

## פתרון אתגרים

נכתב ע"י דין אביאני

### אתגר מספר 4 של HTML

עם הכניסה לאתגר נראה את ה- URL הבא:

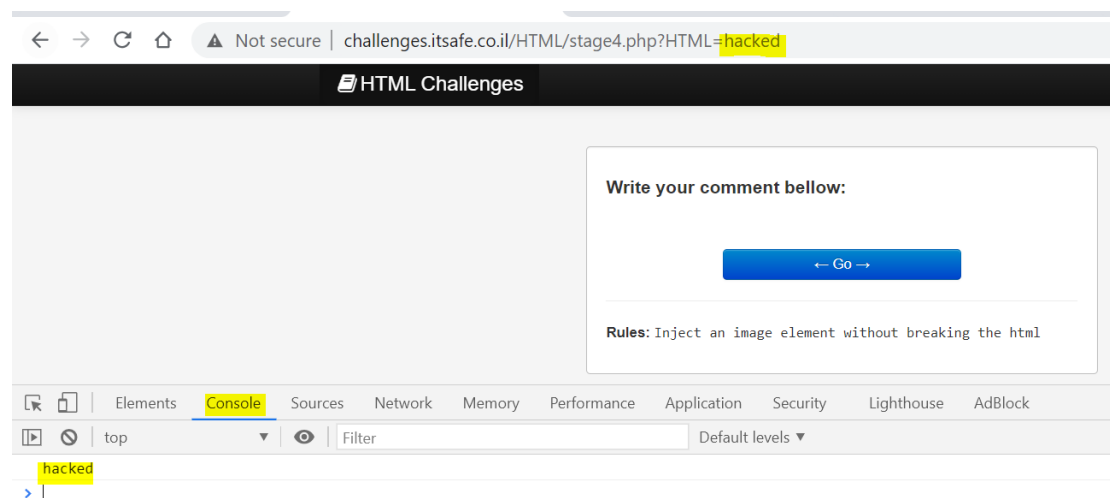
<http://challenges.itsafe.co.il/HTML/stage4.php?HTML=apple>

כניסה לקוד המקור של העמוד מראה את הקטע הבא:

```
<div class="row ">
  ::before
  <div class="span3"></div>
  <div id="login" class="span6 well" style="background :white; border:1px silver solid;">
    <h4>Write your comment bellow:</h4>
    <script> console.log("apple");</script> == $0
  <br>
  <b>
    <span id="notification"></span>
  </b>
```

על כן, ניתן להבין ששינוי המילה apple ב- URL ישפיע על מה שיוצג ב- console.

לדוגמה, שינוי למילה hacked יציג את אותה מילה ב- console:




כעת, על מנת להזריק תמונה, נכניס במקום המילה apple את הקוד הבא:

```
");</script><script>console.log("
```

← → ↻ 🏠 ⚠ Not secure | challenges.itsafe.co.il/HTML/stage4.php?HTML=");</script><img%20src="https://upload.wikimedia.org/wikipedia... 🔍 ☆

HTML Challenges Login

Write your comment below:



← Go →

Rules: Inject an image element without breaking the html

## אתגר מספר 4 של CSS

עם הכניסה לאתגר נראה את ה- URL הבא:

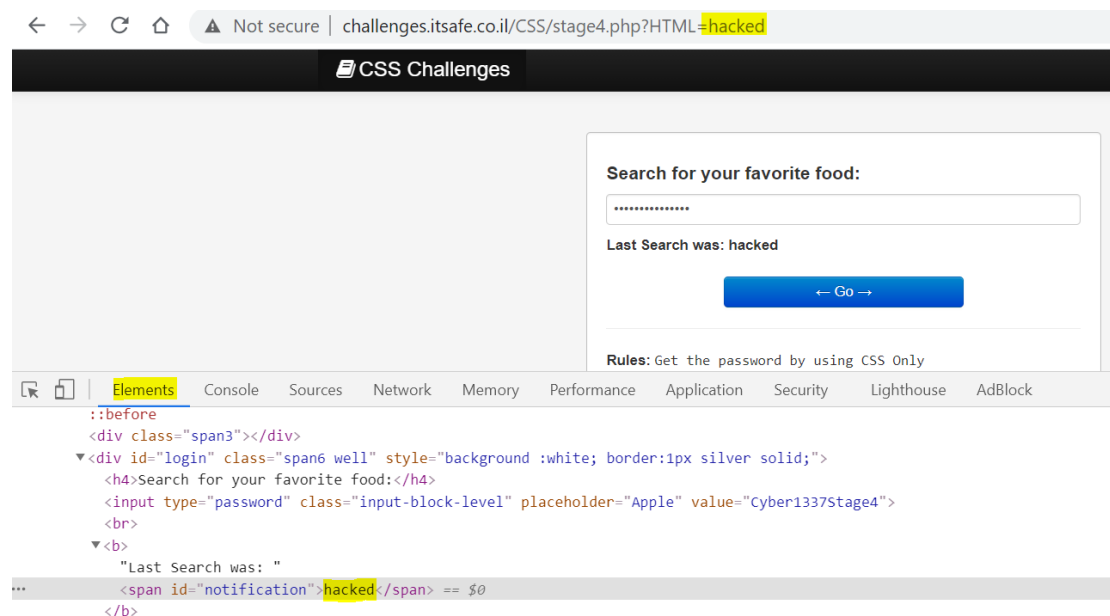
<http://challenges.itsafe.co.il/CSS/stage4.php?HTML=apple>

כניסה לקוד המקור של העמוד מראה את הקטע הבא:

```
▼ <b>
  "Last Search was: "
...   <span id="notification">apple</span> == $0
      </b>
```

על כן, ניתן להבין ששינוי המילה apple ב- URL ישפיע על מה שיוצג בתגית span.

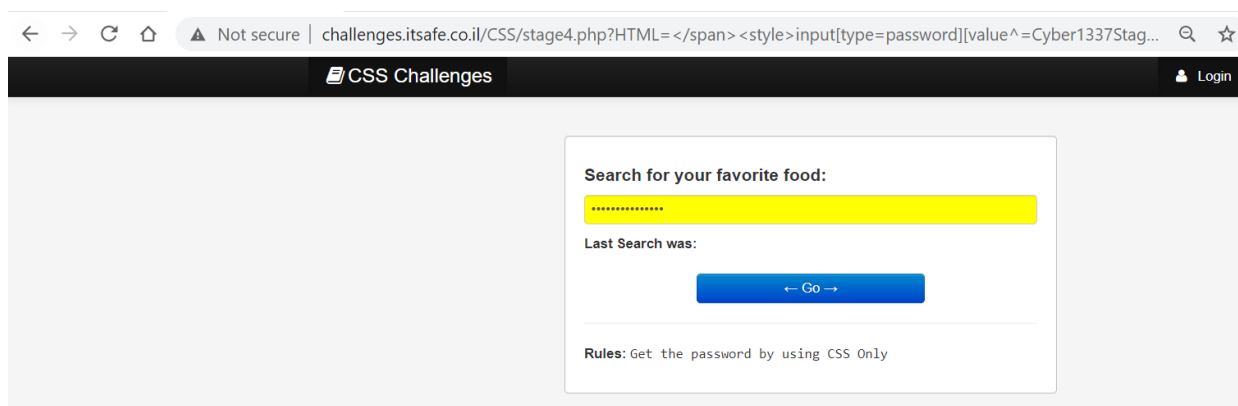
לדוגמה, שינוי למילה hacked יציג את אותה מילה ב-תגית span:



כעת, על מנת למצוא את הסיסמה, נזריק את הקוד הבא במקום המילה apple:

```
</span><style>input[type=password][value^=Cyber1337Stage4]{background:yellow}</style><span>
```

## התוצאה הסופית מראה שה-input של הסיסמה נצבע בצהוב ברגע שמצאנו את הסיסמה:



## אתגר מספר 3 של JQUERY

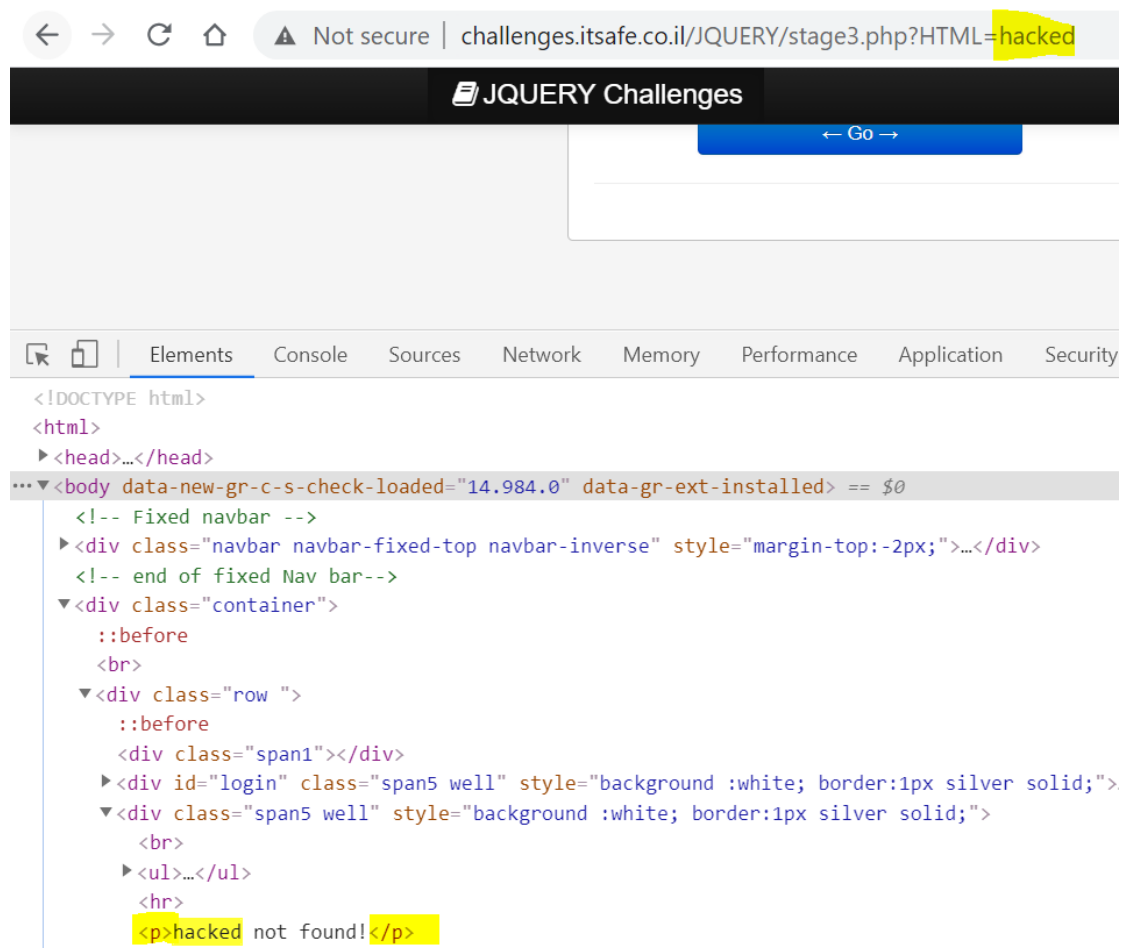
עם הכניסה לאתגר נראה את ה-URL הבא:

<http://challenges.itsafe.co.il/JQUERY/stage3.php?HTML=apple>

על מנת לצבוע את הקטע עם המילה there, נחפש אותו בקוד המקור של הדף. לאחר החיפוש, נמצא כי אותה מילה נמצאת תחת תג li לו יש id ייחודי בשם there.

```
<li id="there" style="font-size: 30px">
  ::marker
  "
  try to get there
</li>
```

בנוסף, ניתן לראות שה-URL מכיל בסופו את המילה apple. מבדיקה בקוד המקור נמצא כי שינוי המילה משפיע על התג p:



על מנת לצבוע את הרקע של הקטע המכיל את המילה there, נתמקד ב-id שלו. בנוסף, מכיוון ששינוי ה-URL משפיע על התג p, נצטרך לדאוג לסגור את אותה תגית לפני הכנסת הסקריפט שלנו ולפתוח אותה מחדש בסוף. הסקריפט.

להלן קטע הקוד שנזריק ב-URL:

```
</p><script>$('#there').css("background-color",
"blue");</script><p>
```

← → ↻ 🏠 ⚠ Not secure | challenges.itsafe.co.il/JQUERY/stage3.php?HTML=</p><script>\$(%27#there').css("background-color",%20"... 📄 🔍 ☆

**JQUERY Challenges** Login

**Search for your favorite food:**

- grape
  - banana
  - pomegranate
- **passion\_fruit**
  - tangerine
    - cantaloupe
    - orange
    - plum
    - mango
    - papaya

← Go →

- grape
  - banana
  - pomegranate
- **passion\_fruit**
  - apple
  - cantaloupe
  - pear
  - boysenberry
  - jujube
- **watermelon**
  - strawberry
  - fig
  - clementine
  - **lemon**

### אתגר מספר 3 של JAVASCRIPT

נכנס לקוד המקור של העמוד ונראה את הסקריפט הבא:

```
<script>
var pass = [];

$("#search").click(function () {

    for(item of password.value)
    {
        if (item.charCodeAt(0) % 2 == 0){
            pass.push(item.charCodeAt(0)+3)
        }else{
            pass.push(item.charCodeAt(0)-1)
        }
    }

    if (String.fromCharCode(...pass) == "leet"){
        alert("you rock");
    }
    else
    {
        alert("try again... ");
    }
});

</script>
```

מתוך סקריפט זה, ניתן ללמוד כמה דברים:

1. נעשה שימוש במחסנית, מה שאומר שהכנסת האיברים עובדת עפ"י LIFO (האחרון שנכנס הוא הראשון שיוצא). על כן, בכדי לשחזר את הסיסמה שמביאה את הערך "leet" התו הראשון שנצטרך להפוך הוא t.
2. הבדיקה שהסקריפט עושה היא עבור כל תו, כאשר הוא בודק אם ערכו הדצימלי מול טבלת ה-ascii הוא זוגי או לא. על מנת לבצע את השחזור, עבור כל תו ננסה לבצע את הפעולה ההפוכה שכל תנאי עושה. כלומר, ננסה להוסיף לכל ערך דצימלי של תו את הספרה 1 או נפחית את ערכו בספרה 3. לאחר מכן, נבדוק אם הערך שהתקבל הוא זוגי או לא ובהתאם נדע לבחור מה התנאי והמספר הנכונים. לדוגמה: הערך הדצימלי של האות t עפ"י טבלת ה-ascii הוא 116. אם נוסיף ל-116 את הספרה 1 נקבל 117 (אי זוגי) ואם נפחית מ-116 את הספרה 3 נקבל 113 (אי זוגי). זאת אומרת, בכל מקרה המספר יהיה אי זוגי. מכיוון שהתנאי if מתייחס למצב של מספר זוגי בלבד, נבחר במצב של ה- else – מה שאומר שהמספר הדצימלי שהוביל ל-t הוא 117 והתו המייצג אותו הוא u.

להלן השחזור שנעשה למילה leet עפ"י הסקריפט:

=>109=>m	e=>98=>b	e=>98=>b	t=>117=>u
----------	----------	----------	-----------

נמיר כל ספרה דצימלית לתו על בסיס טבלת ה-ascii ונקבל את הסיסמה : **mbbu**

