**Title:** Click Jacking Getting FB Likes from Website visitors

**Abstract:**

With the growth of information technology, World Wide Web is experiencing a rapid increase in online social networks' users. A serious threat to the integrity of these users' data which has come into picture these days is Clickjacking. Many server side and client side defense mechanisms are available for clickjacking but many attackers are still exploiting popular online social networks like Facebook and twitter so that a user clicks on a spam link and it leads to unwanted posts flooding on his Facebook wall. We have implemented a clickjacking script on our website that runs automatically when the website is loaded. When the user clicks anywhere on the body part of our website his click is hijacked and he actually likes our Facebook page.

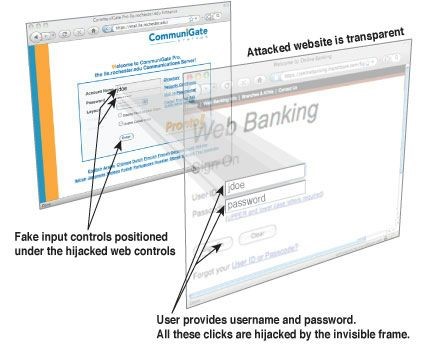
**Introduction:**

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.

A Clickjacking attack uses seemingly innocuous features of HTML and JavaScript to force the victim to perform undesired actions, such as clicking on a button that appears to perform another operation. This is a "client side" security issue that affects a variety of browsers and platforms.

To carry out this type of technique the attacker has to create a seemingly harmless web page that loads the target application through the use of an iframe (suitably concealed through the use of CSS code). Once this is done, the attacker could induce the victim to interact with his fictitious web page by other means (like for example social engineering). Like others attacks, and usual prerequisite is that the victim is authenticated against the attacker's target website.



Once the victim is surfing on the fictitious web page, he thinks that he is interacting with the visible user interface, but effectively he is performing actions on the hidden page. Since the hidden page is an authentic page, the attacker can deceive users into performing actions which they never intended to perform through an "ad hoc" positioning of the elements in the web page.

**Implementation details:**

Click jacking is an attack that tricks a web user into clicking a button, a link or a picture, etc. that the web user didn’t intend to click, typically by overlaying the web page with an iframe. This malicious technique can potentially expose confidential information or, less commonly, take control of the user’s computer. For example, on Facebook, a click jack can lead to an unauthorized user spamming your entire network of friends from your account.

We’ve known about clickjacking, also called “UI redress attacks,” for years now, as they were originally described in 2008 by Robert Hansen and Jeremiah Grossman. There are countermeasures that websites can implement to protect against clickjacking attacks, such as frame busters, the X­ Frame Option and some client side plug­ins that can be installed in the browser. However, recent studies have shown that web sites may not be taking this vulnerability seriously – or at least they aren’t attempting to protect their web sites from clickjacking.

**So Why Aren’t Web Sites Taking Measures to Protect Against Clickjacking?**

There could be many answers to this question, but I think three main factors contribute to ignorance of clickjacking vulnerabilities in web sites.

1. **Clickjacking is not considered a serious issue because it is hard to manipulate**​ ​.

I believe this is the most common reason. Some web developers consider clickjacking lower risk since it is harder to get sensitive information from an end-user, as compared with other attacks like XSS and SQL injection. However, the clickjacking attacks on Facebook in 2010 showed that harm is done even by sending spam to everyone in your address book. Also, when a web site is vulnerable to clickjacking, it is possible for the attacker to disable cross site request forgery (CSRF) token protection, which protects against CSRF attacks that trick browsers into doing things without the user’s knowledge or permission.

1. **Countermeasures for click jacking are not reliable**​ ​.

Many countermeasures have been described that help web users protect against clickjacking attacks. But currently the only way that could completely prevent clickjacking attacks is to use a web browser like Lynx, a pure text based web browser that doesn’t support JavaScript. Not only is Lynx outdated, but it's hard to imagine a modern website user experience without the use of JavaScript. According to Robert Hansen, one of the first people to discover this vulnerability, “the combination of Firefox and No Script, an extension that blocks JavaScript, Flash and Java content, would keep you safe from ‘a very good chunk of issues, 99.99% at this point’.” But again, the trade­off is a diminished user experience because JavaScript is blocked.

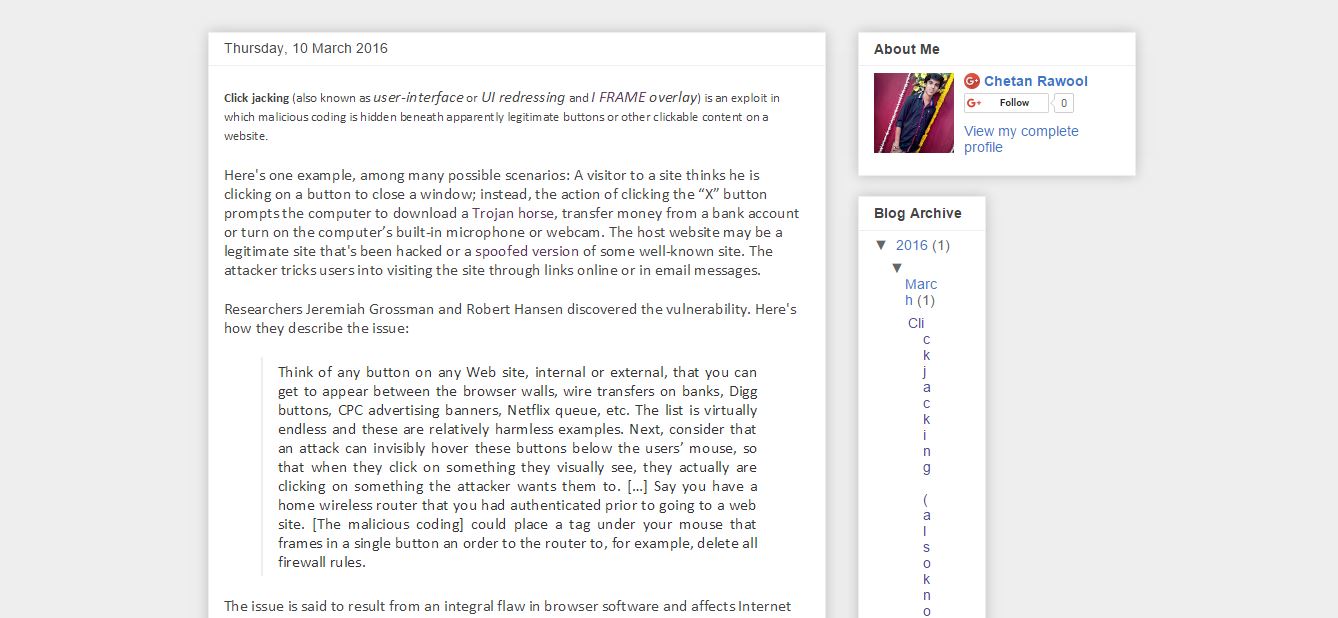
1. **Lack of awareness**​

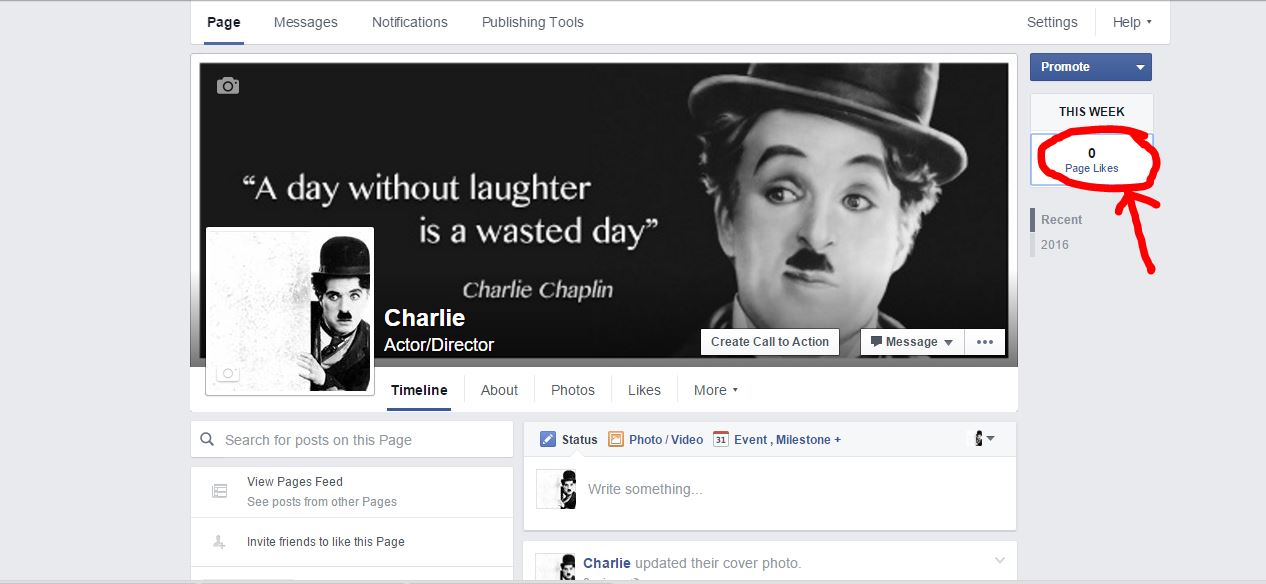
Because clickjacking is a relatively new malicious technique, the damage caused by this vulnerability is not widely known.

**Methodology:**

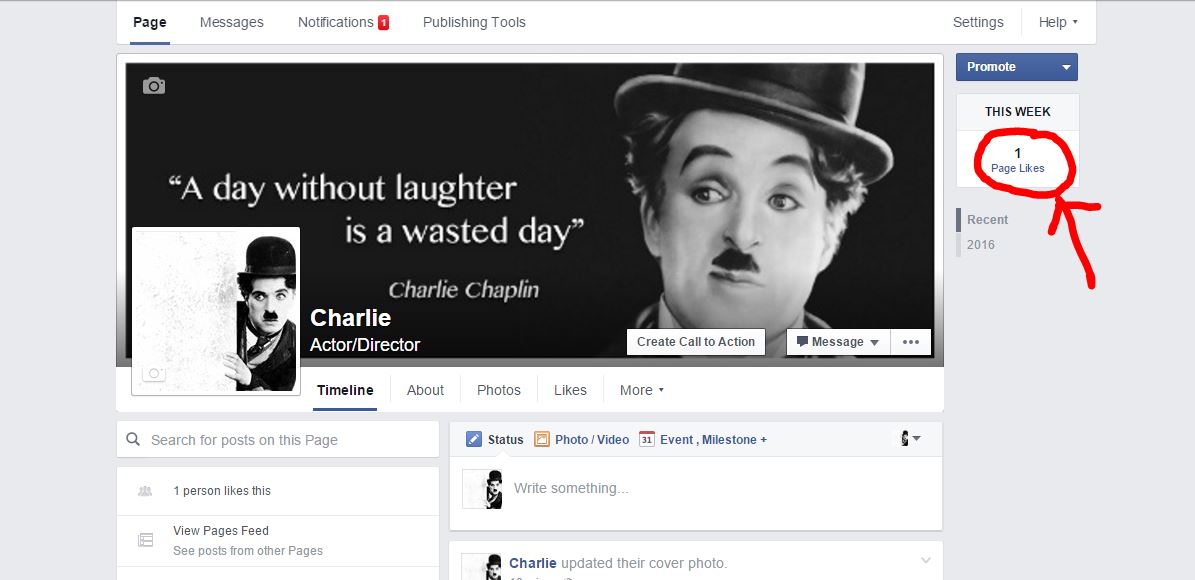
Simple scripts are written to implement clickjacking. The like button code from API of Facebook is taken. The like button is hidden by making its opacity 0 using CSS. HTML and JavaScript is used to configure the movement of the like button wherever the cursor moves. Whenever the user clicks anywhere on the website he gives his Like on our FB page.

**Result:**

Our website, Visitor is completely unaware of the clickjacking script­

Before visiting our website, there is no like on our FB page­

After clicking anywhere on our website, the visitors automatically Likes our FB page­



**Conclusion:**

With the increased use of Information Systems in society, security is becoming more and more important for strategic and operational concerns. Particularly network security is of more immediate consideration for protecting the system externally and internally. Clickjacking can be used for destructive activities like transfer of money or stealing password of confidential accounts. There are some existing measures against Clickjacking that can be implemented to secure your website.

**References:**

1) OWASP Clickjacking­ ​https://www.owasp.org/index.php/Clickjacking

1. ​http://sniperhaxx.com/2014/09/clickjacking­script­tutorial­click­jacking.html
2. JavaScript based attacks: Exploiting Web 2.0 ISBN­ ​978­1­4673­4452­4