Website name

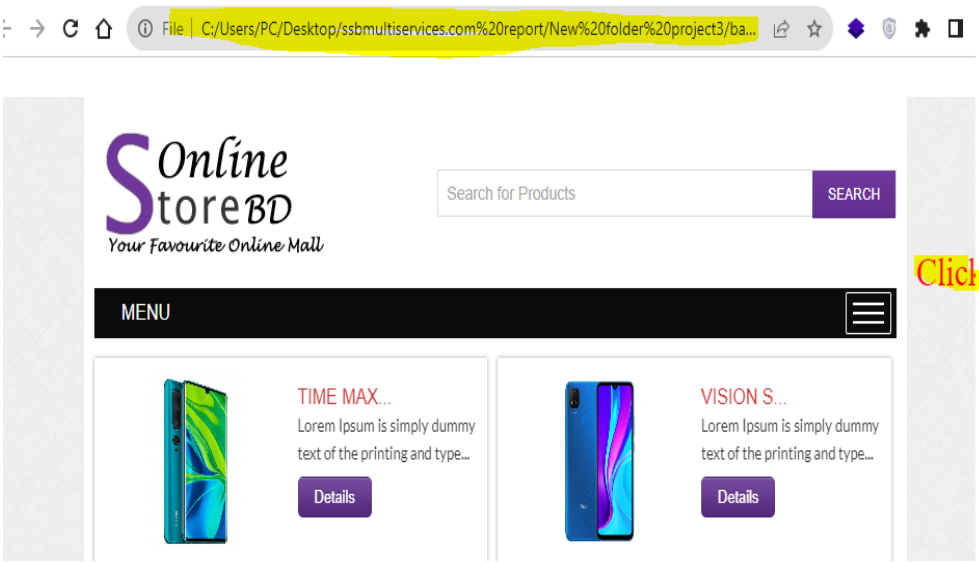
https://banglamobile.ssbmultiservices.com/

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

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

CVSS: Base Score: 5.8

POC:



HTML File:

iframe{

width: 100%;

height: 600px;

border: none;

}

</style>

<title>Clickjacking PoC</title>

</head>

<body >

clickjacking

<iframe sandbox="allow-modals allow-popups allow-forms allow-same-origin allow-scripts"

style="opacity:1" src=" https://banglamobile.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

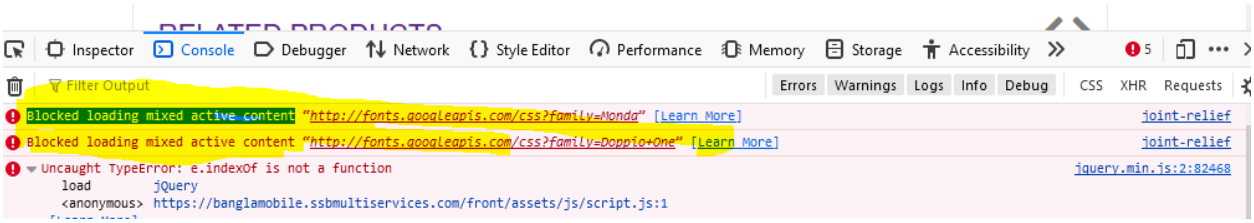
directive. Consult Web references for more information about the possible values for this header.

2.Vulnerability name: Active Mixed Content over HTTPS

Vulnerable URL: https://banglamobile.ssbmultiservices.com/product/view/joint-relief

Severity : Medium

POC:



Impact:

A man-in-the-middle attacker can intercept the request for the HTTP content and also rewrite the response to include malicious codes. Malicious active content can steal the user's credentials, acquire sensitive data about the user, or attempt to install malware on the user's system (by leveraging vulnerabilities in the browser or its plugins, for example), and therefore the connection is not safeguarded anymore.

Recommendation:

There are two technologies to defense against the mixed content issues: - HTTP Strict Transport Security (HSTS) is a mechanism that enforces secure resource retrieval, even in the face of user mistakes (attempting to access your web site on port 80) and implementation errors (your developers place an insecure link into a secure page) - Content Security Policy (CSP) can be used to block insecure resource retrieval from third-party web sites – Last but not least, you can use "protocol relative URLs" to have the user's browser automatically choose HTTP or HTTPS as appropriate, depending on which protocol the user is connected with. For example: A protocol relative URL to load an style would look like >link rel="stylesheet" href="//example.com/style.css"/<. Same for scripts >script type="text/javascript" src="//example.com/code.js"<>/script< The browser will automatically add either "http:" or "https:" to the start of the URL, whichever is appropriate.

References

MDN: Mixed Content

1. https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content

What is mixed content?

2.https://web.dev/what-is-mixed-content/

Fixing mixed content

3.https://web.dev/fixing-mixed-content/

3.Vulnerability name: Development configuration files

POC: False Positive