Website name

https://habigonjzilasamiti.ssbmultiservices.com

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

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

CVSS: Base Score: 5.8

POC:



HTML File:

```
iframe{
width: 100%;
height: 600px;
border: none;
}
</style>
```

<title>Clickjacking PoC</title>
<body></body>
<pre>clickjacking</pre>
<iframe <="" sandbox="allow-modals allow-popups allow-forms allow-same-origin allow-scripts" td=""></iframe>
style="opacity:1" src=" https://habigonjzilasamiti.ssbmultiservices.com">

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

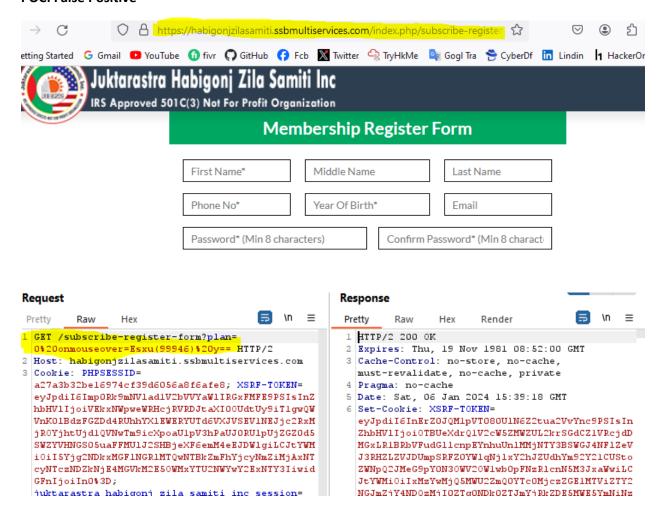
Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors

directive. Consult Web references for more information about the possible values for this header.

2. Vulnerability name: Cross site scripting

Vulnerable URL: https://habigonjzilasamiti.ssbmultiservices.com/subscribe-registerform?plan=0%20onmouseover=Esxu(99946)%20y==

POC: False Positive



3. Vulnerability name: Sensitive Information Disclosure

Severity: High

Vulnerable URL: uhttps://habigonjzilasamiti.ssbmultiservices.com/sql/laravel-habiganj.sql

POC:

```
INSERT INTO `users` (`id', `name', `image', `email', `email_verified_at', `password', `remember_token', `created_at', `updated_at') VALUES (1, 'Giash Ahmed', NULL, 'giashahmed123@gma11.com', '2020-12-21 06:51:04', '$2b$10$RwWJM5mJwvvxdfgz0ms430B7n67C4bVV1mcIOHG6er wCwBgDPjTPm', NULL, '2020-12-21 06:51:04', '2020-12-21 06:51:04'), (2, 'Bijoytech', 'upload/admin-image/img_1608973166_5fe6fb6ee289d.jpg', 'info@gmail.com', '2020-12-21 06:51:04', '$2y$10$ycns9Ffqp.4C05xYNmvge0zZsD5M1Bl.8qxwDI3iNcZ4eijUGy.e.', 'ZTFqdYZgQMfM2Jye9hIOFRy9ErF8R096yQLaDrJgSE50uhNztR69GvidOUgz', '2020-12-21 06:51:04', '2020-12-26 02:59:26');
```

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).