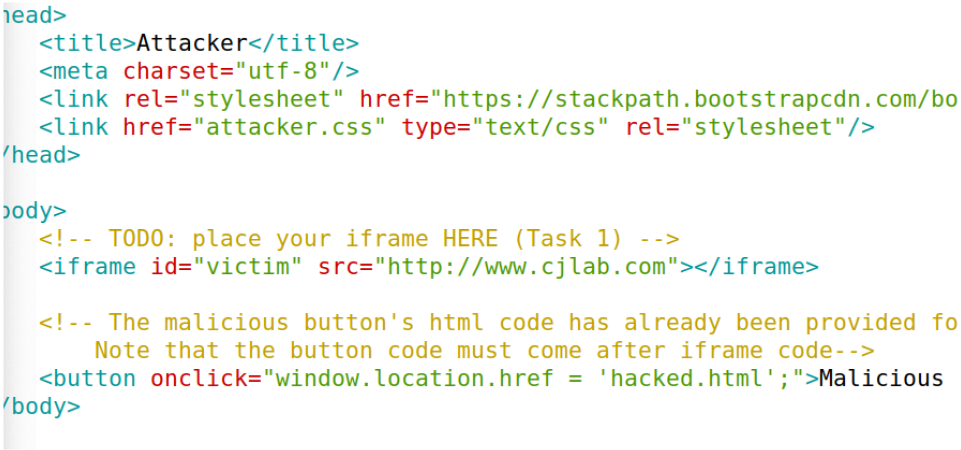
Click-Jacking

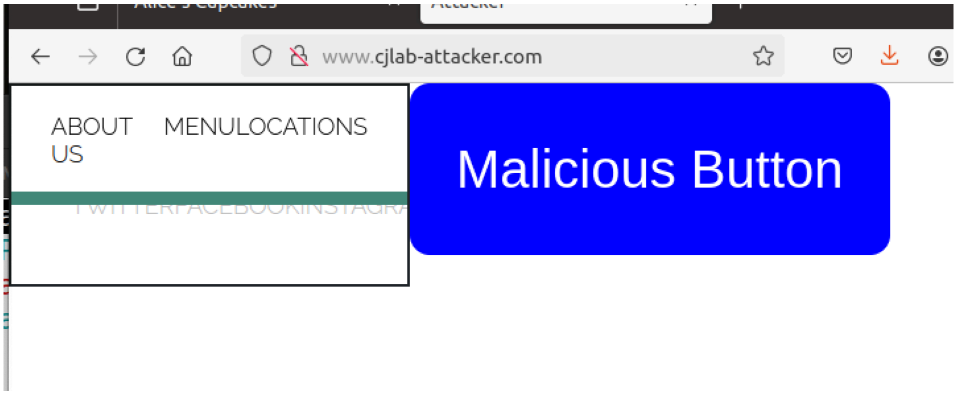
Task 1; Copy That Site!

To start I included an iframe named victim where I included the defender website as the source;

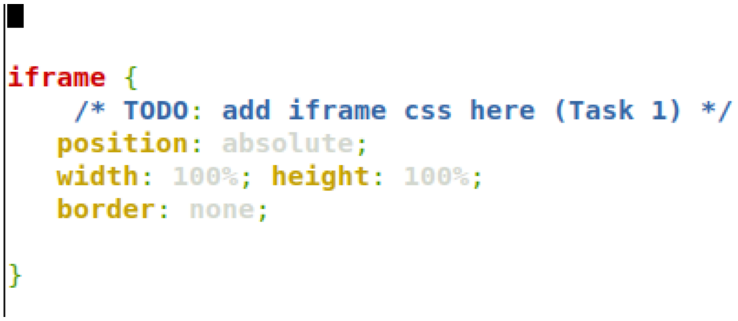


```
ead>
   <title>Attacker</title>
   <meta charset="utf-8"/>
   <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bo
   <link href="attacker.css" type="text/css" rel="stylesheet"/>
/head>

ody>
   <!-- TODO: place your iframe HERE (Task 1) -->
   <iframe id="victim" src="http://www.cjlab.com"></iframe>

   <!-- The malicious button's html code has already been provided fo
       Note that the button code must come after iframe code-->
   <button onclick="window.location.href = 'hacked.html';">Malicious
/body>
```

The website is in a tiny box next to my button so I need to fill the website to the full page;

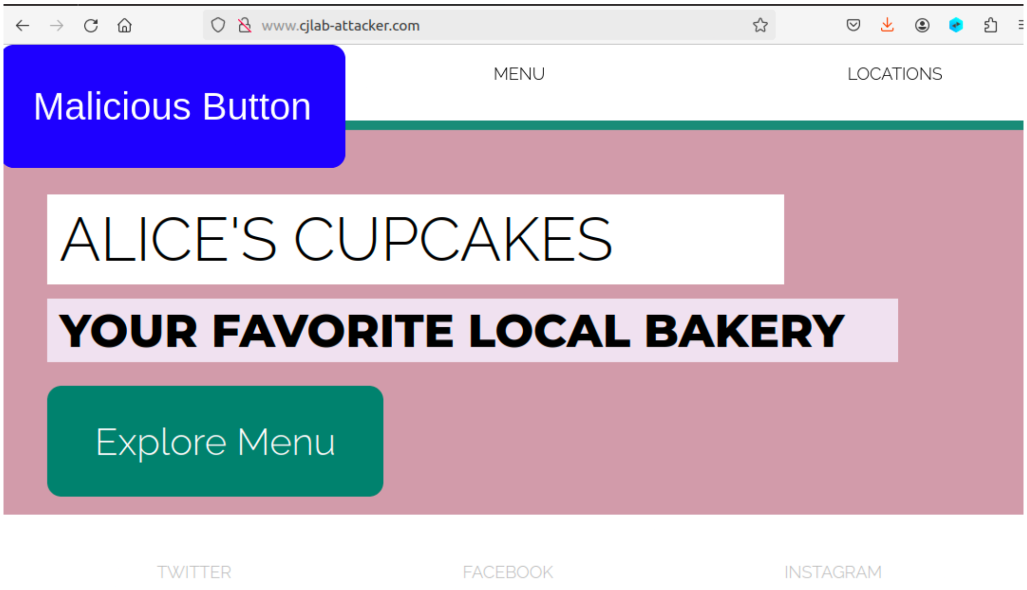


We must use absolute because if we don't the button won't overlay on the page correctly;



```
iframe {
     /* TODO: add iframe css here (Task 1) */
   position: absolute;
   width: 100%; height: 100%;
   border: none;

}
```

Now we have a button overlaying the defenders website;



Questions:

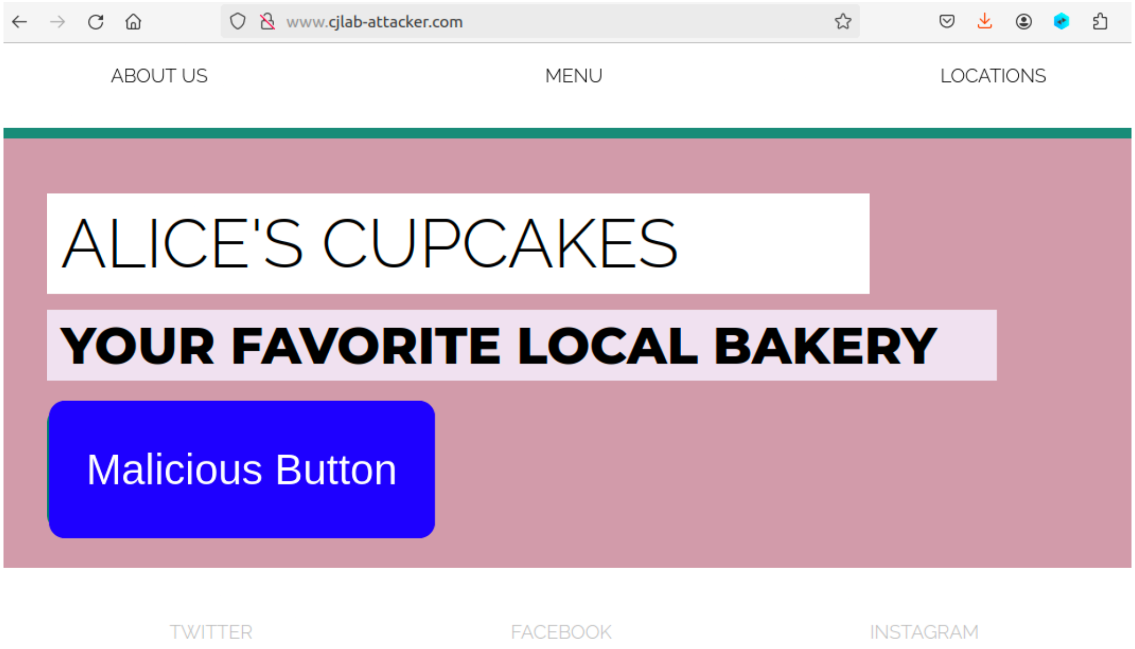
- **When the Iframe is inserted we can see the website place a box with the entire webpage crammed into it. When we expand the box we can see the page with all working buttons, headers and footers.**

Task 2; Let's Get Clickjacking!

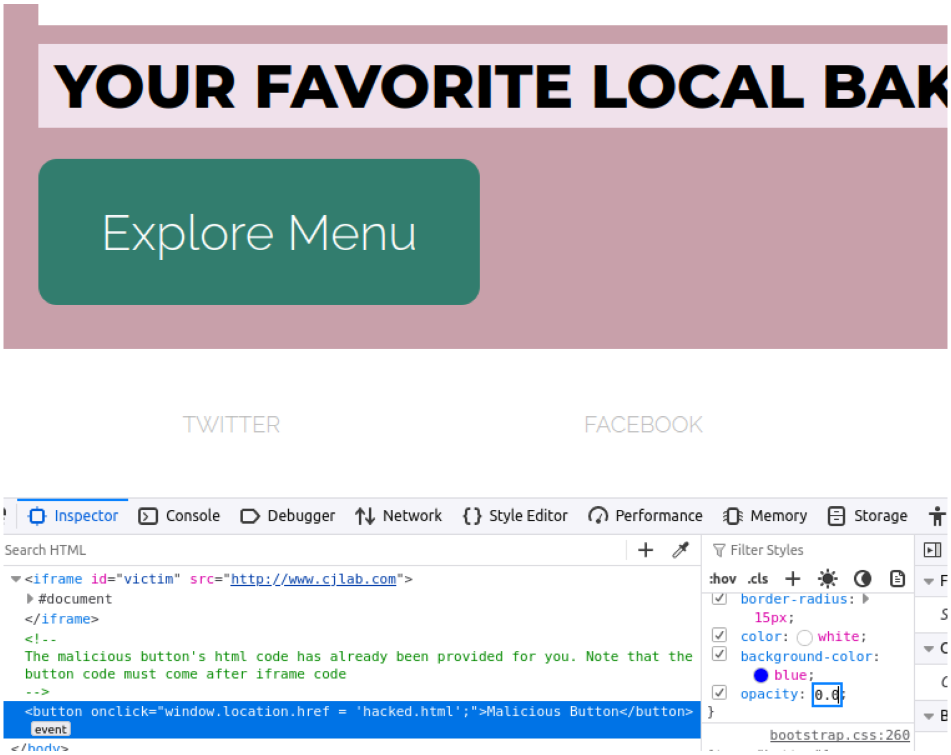
First, we need to position the button so it is fully overlaying the explore menu button;

```
button{
    /* Given button code for size and shape. You do not need to edit this. */
    position: absolute; top: 338px; left: 52px;
    border: none;
    color: white;
    padding: 35px 35px;
    text-align: center;
    font-size: 40px;
    border-radius: 15px;
    /* end of given button code */
```

We can see the big blue malicious button is where the explore menu button should be;



Let’s make the button transparent using the opacity attribute to make it invisible (Done through the web inspector;



```
<iframe id="victim" src="http://www.cjlab.com">
  #document
</iframe>
<!--
The malicious button's html code has already been provided for you. Note that the
button code must come after iframe code
-->
<button onclick="window.location.href = 'hacked.html';">Malicious Button</button>
 event
</body>
```

```
border-radius:
  15px;
color: white;
background-color:
  blue;
opacity: 0.0;
}
bootstrap.css:260
```

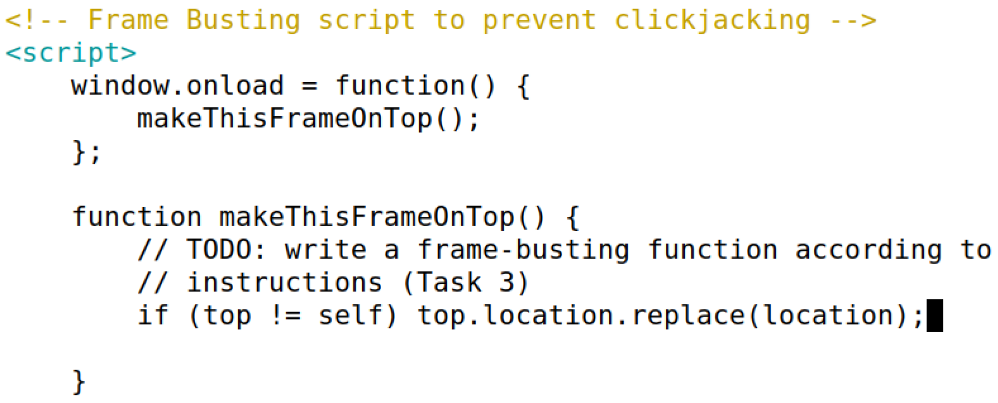
Questions:

- **The attacker site looks identical to the victim website however there is an invisible button sitting on top of the explore menu.**

- **When you click the explore menu button you get taken to the 'YOU GOT HACKED' page.**
- **If I am trying to like someone's profile post and it makes me like someone else's instead.**

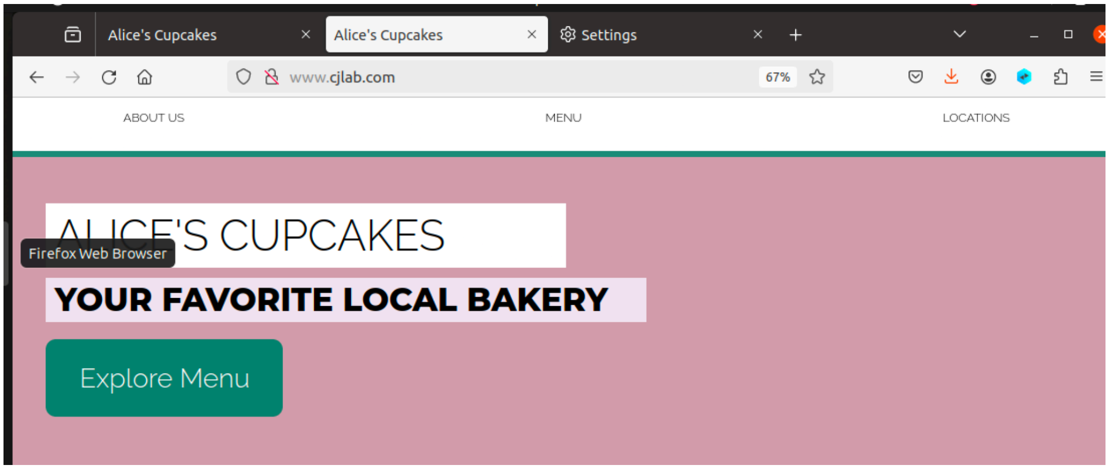
Task 3; Bust that Frame!

To do this we need javascript code that will check that it's self page is on the top if it isn't, make it;



```
<!-- Frame Busting script to prevent clickjacking -->
<script>
    window.onload = function() {
        makeThisFrameOnTop();
    };

    function makeThisFrameOnTop() {
        // TODO: write a frame-busting function according to
        // instructions (Task 3)
        if (top != self) top.location.replace(location);

    }
```

Now when we try to access the attackers website, it will force redirect us to the defenders actual website;

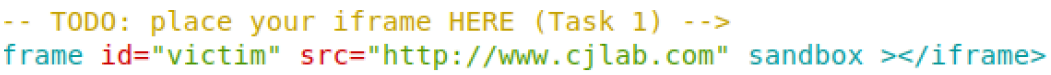


Questions:

- **With the new javascript addition when we visit the attacker website, we get redirected to the defenders legitimate page;**
- **When I click the button now nothing happens just like on the normal defenders page.**

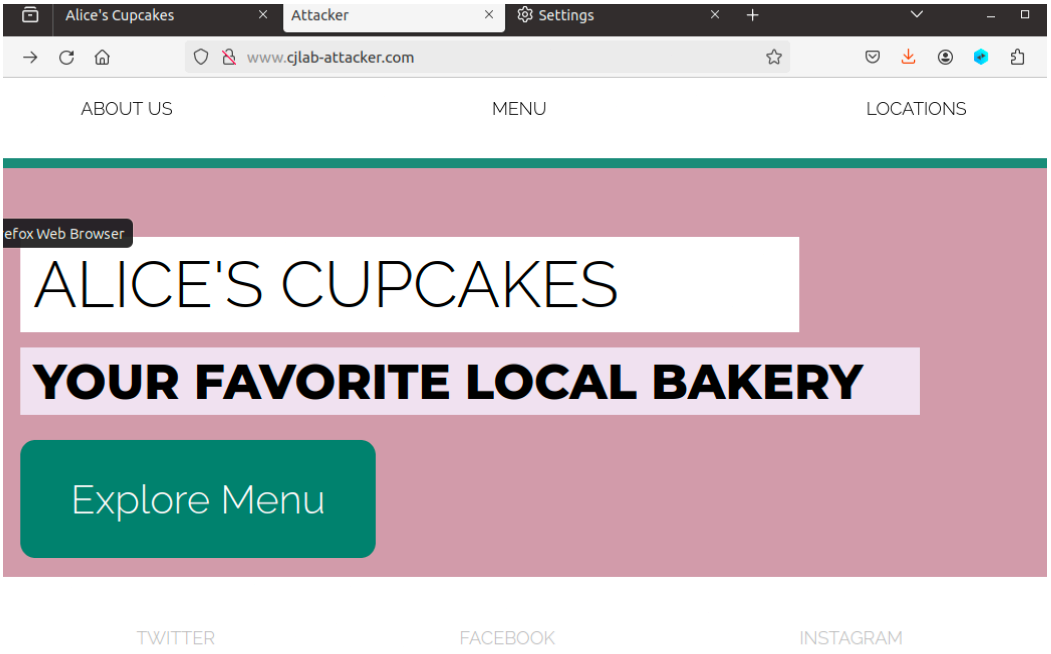
Task 4; Attacker Countermeasure (Bust the Buster)

We can bypass this simple countermeasure by using the sandbox attribute;

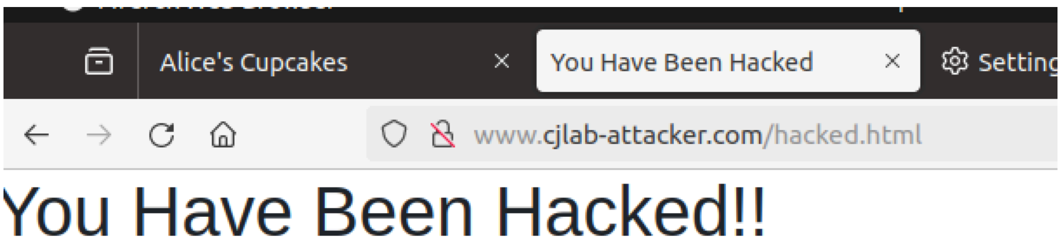


```
-- TODO: place your iframe HERE (Task 1) -->
frame id="victim" src="http://www.cjlab.com" sandbox ></iframe>
```

Now we are in the clear again and are clickjacking as we were in the beginning;



With the button still working;

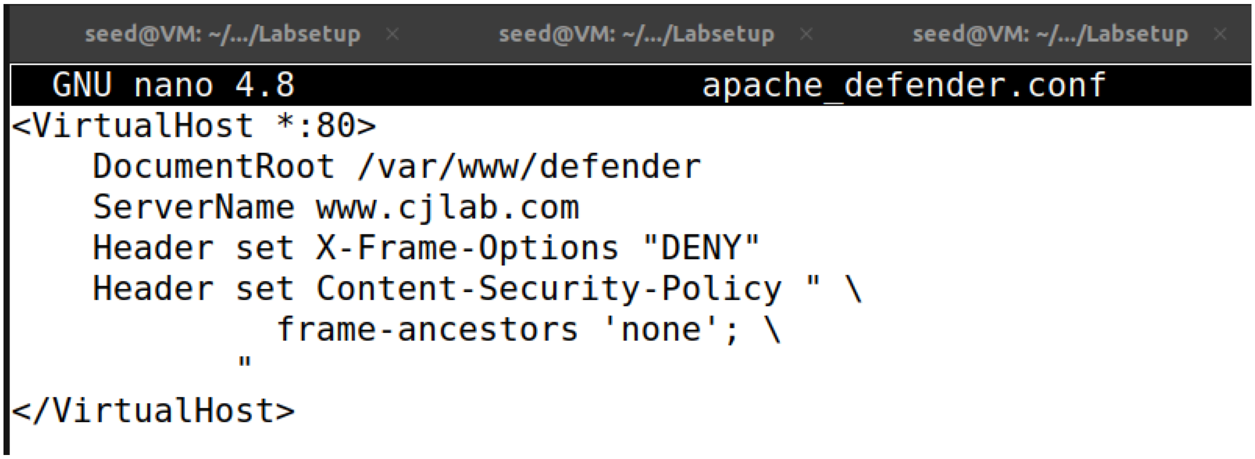


Questions:

- **The Sandbox attribute controls the restrictions applied to the attributes in iframes.**
- **The attacker website no longer redirects back to the defenders website and we have full control again.**
- **The button works again once the sandbox attribute is set as it can bypass the buster;**

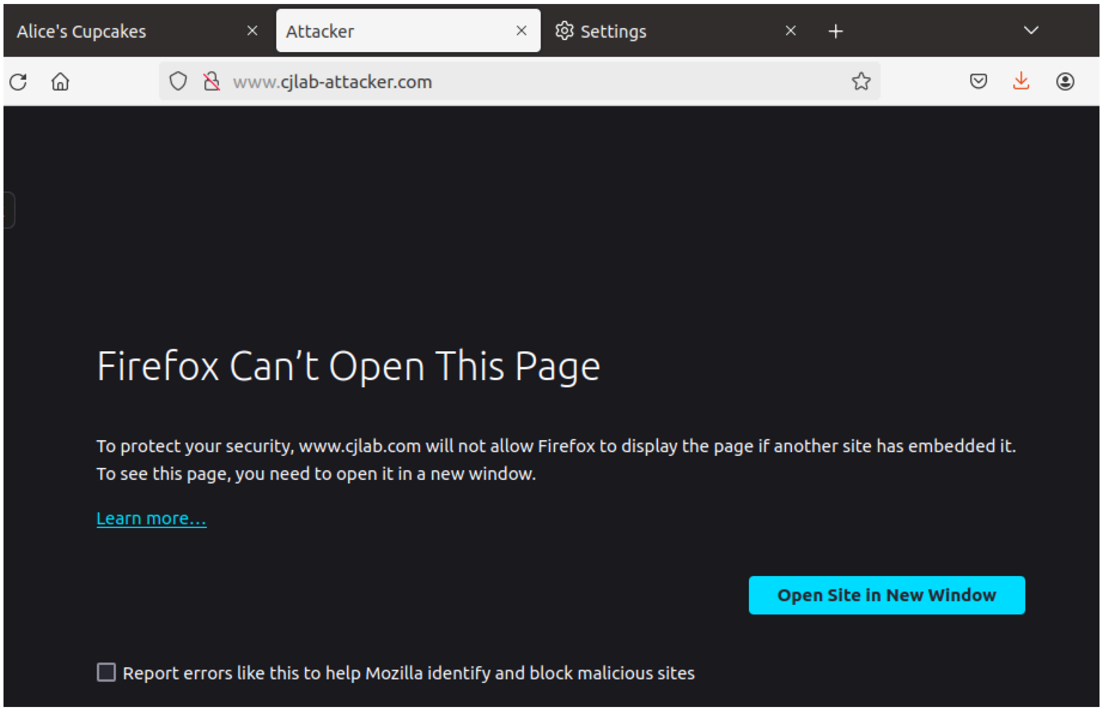
Task 5; The Ultimate Bust

To finish this back and forth we can set the html header on every page to deny anyone else from embedding our website;



```
<VirtualHost *:80>
    DocumentRoot /var/www/defender
    ServerName www.cjlab.com
    Header set X-Frame-Options "DENY"
    Header set Content-Security-Policy " \
             frame-ancestors 'none'; \
           "
</VirtualHost>
```

Now when we try to access the attacker website we get this error through the browser;



Firefox Can’t Open This Page

To protect your security, www.cjlab.com will not allow Firefox to display the page if another site has embedded it. To see this page, you need to open it in a new window.

Learn more…

□ Report errors like this to help Mozilla identify and block malicious sites

Questions:

- **The X-Frame-Options HTTP Header is a setting that tells the browser who can make frames out of its page. Setting it to none means that no one can use it.**
- **Content-Security-Policy . It is set to none because the back-end server needs to defend against clickjacking, because the attacker can beat any front-end attempts on their side.**
- **The button does not pop up, not even giving us a chance to see if we can do the attack still**