תרגיל ראשון

SQL injection

מועד הגשה – 27.04.23

תכנות בטוח – 89509

הנחיות כלליות

- עבודה ביחידים בלבד.
- ניתן להיעזר במקורות אינטרנטיים, אך יש לציין באילו מקורות השתמשתם. בכל מקרה, אל הפתרון הסופי יש להגיע לבד.
- כל סקריפט אותו כתבתם לצורך פתרון התרגיל חייב להיות מצורף. בראש הסקריפט יש לכתוב בהערה מדוע כתבתם את הסקריפט ואיך הוא עזר לכם לפתרון התרגיל. הסקריפט צריך להיות מותאם לפייתון גרסה 3.8 ללא תלויות שאינן טריוויאליות.
- הפעילו שיקול דעת.

מבוא – טעינת Container של התרגיל

לצורך הרצת התרגיל, עליכם להתקין דוקר, תוכנה נפוצה שמטרתה להריץ קונטיינרים – מעין vmים קלי משקל. התקנת דוקר עלולה להיות מסובכת, ולכן אנו מאחלים לכם הצלחה רבה בתהליך ההתקנה.

צורפו לכם images docker שמטרתם לדמות שאת Web ושרת SQL מסוג MySQL החשופים להתקפה מסוג SQLi. על מנת לטעון את התמונות, ניתן ורצוי להשתמש ב-docker-compose. לאחר טעינה מוצלחת, השרת יופעל בפורט 8000, בכתובת localhost.

על מנת שהתרגיל יעבוד כראוי, לפני ההתחלה עליכם לגלוש לכתובת `localhost:8000/resetdb.php` גישה לכתובת זו מוחקת את כל נתוני השרת, ולכן גם במידה וברצונכם להחזיר את השרת למצבו המקורי, ניתן לגלוש לכתובת זו.

לחלק מהURLים אליהם תגלשו, ניתן להוסיף GET parameters מהצורה `hint=<number>` ולראות רמזים עבור התרגיל. לפעמים יש רמז אחד, לפעמים יותר, ולפעמים אין. השתדלו לפתור את התרגיל בלי רמזים. בכל מקרה, בפתרון הסופי שלכם, אין להשתמש ברמזים.
בתרגיל ניתן להוסיף משתמשים לצורך בדיקה, ניתן להשתמש בתכולה הזו, אך אין להסתמך עליה בפתרון התרגיל.

צורף סקריפט start.sh שמטרתו לבנות ולהפעיל את התרגיל. הסקריפט הוא אמצעי עזר ולכן כנראה לא יעבוד בחלק מהמחשבים. בכל מקרה, מומלץ לקרוא אותו על מנת להבין כיצד מצופה מכם להריץ את התרגיל.

סעיפי התרגיל

סעיף ראשון - page injection basic - php.login – נסו להתחבר למסד הנתונים, בעזרת המשתמש של בוב! שם המשתמש של בוב הוא bob.
סעיף שני – בעזרת ממשק החיפוש, מצאו מידע על השרת – איזה user מחובר, באיזה host ומה הגרסה של השרת.
סעיף שלישי – בעזרת ממשק החיפוש, גלו מה הסיסמא של פרודו.
סעיף רביעי– קיימת טבלה סודית במסד הנתונים sqlitraining. בעזרת ממשק החיפוש, מצאו את הטבלה הסודית, ואת כל השדות שנמצאים בה.
סעיף חמישי – נאמר שיש מסד נתונים מסתורי בשם secure. בעזרת חולשת blind sql, מצאו את שם הטבלה שנמצאת בו, כמה ערכים יש בה, ומה הם.
סעיף שישי – בעזרת os sql, כתבו Hello, World לנתיב /home/hello_world.txt. הסבירו במילים כיצד הייתם מטילים קובץ בינארי, ואילו מגבלות יש על הקובץ שתטילו.
סעיף שביעי – נאמר שיש קובץ בשם flag.txt בתיקייה /home. מצאו את תכנו.

סעיף שמיני (רשות – קשה) – התחברו כאדמין. מצאו את הסיסמא של האדמין.
סעיף תשיעי (רשות – קשה) – נסו לקרוא את התוכן של הקובץ /etc/shadow או קובץ דומה. אם אתם מצליחים, כל הכבוד! אם אתם לא מצליחים, הסבירו מדוע, ומה ניסיתם.

הנחיות להגשת התרגיל

את התרגיל יש להגיש בסבמיט לפי ההנחיות המפורטות. עיקר ההגשה הוא קובץ PDF המסביר עבור כל אחד מסעיפי התרגיל כיצד פתרתם אותו באופן מפורט, כולל צירופים של סקריפטים לא טריוויאלים.

את כל הערכים שאתם מוצאים, יש לצרף במלואם. במידה וערך מסוים הוא בינארי, יש לציין זאת ולצרף אותו בפורמט hex .במידה וערך מסוים הוא ארוך מאוד, ניתן לצרף אותו בנפרד.
את התוכן של הקובץ flag.txt יש לצרף בנפרד בקובץ בשם flag.txt.

אין להעלות קבצים מיותרים או כבדים.

במידה ויש שאלות בנוגע לתוכן התרגיל, נא להפנות לסגל הקורס בהקדם האפשרי.

הערות

לא למדנו בתרגולים כיצד קוראים וכותבים קבצים בעזרת SQL, אך ישנם חומרי עזר רבים באינטרנט.

טעות לעולם חוזר.

בהצלחה!
