

תרגיל זה יעסוק בSQLi.

**כמו שאמרתי בשיעור, אין להתקיף/להשתמש במתודה אחרת על אתר המודל של האוניברסיטה. מי שיחליט לבצע דבר אחר, אינו באחריות הקורס. הוראה מאחראי המסלול.**

הרעיון של תקיפה זו הוא שימוש באלמנטים מתוך דפי טפסים ומתוך שורת הURL של אתר מסוים. אתם נדרשים לבצע את הדברים הבאים:

1. הכנסו למודל שלכם.
2. הכנסו לאחד מהקורסים שלכם.
3. נסו להשתמש בשורת הURL הקיימת כרגע(לאחר שינוי קל שלכם) כדי למצוא 5 קורסים שונים וצלמו את המסך שלהם. יש בה חולשה מסוימת שמאפשרת זאת. מהי החולשה? הסבירו מה אתם מבינים מכך על טופס הPHP שיושב באתר עצמו.
4. מצאו קורס אחד שניתן להכנס אליו בצורה חופשית על ידי שימוש בחיפוש זה. כלומר, לגשת לכל תכני הקורס ללא רישום מוקדם. יש ליצר סקריפט פייטון שיעשה זאת בצורה שיטתית. כלומר, לייצר סקריפט פייטון (גרסא 2.x) שימצא דף קורס שפתוח להצגה. יש לצלם את הקורס ולצרף את הקוד שכתבתם. רמז: אפשר להשתמש בספריית beautifulsoup וספריות דומות. כמו כן, חשבו איך תגיעו לדף שכזה בלי לעבור על מספר רב של דפים, בלי לדעת מראש איזה דף פתוח להצגה.
5. עתה, נסו לבצע SQLi קטן ופשוט על שורת החיפוש בעמוד המודל הראשי. נסו להבין אם יש אמצעי הגנה שהושתל במקום זה נגד התקיפה ואיזה אמצעי הגנה זה.

הגשה:

יש לצרף את כל צילומי המסך לעיל עם הסברים, וכן את הקוד אם השתמשתם מסעיף 3 והלאה.

הגשת הקבצים תהיה בקובץ ZIP דחוס, כאשר שם הקובץ הוא ת.ז. שלכם. במידה ויש שני מגישים יחדיו, רשמו את ת.ז. שלכם עם \_ מפריד ביניהם.