Application Layer Attacking

Insufficient Transport Layer Protection Vulnerability

1 X-Frame-Options Header Not Set

Threat Description

Refers to a Frame set to prevent an attacker from tricking users to providing them with credentials such as passwords.Setting a server against allowing X-Frame headers protects it from clickjacking. Clickjacking is where an attacker uses an iframe similar to the original window which is used to trick a user that it is the legitimate site allowing the user to give credentials to another system without knowledge.

Exploitation

Clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact, they are clicking an invisible element in the additional page transposed on top of it.

The invisible page could be a malicious page or a legitimate page the user did not intend to visit – for example, a page on the user's banking site that authorizes the transfer of money.

Illustration

1.The attacker creates an attractive page which promises to give the user a free trip to Tahiti.

2. In the background the attacker checks if the user is logged into his banking site and if so, loads the screen that enables transfer of funds, using query parameters to insert the attacker's bank

3. The bank transfer page is displayed in an invisible iframe above the free gift page, with the "Confirm Transfer" button exactly aligned over the "Receive Gift" button visible to the user.

4. The user visits the page and clicks the "Book My Free Trip" button.

5. In reality, the user is clicking on the invisible iframe and has clicked the "Confirm Transfer"

6. The user is redirected to a page with information about the free gift (not knowing what happened in the background)

Damage Potential: Average

Failure to set the X-Frame Header results to clickjacking where an attacker creates a look-alike template to the real site where a user is tricked giving out details. Might lead to the user gaining unauthorized access to the system

Damage Risk: : Average

Business Impact: Average

16

Total Security Point

Unauthorized access could result in identity theft and fraud. Clickjacking results to the user providing credentials granting access to the system. The attacker is able to login to the system and carries out duties that a legitimate user would. This could cause the company loses or even their critical data stolen/exposed.

Counter Measures & Solution against Threat:

Set the server against X-Frames.

Steps to take

1. For apache got to the configuration file httpd.conf
2. Add the line Header always append X-Frame-Options DENY
3. Restart the server.