עבודה 3 -תיאוריה

מגישים: מאור חדד 308201565, עדי הדר 315748749

חלק א-

2.ASP.NET - בעזרת שפה זו ניתן ליצור אתרים דינאמיים בשילוב של נתונים מבסיסי נתונים ולטפל במידע שנשלח מהמשתמש- ניתן ליצור פלט בהתאם למידע שהתקבל מהמשתמש

יתרון: מהיר ונוח- חוסך בכתיבת קוד נותן אופציה של "code reviews "- ניתן לפתח אפליקצית web בקלות.

חיסרון: שינויים עלולים לא להישמר בגרסה הבאה- שינויים יבדו רק בגרסה הנוכחית לכן צריך לעדכן בכל גרסה.

JavaServer Pages- היא טכנולוגיית צד שרת מבוססת java+

יתרון: תומכת בגאווה, ממש קלה לשימוש

חסרונות: מתורגמת להרבה קומפיילים לכן קשה לעקוב אחריה , תופסת הרבה מקום בזיכרון.

3. מכיוון שהלקוח זה מי שמתחבר לשרת, אז אלא אם יש בשרת הציבורי עצמו תוכנה כלשהיא 3 שמקבלת מידע מהשרת, אז זה לא אפשרי. במצבים אחרים זה כן אפשרי, למשל כשהמפתח מתקין סביבה מקומית אצלו במחשב, ואז הוא מריץ גם את השרת וגם את הקליינט באותו מחשב.

4. ניתן לקבל השלמה אוטומטית של המשתנים וכו' ע"י ide ובכך להקל על כתיבת הקוד ומהיר

6. כשקולטים מידע מהמשתמש בFORM המשתמש יוכל להכניס מידע זדוני בתור קלט, לדוג: אם נדפיס את הקלט והמשתמש רשם js אז האתר יריץ את הקוד(xss) כנ"ל בsql כשנעביר מידע מהמשתמש לשאילתה המשתמש יוכל להכניס חלקים שישנו את המטרה של השאילתה לדוג: $input="""OR"1"=1';

Select \*from'users'WHERE'username'=$"input"

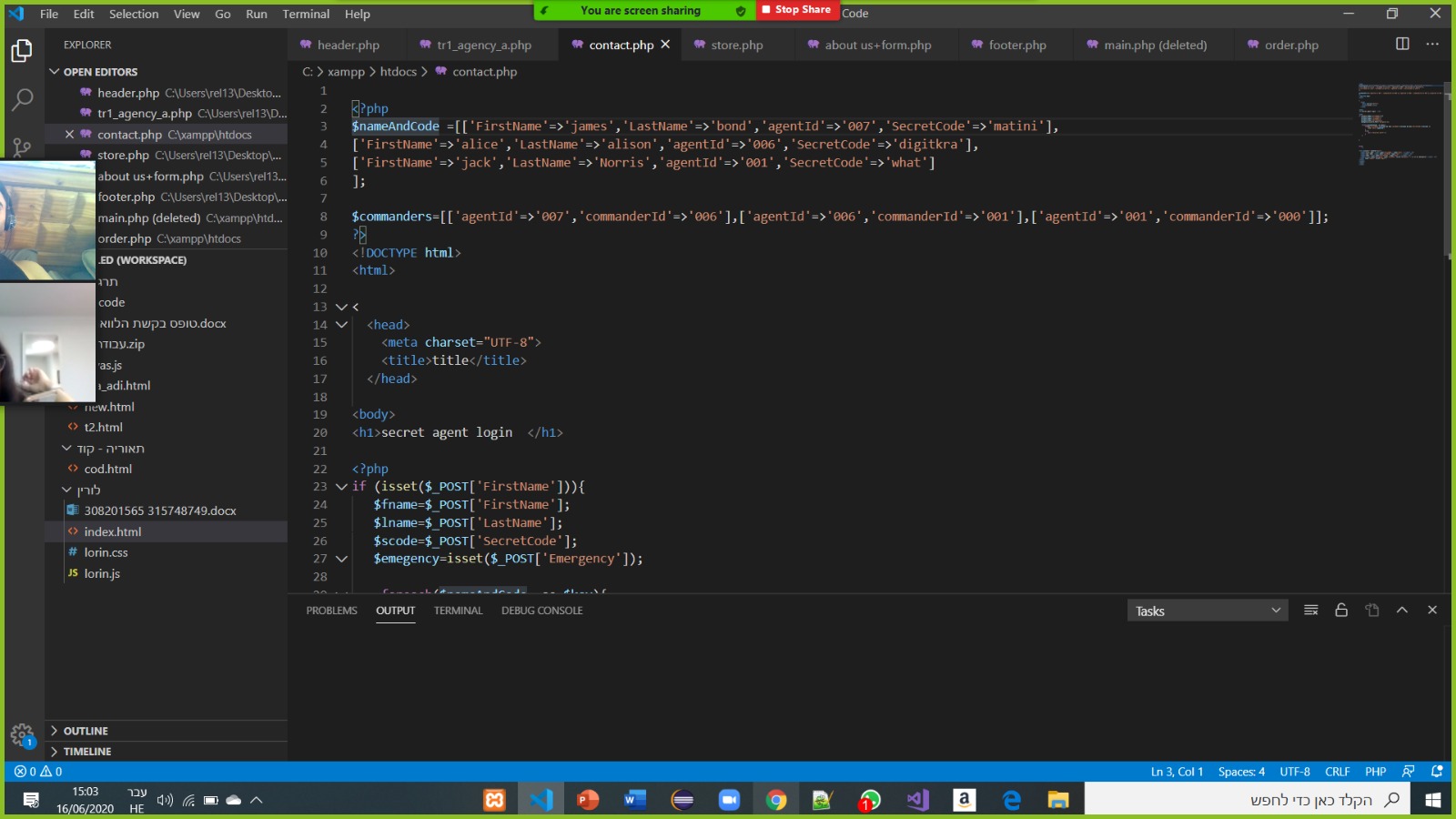
במצב כזה תחזיר השאילתה את כל המשתמשים בטבלה הפתרון זה לעשות escaping לתווים הבעייתיים כך שהקוד ידע להתעלם מהם באמצעות פונק preg\_replace נעשה ביטוי רגולרי שיזהה דברים כאלו וימחק אותם

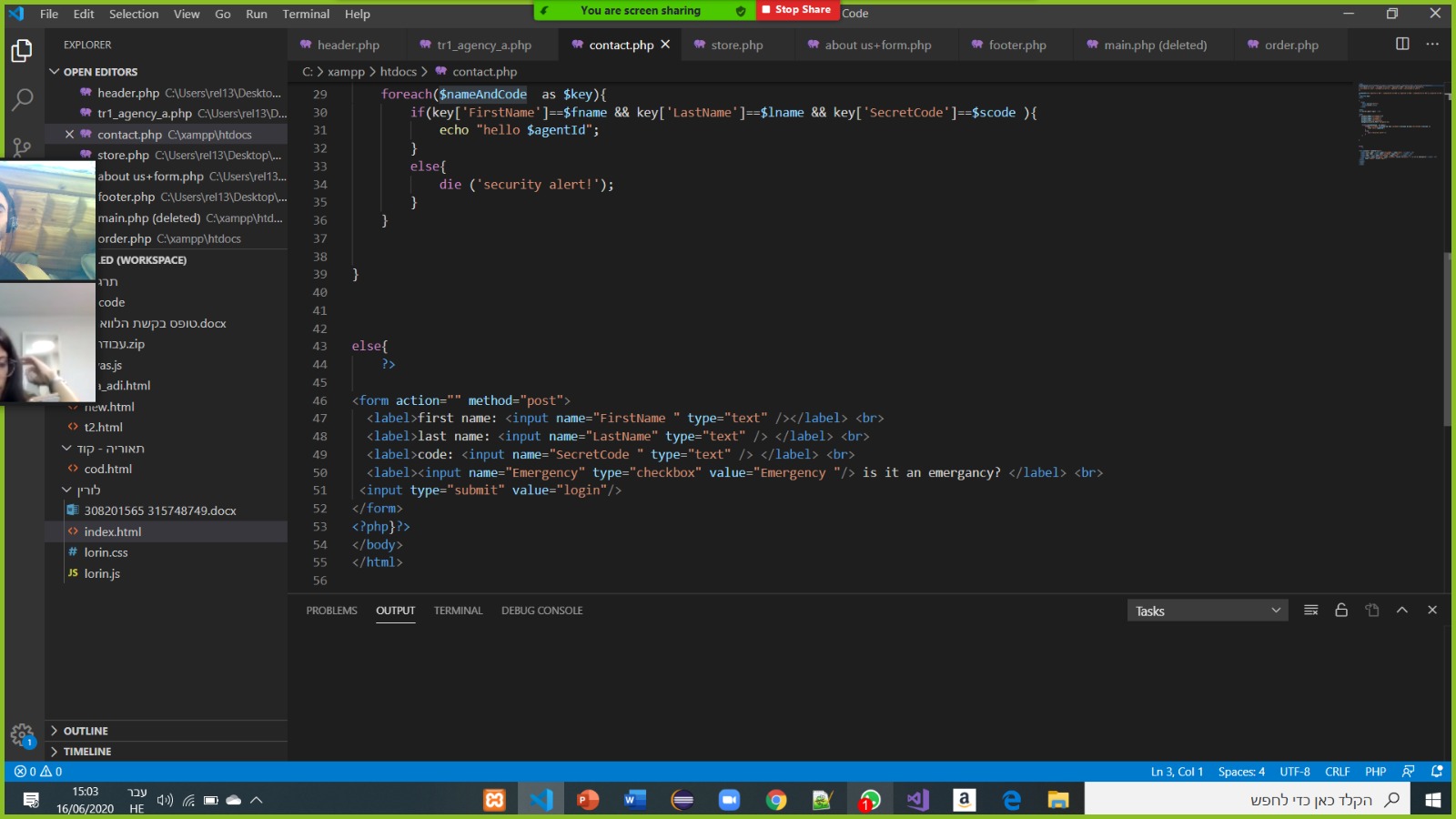
10. אם נשתמש בjs ניתן לשלוח את הטופס בכל מקום, נכתוב את הקוד הבא בחלק הרלוונטי

Document.getElementById('form').submit();

ואם נשתמש בHTML נוכל לעשות זאת רק באמצעות הכפתור.

חלק ב-

1.



2.

