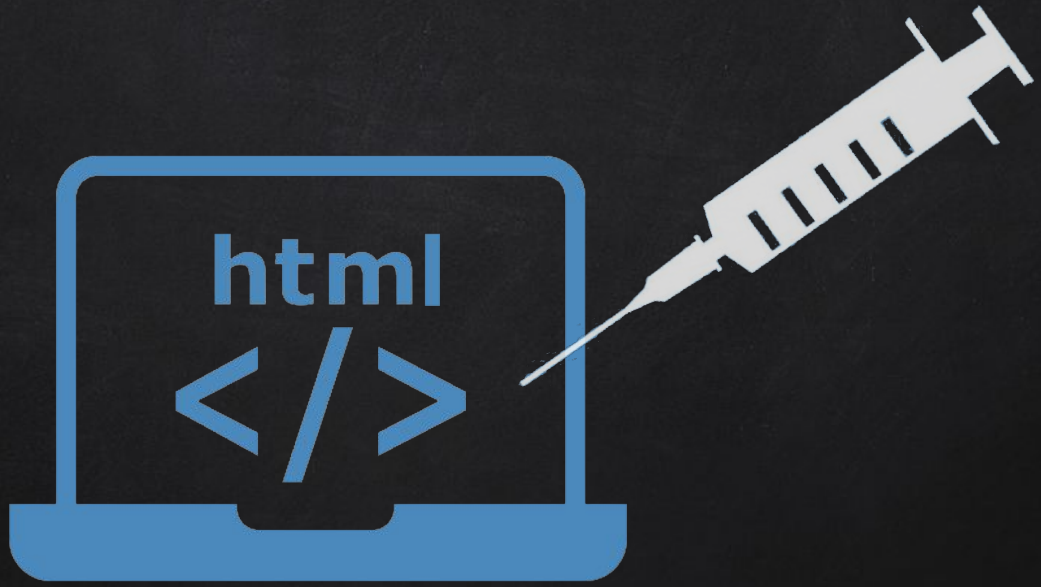
XSS Cross Site Scripting

- Allow an attacker to inject javascript code into the page.
- Code is executed when the page loads.
- Code is executed on the client machine not the server.

Three main types:

1. Reflected XSS
2. Persistent/Stored XSS
3. DOM based XSS

HTML Injection

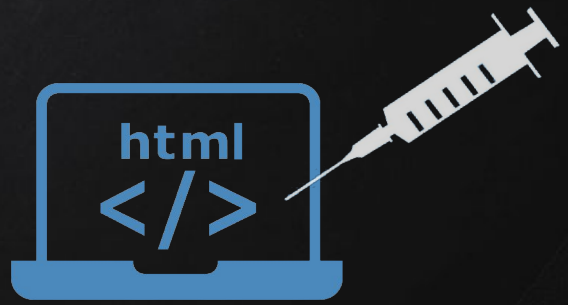


HTML Injection

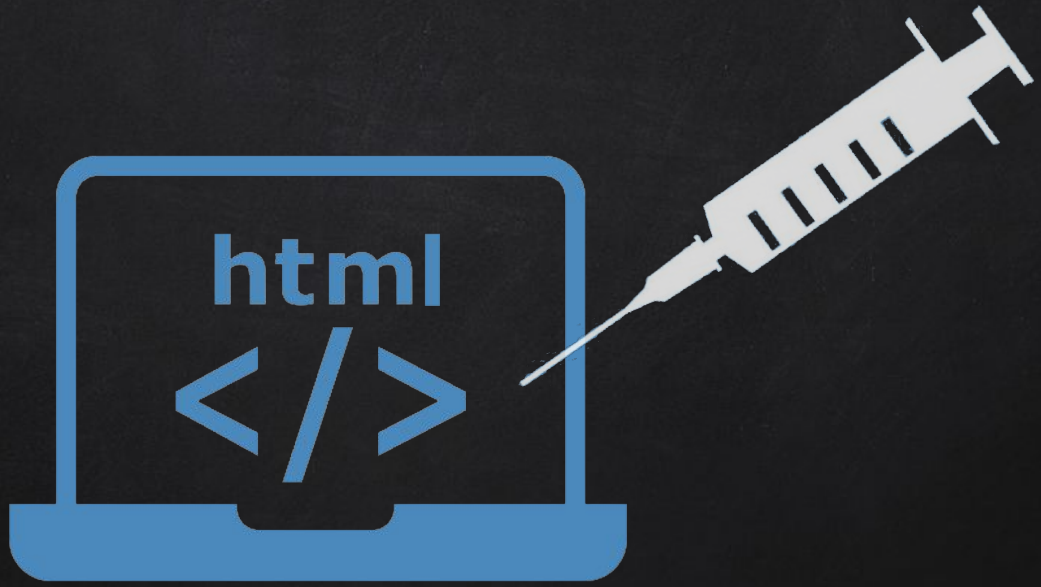
- Allow an attacker to inject HTML code into the page.
- Code is executed when the page loads.
- Code is executed on the client machine not the server.

→ Similar to XSS but simpler.

→ Hints at the existence of an XSS.



XSS Cross Site Scripting



XSS Cross Site Scripting

Discovering XSS

- Try to inject Javasript code into the pages.
- Test text boxes and url parameters on the form
  http://target.com/page.php?something=something

XSS Cross Site Scripting

Reflected XSS

- None persistent, not stored.
- Only work if the target visits a specially crafted URL
- EX
  http://target.com/page.php?something=<script>alert("XSS")</script>

XSS Cross Site Scripting

Stored XSS

- Persistent, stored on the page or DB.
- The injected code is executed everytime the page is loaded.

XSS Cross Site Scripting

Dom Based XSS

- Similar to reflected and stored XSS.
- Can be discovered and exploited similarly.
- Main difference is that it occurs entirely on the client side.
- Payload is never sent to the server.

  → No logs, no filters, no server side protection

XSS Cross Site Scripting

Bypassing Security

Filters & Firewalls

XSS

Cross Site Scripting

Request with XSS Payload

http://target.com/?search=test<script>alert('xss')</script>

Target.com Server

Server-side

Response with the XSS Payload embedded within the page

Client-Side

Reflected / Stored XSS

Request with XSS Payload

http://target.com/?search=test<script>alert('xss')</script>

Target.com Server

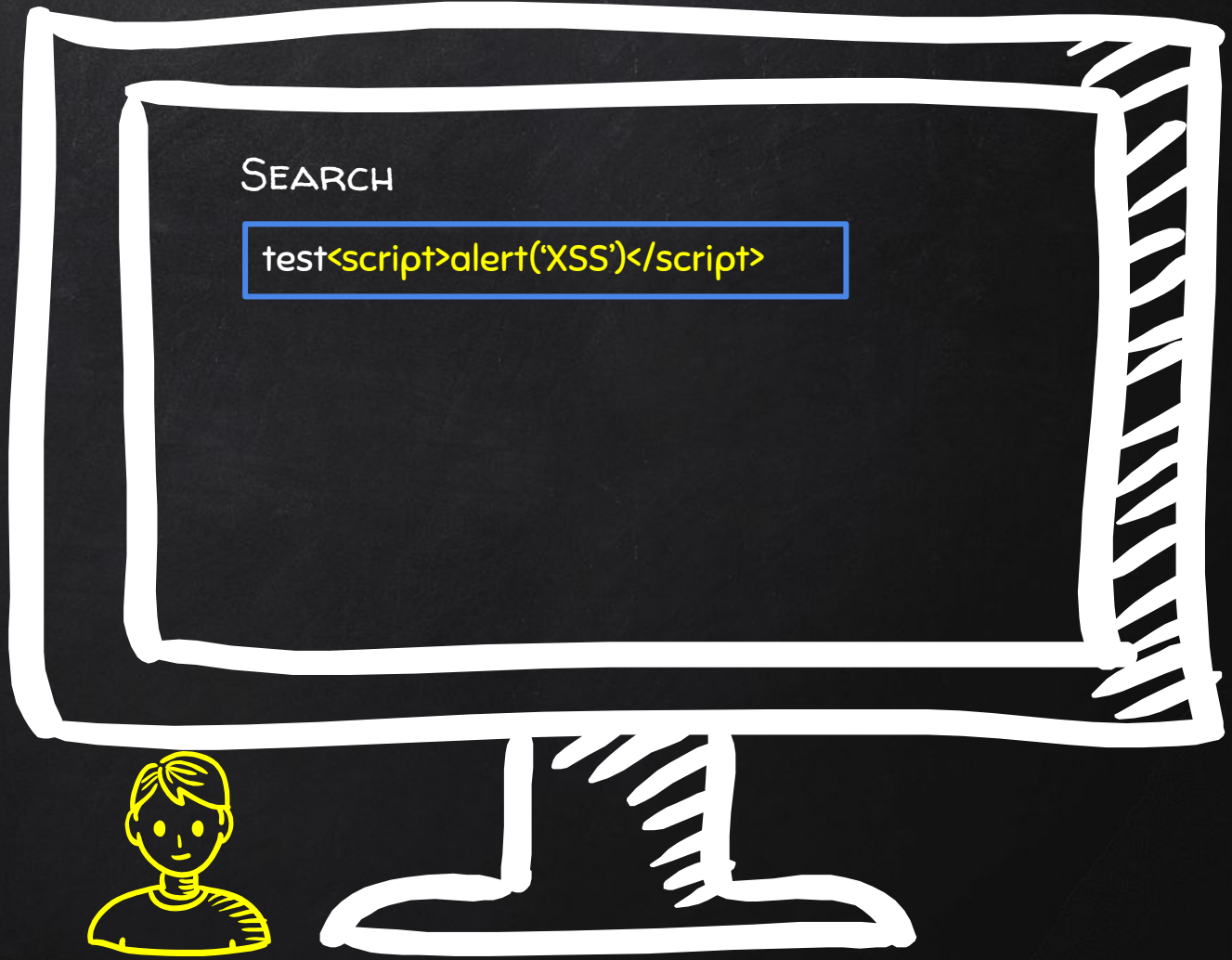
Response with the XSS Payload embedded within the page

XSS

Cross Site Scripting

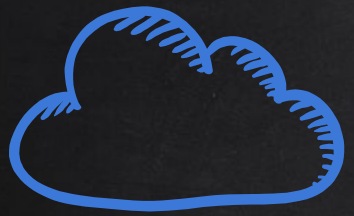
Dom Based XSS

Target.com
Server



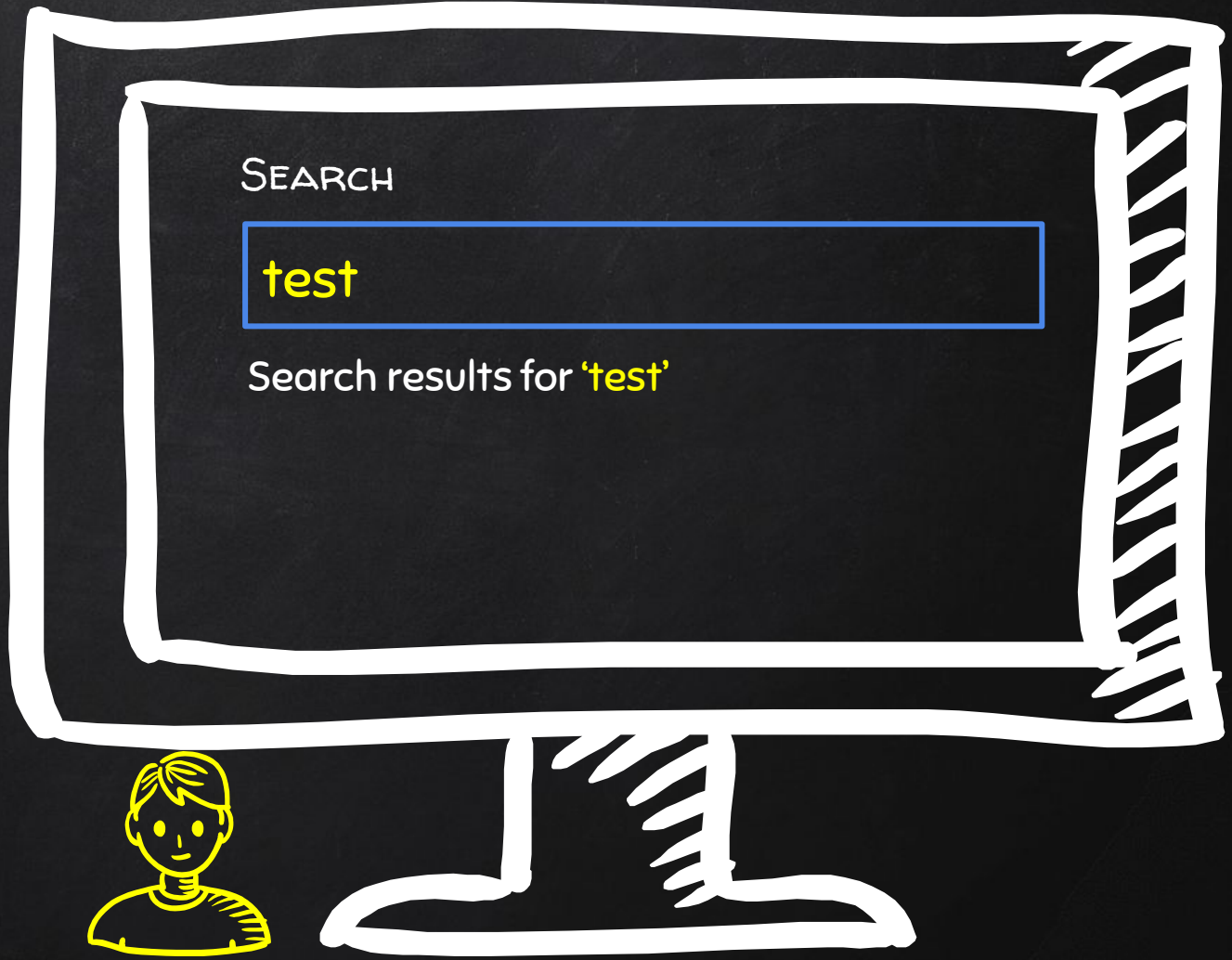
Dom Based XSS

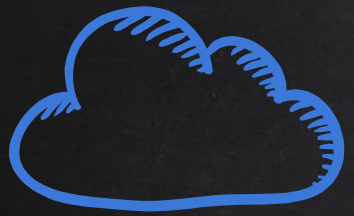
Target.com
Server



Target.com
Server

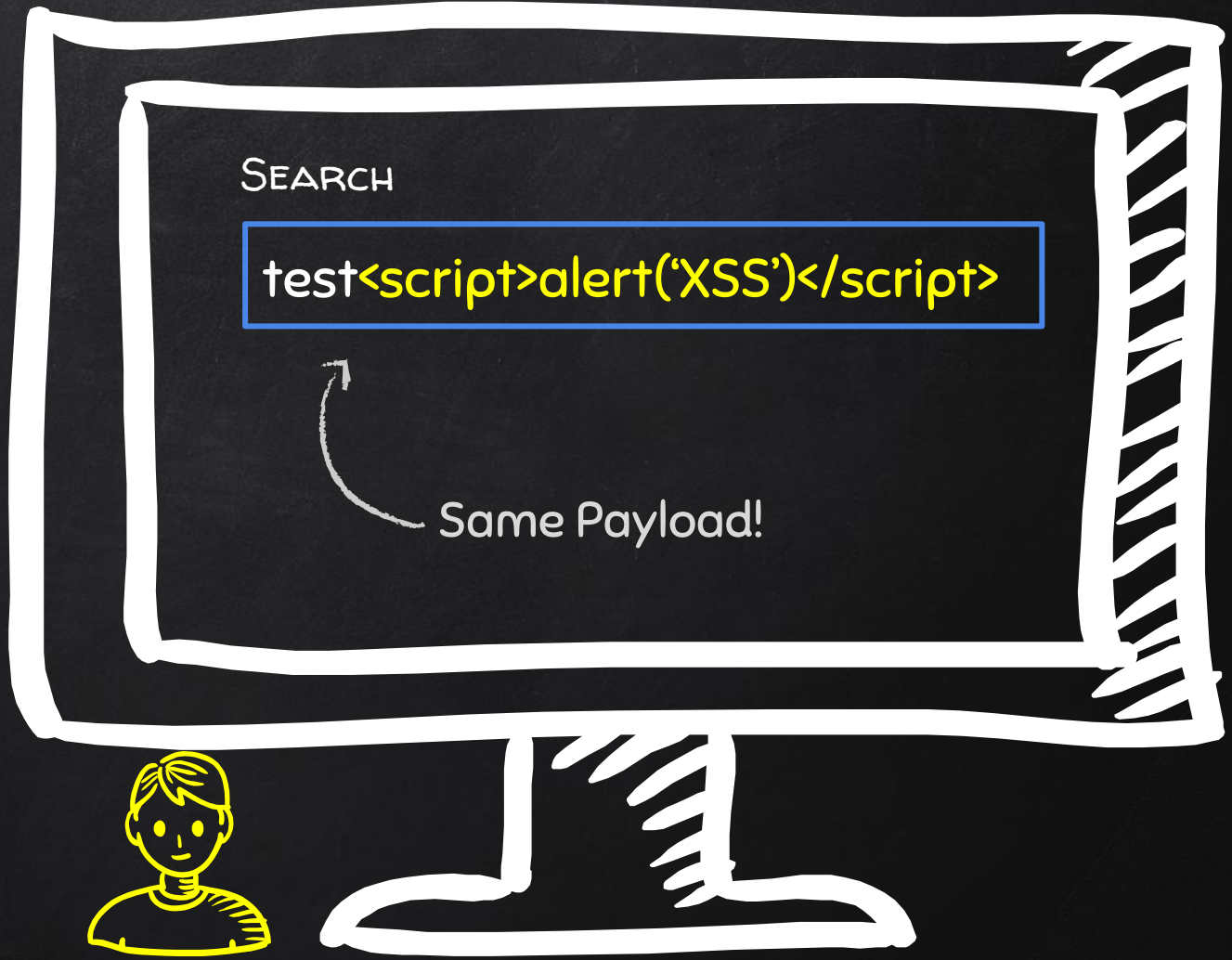
DOM
Stored
Reflected
XSS

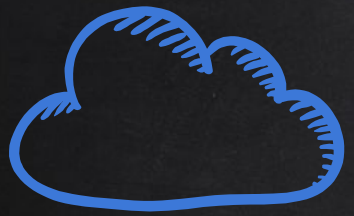




Target.com
Server

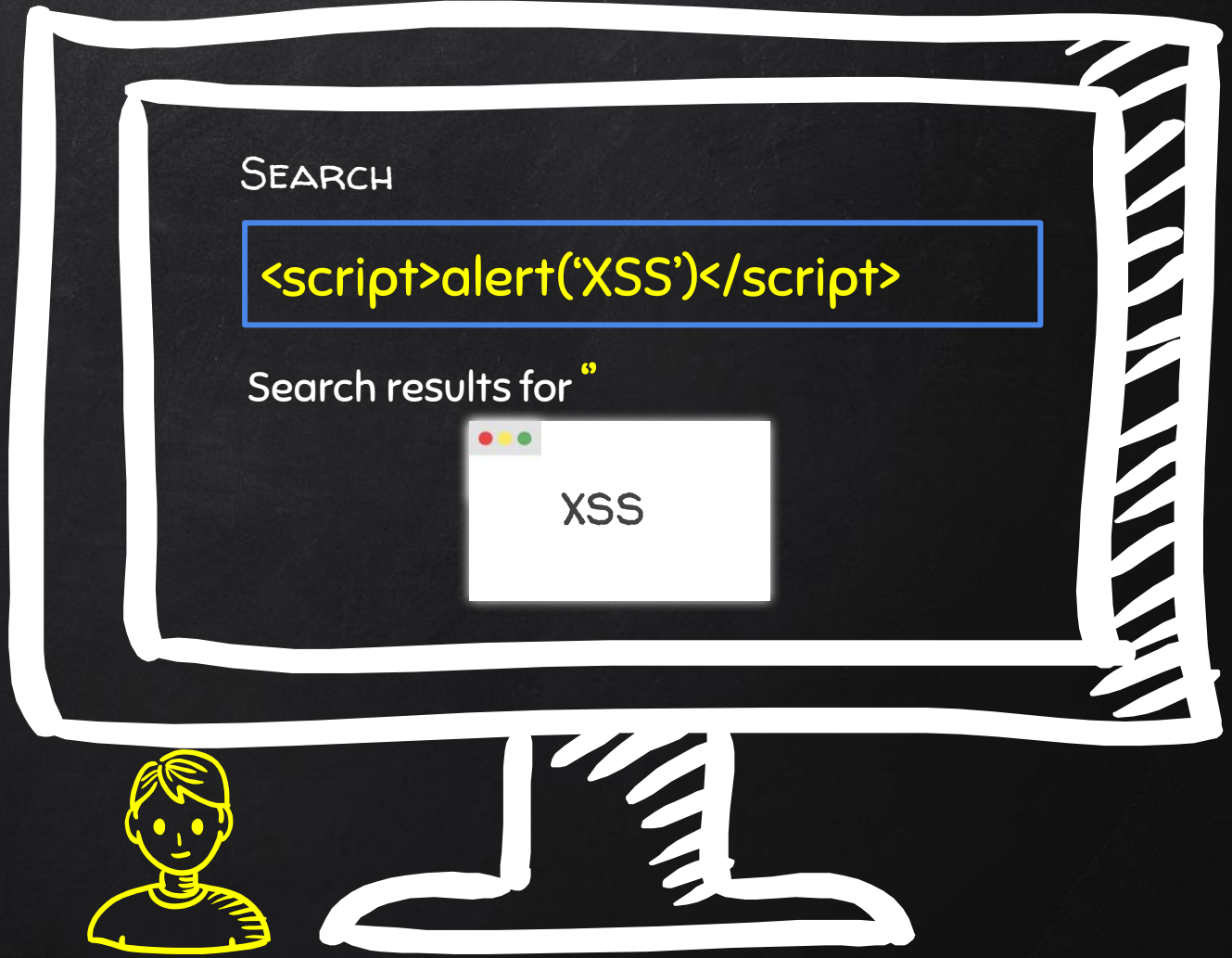
DOM
Stored
Reflected
XSS





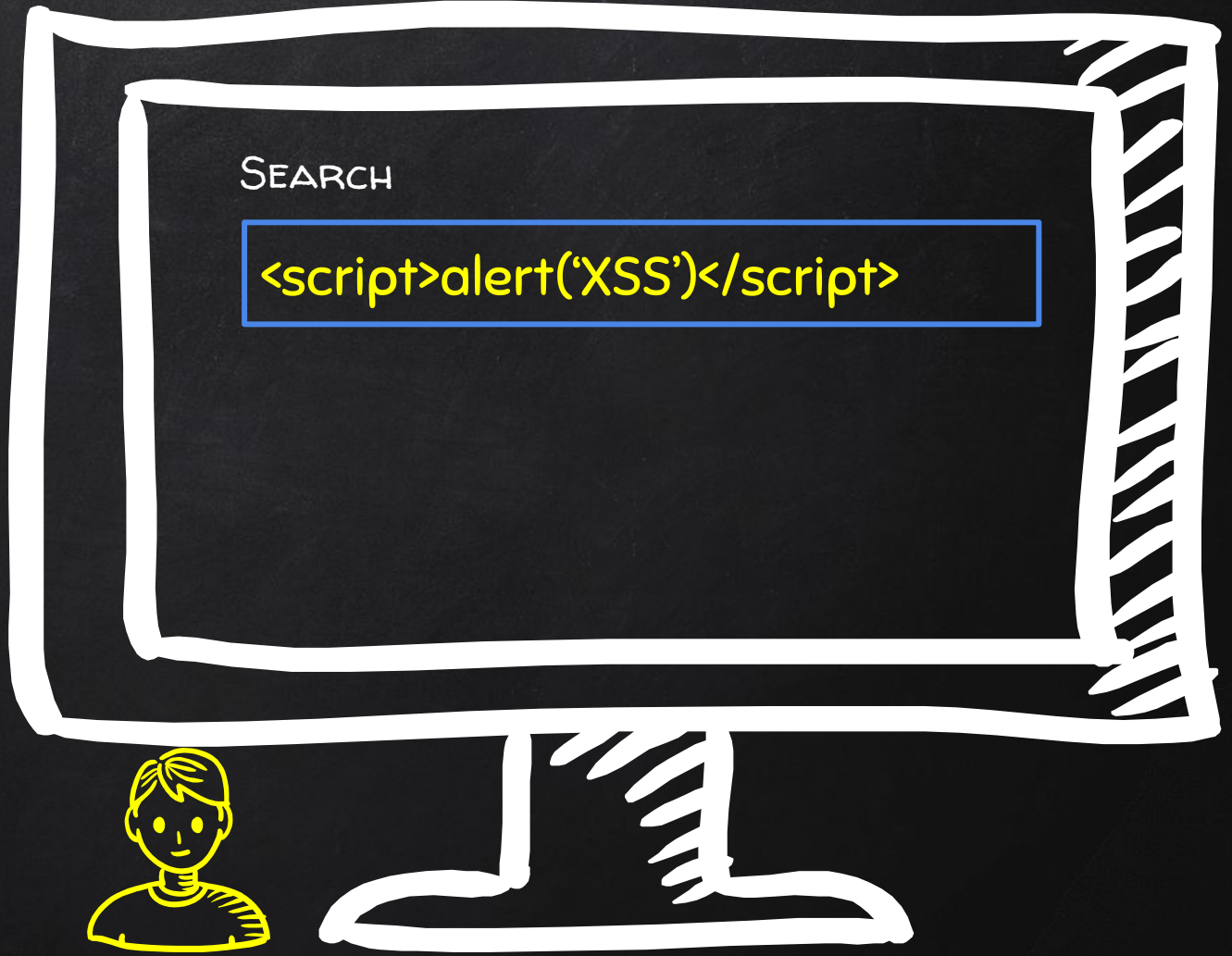
Target.com
Server

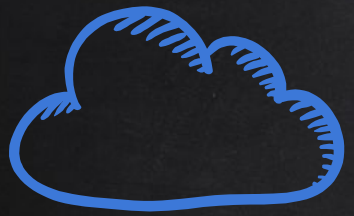
DOM
Stored
Reflected
XSS



Target.com
Server

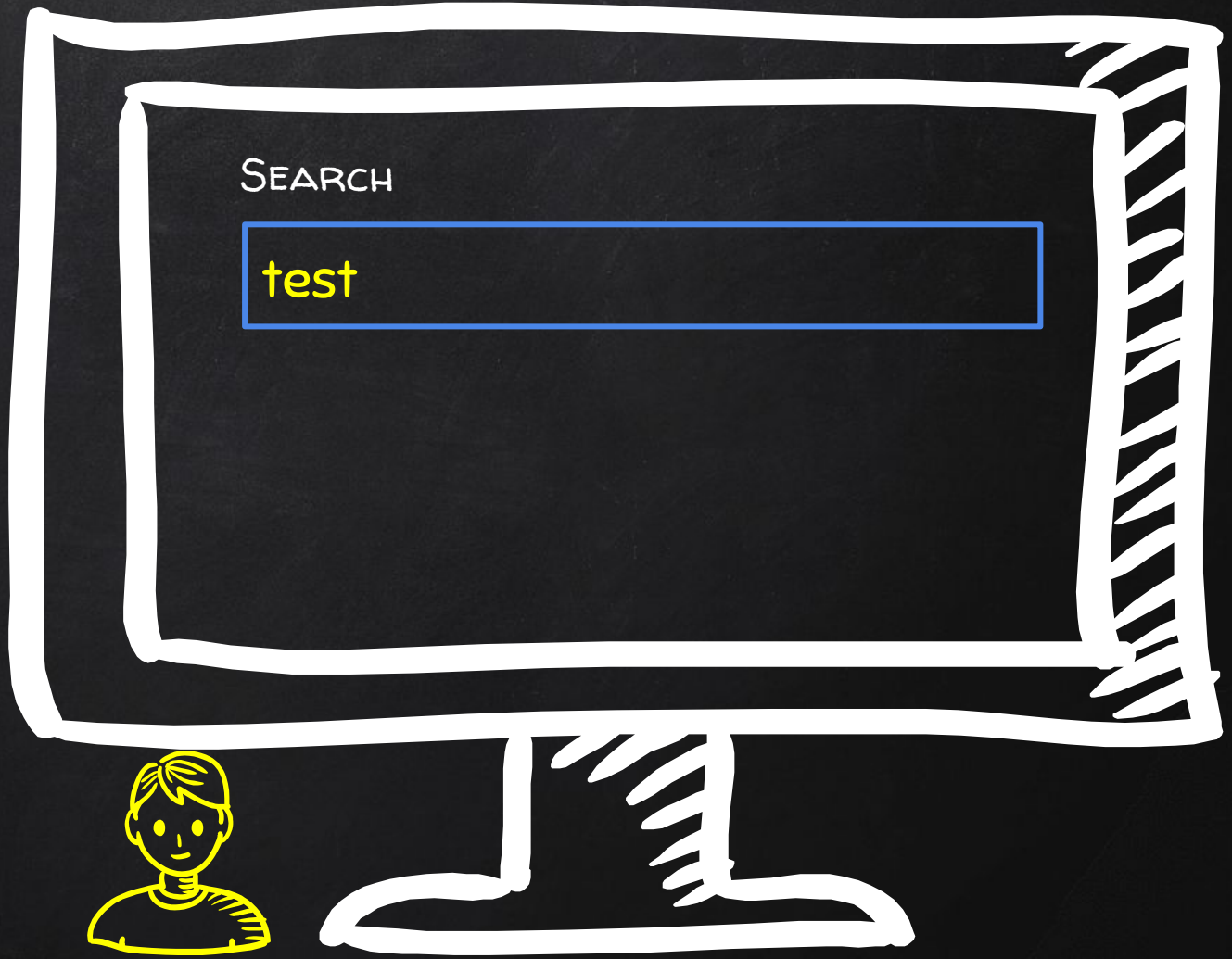
DOM
Stored
Reflected
XSS

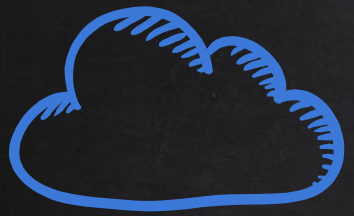




Target.com
Server

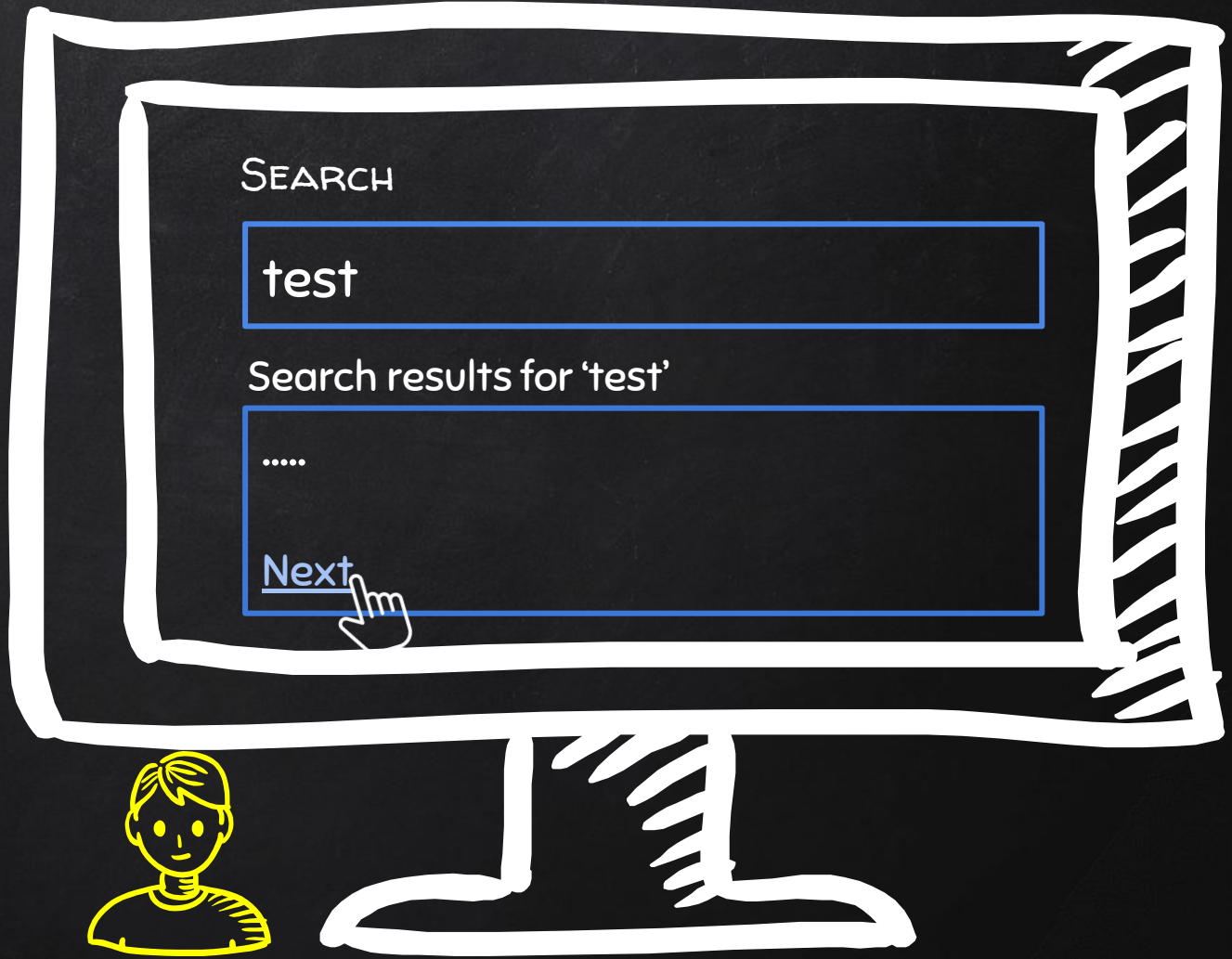
DOM
Stored
Reflected
XSS





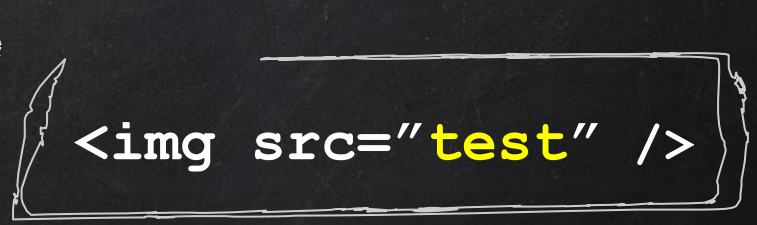
Target.com
Server

DOM
Stored
Reflected
XSS



Search

test



Search

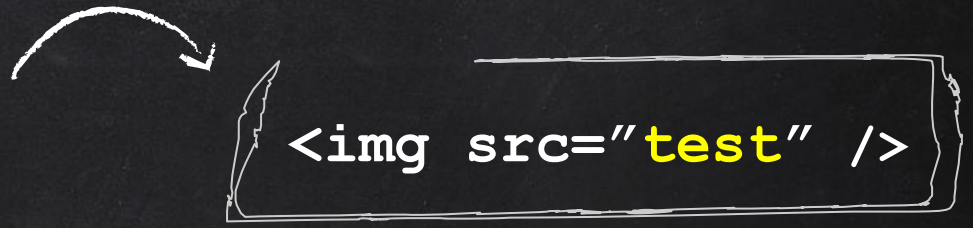
" onload=alert(2)>

Search

"><script>alert(2)</script>

Search

test

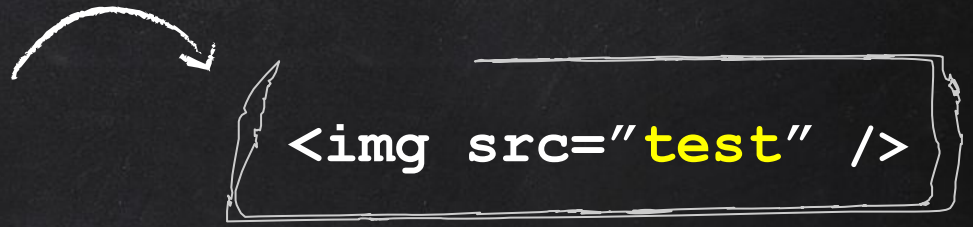


Search

"> <script>alert(2)</script>

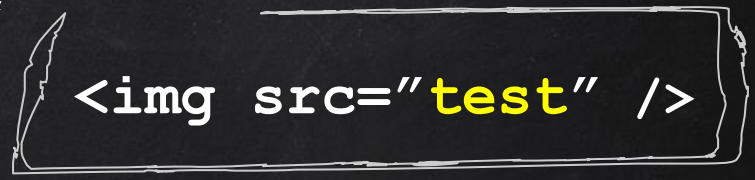
Search

test



Search

test



Search

" onload=alert(2)>

CSP & XSS

Content Security Policy CSP

- Browser feature that prevents XSS and other attacks.
- To enable it, response headers would include

```
Content-Security-Policy
```

XSS

Cross Site Scripting

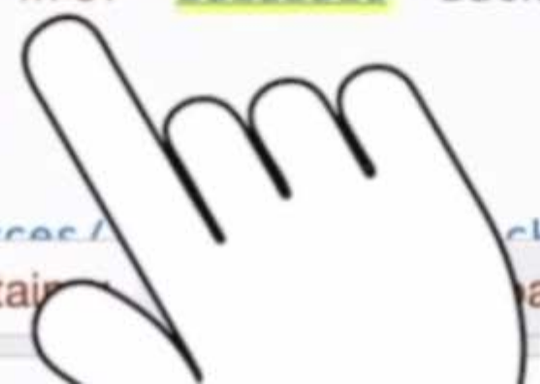
Bypassing Security

Submit feedback

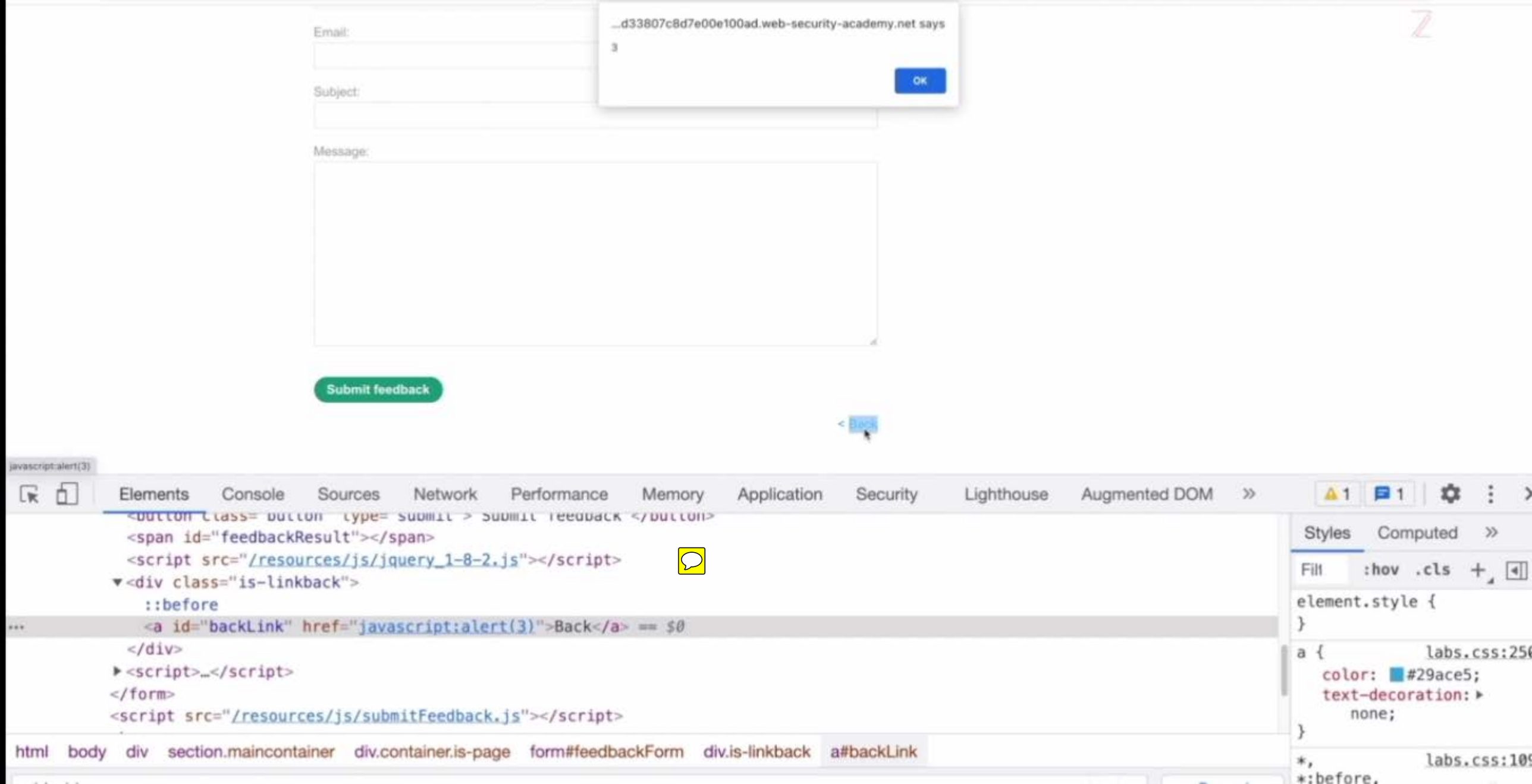
< Back

Elements Console Sources Network Performance Memory Application Security

```
<button class="button" type="submit"> Submit feedback </button>
<span id="feedbackResult"></span>
<script src="/resources/js/jquery_1-8-2.js"></script>
▼<div class="is-linkback">
  ::before
  <a id="backLink" href="zaidzaid">Back</a>
</div>
▶<script>…</script>
</form>
```



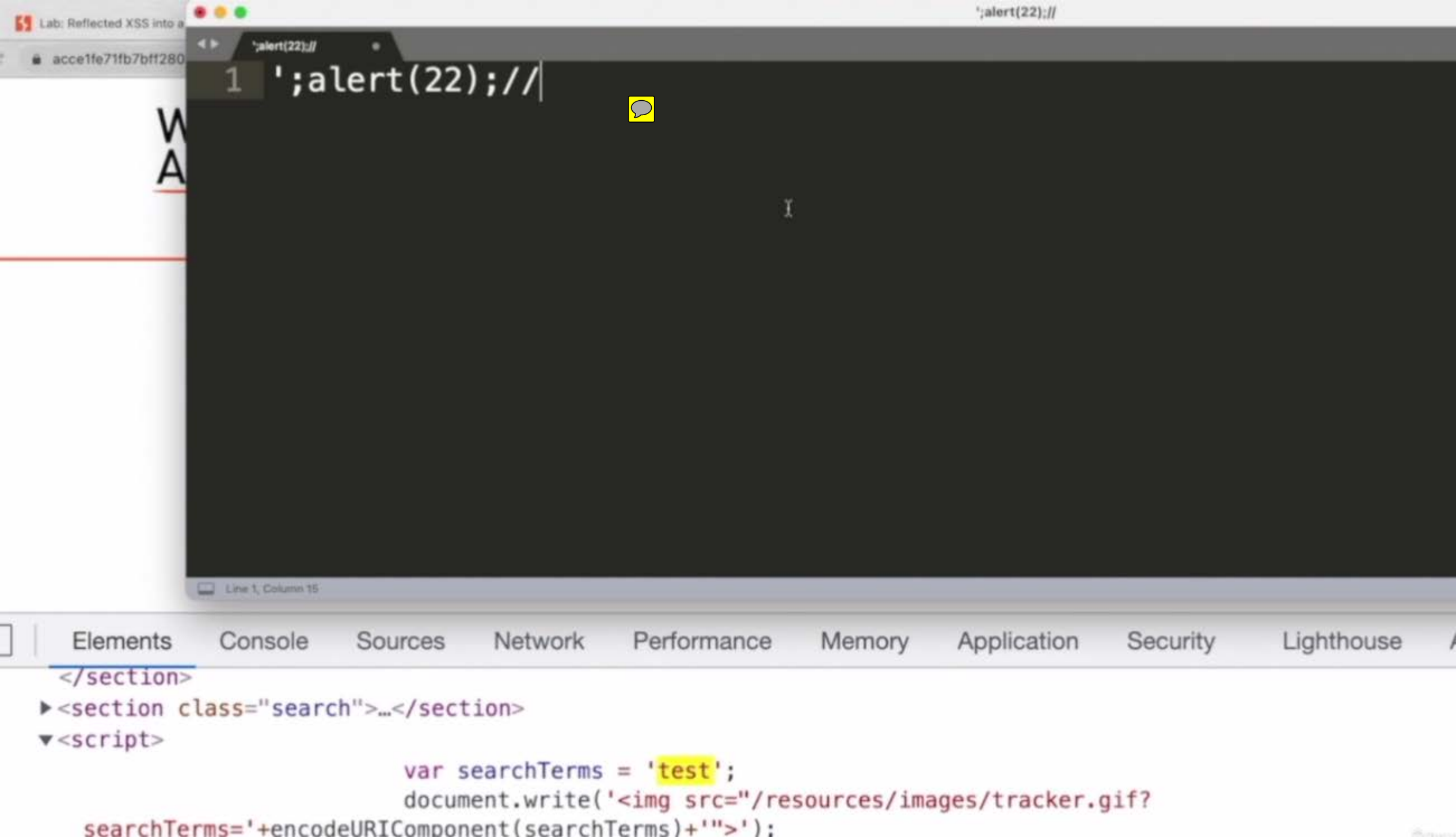
html body div section.maincontai age


...d33807c8d7e00e100ad.web-security-academy.net says
3
OK
Email:
Subject:
Message:
Submit feedback
< Back
javascript:alert(3)
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Augmented DOM

<script src="/resources/js/jquery_1-8-2.js"></script>

::before
Back == $0

<script>…</script>
</form>
<script src="/resources/js/submitFeedback.js"></script>
html
body
div
section.maincontainer
div.container.is-page
form#feedbackForm
div.is-linkback
a#backLink
Styles
Computed
Filt
:hov
.cls
element.style {
}
a {
color: #29ace5;
text-decoration:
none;
}
labs.css:256
labs.css:109


';alert(22);//
';alert(22);//
1 ';alert(22);//
Line 1, Column 15
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
</section>
<section class="search">…</section>
<script>
var searchTerms = 'test';
document.write('<img src="/resources/images/tracker.gif?
searchTerms='+encodeURIComponent(searchTerms)+'">');

Description:

On a dull grey day, when everyone needs a little color or sunshine in their lives, you can be the hero of the hour. Our new 'Paint A Rainbow' running suit will not only enhance your performance but will improve the lives of everyone around you.

Super lightweight material gives you the cutting edge when it comes to speed, but not only that; a million embedded nano super lights will give you a rainbow streak lighting up the sky as you run. They say not every superhero wears a suit, but you CAN. Bring some color and light into the lives of others by doing what you already do every day.

These are limited edition running suits, be one of only 100 people who have access to our brand new range. So, don't delay Paint A Rainbow today.

Milanaaa Check stock

< Return to list

Elements Console Sources Network Performance Memory Application Security Lighthouse »

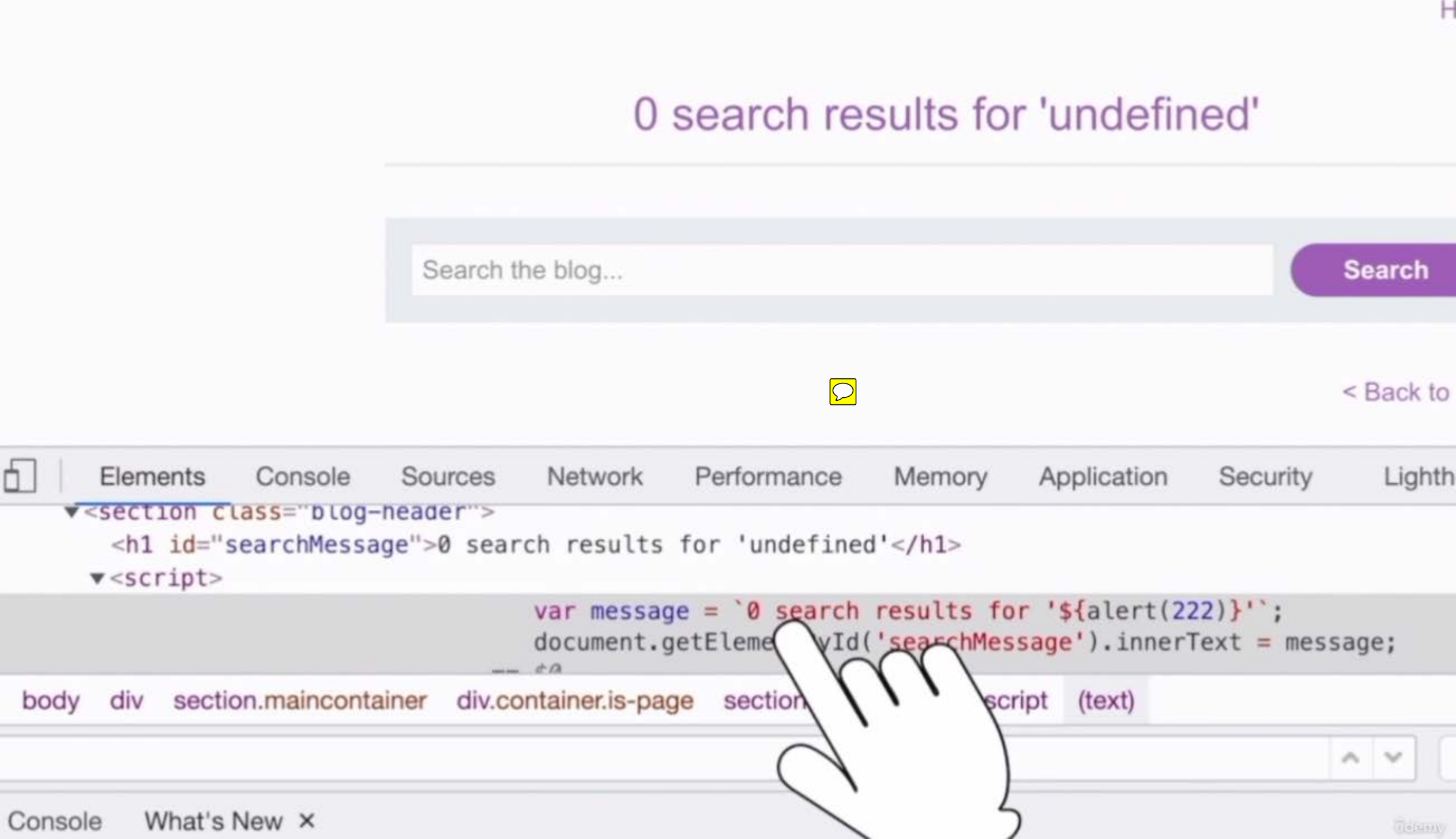
```
<p>…</p>
<p>…</p>
<form id="stockCheckForm" action="/product/stock" method="POST">
  <input required type="hidden" name="productId" value="3">
  <script>…</script>
  <select name="storeId"> == $0
    <option selected>Milanaaa</option>
    <option>London</option>
    <option>Paris</option>
    <option>Milan</option>
  </select>
```

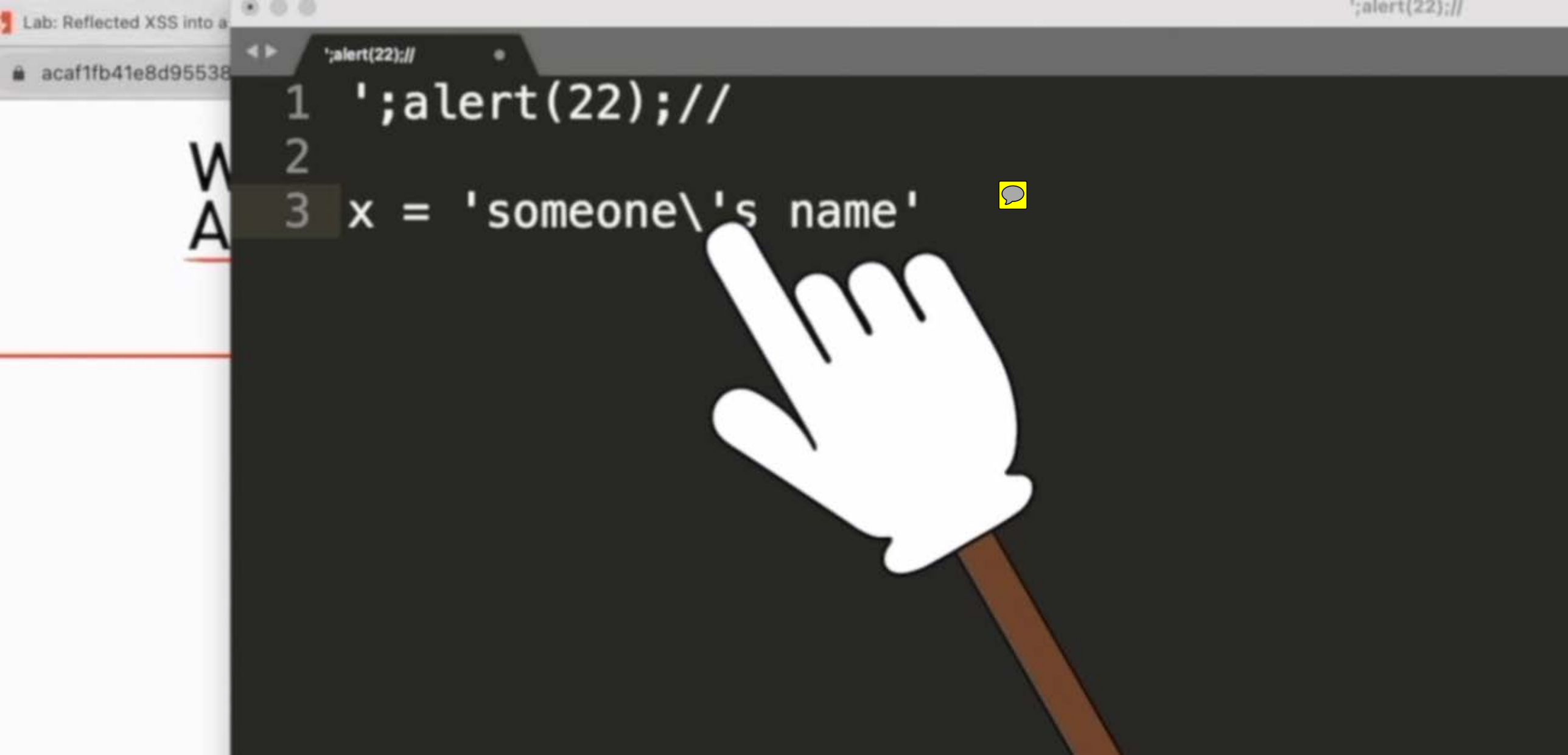
body div section maincontainer div.container.is-page section.product form#stockCheckForm select

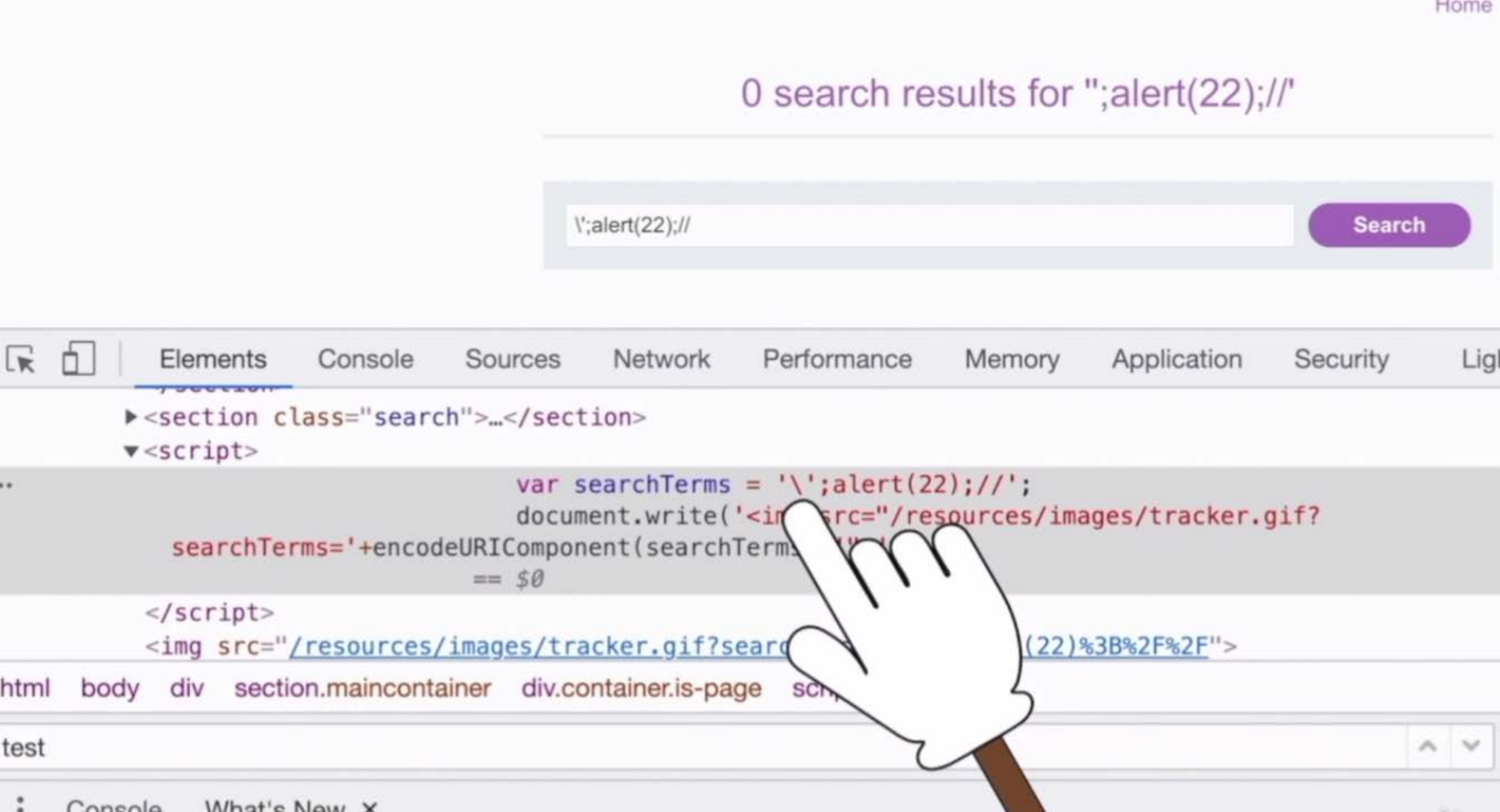
Styles Computed »

Filt :hov .cls +

```
element.style {
}
se   labsEcommerce.css:694
le
ct {
  -webkit-border-radius
    : 0;
  -moz-border-radius: 0;
  border-radius: ▸ 0;
  margin: ▸ 4px 0px;
```


0 search results for 'undefined'
Search the blog...
Search
< Back to
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighth
<section class="blog-header">
<h1 id="searchMessage">0 search results for 'undefined'</h1>
<script>
var message = `0 search results for '${alert(222)}'`;
document.getElem yId('searchMessage').innerText = message;
body
div
section.maincontainer
div.container.is-page
section
script
(text)
Console
What's New


Lab: Reflected XSS into a
acaf1fb41e8d95538
';alert(22);//
';alert(22);//
1 ';alert(22);//
2
3 x = 'someone\'s name'


Home
0 search results for ';alert(22);//'
\';alert(22);//
Search
Elements
Console
Sources
Network
Performance
Memory
Application
Security
<section class="search">…</section>
<script>
var searchTerms = '\';alert(22);//';
document.write('<im src="/resources/images/tracker.gif?
searchTerms='+encodeURIComponent(searchTerms
== $0
</script>
<img src="/resources/images/tracker.gif?searc
(22)%3B%2F%2F">
html
body
div
section.maincontainer
div.container.is-page
test
Console
What's New

0 search results for '\';alert(22);//

Search the blog...

Elements Console Sources Network Performance Memory Application Securi

```
<header class="notification-header"> </header>
<section class="blog-header">…</section>
<section class="search">…</section>
<script>
                    var searchTerms = '\\';alert(22);//';
                    document.write('<img src="/resources/images/tracker.gif?
searchTerms='+encodeURIComponent(searchTerms)
                  == $0
```

div section.maincontainer div.container.is-page script

Go to exploit server Back to lab description »

0 search results for 'spider'

Search the blog... Search