

עבודה מסמכת בסדנת סייבר ב'

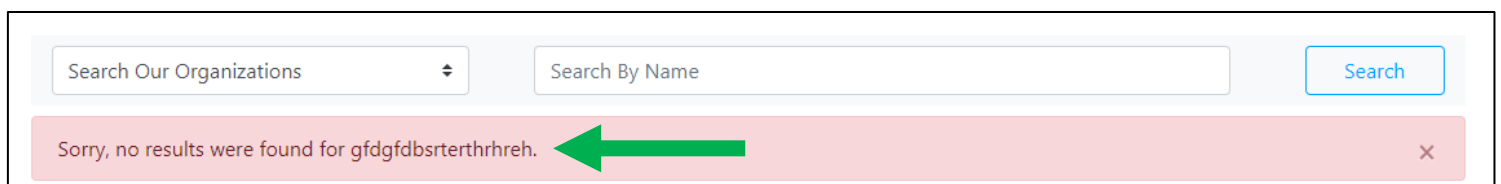
מגיש: אופיר ג'רבי

האתר שעליו נבנה האתגר הוא אתר שבניתי כחלק מפרוייקט מקורס צד שרת. החלק הרלוונטי נמצא בדף Our Organizations ובקובץ **organizations.php** בתיקיית includes.

אצרף צילומים לעזר עם שורות הקוד הרלוונטיות.

בדף קיים חיפוש של ארגונים באתר, שכחלק מהחיפוש, כאשר אין תוצאות, הוא מציג הודעה כי אין תוצאות עבור ____ (ומציין את מילת החיפוש אשר הוכנסה).

```
234         if($found==false && isset($_GET["search"])) { ?>
235         <div class="alert alert-danger alert-dismissible fade show mt-2 " role="alert">
236             Sorry, no results were found for <?php echo $_GET["search_term"] ?>.
237             <button type="button" class="close" data-dismiss="alert" aria-label="Close">
238                 <span aria-hidden="true"><img alt="Close icon" data-bbox="815 395 835 415"/></span>
239             </button>
240         </div>
```

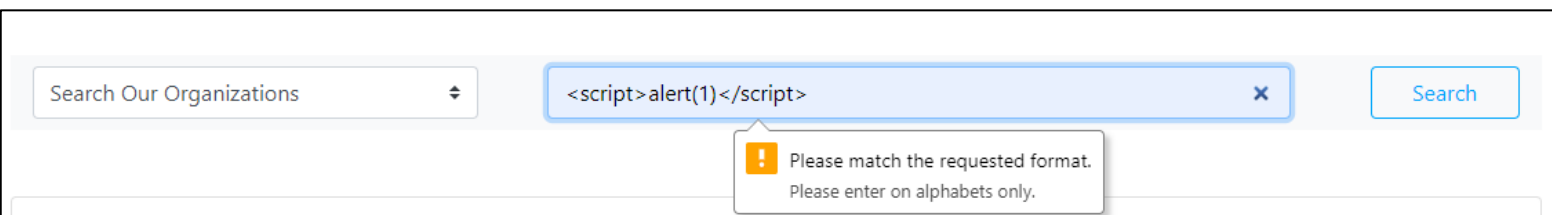


The screenshot shows a web application with a search bar labeled "Search Our Organizations" and a "Search By Name" input field. A "Search" button is to the right. Below the search bar, a red message box displays the text: "Sorry, no results were found for gfdgfdbsrterthreh." A green arrow points to the message box.

באג זה נקרא **Reflected XSS** והוא חלק מבאג XSS אשר מאפשר הזרקת סקריפט זדוני באתר ומאפשר לבצע פעילויות זדוניות כאלו ואחרות באתר. Reflected XSS מתאר מצב בו דף האינטרנט "משקף" (reflect) את הקלט אותו הכניס המשתמש ומכניס אותו באופן דינמי בדף האינטרנט, מבלי לוודא האם קלט זה מכיל קוד זדוני. כלומר, במידה ונזין קלט שהוא קוד/סקריפט – כעת הוא חלק מהאתר, שלמעשה יריץ את הקוד כחלק מהשיקוף.

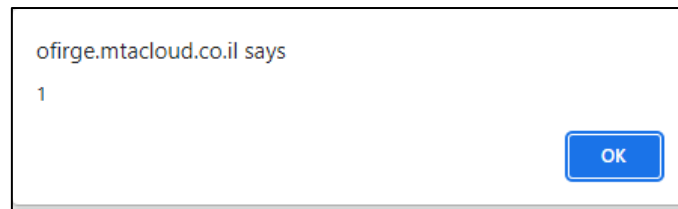
באתגר שלי, בעת חיפוש ללא תוצאות, האתר ישקף/יציין את הקלט מהמשתמש כמו שהוא, כך שהוא יהיה יכתב בדף עצמו, ולמעשה יריץ את הסקריפט אשר נזין לחיפוש.

אם נבצע חיפוש של הפרמטר: `<script>alert(1)</script>` נוכל לראות שיש ולידציה בצד לקוח.



The screenshot shows the same web application. The search bar now contains the payload `<script>alert(1)</script>`. A blue message box above the search bar displays the text: "Please match the requested format. Please enter on alphabets only." A green arrow points to the search bar.

אך בעת עקיפה של של צד לקוח – בשימוש ב-Burp – ניתן להזין לפרמטר את הסקריפט שירוצ באתר (ראה נספח). בעת העתקה של ה-URL עם הפרמטר הסקריפט ירוץ:



ניתן לתקן באג זה ע"י שימוש בשימוש בפונקציית **htmlentities** על הקלט של המשתמש. הפונקציה תתרגם את הסימנים המיוחדים (<>) שיוצגו ע"י סימנים מיוחדים של html.

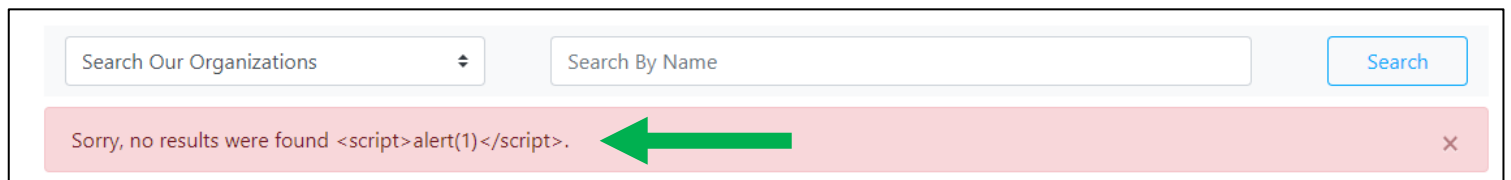
כלומר, במקום שהאתר יזין לדף `<script>alert(1)</script>`

הוא יזין `<script>alert(1)</script>`

כשבפועל זה יוצג באופן זהה על הדף – אבל זה לא יריץ את הסקריפט, מכיוון שאילו סימנים מיוחדים של html לצורך כתיבת הסימנים הללו. זה ימנע שימוש בסימנים מיוחדים בקלט מהמשתמש הנדרשים להרצת סקריפט.

*במידה ורוצים שהחיפוש כלל לא יקבל סימנים מיוחדים נוכל לבצע ולידציה גם בצד שרת.

```
234     if($found==false && isset($_GET["search"])) { ?>
235     <div class="alert alert-danger alert-dismissible fade show mt-2 " role="alert">
236       Sorry, no results were found for <?php echo htmlentities($_GET["search_term"]) ?>.
237       <button type="button" class="close" data-dismiss="alert" aria-label="Close">
238         <span aria-hidden="true">x</span>
239     </button>
```



נספח צילומי מסך מתוך ה-Burp:

זיהוי החבילה (Get request) והיכן היא בדף:

Request

Pretty Raw Hex

```
1 GET /cyber/xxs/includes/organizations.php?select=our&search_term=0000&search=
2 Host: ofirge.mtacloud.co.il
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/101.0.4951.54 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
  =0.8,application/signed-exchange;v=b3;q=0.9
6 Referer: http://ofirge.mtacloud.co.il/cyber/xxs/includes/organizations.php
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: PHPSESSID=67bb712e3ae4eb92d17592bde0719a7f
10 Connection: close
11
12
```

Response

Pretty Raw Hex Render

```
133
134
135 <!-- Our Search results -->
136
137 <div class="alert alert-danger alert-dismissible fade show mt-2 " role="alert">
138   Sorry, no results were found 0000.
139   <button type="button" class="close" data-dismiss="alert" aria-label="Close">
140     <span aria-hidden="true">
141       &times;
142     </span>
143   </button>
144 </div>
145 </main>
```

שינוי הפרמטר לסקריפט:

Request

Pretty Raw Hex

```
1 GET /cyber/xxs/includes/organizations.php?select=our&search_term=<script>alert(1)</script>&
  search= HTTP/1.1
2 Host: ofirge.mtacloud.co.il
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/101.0.4951.54 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
  =0.8,application/signed-exchange;v=b3;q=0.9
6 Referer: http://ofirge.mtacloud.co.il/cyber/xxs/includes/organizations.php
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: PHPSESSID=67bb712e3ae4eb92d17592bde0719a7f
10 Connection: close
11
```

הסקריפט רץ על הדפד:

```
Response
Pretty Raw Hex Render
133
134
135 <!-- Our Search results -->
136
137 <div class="alert alert-danger alert-dismissible fade show mt-2 " role="alert">
138   Sorry, no results were found <script>
139     alert(1)
140   </script>
141   .
142   <button type="button" class="close" data-dismiss="alert" aria-label="Close">
143     <span aria-hidden="true">
144       &times;
145     </span>
146   </button>
147 </div>
```

לאחר תיקון הבאג:

```
Response
Pretty Raw Hex Render
133
134
135 <!-- Our Search results -->
136
137 <div class="alert alert-danger alert-dismissible fade show mt-2 " role="alert">
138   Sorry, no results were found &lt;script&gt;alert(1)&lt;/script&gt;.
139   <button type="button" class="close" data-dismiss="alert" aria-label="Close">
140     <span aria-hidden="true">
141       &times;
142     </span>
143   </button>
144 </div>
145
146 </main>
```