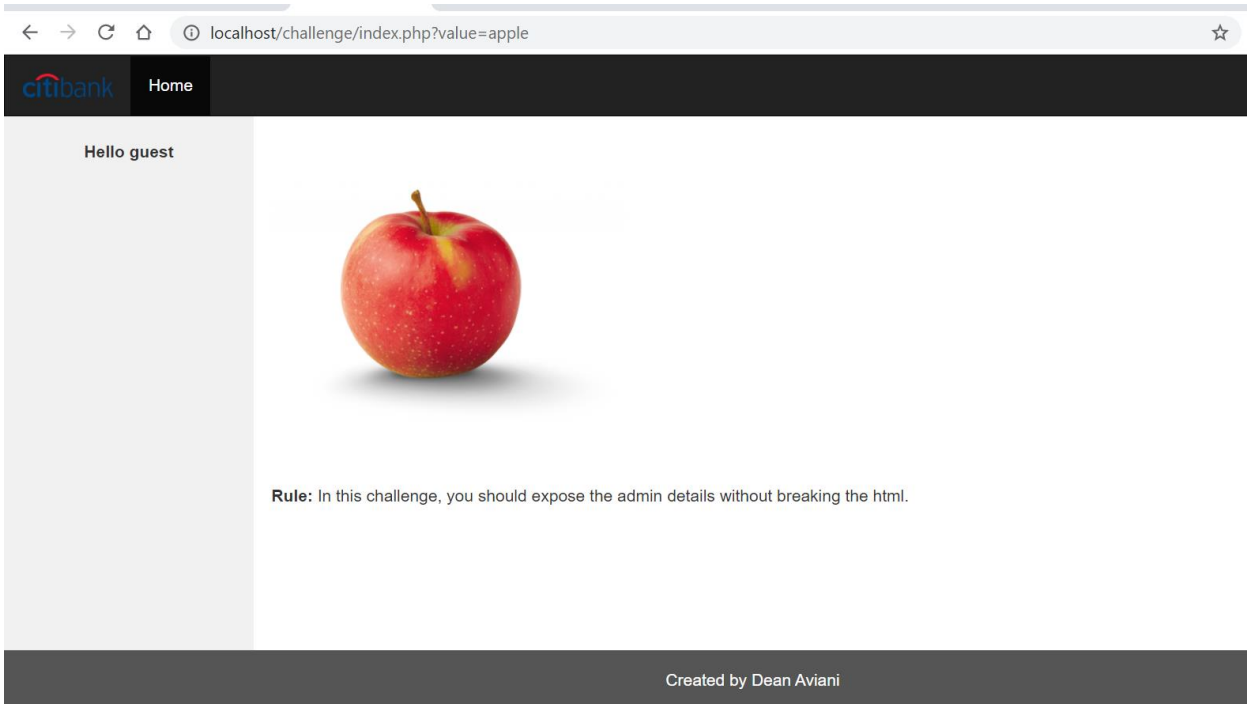
פיתוח אתגר

נוצר ע"י דין אביאני

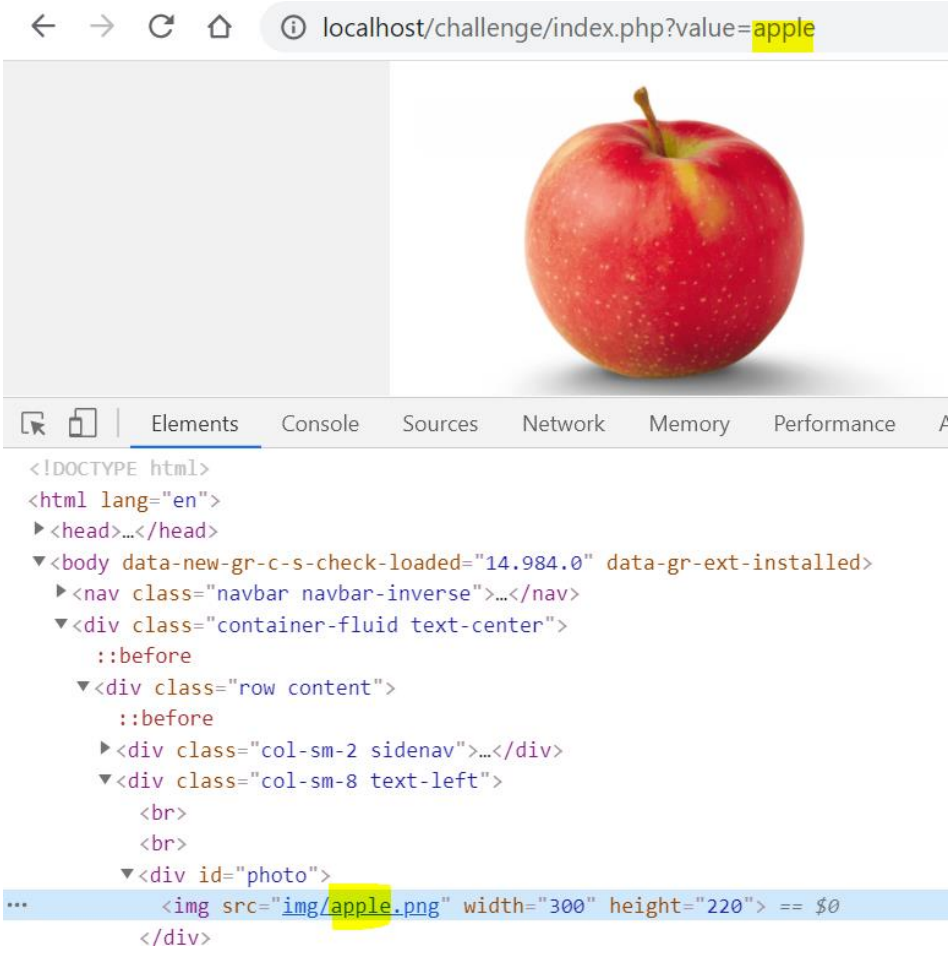
<u>מטרה</u>: על המשתמש לחשוף את פרטי ההתחברות של משתמש admin בעזרת ה-URL בלבד וללא שבירת ה-HTML.

<u>פתרון האתגר</u>

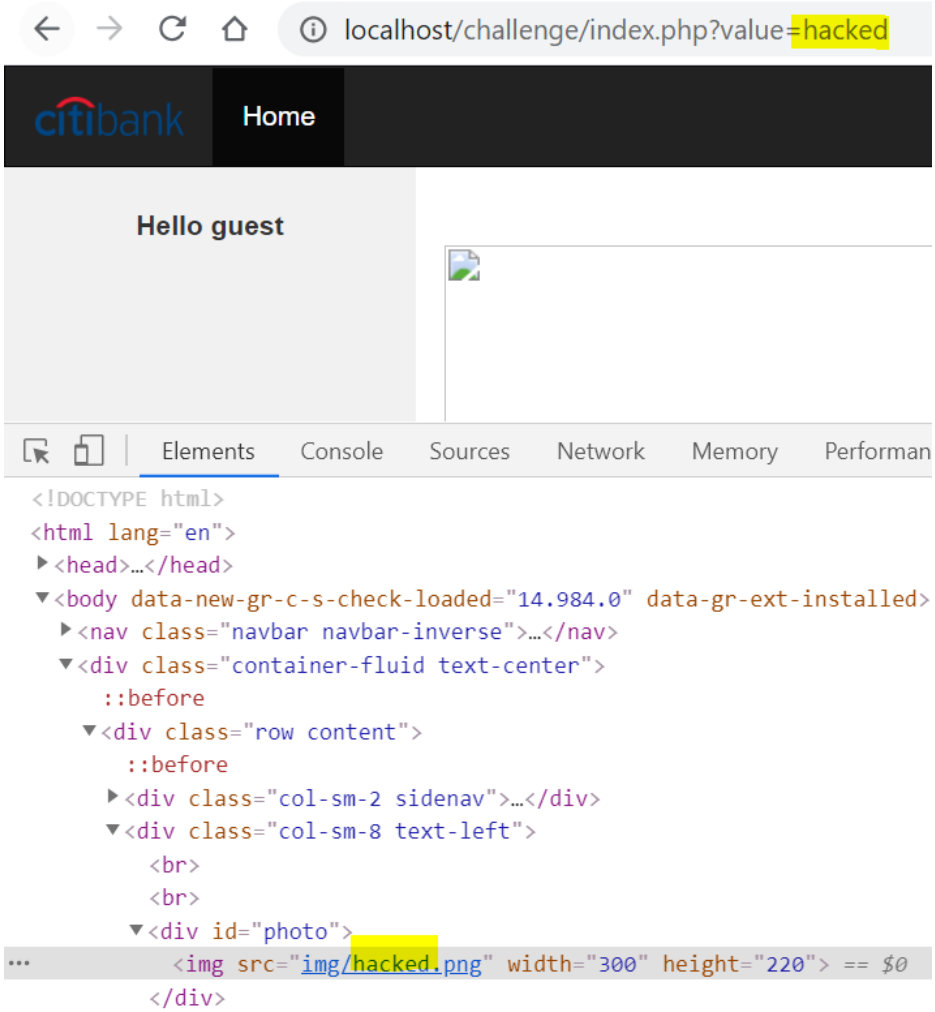
עם הכניסה לאתר, מופיע הדף הבא:



כניסה לדף המקור של העמוד מראה כי הערך המופיע תחת המשתנה value בשורת ה- URL משפיע על התמונה שתוצג.



למשל, שינוי המילה apple למילה hacked ישנה את שם התמונה תחת התגית img:



בנוסף, ניתן לראות כי לא משנה איזה ערך נשים תחת המשתנה value, תמיד לפניו תבוא המחרוזת "img/" ואחריו תבוא המחרוזת "png.".

בהמשך הקוד, ניתן לראות שפרטי המשתמש admin מוסתרים:

```
<script>
        document.getElementById("details").style.visibility = "hidden";
    </script>
```

על מנת להציג את אותם פרטים, עלינו לשנות את התכונה visibility מ- hidden ל- visible.

בנוסף לזאת, מכיוון שאותו script מופיע לאחר התגית img, עלינו לדאוג שהשינוי שנעשה לתכונה visibility תקרא רק לאחר שכל העמוד יטען.

לאור כל הממצאים שנאספו עד כה, להלן הקוד שנזריק למשתנה value בשורת ה- URL :

```
apple.png" width="300" height="220"></div><script>$( document
).ready(function()
{document.getElementById("details").style.visibility =
"visible";});</script><div><img src="img/apple
```

תוצאה סופית:

ניתן לראות שגם הצלחנו לחשוף את הפרטים של משתמש admin וגם לא שברנו את קוד ה- HTML