Cole Ramos

IST590-Instuctor Anastacia Webster

May 17, 2018

**Clickjacking**

Clickjacking is a malicious technique that invalids tricking the web user into interacting with a false or different web site. Many of these attacks can be used alone or in combination with hacker’s attacks. Sending unauthorized or false information while the victim is interacting with seemingly harmless web pages. A Clickjacking attack uses seemingly innocuous features of HTML and Javascript to force the victim to perform undesired actions, such as clicking a button that appears to perform another operation. This is a “client side” security issue that affects a variety of browsers and platforms. (OWASP)

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

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 they never intended to perform through an “ad hoc” positioning of the elements in the web page. (OWASP)

The power of this method is since the actions performed by the victim are originated from the authentic target web page (hidden but authentic). Consequently, some of the anti-CSRF protections, that are deployed by the developers to protect the web page from CSRF attacks, could be bypassed. (OWASP)

Depending on the clickjacking attack you have many ways to fix or correct the site vulnerabilities. Sending the proper Content Security Policy (CSP) frame-ancestors directive response headers that instruct the browser to not allow framing from other domains. (This replaces the older X-Frame-Options HTTP headers.) (OWASP)

In conclusion clickjacking is a form of attack that hackers use to convince users to click on a false site and began to hijack the user site and began to attack with malicious and propagated massively. One way to avoid these types of attacks is be caution about email or site that are offing free things or question everything you come a cross.

References

https://www.owasp.org/index.php/Clickjacking

https://www.owasp.org/index.php/Testing\_for\_Clickjacking\_(OTG-CLIENT-009)