Part 1 (click jacking)

W5.1. Please describe two common approaches used by clickjacking attacks?

ANS => {

THE TWO COMMON APPROACH ARE **IFRAME AND POSITIONING.**

}

W5.2. Please answer these questions based on the following HTML page:

1. Which iframe is on top of which one is on the bottom
   Ans => {
   The attackers button should be on top and invisible while the actual iframe is on the bottom.
   }
2. If we click on the page, where does click go?
   ANS => {
   To the hack page with a text saying you have been hacked.
   }
3. Please decide the opacity value for X and Y for a typical clickjacking attack.
   ANS => {
   The opacity value should be “0” this is to make the iframe invisible to the user.
   }

   ……

4. Please construct two iframes, such that one of the iframes seems to be part of the page in another iframe. Please then describe how this setup can be used in clickjacking attacks
   ANS => {

   <iframe src=”http://localhost:3000 ”, style=”width: 100%; height: 100vh;” />

   <iframe src=”http://hack.com”, style=”width: 100%; height: 100vh; opacity: 0; position: absolute; top: 0; left: 0” />

First, I went to website I want to iframe, and click on [ctrl + u] to view the source code. I Then copied all the source code including their css for styling so I can get the exact position of every button and write my own actions for every click. As you can see http://hack.com is my own iframe hackpage. With my embedded code. With my setup, I will be able to fool the user in clicking on any where on the page and my attack will be successful. I'll later disable right click and every keys on the page so other developers can't view the source code to identify if it's an iframe. ^_^.

}

5.4 The followings are the responses from a web server www.example32.com. Each of these responses is placed inside an iframe. (1) If the host page of these iframes come from www.example32.com, which of the following pages can be displayed? (2) If the host page come from www.example99.com, which of the following pages can be displayed?

ANS => {

Page 1. Why because it accept from all origin… Content-Security-Policy: frame-ancestors *

}

5.5 What is the common idea behind the X-Frame-Options and CSP mechanisms? Why is it effective in defeating the Clickjacking attack?

ANS => {

The main idea behind x-frame-opts, is to stop the page from loading in another wesbte. Why is it use to defeat clickjacking, It's because it disable viewing the website to the client side.

}

5.6 When a host page puts a page inside an iframe, can the host page access the content inside the iframed page?

Ans => {

No! the host only has control over their own page.

}

5.7 . The following JavaScript code displays content inside a page. The content comes from an untrusted place. If the content, which is supposed to be data only, contains JavaScript code, can the code be executed? Why?

Ans => {

No! Because of sandbox

}

CLICK-JACKING-SEED-LAB