Assignment 11

1. TASK-1:

1. TITLE OF THE VULNERABILITY: Host Header Injection Vulnerability.

2. CVSS SCORE: 6.5 (Medium)

3. RELATE TO OWASP TOP 10:

A05:2024 - Security Misconfiguration

4. DESCRIPTION:

Host Header Injection occurs when an attacker manipulates the Host HTTP header to interfere with server-side processing. Applications relying on the Host header without proper validation may be vulnerable to attacks like cache poisoning, password reset link manipulation, or bypassing security restrictions.

5. DETAILED EXPLANATION:

The Host header is used by web servers and applications to identify the domain requested by the client. An attacker can craft malicious requests with a spoofed Host header to:

Redirect users to malicious sites.

Generate misleading links in password reset emails.

Poison cache or CDN responses.

6. IMPACT:

Confidentiality: Exposure of sensitive user data through phishing.

Integrity: Manipulated or misleading content delivery.

Availability: Potential denial of service via cache poisoning.

Reputation Damage: Users redirected to malicious sites harm brand trust.

7. RECOMMENDATIONS:

Validate and sanitize the Host header to ensure it matches the expected domain.

Avoid relying on the Host header for critical operations; use server configurations to define trusted domains.

Implement a whitelist of allowed hostnames.

Use HTTPS and enable strict Transport Security (HSTS) to mitigate redirection-based attacks.

Conduct regular security testing to identify and fix misconfigurations.

8. STEP BY STEP PROCEDURE:

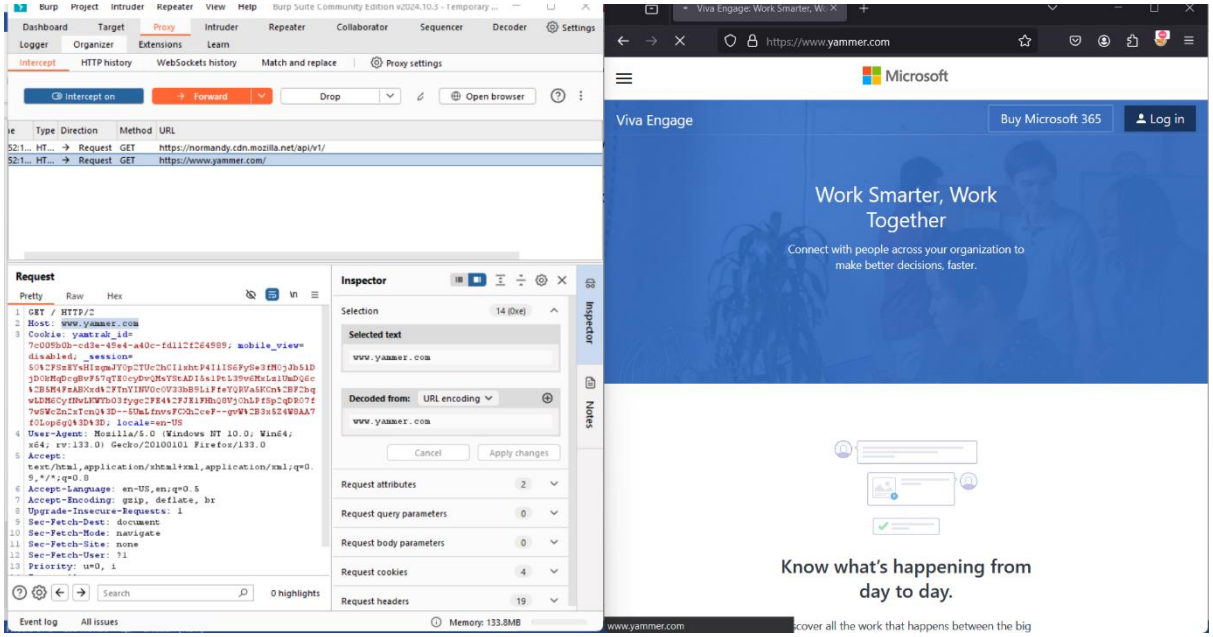
1. Now we done the host header injection

2. For that we need to find it on website

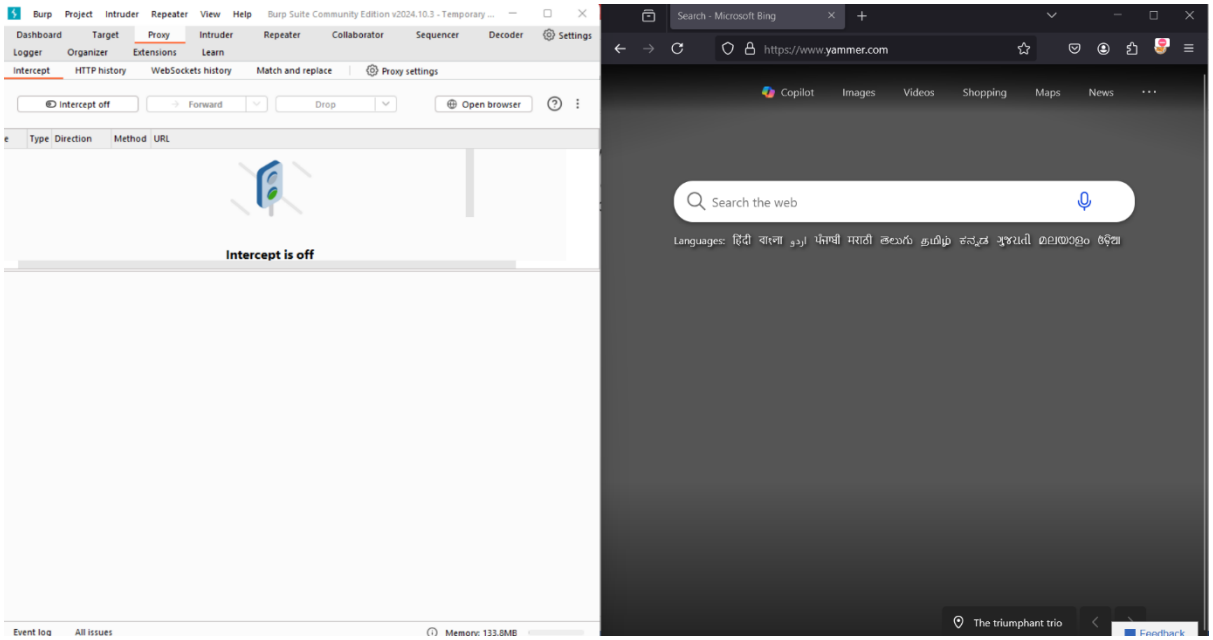
3. After finding the website we use the burp suite to known that mentioned website is vulnerable or not

4. To know this we need to catch the proxy and change it by the redirection url it may redirected it will become the host header vulnerable.

9. PROOF OF THE CONTENT:



After we change it to Bing and then enter we gets the Bing website.



TASK-2:

1. TITLE OF VULNERABILITY:

URL Redirection Vulnerability

2. CVSS SCORE:

6.1 (Medium)

3. RELATE TO OWASP TOP 10:

A03:2024 - Injection

4. DESCRIPTION:

URL Redirection Vulnerability occurs when an application redirects users to external URLs based on unvalidated or user-controlled input. Attackers exploit this flaw to redirect victims to malicious websites, often as part of phishing or social engineering attacks.

5. DETAILED EXPLANATION:

Applications that dynamically construct redirection URLs based on query parameters or input values can be exploited if the input is not validated. For example:

https://example.com/redirect?url=http://malicious-site.com

An attacker could send a phishing email containing the above link, misleading users into thinking they are navigating to the legitimate site. Once redirected, the attacker could steal sensitive information or infect users with malware.

6. IMPACT:

Confidentiality: Users redirected to malicious sites may expose sensitive data.

Integrity: Trust in the application's URLs is compromised.

Reputation Damage: Users lose trust in the platform due to phishing risks.

7. RECOMMENDATIONS:

Avoid using dynamic redirections; use static or predefined URLs whenever possible.

Validate and sanitize user-provided URL inputs to ensure they conform to allowed domains.

Implement an allow list of trusted domains for redirection.

Notify users before redirecting them, displaying the destination URL for confirmation.

Regularly test for open redirection vulnerabilities using automated tools and manual reviews.

8. STEP BY STEP PROCEDURE:

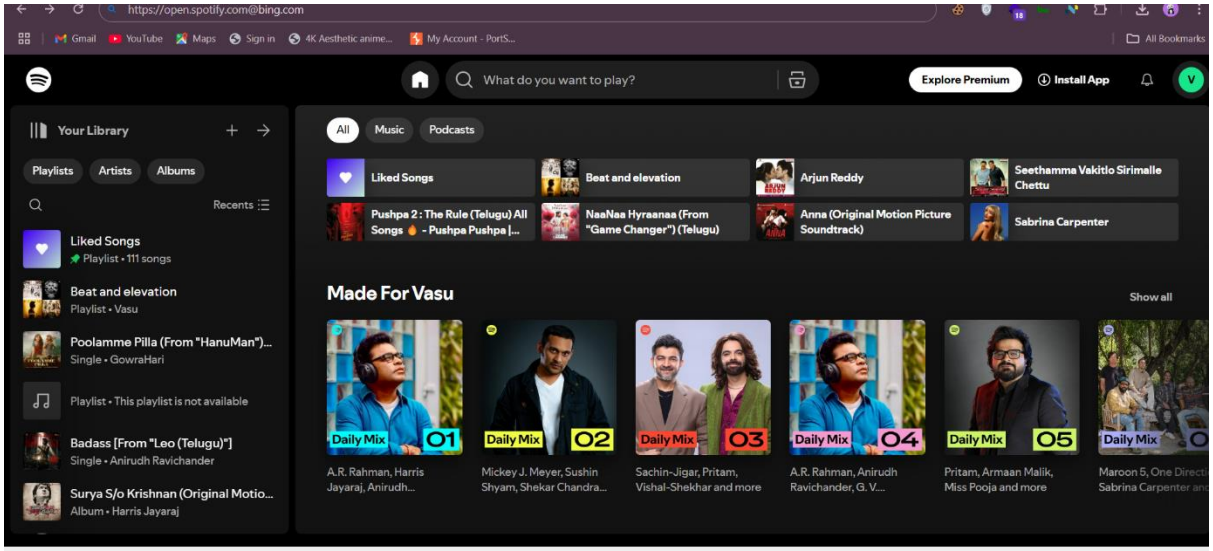
1. Now we done the targeted websites url direction.

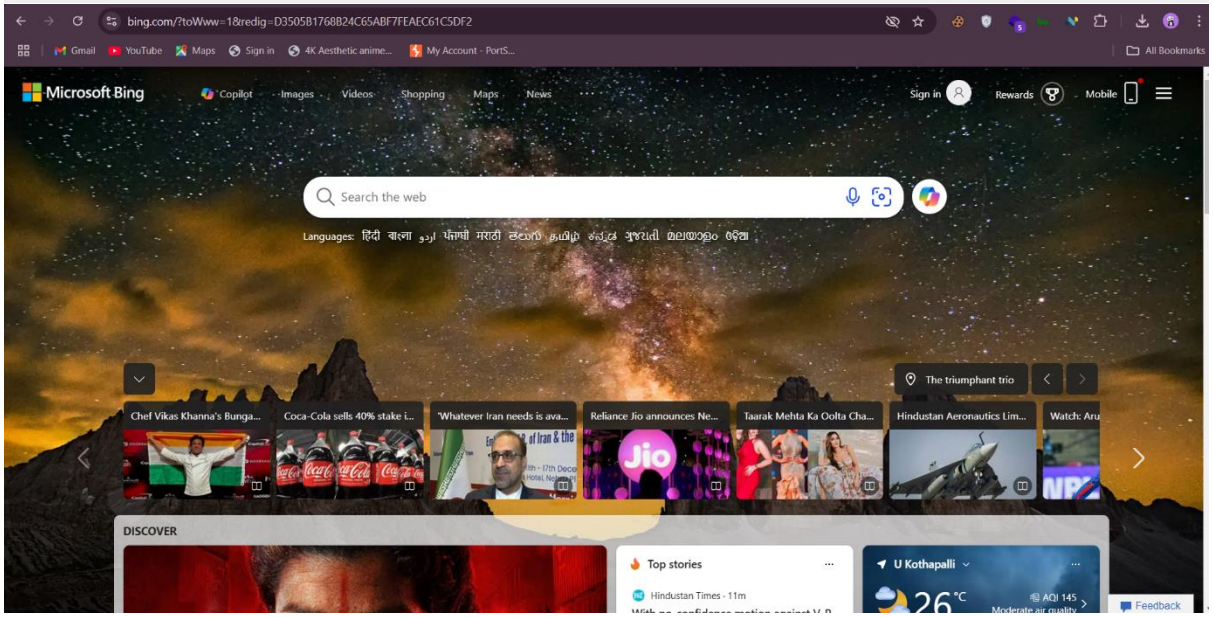
2. We choose the target websites from the internet.

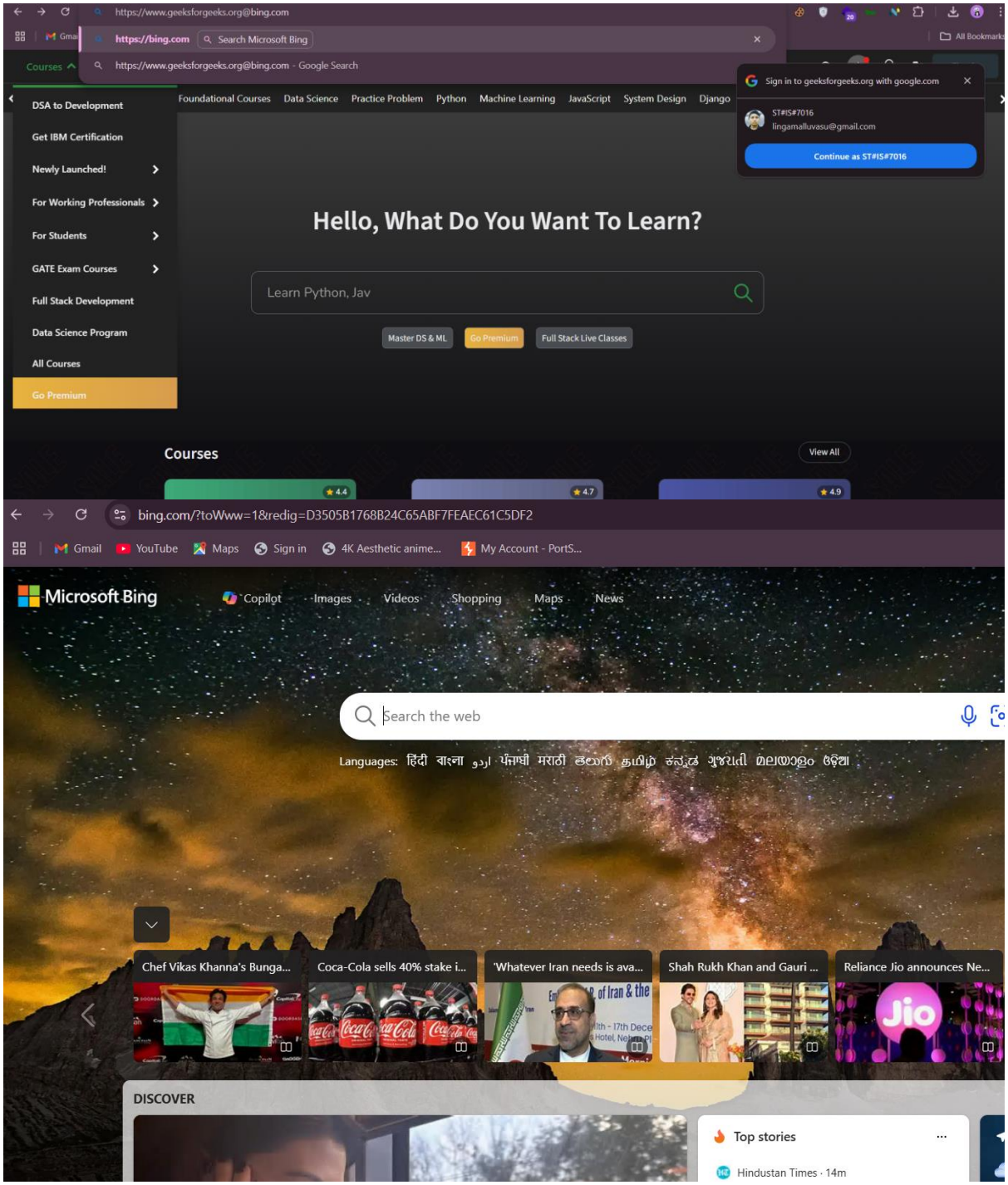
3. Now add the redirecting urls to the websites.

4. If the response was capture and redirected it will be vulnerable.

9. PROOF OF CONTENT:


https://open.spotify.com@bing.com
What do you want to play?
Explore Premium
Install App
Your Library
Playlists
Artists
Albums
Recents
Liked Songs
Playlist • 111 songs
Beat and elevation
Playlist • Vasu
Poolamme Pilla (From "HanuMan")...
Single • GowraHari
Playlist • This playlist is not available
Badass [From "Leo (Telugu)"]
Single • Anirudh Ravichander
Surya S/o Krishnan (Original Motio...
Album • Harris Jayaraj
All
Music
Podcasts
Liked Songs
Beat and elevation
Arjun Reddy
Seethamma Vakitlo Sirimalle Chettu
Pushpa 2 : The Rule (Telugu) All Songs - Pushpa Pushpa |...
NaaNaa Hyraanaa (From "Game Changer") (Telugu)
Anna (Original Motion Picture Soundtrack)
Sabrina Carpenter
Made For Vasu
Show all
Daily Mix 01
A.R. Rahman, Harris Jayaraj, Anirudh...
Daily Mix 02
Mickey J. Meyer, Sushin Shyam, Shekar Chandra...
Daily Mix 03
Sachin-Jigar, Pritam, Vishal-Shekhar and more
Daily Mix 04
A.R. Rahman, Anirudh Ravichander, G.V....
Daily Mix 05
Pritam, Armaan Malik, Miss Pooja and more
Daily Mix
Maroon 5, One Direct
Sabrina Carpenter


bing.com/?toWww=1&redig=D3505B1768B24C65ABF7FEAEC61C5DF2
Microsoft Bing
Copilot
Images
Videos
Shopping
Maps
News
Sign in
Rewards
Mobile
Search the web
Languages: हिंदी বাংলা اردو ਪੰਜਾਬੀ मराठी తెలుగు தமிழ் ಕನ್ನಡ ગુજરાતી മലയാളം ଓଡ଼ିଆ
The triumphant trio
Chef Vikas Khanna's Bunga...
Coca-Cola sells 40% stake i...
'Whatever Iran needs is ava...
Reliance Jio announces Ne...
Taarak Mehta Ka Oolta Cha...
Hindustan Aeronautics Lim...
Watch: Aru
DISCOVER
Top stories
Hindustan Times · 11m
U Kothapalli
26 °C
AQI 145
Feedback


https://www.geeksforgeeks.org@bing.com
https://bing.com
Search Microsoft Bing
https://www.geeksforgeeks.org@bing.com - Google Search
Courses
DSA to Development
Get IBM Certification
Newly Launched!
For Working Professionals
For Students
GATE Exam Courses
Full Stack Development
Data Science Program
All Courses
Go Premium
Foundational Courses
Data Science
Practice Problem
Python
Machine Learning
JavaScript
System Design
Django
Sign in to geeksforgeeks.org with google.com
ST#IS#7016
lingamalluvasu@gmail.com
Continue as ST#IS#7016
Hello, What Do You Want To Learn?
Learn Python, Jav
Master DS & ML
Go Premium
Full Stack Live Classes
Courses
View All
4.4
4.7
4.9
bing.com/?toWww=1&redig=D3505B1768B24C65ABF7FEAEC61C5DF2
Gmail
YouTube
Maps
Sign in
4K Aesthetic anime...
My Account - PortS...
Microsoft Bing
Copilot
Images
Videos
Shopping
Maps
News
Search the web
Languages: हिंदी বাংলা اردو ਪੰਜਾਬੀ मराठी తెలుగు தமிழ் ಕನ್ನಡ ગુજરાતી മലയാളം ଓଡ଼ିଆ
Chef Vikas Khanna's Bunga...
Coca-Cola sells 40% stake i...
'Whatever Iran needs is ava...
Shah Rukh Khan and Gauri ...
Reliance Jio announces Ne...
DISCOVER
Top stories
Hindustan Times · 14m

TASK-3:

1. TITLE OF VULNERABILITY:

Clickjacking Vulnerability

2. CVSS SCORE:

4.3 (Medium)

3. RELATE TO OWASP TOP 10:

A07:2024 - Identification and Authentication Failures

4. DESCRIPTION:

Clickjacking occurs when an attacker tricks a user into clicking on an invisible or disguised UI element, such as a button or link, within an application. This exploit leverages iframes or layers to hide malicious actions beneath legitimate web pages, enabling attackers to perform unintended actions on behalf of the user.

5. DETAILED EXPLANATION:

An attacker creates a malicious page that embeds the target application in an invisible iframe. They then position the iframe under a deceptive element like a fake button. When the victim clicks on the visible element, the click is registered on the underlying iframe, executing the attacker's intended action.

Example scenario: A user unknowingly clicks a "Like" button on a malicious page, but the click triggers a fund transfer on a banking app.

6. IMPACT:

Confidentiality: Sensitive operations may be triggered without user consent.

Integrity: Unauthorized actions may compromise data or accounts.

Reputation Damage: Loss of user trust in the application due to exploitation.

7. RECOMMENDATIONS:

Implement the X-Frame-Options HTTP header to prevent framing of your application (DENY or SAMEORIGIN).

Use the Content-Security-Policy (CSP) frame-ancestors directive to define allowed origins for embedding content.

Clearly inform users about critical actions and require explicit confirmations (e.g., CAPTCHA or multi-factor authentication).

Regularly test for clickjacking vulnerabilities during application assessments.

Educate users about clickjacking risks and encourage cautious behaviour when interacting with unknown links or pages.

8. STEP BY STEP PROCEDURE:

1. Now we use to find the website which can have the iframe clickjacking vulnerability

2. We find on internet by search and test using payload of html code.

3. Now it opens it has vulnerability.

Payload code:

```
<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">
```

```
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Clickjacking Test</title>
<style>
iframe {
position: absolute;
top: 50px;
left: 50px;
width: 800px;
height: 600px;
opacity: 0.5; /* Make it semi-transparent */
border: 2px solid red;
}
.overlay {
position: absolute;
top: 50px;
left: 50px;
width: 800px;
height: 600px;
background-color: rgba(255, 0, 0, 0.1);
z-index: 10;
}
</style>
</head>
<body>
<h1>Clickjacking Test</h1>
```

If the target page loads in the iframe below, it may be vulnerable to clickjacking.

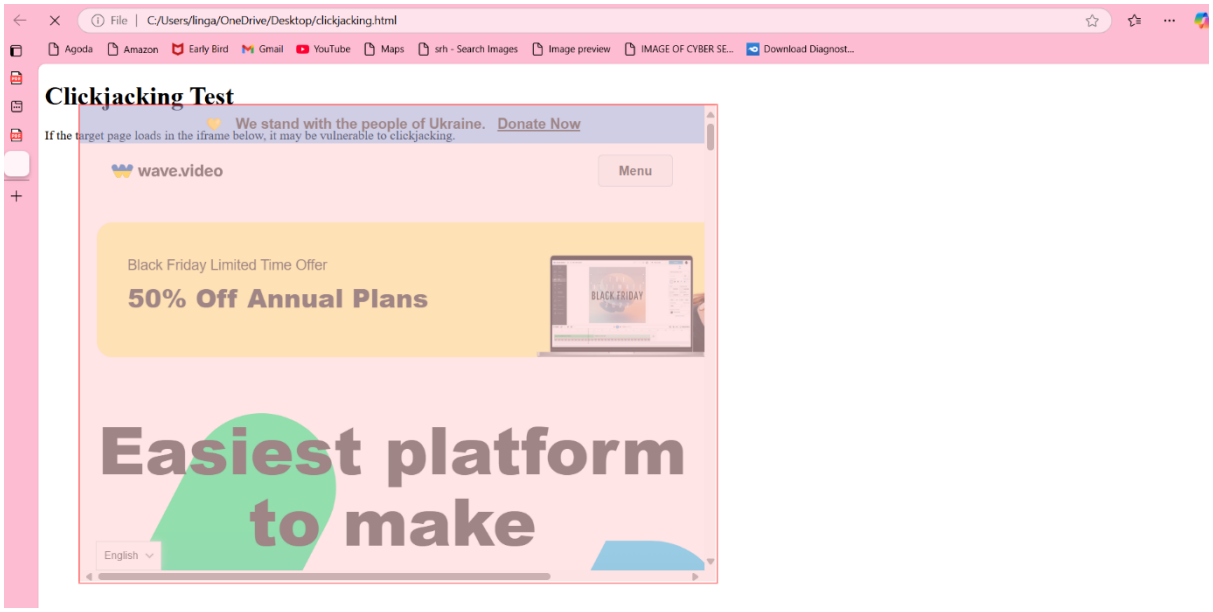
<iframe src="https://example.com"></iframe> <!-- Replace with the target URL -->

</body>

</html>

9. PROOF OF CONTENT:

```
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
   <title>Clickjacking Test</title>
   <style>
      iframe {
         position: absolute;
         top: 50px;
         left: 50px;
         width: 800px;
         height: 600px;
         opacity: 0.5; /* Make it semi-transparent */
         border: 2px solid red;
      }
      .overlay {
         position: absolute;
         top: 50px;
         left: 50px;
         width: 800px;
         height: 600px;
         background-color: rgba(255, 0, 0, 0.1);
         z-index: 10;
      }
   </style>
</head>
<body>
   <h1>Clickjacking Test</h1>
   <p>If the target page loads in the iframe below, it may be vulnerable to clickjacking.</p>
   <iframe src="https://wave.video/"></iframe> <!-- Replace with the target URL -->
   <div class="overlay"></div>
</body>
</html>
```


File | C:/Users/linga/OneDrive/Desktop/clickjacking.html
Agoda
Amazon
Early Bird
Gmail
YouTube
Maps
srh - Search Images
Image preview
IMAGE OF CYBER SE...
Download Diagnost...
Clickjacking Test
If the target page loads in the iframe below, it may be vulnerable to clickjacking.
We stand with the people of Ukraine. Donate Now
wave.video
Menu
Black Friday Limited Time Offer
50% Off Annual Plans
Easiest platform to make
English