ברוכים הבאים לאתגר ה-CTF של Bleichenbacher

התקפתו של Bleichenbacher

במהלך האתגר נממש את ההתקפה Bleichenbacher אשר מאפשרת להעלות מספר בחזקת המפתח הפרטי של פרוטוקול הצפנה בהינתן אורקל לריפוד.

אנא קראו על ההתקפה כאן (עמודים 1-5).
לאחר מכן נעבור לממש חלקים מהמתקפה כחלק מאתגרי ה-CTF.
אם חלק מסוים בטקסט אינו ברור, אתם מוזמנים לחפש באינטרנט מונחים שלא הבנתם.
ניתן לפנות אלינו בכל שאלה.

במהלך ה-CTF עומדים לרשותכם שני שרתים: שרת אורקל ושרת CTF.

מטרתו של שרת האורקל היא לספק תשובה לשאילתות ריפוד.
בהינתן c,N השרת יחזיר האם c^d % N מרופד היטב.

מטרתו של שרת ה-CTF הוא לנהל תקשורת עם קוד הממשמש חלקים מהמתקפה ולבחון את נכונות הפתרון המתקבל אליו.
למשל אם עליכם לשלוח מספר s אשר מהווה ערך blinding חוקי (אתגר 1), בהינתן מספר השלב והפיתרון שלכם לשלב הזה השרת יבדוק האם s הוא אכן ערך blinding אפשרי. אם כן, תוחזר אליכם הסיסמה לשלב הבא.

שימו לב: לאורך כל השלבים E=65537. עם זאת N ו-m משתנים משלב לשלב.

אתגר 1 - (Step 1 במאמר) - (10 נק')

במהלך אתגר זה תממשו את פעולת ה-blinding.
באתגר יהיו נתונים לכם

N : int
E : int
C : int

עליכם לשלוח ערך s אשר מהווה ערך blinding התחלתי חוקי בהתאם ל-Step 1 במאמר.
במידה ותצליחו תוחזר אליכם הסיסמה לשלב הבא.

אתגר 2 - (Step 2a במאמר)- (15 נק')

במהלך אתגר זה תממשו את חישוב ערכו של s1 באיטרציה הראשונה של המתקפה.
באתגר יהיו נתונים לכם

N : int
E : int
C0 : int

עליכם לשלוח ערך s1 חוקי עבור האיטרציה הראשונה בהתאם ל-Step 2a במאמר.

אתגר 3 - (Step 2b במאמר)- (15 נק')

במהלך אתגר זה תממשו את חישוב ערכו של s_i באיטרציה של המתקפה כאשר בקבוצת הטווחים הנוכחית יש יותר מטווח אחד.

באתגר יהיו נתונים לכם

N : int
E : int
C : int
M : DisjointSegments
prev_s : int

כאשר M הוא מטיפוס DisjointSegments אשר הוגדר בקוד בקובץ disjoint_segments.py, אשר מייצג את קבוצת הטווחים בהם ידוע כי ההודעה נמצאת באחד מהם.
בנוסף, prev_s מייצג את ערך ה-s מהאיטרציה הקודמת.
עליכם לשלוח ערך s חוקי עבור האיטרציה הנוכחית בהתאם ל-Step 2b במאמר.

אתגר 4 - (Step 2c במאמר)- (20 נק')

במהלך אתגר זה תממשו את חישוב ערכו של s_i באיטרציה של המתקפה כאשר בקבוצת הטווחים הנוכחית יש טווח אחד בדיוק.

באתגר יהיו נתונים לכם

N : int
E : int
C : int
M : DisjointSegments
prev_s : int

כאשר M מייצג את קבוצת הטווחים בהם ידוע כי ההודעה נמצאת באחד מהם. קבוצה זו היא בגודל 1.
בנוסף, prev_s מייצג את ערך ה-s מהאיטרציה הקודמת.
עליכם לשלוח ערך s חוקי עבור האיטרציה הנוכחית בהתאם ל-Step 2c במאמר.

<u>הבהרה:</u>
נגדיר את פתרון צעד 2c במאמר באופן מפורש:
עליכם למצוא את ערך ה-r השלם המינימלי כך ש- $r_i \geq 2 \cdot \frac{b \cdot prev\_s - 2B}{N}$ ועבור $s_i = \lceil \frac{2B + r_i N}{b} \rceil$

מתקיים כי $\left(c_0 \cdot s_i^E\right) \ \% \ N$ מרופד היטב.

אתגר 5 - (Step 3 במאמר)- (30 נק')

במהלך אתגר זה תממשו את חישוב ערכו של M_i באיטרציה של המתקפה.

באתגר יהיו נתונים לכם

N : int
E : int
C : int

prev_M : DisjointSegments
prev_s : int

כאשר prev_M הוא קבוצת הטווחים האפשריים עבור ההודעה באיטרציה הקודמת.
בנוסף, prev_s מייצג את ערך ה-s מהאיטרציה הקודמת.
עליכם לשלוח ערך M חוקי עבור האיטרציה הנוכחית בהתאם ל-Step 3 במאמר.

אתגר 6 - (Steps 1-4 במאמר)- (20 נק')

במהלך אתגר זה תפענחו את ההודעה המוצפנת.

באתגר יהיו נתונים לכם

N : int
E : int
C : int

עליכם לשלב את השלבים הקודמים, לפענח את ההודעה (בהתאם ל-Step 4 במאמר) **ולשלוח** את m (ההודעה המקורית [כמספר שלם]).