

TASK – 5

TARGET:

-> You need to complete 5 XSS (Cross Site Scripting) from the following platform.

-> <https://xss-quiz.int21h.jp/>

- You need to prove there is a XSS vulnerability in that particular web page.

NOTE:

- ❖ You need to complete challenges one after the other because after the completion of 1st challenge only you will enter into the 2nd challenge.
- ❖ Challenges 2 to 6 are considered as task-5.

SYNOPSIS:

XSS – cross site scripting:

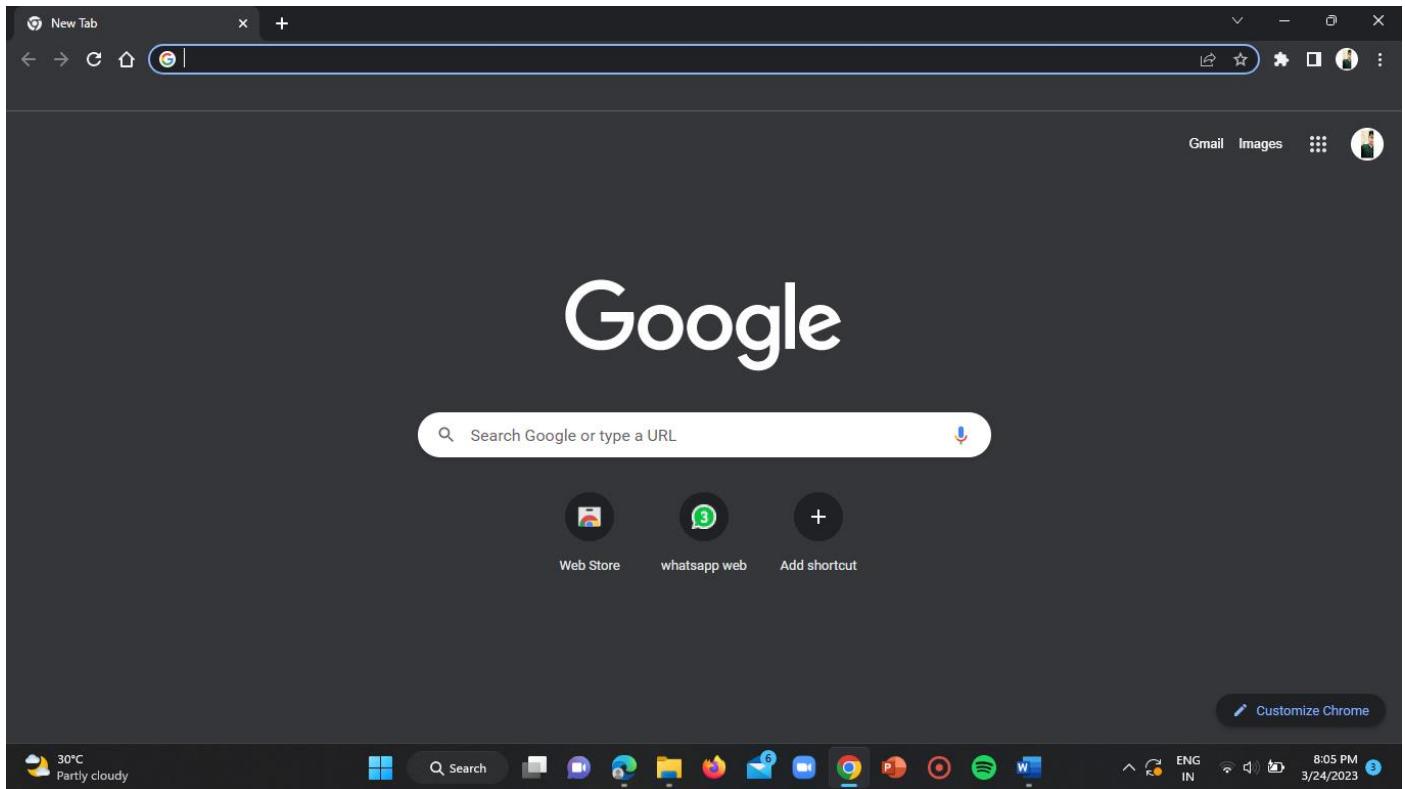
- Cross site scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise being and trusted websites.
- XSS attacks occur when:
 - Data enters a web application through an untrusted source, most frequently a web request.
 - Data is included in dynamic content that is sent to a web user without being validated for malicious content.
- Example of XSS include running unverified code on social media platforms or online games.

SOLUTION:

Step-1:

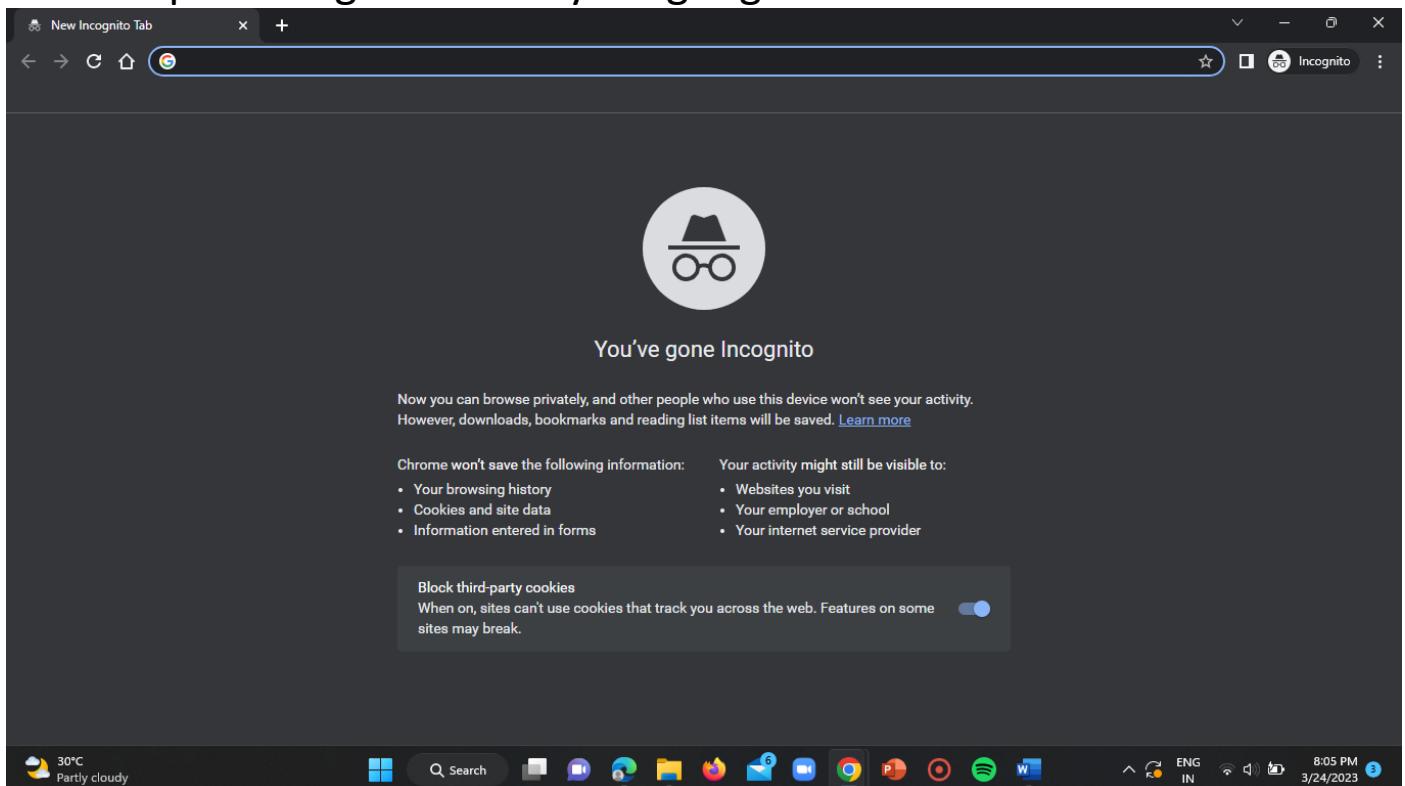
Open google chrome on your PC.

ST#IS#4899



Step-2:

Open incognito tab in your google browser.



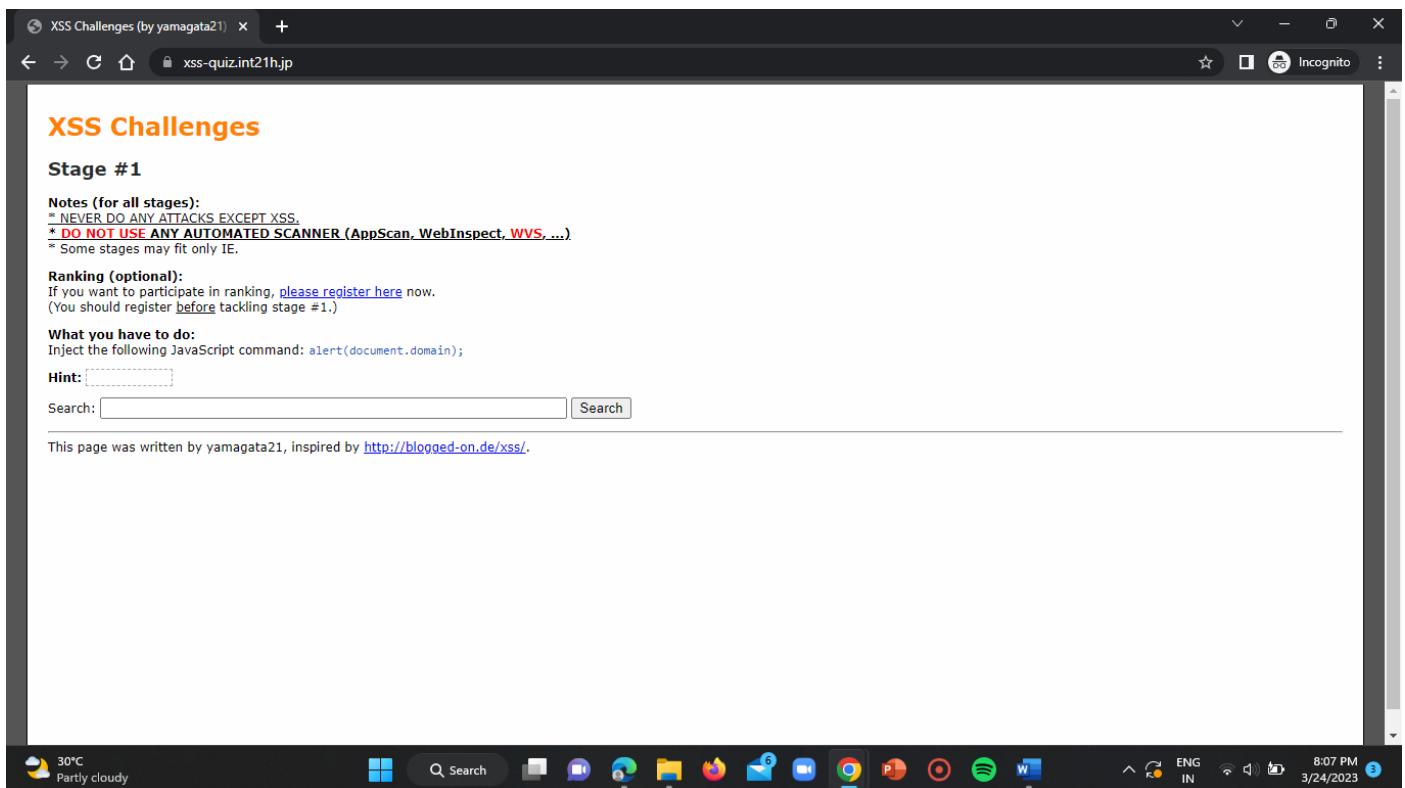
Challenge – 1:

Step-3:

Now go to above mentioned site i.e,

ST#IS#4899

<https://xss-quiz.int21h.jp/>



Step-4:

Now we can start the challenge 1 and we can use the hint given there (highlight that to see the hint). Now try to give the script to complete the challenge 1 in search field.

The script to use in this stage is:

“ <script>alert(document.domain)</script> ”

ST#IS#4899

The screenshot shows a web browser window titled "XSS Challenges (by yamagata21)". The URL is "xss-quiz.int21h.jp". The page content includes:

- XSS Challenges**
- Stage #1**
- Notes (for all stages):**
 - * NEVER DO ANY ATTACKS EXCEPT XSS.
 - * **DO NOT USE ANY AUTOMATED SCANNER (AppScan, WebInspect, WVS, ...)**
 - * Some stages may fit only IE.
- Ranking (optional):**

If you want to participate in ranking, [please register here](#) now.
(You should register before tackling stage #1.)
- What you have to do:**

Inject the following JavaScript command: `alert(document.domain);`
- Hint:** very simple...
- A search bar containing the injected script: `<script>alert(document.domain)</script>`
- A message at the bottom: "This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>.

The task is to inject the provided JavaScript code into the search bar to trigger an alert box.

Step-5 :

Click on enter and observe if any popup occurs. If there is any popup coming then click on yes.

The screenshot shows a web browser window with a confirmation dialog box in the foreground. The dialog box contains the text:

xss-quiz.int21h.jp says
xss-quiz.int21h.jp

An "OK" button is visible at the bottom right of the dialog box. The background of the browser window is dark, and the taskbar at the bottom shows various application icons.

Step-6:

ST#IS#4899

Now you will be displayed with a congratulations note which means you've completed the challenge now you are ready to move to challenge 2.

Then click on "stage2.php" then you will be redirected to the challenge 2 page.

XSS Challenges (by yamagata21) x +

xss-quiz.int21h.jp/?sid=8c0dc3bf17f94128926784faac4178decb04f448

Incognito

XSS Challenges

Stage #1

Notes (for all stages):

- * NEVER DO ANY ATTACKS EXCEPT XSS.
- * **DO NOT USE ANY AUTOMATED SCANNER (AppScan, WebInspect, WVS, ...)**
- * Some stages may fit only IE.

Ranking (optional):
If you want to participate in ranking, [please register here](#) now.
(You should register [before](#) tackling stage #1.)

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint:

Search: Search

No results for ""

Congratulations!! Next stage [stage2.php](#).

This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>.

30°C Partly cloudy

Search

8:14 PM 3/24/2023

Challenge – 2:

ST#IS#4899

The screenshot shows a browser window with the URL xss-quiz.int21h.jp/stage2.php?sid=bd8bd8965260ad8fe8df76e4095d13e1fa98b1a. The page title is "XSS Challenges". The main content area displays the challenge instructions: "What you have to do: Inject the following JavaScript command: alert(document.domain);". A "Hint" field contains the placeholder "[...]" and a search bar below it has the placeholder "Search: [...]".

This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>.

The screenshot shows the same browser window with developer tools open. The "Elements" tab is selected in the DevTools sidebar. The DOM tree shows the structure of the page, including the `<html>`, `<head>`, and `<body>` elements. The right panel displays the CSS styles for the `body` element, which includes a font family of Verdana, a background color of #555555, margins of 3px 20px 3px 20px, and a font size of 12px. The status bar at the bottom of the browser indicates a temperature of 30°C and light rain.

Here as we see in above picture, the input is taken as a string. So now we need to close the current tag and script tag (by adding “> at the start of the given script).

SCRIPT:

“ “><script>alert(document.domain)</script>”

ST#IS#4899

XSS Challenges (by yamagata21) +

xss-quiz.int21h.jp/stage2.php?sid=60a27283c909524c7eaf8e4de1e9247b27000f11

Incognito

XSS Challenges

Stage #2

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: [.....]

No results for your Query. Try again: "><script>alert(document.domain)</script>"

This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>.

30°C Rain showers

Search

File Explorer

Firefox

Mail

YouTube

Google Chrome

PowerShell

Microsoft Edge

Spotify

Word

ENG IN

9:40 PM 3/24/2023

Click on enter.

XSS Challenges (by yamagata21) +

xss-quiz.int21h.jp/stage2.php?sid=93dab94115273290ffeb9340ed817bbab0018529

Incognito

xss-quiz.int21h.jp says
xss-quiz.int21h.jp

OK

Elements

Console

Sources

Network

Performance

Styles

Computed

Layout

Event Listeners

DOM Breakpoints

Properties

Accessibility

Filter

No matching selector or style

Console

What's New

top Filter Default levels No Issues

30°C Rain showers

Search

File Explorer

Firefox

Mail

YouTube

Google Chrome

PowerShell

Microsoft Edge

Spotify

Word

ENG IN

9:43 PM 3/24/2023

Click on OK.

ST#IS#4899

XSS Challenges (by yamagata21) +

xss-quiz.int21h.jp/stage2.php?sid=93dab94115273290ffeb9340ed817bbab0018529

XSS Challenges

Stage #2

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: []

No results for your Query. Try again: [] > Search

Congratulations!! Next stage [stage-3.php](#).

This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>.

30°C Rain showers

Search

Console What's New

2 Issues: 2

(i.e. different eID+1) script, <https://ssl.google-analytics.com/ga.js>, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See <https://www.chromestatus.com/feature/5718547946799104> for more details.

9:44 PM 3/24/2023

Click on stage-3.php .

Challenge-3 :

XSS Challenges (by yamagata21) +

xss-quiz.int21h.jp/stage-3.php?sid=66c6d53d12cff22a2f94de319fa4012c0fdf68bb

XSS Challenges

Stage #3

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: []

Search a place: [] Search Choose a country: Japan

This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>.

30°C Rain showers

Search

Console What's New

2 Issues: 2

⚠ A parser-blocking, cross site `stage-3.php?sid=66c6_9fa4012c0fdf68bb:33` (i.e. different eID+1) script, <https://ssl.google-analytics.com/ga.js>, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See <https://www.chromestatus.com/feature/5718547946799104> for more details.

9:45 PM 3/24/2023

ST#IS#4899

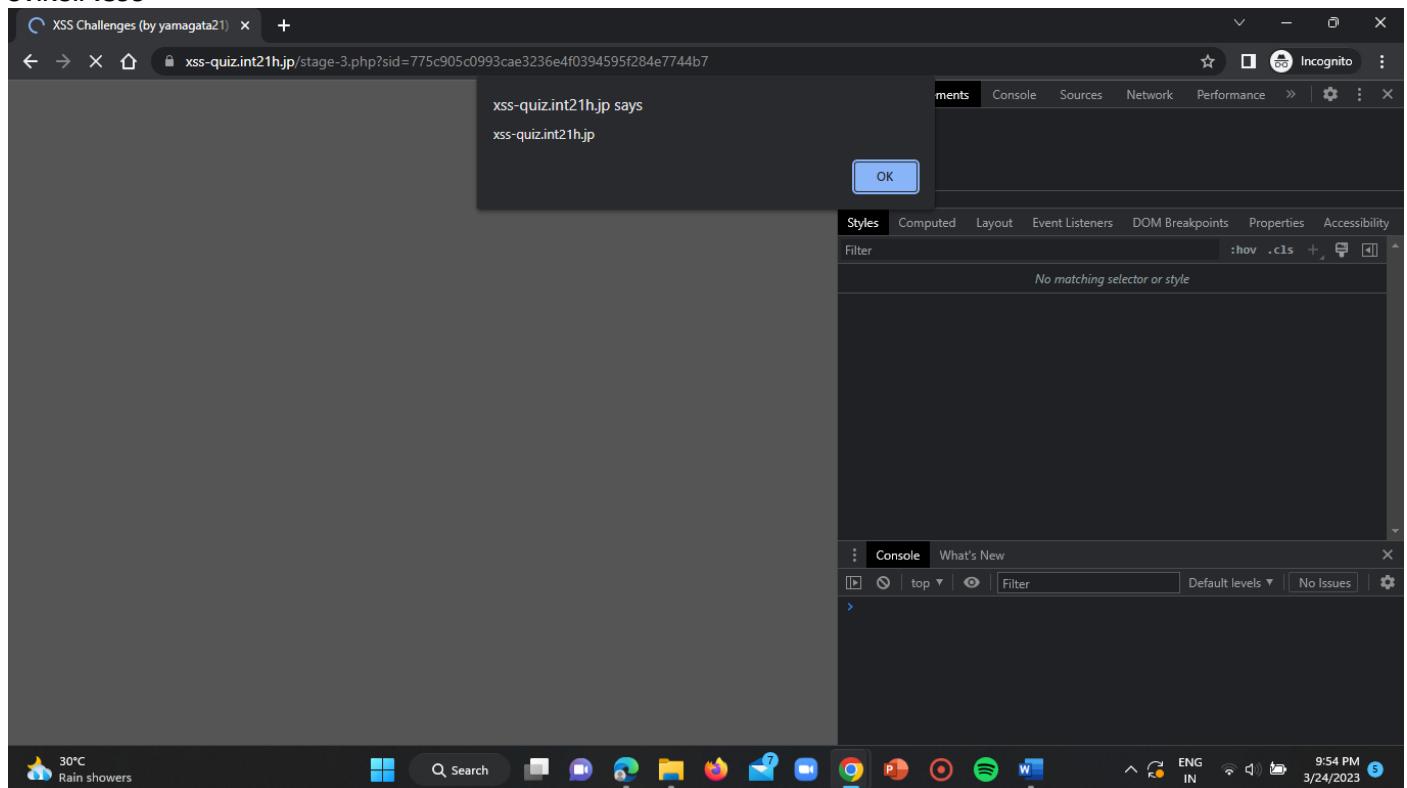
The screenshot shows a browser window with the URL xss-quiz.int21h.jp/stage-3.php?sid=69bf411d74f2190bb8af57eb37d28dfbd2583f5. The page title is "XSS Challenges" and the stage is "#3". The task is to inject the JavaScript command `alert(document.domain);`. A hint suggests using the "Search" field. The search bar contains `<script>alert(document.domain)</script>`. The message "We couldn't find any places called 'hello' in Japan." is displayed. The developer tools show the DOM structure and the injected script in the console.

As we given hello it is saying that “we could not find any places called ‘hello’ in Japan”. As we can see that by searching something it is shifting to another field called “choose a country”, so let us change the script at “`p2.Script(<script>alert(document.domain)</script>)`”.

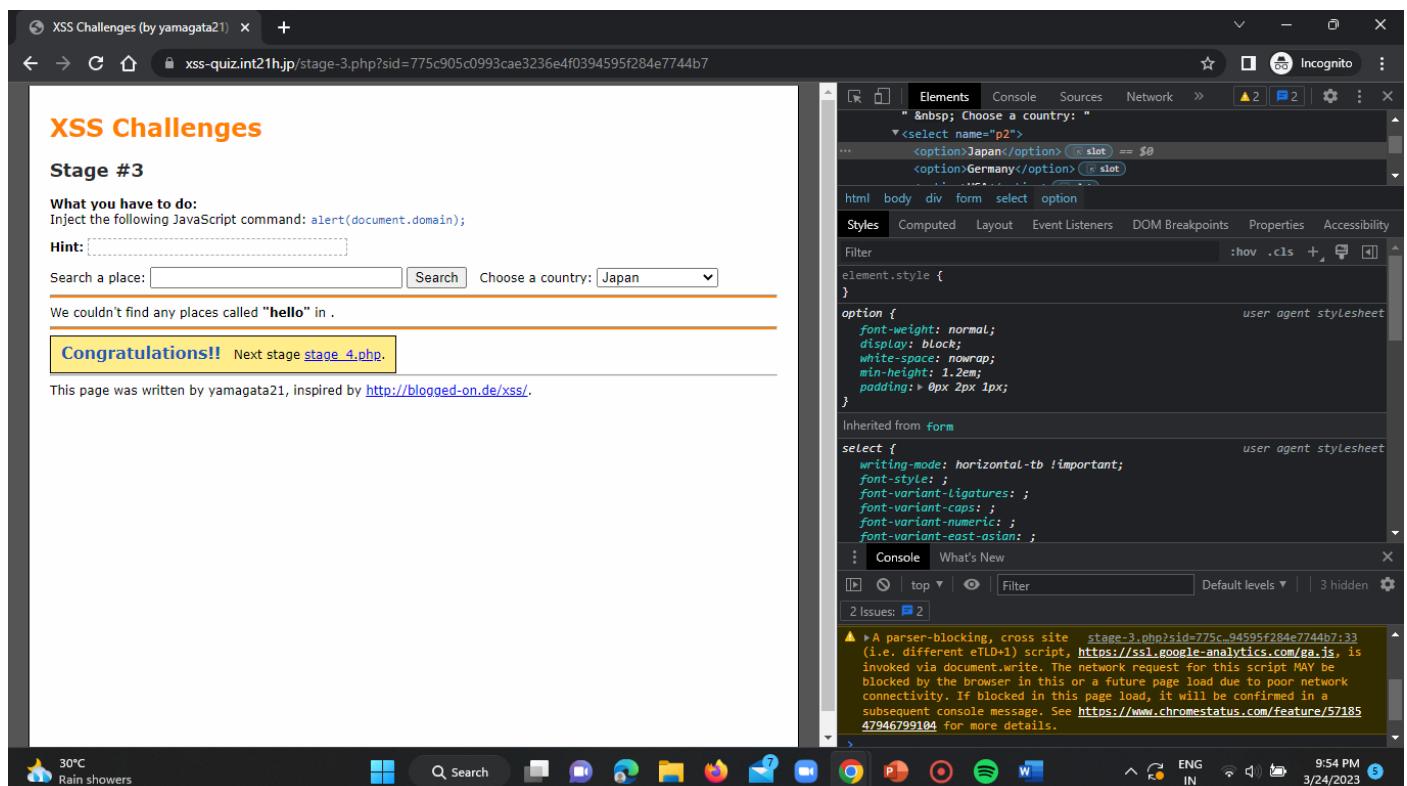
The screenshot shows a browser window with the URL xss-quiz.int21h.jp/stage-3.php?sid=810072e0095d60488cdf78dd77e405d96fb1f22c. The page title is "XSS Challenges" and the stage is "#3". The task is to inject the JavaScript command `alert(document.domain);`. A hint suggests using the "Choose a country" dropdown. The dropdown menu shows options for "Choose a country:" and "Germany". The message "We couldn't find any places called 'hello' in Japan." is displayed. The developer tools show the DOM structure and the injected script in the console.

Click on enter.

ST#IS#4899



Click on OK.



Now click on “stage-4.php”.

ST#IS#4899

The screenshot shows a browser window with the URL xss-quiz.int21h.jp/stage_4.php?sid=84d4c2d4563bf102c17d1a0048b7d6480a80ee01. The page title is "XSS Challenges" and the stage is "#4". The task is to inject the JavaScript command `alert(document.domain);`. A hint suggests using the search bar. The developer tools' Elements tab is open, focusing on a dropdown menu with options "Japan" and "Germany". The console tab shows a warning about a parser-blocking script from Google Analytics.

Challenge-4:

Paste the script in the search bar and click on enter.

The screenshot shows the same browser window after pasting the script. The search bar now contains "`<script>alert(document.domain)</script>`". The developer tools show the script has been injected into the search bar's value. The console tab again displays a warning about the Google Analytics script.

The given script could not find any places. Now observe the inspect we can see the hidden value 'hackme'. Replace that with "`<script>alert(document.domain)</script>`" and add '‘“>’ at the start of the script.

ST#IS#4899

The screenshot shows a browser window with the title "XSS Challenges" and a sub-section "Stage #4". The page contains a search bar, a dropdown for "Choose a country" set to "Japan", and a message stating "We couldn't find any places called '<script>alert(document.domain)</script>' in Japan.". Below this, a note says "This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>". To the right, the browser's developer tools are open, specifically the Elements tab. In the DOM tree, there is a hidden input field with the name "p3" and value "<script>alert(document.domain)</script>". The developer tools also show the user agent stylesheet for various input types and a console log with a warning about a parser-blocking script.

After clicking on enter we observe that the script disappears due to more number of double quotes so add ‘#34’ to replace the double quotes.

Now place the given script which is given below in inspect:
“#34><script>alert(document.domain)</script>”

The screenshot shows the same browser setup as before, but now the developer tools inspect element shows the injected script: "<input type='hidden' name='p3' value='#34><script>alert(document.domain)</script>'>". The browser's status bar at the bottom indicates "27°C Partly cloudy". The developer tools console still shows the parser-blocking warning.

Now click on enter and give the given script in search bar on webpage.

ST#IS#4899

The screenshot shows a browser window with the title "XSS Challenges (by yamagata21)". The main content area displays the text "XSS Challenges" and "Stage #4". Below this, there is a "What you have to do:" section with the instruction "Inject the following JavaScript command: alert(document.domain);". A "Hint" field contains the placeholder "[...]" and a search bar with the placeholder "Search". A dropdown menu for "Choose a country" is set to "Japan". A message below the search bar states, "We couldn't find any places called ""<script>alert(document.domain)</script>" in Japan." At the bottom, a note says, "This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>". To the right of the main window is the Chrome DevTools interface. The "Elements" tab is selected, showing the DOM structure with a highlighted element containing the injected script. The "Console" tab shows a warning message about a parser-blocking cross-site script being invoked via document.write. The system tray at the bottom indicates it's 10:16 PM on March 24, 2023, with a weather forecast of 27°C Partly cloudy.

Click on enter and click on OK on the popup raised.

The screenshot shows a browser window with the same XSS challenge page. A confirmation dialog box is overlaid on the page, containing the text "xss-quiz.int21h.jp says" and "xss-quiz.int21h.jp", with an "OK" button. The browser's developer tools are open, showing the "Elements" tab with the injected script highlighted. The "Console" tab is empty. The system tray at the bottom indicates it's 10:17 PM on March 24, 2023, with a weather forecast of 27°C Partly cloudy.

Click on OK.

ST#IS#4899

XSS Challenges (by yamagata21) +
xss-quiz.int21h.jp/stage_4.php?sid=9d6be37e9377c1a6953b7f2f659bee8ca5c3a405

XSS Challenges

Stage #4

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: [.....]

Search a place: Search Choose a country: Japan >

We couldn't find any places called "<script>alert(document.domain)</script>" in Japan.

Congratulations!! Next stage [stage-5.php](#).

This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>.

27°C Partly cloudy Search Home Back Forward Stop Reload Incognito More
ENG IN 10:17 PM 3/24/2023

Elements Console Sources Network Cancel
Styles Computed Layout Event Listeners DOM Breakpoints Properties Accessibility
Filter :hover .cls +
element.style {}
input:not([type="image"] i) { user agent stylesheet
 box-sizing: border-box;
}
input[type="hidden"] i { user agent stylesheet
 appearance: none;
 background-color: initial;
 cursor: default;
 display: none !important;
 padding: 0 initial;
 border: 0 initial;
}
input { user agent stylesheet
 writing-mode: horizontal-tb !important;
 font-style: ;
 font-variant-Ligatures: ;
};
Console What's New
top Filter Default levels 3 hidden
2 Issues: 2
⚠ A parser-blocking, cross site stage_4.php?sid=9d6b-659bee8ca5c3a405:35 (i.e. different eTLD+1) script, https://ssl.google-analytics.com/ga.js, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See https://www.chromestatus.com/feature/5718547946799104 for more details.

Now click on “stage-5.php” to be redirected to the challenge 5 page.

XSS Challenges (by yamagata21) +
xss-quiz.int21h.jp/stage--5.php?sid=e1bfbb321d15c6ce2a606c3c4cc5e04bea22e53

XSS Challenges

Stage #5

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: [.....]

Search: Search

This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>.

27°C Partly cloudy Search Home Back Forward Stop Reload Incognito More
ENG IN 10:18 PM 3/24/2023

Elements Console Sources Network Cancel
Styles Computed Layout Event Listeners DOM Breakpoints Properties Accessibility
Filter :hover .cls +
element.style {}
body { style.css:2
 font-family: Verdana;
 background-color: #555555;
 margin: 3px 20px 3px 20px;
 font-size: 12px;
}
body { user agent stylesheet
 display: block;
 margin-top: 8px;
};
margin 3
border -
Console What's New
top Filter Default levels 3 hidden
2 Issues: 2
⚠ A parser-blocking, cross site stage_4.php?sid=9d6b-659bee8ca5c3a405:35 (i.e. different eTLD+1) script, https://ssl.google-analytics.com/ga.js, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See https://www.chromestatus.com/feature/5718547946799104 for more details.

Challenge – 5:

ST#IS#4899

The screenshot shows a browser window with the URL xss-quiz.int21h.jp/stage--5.php?sid=e1bfbfb321d15c6ce2a606c3c4cc5e04bea22e53. The page title is "XSS Challenges" and the stage is "#5". A hint says "length limited text box". Below is a search form with a text input and a "Search" button. The developer tools' Elements tab is open, showing the HTML structure and styles for the page. The body has a font-family of Verdana, background-color of #555555, margin of 3px 20px 3px 20px, and a font-size of 12px. The user agent stylesheet adds a margin of 3px and a border of 1px solid black to the input element.

open the inspect.

So now change the size and length to 50 or high.

The screenshot shows the same browser setup as before, but with changes made to the input field. The developer tools' Elements tab shows the input element now has a size of 50 and a value of "Search". The user agent stylesheet for the input element now includes a padding of 1px and a border of 2px solid black. The browser status bar at the bottom shows the date and time as 10:19 PM 3/24/2023.

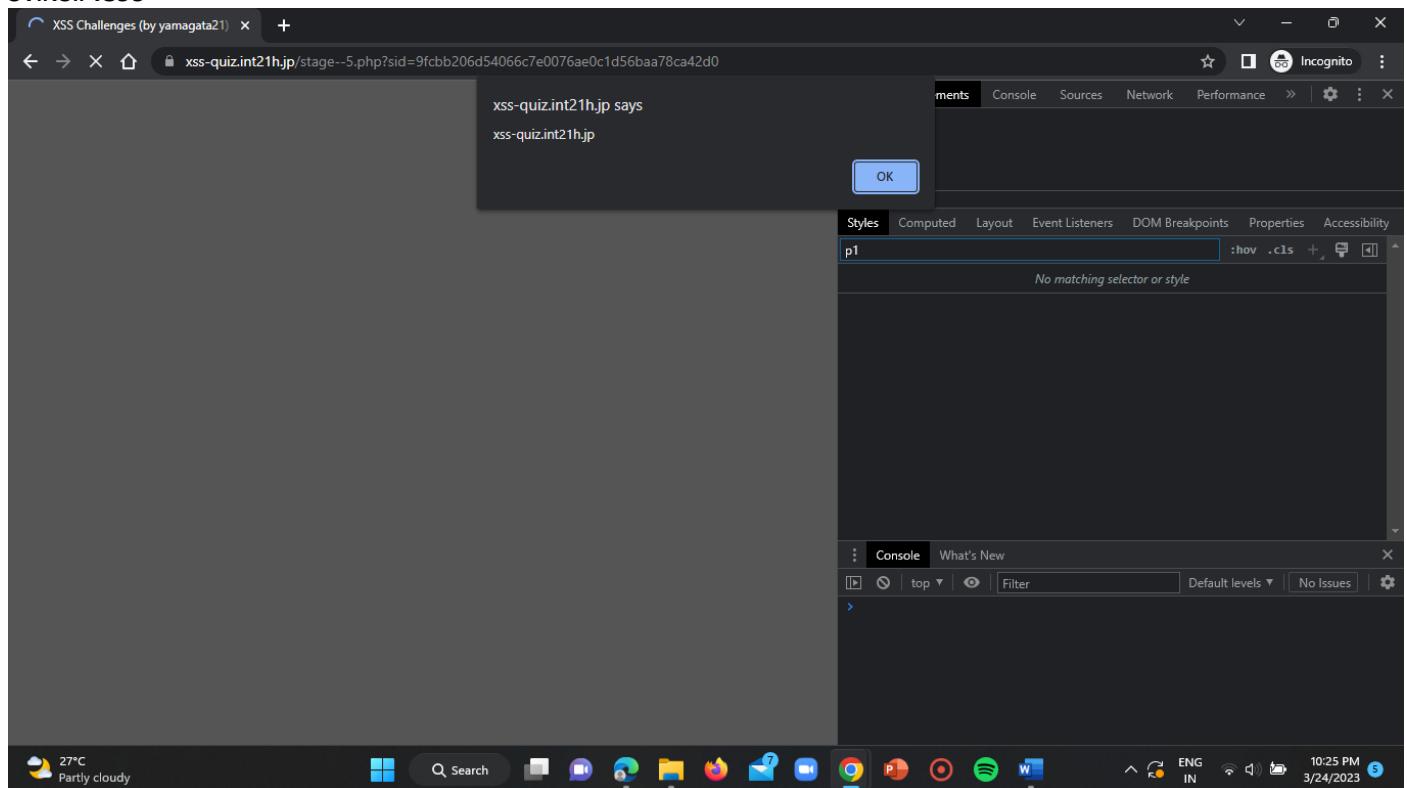
Now enter the script on search bar of the webpage.

Script: <script>alert(document.domain)</script>

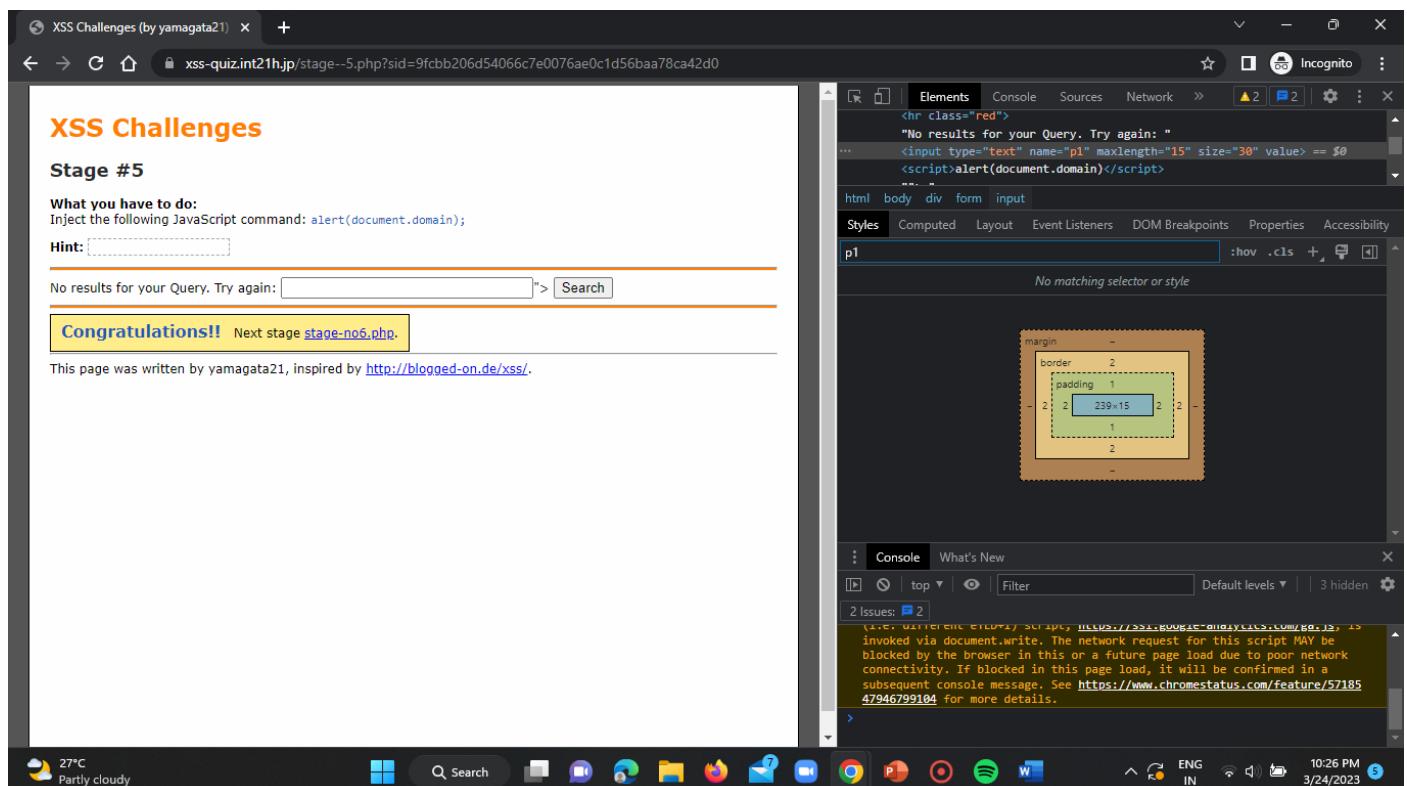
ST#IS#4899

The screenshot shows a browser window with the title "XSS Challenges (by yamagata21)". The URL is "xss-quiz.int21h.jp/stage--5.php?sid=71bf4bfff6a681c694579f1d012ab482d18a4180". The page content includes a heading "XSS Challenges" and "Stage #5". It displays a "What you have to do:" section with the instruction "Inject the following JavaScript command: alert(document.domain);". A "Hint" input field is present. Below it, a search bar contains the query "

ST#IS#4899



Click on OK.



Now click on “stage-no6.php”. you will be redirected to the challenge 6 webpage.

ST#IS#4899

The screenshot shows a web browser window with the URL xss-quiz.int21h.jp/stage-no6.php?sid=c9d5e9b58895896efe62a3e4b3a3097f2170fab8. The page title is "XSS Challenges" and the stage is "Stage #6". The challenge instructions ask to inject the JavaScript command `alert(document.domain);`. A hint suggests using event handler attributes. The search bar contains the placeholder "Search:". Below the search bar is a note: "This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>". The browser's status bar at the bottom shows the date as 3/24/2023 and the time as 10:27 PM.

Elements

```
<hr class="red">
"Search: "
<input type="text" name="p1" size="60" value="">
<input type="submit" value="Search">
```

html body div form input

Styles Computed Layout Event Listeners DOM Breakpoints Properties Accessibility

p1 :hov .cls +

No matching selector or style

margin - border 2 padding 1 449x15 2 2 1 2

Console What's New

top Filter Default levels 3 hidden

2 Issues: 2

A parser-blocking, cross site `stage-no6.php?sid=c9-b3a3097f2170fab8:28` (i.e. different eID+1) script, <https://ssl.google-analytics.com/ga.js>, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See <https://www.chromestatus.com/feature/5718547946799104> for more details.

Challenge – 6:

The screenshot shows a web browser window with the URL xss-quiz.int21h.jp/stage-no6.php?sid=c9d5e9b58895896efe62a3e4b3a3097f2170fab8. The page title is "XSS Challenges" and the stage is "Stage #6". The challenge instructions ask to inject the JavaScript command `alert(document.domain);`. A hint suggests using event handler attributes. The search bar contains the placeholder "Search:". Below the search bar is a note: "This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>". The browser's status bar at the bottom shows the date as 3/24/2023 and the time as 10:27 PM.

Elements

```
<hr class="red">
"Search: "
<input type="text" name="p1" size="60" value="">
<input type="submit" value="Search">
```

html body div form input

Styles Computed Layout Event Listeners DOM Breakpoints Properties Accessibility

p1 :hov .cls +

No matching selector or style

margin - border 2 padding 1 449x15 2 2 1 2

Console What's New

top Filter Default levels 3 hidden

2 Issues: 2

A parser-blocking, cross site `stage-no6.php?sid=c9-b3a3097f2170fab8:28` (i.e. different eID+1) script, <https://ssl.google-analytics.com/ga.js>, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See <https://www.chromestatus.com/feature/5718547946799104> for more details.

Now give a script in search bar.

Script: "<script>alert(document.domain)</script>"

ST#IS#4899

XSS Challenges

Stage #6

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: [.....]

Search: `<script>alert(document.domain)</script>`

This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>.

27°C Partly cloudy

2 Issues: 2

A parser-blocking, cross site `stage-no6.php?sid=c9-b3a3097f2170fab8:28` (i.e. different eID+1) script, <https://ssl.google-analytics.com/ga.js>, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See <https://www.chromestatus.com/feature/5718547946799104> for more details.

Click on enter.

XSS Challenges

Stage #6

What you have to do:
Inject the following JavaScript command: `alert(document.domain);`

Hint: [.....]

No results for your Query. Try again: `<script>alert(document.domain)</script>`

This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>.

27°C Partly cloudy

2 Issues: 2

A parser-blocking, cross site `stage-no6.php?sid=56_901ba6fba9f18488:28` (i.e. different eID+1) script, <https://ssl.google-analytics.com/ga.js>, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See <https://www.chromestatus.com/feature/5718547946799104> for more details.

We get no results for our query. So, add closing start at the start i.e ““>”.

ST#IS#4899

The screenshot shows a browser window with the title "XSS Challenges (by yamagata21)". The URL is "xss-quiz.int21h.jp/stage-no6.php?sid=5a1b1a997caa9d5e6b2abda656380dd53fc6a2a1". The page content includes a heading "XSS Challenges" and "Stage #6". A "What you have to do:" section with the instruction "Inject the following JavaScript command: alert(document.domain);". A "Hint:" input field containing ".....". Below it is a search bar with the placeholder "No results for your Query. Try again: [input field] Search". A note at the bottom says "This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>". To the right, the browser's developer tools are open, specifically the Elements tab. It shows the HTML structure: a form with an input element named "p1". The input has a value of ">alert(document.domain)< script>" and a type of "text". The "Computed" tab shows the element's style: margin: 0, border: 2px solid black, padding: 1px, width: 379px, height: 15px. The "Console" tab shows a warning about a parser-blocking script from Google Analytics. The system tray at the bottom indicates it's 27°C and partly cloudy.

Here we can observe that in inspect it is encoded but we get no results. So, now try the given below script in the search bar.
Script: "hello "onmouseover=" alert(document.domain)"

The screenshot shows the same browser setup as before, but the search bar now contains the injected script: "hello "onmouseover=" alert(document.domain)". The developer tools show the script is still encoded in the input field. The "Console" tab now displays a warning about a parser-blocking, cross-site script from Google Analytics. The system tray at the bottom indicates it's 27°C and partly cloudy.

Click on enter.

ST#IS#4899

The screenshot shows a browser window with the URL xss-quiz.int21h.jp/stage-no6.php?sid=9fd5783eaf5285292144c35cf0db4811df8637f1. The page title is "XSS Challenges" and the stage is "#6". The "What you have to do:" section instructs to inject the command `alert(document.domain);`. A "Hint:" input field contains a placeholder. Below it is a search bar with the query "hello" and a "Search" button. A message at the bottom states, "This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>". On the right, the Chrome developer tools are open, showing the Elements tab with the code `<hr class="red">`, `"No results for your Query. Try again: "`, and `... <input type="text" name="p1" size="50" value="hello" onmouseover="alert(document.domain)"> == $0`. The Styles tab shows a CSS rule for `p1` with properties: margin: 0, border: 2px solid black, padding: 1px, width: 379px, height: 15px. The Console tab shows a warning about a parser-blocking script from <https://ssl.google-analytics.com/ga.js>.

You will get a popup then click on OK.

The screenshot shows a browser window with the URL xss-quiz.int21h.jp/stage-no6.php?sid=3868103881319166b3f7205f6d95392a1a4d0508. The page title is "XSS Challenges" and the stage is "#6". The "What you have to do:" section instructs to inject the command `alert(document.domain);`. A "Hint:" input field contains a placeholder. Below it is a search bar with the query "hello" and a "Search" button. A yellow box highlights the text "Congratulations!! Next stage [stage07.php](#)". A message at the bottom states, "This page was written by yamagata21, inspired by <http://blogged-on.de/xss/>".

Now you've successfully completed the challenge-6.

CONCLUSION:

I hereby conclude that by attempting this task I have learnt about some vulnerabilities using scripts. I also gained knowledge about XSS and we have three types of XSS attacks. They are “Reflected XSS, DOM based XSS attack, Stored XSS attack”.