .

שלב ד – http

בשלב הזה המשתמש יחזור לאתר לדף שאליו הוא לא ידע מה הסיסמא במקור, אלא שעכשיו הוא מצא.

במידה והמשתמש יכניס את שם המשתמש "יוסי", ואת הסיסמא שהוא מצא ביוטיוב, הוא יקבל הודעה שזהו, הוא סיים את ה CTF!

---

[1] עדיין לא חיברתי לגמרי את הסיפור, אני אמציא משהו מעניין

[2] עדיין לא החלטתי מה בדיוק זה יהיה, בכל מקרה אני אעשה שזה יהיה משהו בולט