תרגיל 1

HTTP Proxy & Local File Inclusion & SQL injection & SQLmap

העבודה בזוגות בלבד!

הוראות הגשה

עליכם להגיש קובץ **PDF** (בלבד!). יש לכלול בשם קובץ התרגיל את תעודות הזהות של הסטודנטים המגישים. פרטי הסטודנטים צריכים להופיע בתוך התרגיל עצמו.

זכרו שאתם נבחנים על התרגיל בהגנה בסוף הקורס. עליכם להכיר כל מושג שמוזכר בתרגיל ובפיתרון שלכם, וכן להיות מסוגלים לבצע חלקים מהתרגיל ולהסביר מדוע עשיתם דברים גם מבלי להסתכל בתרגיל עצמו או בחומר עזר.

כמו כן – עליכם לכתוב את כל התשובות בשפה שלכם ולא להעתיק (מחברים או מכל מקור אחר).

שימו לב לשתי השאלות שעליהן אתם נדרשים לענות בסוף חלק ב' (בעמוד האחרון של התרגיל!)

חלק א' (20 נק')

התקינו Burp וקנפגו אותו כך שתוכלו ליירט באמצעותו תעבורת HTTP בדפדפן ה-Firefox שלכם.

1. בהנחה שהסתפקתם בהתקנה בסיסית של Burp, כאשר תגלשו לאתר HTTPS (למשל: https://google.com) דרך הדפדפן שתעבורתו עוברת בפרוקסי - תקבלו שגיאה. הסבירו בקצרה מה השגיאה ומדוע היא מתרחשת.
2. בלינק https://portswigger.net/burp/help/proxy_options_installingcacert.html, תוכלו להתחיל לחפש ולהבין כיצד ניתן בכל זאת להעביר תעבורת HTTPS דרך Burp. קנפגו את הדפדפן שלכם כך שתוכלו לגלוש באמצעותו דרך Burp גם מעל HTTPS. הסבירו בקצרה מה עשיתם וכיצד מה שעשיתם סייע לפתור את הבעיה. (מדוע העובדה שמצליחים לבצע MitM על תעבורת HTTPS לא סותרת את הבטיחות של SSL/TLS?)

מי שמתקשה בהבנת HTTPS, מוזמן לחזור על החומר של קורס המבוא המהווה דרישת קדם לקורס.

חלק ב' (80 נק')

בחלק זה זה עליכם לפתור ולתעד פיתרון של אתגר האקינג בעל 4 שלבים. **שימו לב, שעליכם גם לענות גם על שתי שאלות שמתוארות בסוף המסמך.**

האתגר מופיע בלינק הבא: https://hack.me/101303/challenge-lab-0x02.html

מומלץ להשתמש בחשבון gmail בדוי בעת ההרשמה והשימוש באתר.

מומלץ לבצע את התרגיל על מכונה וירטואלית, כיוון שהוא כולל התקנה של תוכנה.

במהלך התרגיל תתנסו בפרצות שייתכן והכרתם בקורס הבסיסי: SQL injection ו-File Inclusion.
קראו מעט על Local File Inclusion (ועל ההבדלים בינו לבין Remote File Inclusion) בלינקים:

1. http://en.wikipedia.org/wiki/File_inclusion_vulnerability
2. http://hakipedia.com/index.php/Local_File_Inclusion
3. http://www.way4hack.com/2013/01/web-hacking-lfilocal-file-inclusion-for.html

כמו כן, השתמשו ב-sqlmap, כלי שחובה על אחד שמתעסק באבטחת מידע (משני הצדדים) להכיר.
ראו לינקים בסיסיים:

1. http://sqlmap.org/ (גם להורדת התוכנה)
2. https://github.com/sqlmapproject/sqlmap/wiki/Usage (פירוט פקודות)
3. חפשו sqlmap tutorial במנוע החיפוש המועדף עליכם

עליכם להגיש מדריך מפורט המסביר כיצד פתרתם את כל אחד מהשלבים. על המדריך להיות מפורט ברמה כזו, כך שבודק שאינו מיומן כמוכם, יוכל לפתור את האתגר וגם להבין כל מה שהוא עשה.

תעדו במדריך שלכם גם נסיונות שכשלו.

על המדריך לכלול גם צילומי מסך (השתמשו בכפתור ה-print screen בו ב-snipping tool שמגיע עם מערכת ההפעלה windows).

יש להפריד בין חלקי התרגיל השונים.

חשוב!
מעבר למדריך, עליכם לענות בנפרד, בקצרה, אך באופן ברור על שתי השאלות הבאות. יש לצרף את התשובות לסוף המסמך.

1. **כתבו ה-URL שבאמצעותו ניתן להריץ SQLi שיוציא מידע ממסד הנתונים.** ז"א URL שניתן לכתוב בשורת הכתובת בדפדפן כאשר המשתמש מחובר לאתגר, וההתקפה תתרחש.
2. **הסבירו על ה-URL שבה השתמשתם.** למשל, באילו אופרטורים או תווים מיוחדים השתמשתם? מה משמעות השאילתא שבפועל הרצתם? וכו'.

בהצלחה!