



The OWASP Foundation

<http://www.owasp.org>

Clickjacking





The screenshot shows a web browser window with the following elements:

- Browser title: Evil Page
- Address bar: <http://evil.com>
- Search bar: Google
- Page content: A banner for "Super Fun Games - Play Now!" with a dice icon.
- Game icons: Pac-Man, a yellow star, a ghost, and a red and white mushroom.
- Buttons: "Start Game!" (pointed to by a red arrow) and "One Player" (pointed to by a red arrow).

First, make a tempting site



Evil Page

http://evil.com

Google

```
<style>iframe {  
width:300px;  
height:100px;  
position:absolute;  
top:0; left:0;  
filter:alpha(opacity=00)  
;  
opacity:0.0;  
></style>  
<iframe  
src="https://mail.google.com/mail/Trash?ui=2" >
```

mail™

Investment Bank Bootcamp - www.i

Archive Report spam Delete

Select: All, None, Read, Unread, Star

- ☆ American Airlines AAdvan.
- ☆ Facebook
- ☆ John Dennis
- ☆ iphonesdk+noreply
- ☆ me, Edward (6)

Trash

owasp

4 more ▾



Evil Page

http://evil.com

Google

Gmail™

by Google

[Compose Mail](#)

- Inbox**
- [Sent Mail](#)
- [Drafts](#)
- [Spam](#)
- [\[Gmail\]Trash](#)

[Investment Bank Bootcamp - www.i](#)

Archive Report spam Delete

Select: All, None, Read, Unread, St

- ☆ American Airlines AAdvan.
- ☆ Facebook
- ☆ John Dennis
- ☆ iphonesdk+noreply
- ☆ me, Edward (6)

iframe is invisible, but still clickable!

[4 more ▾](#)



X-Frame-Options HTTP Response Header

```
// to prevent all framing of this content  
response.setHeader( "X-FRAME-OPTIONS", "DENY" );
```

```
// to allow framing of this content only by this site  
response.setHeader( "X-FRAME-OPTIONS", "SAMEORIGIN" );
```

```
// to allow framing from a specific domain  
response.setHeader( "X-FRAME-OPTIONS", "ALLOW-FROM X" );
```



Legacy Browser Clickjacking Defense

```
<style id="antiCJ">body{display:none !
    important;}</style>
<script type="text/javascript">
    if (self === top) {
        var antiClickjack =
document.getElementById("antiCJ");
antiClickjack.parentNode.removeChild(antiClickjack)
    } else {
top.location = self.location;
    }
</script>
```