|  |  |
| --- | --- |
|  |  |
| IFRAME EXPLOIT |  |
|  |  |
|  | 3/7/2023Azlan Chenlong |
|  | HAI SING CATHOLICSCHOOL |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | EXPLOITIt appears that Mobile Guardian (Chromebook), the Device Manager Application (DMA) for most secondary schools, do not check the contents of the HTML element, iframe, which allows a website to display another website within it (E.g., embedding a YouTube video inside a website). This allows students to access any site they want through that iframe.  A demonstration of the exploit can be found [here](https://azlancoding.github.io/iframe-browser-pwa) with installation instructions [here](https://azlancoding.github.io/iframe-browser/InstallGuide) (Step 2 only). The password for the site is `BZssK37k`. Some sites like WhatsApp Web require extra instructions found [here](https://azlancoding.github.io/iframe-browser/whatsapp-and-others). And for WhatsApp Web, it may require you to sign out if it fails. The source code can also be found [here](https://github.com/AzlanCoding/iframe-browser-pwa). | |  |
|  | The exploit works by using two extensions to ignore “x-frame-headers” and “Content Security Policy” header as well as modifying the request header “Sec-Fetch-Dest” from ‘iframe’ to ‘document’.  The following is a patch that can be written to scan and check for iframes. Please add it to the main loop of Mobile Guardian’s service worker script (sw.js) or whatever script that runs in the background. | A screenshot of a computer  Description automatically generated |  |