

Clickjacking Attack

CS392

iframe

- An inline frame can be defined with HTML tag **<iframe>**
- An inline frame is used to embed another document within the current HTML document.

Example

```
<!DOCTYPE html>
<html>
  <head>
    <title>HTML Iframes
  </title>
</head>
<body>
  <p>Document content goes here...</p>
  <iframe src = "https://www.iitp.ac.in" width = "1000" height = "500">
</iframe>
  <p>Document content also go here...</p>
</body>
</html>
```

Iframe example

Document content goes here...



भारतीय प्रौद्योगिकी संस्थान पटना
Indian Institute of Technology Patna

[Communication Directory](#)

[HOME](#) [THE INSTITUTE](#) [ADMISSION](#) [ACADEMICS](#) [DEPARTMENTS](#) [RESEARCH](#) [SERVICES AND AMENITIES](#) [STUDENTS](#) [CONTACT](#) [INCUBATION C](#)



[International Relation \(IR\) Website](#) [5th International Conference on Data Science and Engineering \(ICDSE 2019\)](#)

[ouncement : M.Tech, Ph.D. \(including Visvesvaraya scheme\) and M.Tech by Research admission July 2019](#) [Addendum to the Visvesvaraya Ph.D. advertis](#)

Director, IIT Patna

- Director's Message
- Director's Profile
- Directorate
- Photo Gallery



News

- Short Term CEP Course on Effective Communication and Presentation Skills (21st-24th May 2019)
- Short Term CEP Course on Principles and Practices in Social Research (22nd - 25th July 2019)

Notice Board

- Prime Minister's Research Fellowship
- Scheme for implementing the reservation for EWS (July 2019 admission)

Document content goes here...

Clickjacking (UI Redressing)

- Attacker overlays multiple transparent or opaque frames to trick a user into clicking on a button or link on another page



- Clicks meant for the visible page are hijacked and routed to another, invisible page

Clickjacking

- Summer 2010: **Facebook** worm superimposes an invisible iframe over the entire page that links back to the victim's Facebook page
 - If victim is logged in, automatically recommends link to new friends as soon as the page is clicked on
- Many clickjacking attacks against **Twitter**
 - Users send out tweets against their will

Clickjacking Meets Spamming

BBC News - Facebook sues x

www.bbc.co.uk/news/technology-16755434

Home US & Canada Latin America UK Africa Asia Europe Mid-East Business Health Sci/Environment Tech Entertainment Video

27 January 2012 Last updated at 17:04 ET

979 Share f t e

Facebook sues alleged clickjacking spammer sparking row

Facebook is suing a marketing firm, accusing it of "spreading spam through misleading and deceptive tactics".

Adscend Media is alleged to have carried out "clickjacking".

The practice involves placing posts on the social network which include code that causes the links to appear on the users' homepages as



Some analysts have linked Facebook's spam

Top stories

 Greek PM gives final euro warning **NEW**

Syria general 'shot in Damascus'

Sun 'will continue' says Murdoch

S Africa to get Mandela banknotes

Iran to make nuclear announcement

Features & Analysis

 Too revealing

It's All About iFrame

- Any site may try to frame any other site

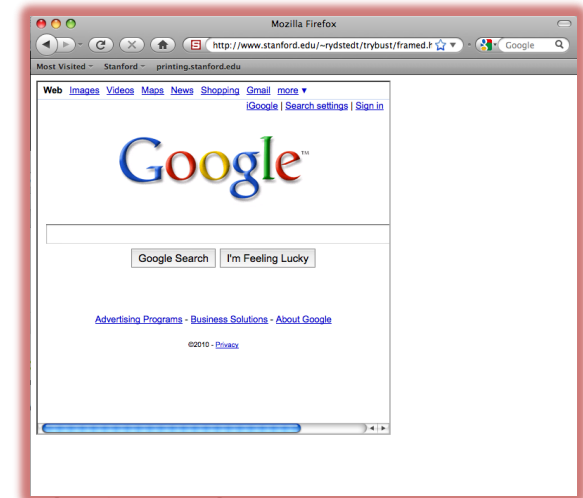
```
<iframe  
  src="http://www.google.com/...">  
</iframe>
```

- HTML attributes

- Style

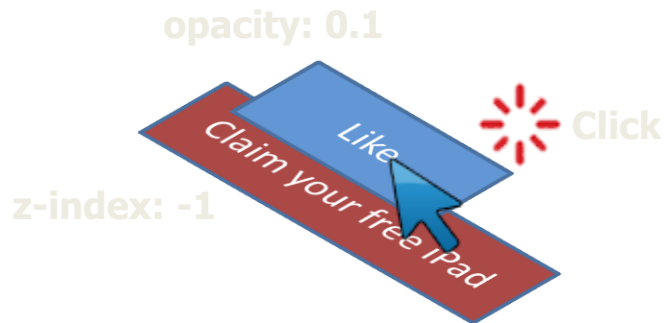
- **Opacity** defines visibility percentage of the iframe

- 1.0: completely visible
- 0.0: completely invisible



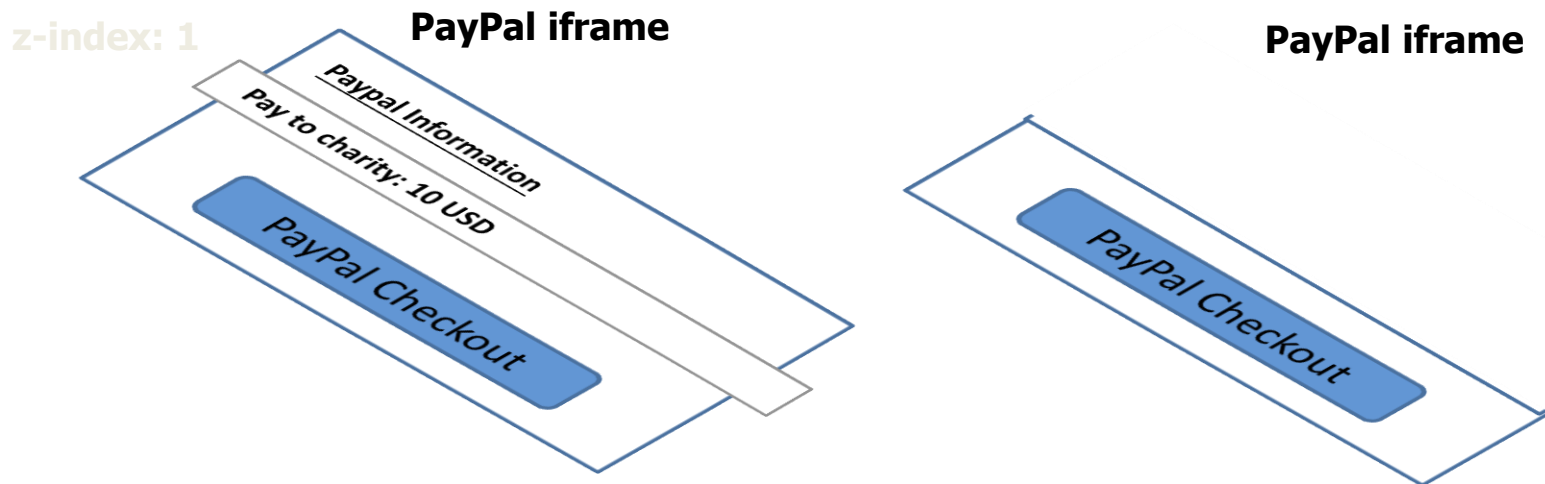
Hiding the Target Element

- Use CSS `opacity` property and `z-index` property to hide target element and make other element float under the target element



Partial Overlays and Cropping

- Overlay other elements onto an iframe using CSS `z-index` property or Flash Window Mode `wmode=direct` property
- Wrap target element in a new iframe and choose CSS position offset properties



Another Example

```
<!DOCTYPE html>
<html>
  <head>
    <title>Clickjacking Times</title>
  </head>
  <body>
    <h1>Clickjacking Example</h1>
    <div style="z-index:2; position:absolute; top:0; left:0; width: 100%; height: 100%">
      <iframe src="http://www.iitp.ac.in" id="frame1" style="opacity:0.1; filter:alpha(opacity=0);"
width="100%" height="100%" />
    </iframe>
    </div>
    <div align="right" style="position:absolute; top:500px; left:500px; z-index:1; width: 100%;
height:100%; background-color: white; text-align:left;">
      <p><input type="submit" value="Press Here" /><br />Press this button for an iPhone</p>
    </div>
  </body>
</html>
```

Clickjacking Example

Indian Institute of Technology Patna

HOME THE INSTITUTE ADMISSION ACADEMICS DEPARTMENTS RESEARCH SERVICES AND AMENITIES STUDENTS CONTACT INCUBATION CENTRE

International Relation (IR) Website 5th International Conference on Data Science and Engineering (ICDSE 2019)

Tentative dates for test/interview for the M.Tech, Ph.D. (

Director, IIT Patna

- Director's Message
- Director's Profile
- Directorate
- Photo Gallery
- Opportunities in IIT Patna
- Director's Talk to Indian Students Abroad

News

- Short Term CEP Course on Effective Communication and Presentation Skills (21st-24th May 2019)
- Short Term CEP Course on Principles and Practices in Social Research (22nd May 2019)
- Short Term CEP Course on Failure Analysis of Engineering Products (10th - 11th May 2019)
- Short Term CEP/FDP Course on Mediation, Moderation and Conditional Process Analysis, 17-18 May 2019

Notice Board

- Prime Minister's Research Fellowship
- Scheme for implementing the reservation for EWS (July 2019 admission)
- Last date for submission of Business plans for the eleventh batch of startup to Incubation Centre is 15th June 2019

Points of Pride

Press Here
Press this button for an iPhone

Countermeasures

- Framebuster or Framekiller
- Content Security Policy (CSP)
- X-Frame-Options

Framebuster

```
<html>
<body>
<p>Document content goes here...</p>
<script>
if(self==top){
document.documentElement.style.display='block';
}else{
top.location=self.location;
}
</script>
<p>This is a good page</p>

</body>
</html>
```

Content Security Policy (CSP)

- The **frame-ancestors** directive can be used in a Content-Security-Policy HTTP response header to indicate whether or not a browser should be allowed to render a page in a `<frame>` or `<iframe>`

CSP

- **Content-Security-Policy: frame-ancestors 'none';**
 - This prevents any domain from framing the content. This setting is recommended unless a specific need has been identified for framing.
- **Content-Security-Policy: frame-ancestors 'self';**
 - This only allows the current site to frame the content.
- **Content-Security-Policy: frame-ancestors 'self' *.somesite.com https://myfriend.site.com;**
 - This allows the current site, as well as any page on somesite.com (using any protocol), and only the page myfriend.site.com, using HTTPS only on the default port

X-Frame-Options

```
<?php  
header("X-Frame Option: DENY")  
?>  
<html>  
<body>  
<p>This is a protected page using X-Frame-Options</p>  
</body>  
</html>
```

X-Frame-Options:

DENY

SAMEORIGIN

ALLOW-FROM %URL%