Website name

http://pos.ssbmultiservices.com/

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

Vulnerable URL: http://pos.ssbmultiservices.com/

CVSS: Base Score: 5.8

POC:False positive
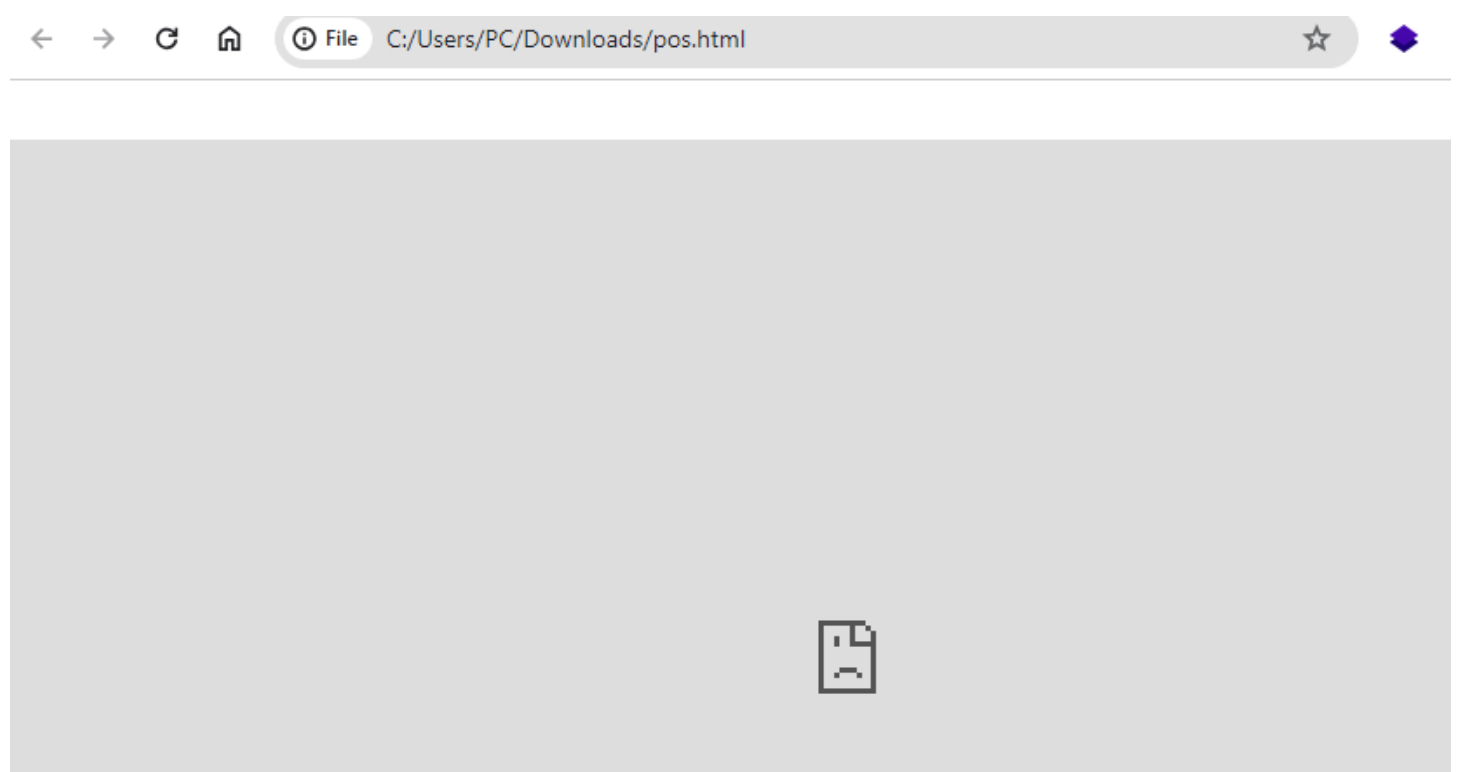
2.Vulnerability name: Cross site scripting

(Vulnerable JavaScript libraries)

Vulnerable URL :   http://pos.ssbmultiservices.com/

POC: False Positive

Pretty | Raw | Hex

```
1  GET /<img src="http://google.com/photo.jpg"
   onerror="console.log(this)" /> HTTP/1.1
2  Host: pos.ssbmultiservices.com
3  User-Agent: Mozilla/5.0 (Windows NT 10.0;
   Win64; x64; rv:122.0) Gecko/20100101
   Firefox/122.0
4  Accept:
   text/html,application/xhtml+xml,application/xml
   ;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Connection: close
8  Cookie: XSRF-TOKEN=
   eyJpdiI6Ik80Yz13Y1h1XC9U0D15T1dTY1wvMD1NQTO9Iiw
   idmFsdWUi0iJ1N1QwU1puU2FrdWF10G1WMHVh0UVGZjNWTO
   VoWnU5NE45WnB4emRj0Ew2K3AzdURMMXd2cDNj0TFYaFQ3U
   kFEIiwibWFjIjoi0DE2MThmMD1iY2E4MGU2MjE3YjMwZGI5
   NjQ1NTJkZTc2NWQ0MDk5MTQxN2RhNGE4MDUwMTM4Y2IyNjE
   1YWUv0SJ9; upos session=
```

Pretty | Raw | Hex | Render

```
1  HTTP/1.1 400 Bad Request
2  Date: Fri, 09 Feb 2024 03:27:01 GMT
3  Server: Apache
4  Upgrade: h2,h2c
5  Connection: Upgrade, close
6  Accept-Ranges: bytes
7  Cache-Control: no-cache, no-store,
   must-revalidate
8  Pragma: no-cache
9  Expires: 0
10 Content-Type: text/html
11
12
13
14
15 <!DOCTYPE html>
16 <html>
17   <head>
18     <meta http-equiv="Content-type" content="
```