Clickjacking Attacks

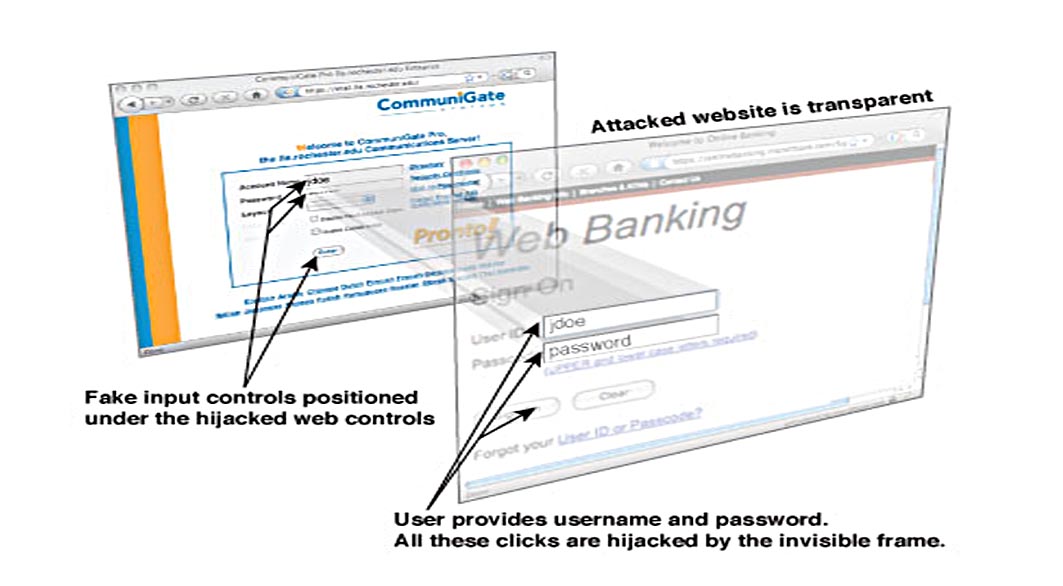
|  |
| --- |
| Copyrights 2016-2017 Frank Xu, Bowie State University.  The lab manual is developed for teaching cyber-related courses. Comments and suggestions can be sent to wxu@bowiestate.edu |

**Introduction**

Clickjacking, also known as a "UI redress attack", is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

The Clickjacking attack allows to perform an action on victim site on visitor’s behalf. Many sites were hacked this way, including Twitter and Facebook (both fixed).



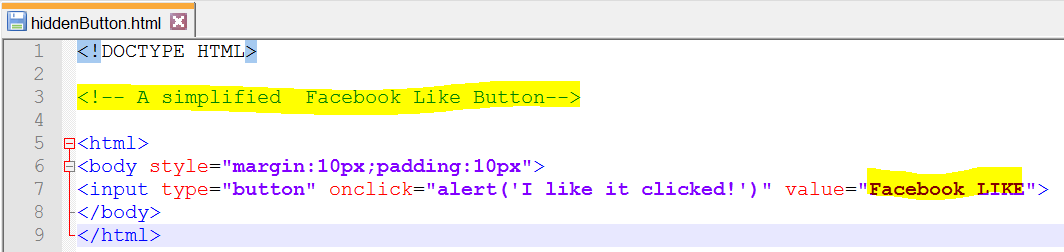
**Lab Environment**

We have created two accounts in the VM. The usernames and passwords are listed in the following:

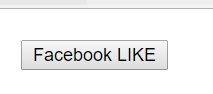
* + User ID: root, Password: *seedubuntu*.
  + Note: Ubuntu does not allow root to login directly from the login window. You have to login as a normal user, and then use the command **su** to login to the root account.
  + User ID: seed, Password: *dees*

**Task 1: Lure Users to Click** Image result for facebook like button **on Facebook**

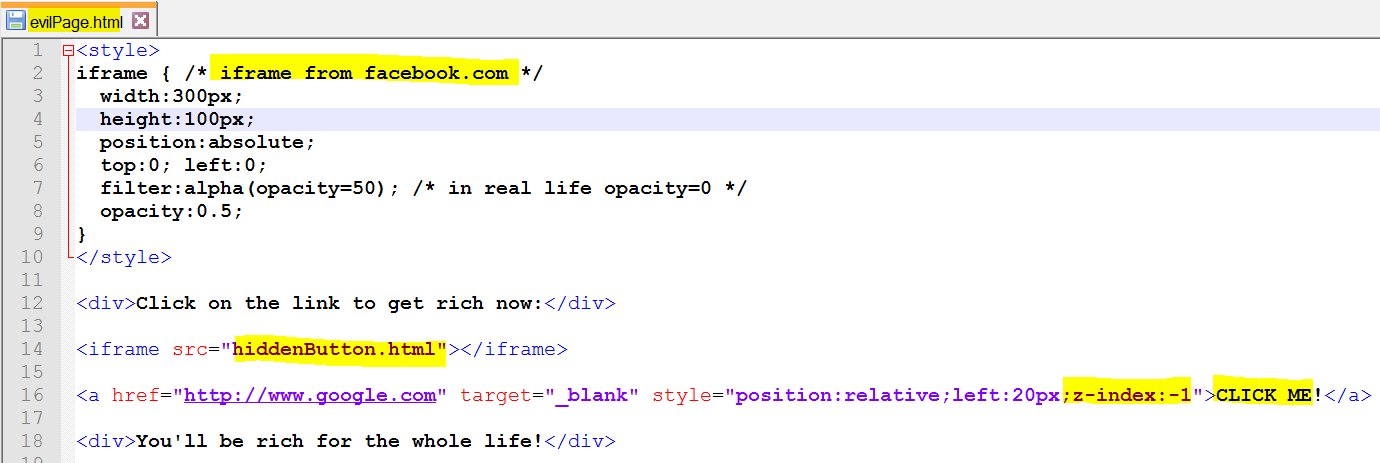
1. Goal: You have posted a message on your Facebook, and you want other people to click the Image result for facebook like button button.
   1. A visitor is lured to the evil page. No matter how. “Click to get 1000000$” or whatever.
   2. The evil page puts a “get rich now” link with z-index=-1.
   3. The evil page includes a transparent iframe from the victim domain, say facebook.com and positions it so that “I like it” button is right over the link.
2. Create a button on a page. The button is linked to your Facebook Image result for facebook like button button. For the purpose of the demonstration, the button only pops an alert message. You can link the button to a real Facebook Image result for facebook like button button.
   1. Source code



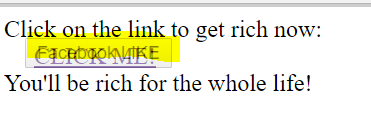
* 1. Webpage



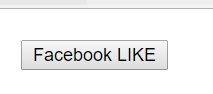
1. Create an evil page
   1. “I like it” button is right over the link

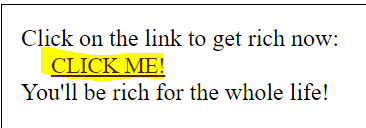


* 1. Webpage. Note that for the demonstration purpose; you will see the link CLICK ME on the top of the button.



* 1. If the visitor is logged into Facebook (and most of time he is), then facebook.com receives the click on behalf of the visitor.

1. Question.
   1. Make the button  transparent completely like the figure below.
   2. Use the transparent iframe

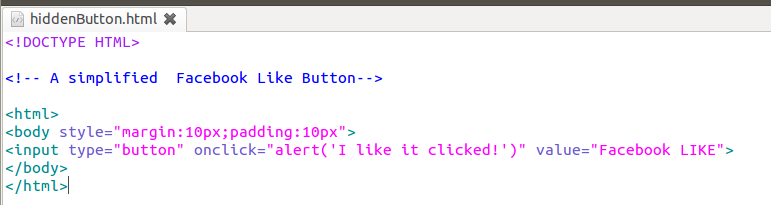


**Task 2: Countermeasure**

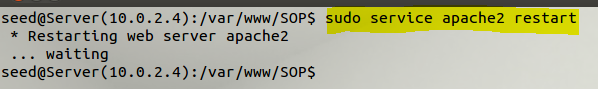
We are going to use Apache web server to demonstrate the countermeasure of the Clickjacking.

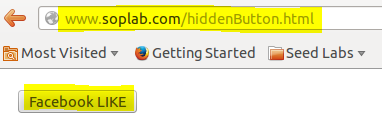
1. Create a web page with a button. The button is linked to a Facebook like button.



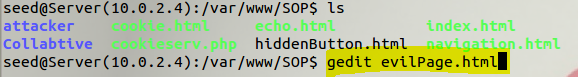


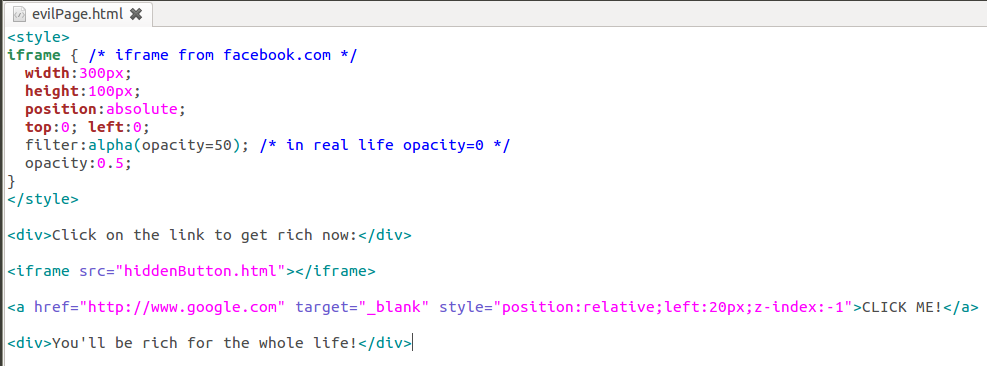
1. Test the button. You need to start the Apache server first.



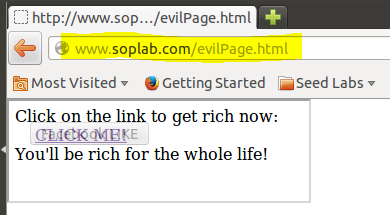


1. Create an evil web page.

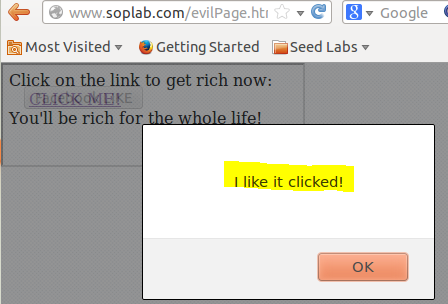




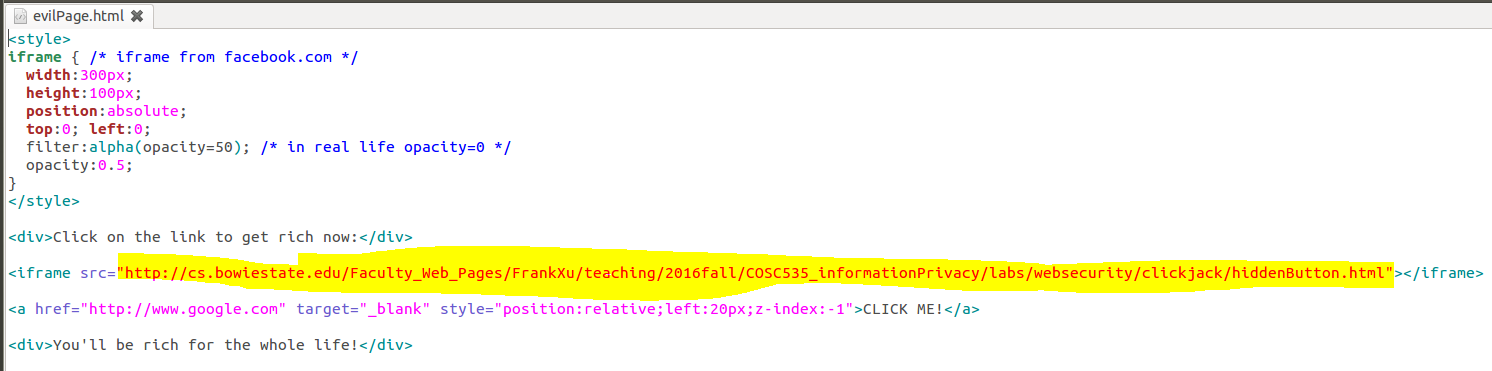
1. The evil page puts the CLICK ME! link to the top of the hidden button



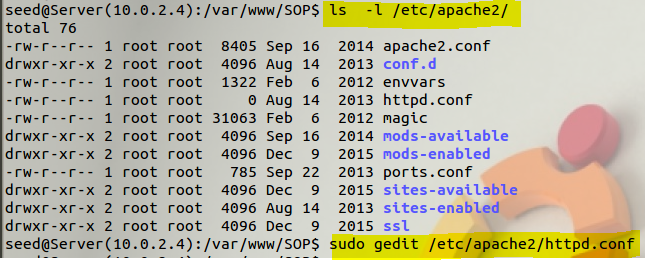
1. You click the link, but **Like** button has been clicked.



1. Question. If you change the link to the follows (see the highlighted link), will the evil page hijack users’ clicks? Why?

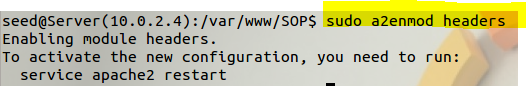


1. Change the web configuration file
   1. Edit httpd.conf





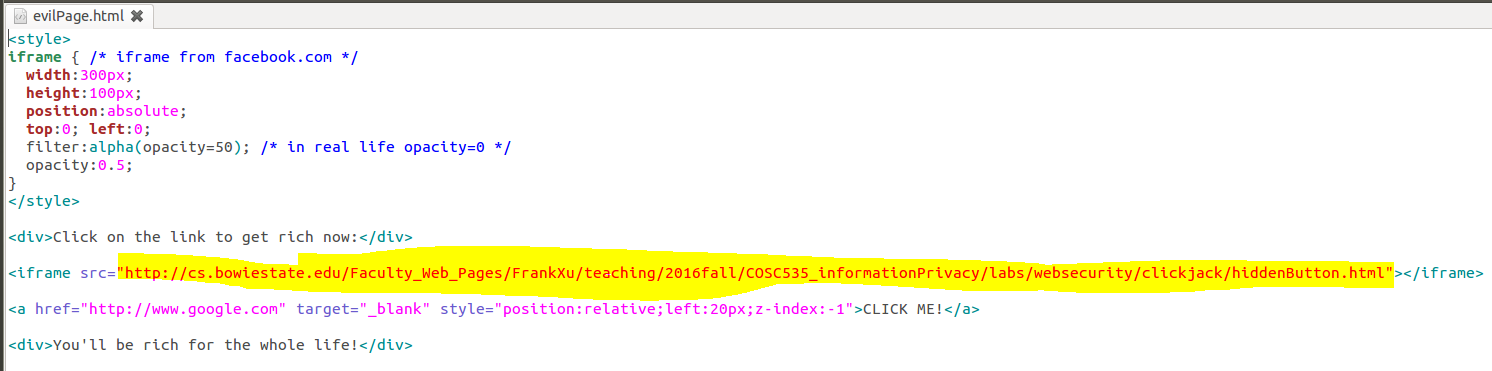
* 1. Install headers module from apache2



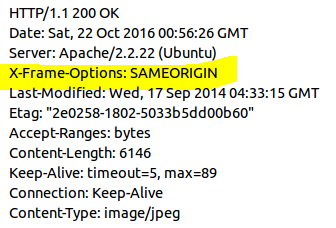
* 1. Restart the apache server



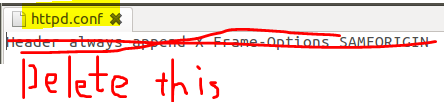
1. Question.
   1. Will the evil page hijack users’ clicks using the following evilPage.html? Why?



* 1. Use Live HTTP Header, can you find the highlighted statement? Why?



1. Change the web configuration file back to original file after you complete the lab. Otherwise, you may encounter problem when you work on other labs



Reference:

* <http://javascript.info/tutorial/clickjacking>
* <https://www.owasp.org/index.php/Clickjacking>
* https://developers.facebook.com/docs/plugins/like-button