IFRAMES

A webpage within a webpage

IFRAMES

An iframe or an inline frame allows you to load content from another site inside your webpage

Iframes add a whole other capability to your browser which allows you to do cool stuff

IFRAMES

iframes have their own URL which
can point to any site on the internet

```
<iframe src=“http://www.nytimes.com/" width="800" height="300"></iframe>
```

This allows you to include
the content of the New
York Times on your site!

IFRAMES

iframes have their own URL which
can point to any site on the internet

```
<iframe src=“http://www.nytimes.com/" width="800" height="300"></iframe>
```

In fact ads displayed on sites are just iframes which reference an **ad network** which supplies contextual ads

IFRAMES

Iframes allow:

1. **Frame based layouts** - where each frame is independent and can be resized separately

2. **3rd party content embedding** - YouTube URLs, audio, forms, documents anything can be embedded

3. **Content isolation** - Content on your page is isolated from iframe and vice versa

IFRAMES

Iframes come with their own set of issues

Clickjacking

If you do not own the source URL you cannot control the content of the iframe

Users might be led to click on hyperlinks **hidden beneath legitimate content** - resulting in unintended actions

IFRAMES

Iframes come with their own set of issues

Display malicious content

What if an ad on your site shows a **login** box?

The user name and password for your site could be **compromised**!

Clickjacking
Display malicious content

IFRAMES

Iframes come with their own set of issues

Webpage redirection

What if the iframe used **location.href** and sent the user to another site?

yourbank.com -> yourbank.fake.com

Clickjacking
Display malicious content
Webpage redirection

IFRAMES

Iframes come with their own set of issues

malware

If the page is from a 3rd party site,
it could infect the user's machine

Clickjacking
Display malicious content
Webpage redirection
malware

IFRAMES

Iframes come with their own set of issues

interference

The page could just be plain annoying - showing popups, autoplaying video etc.

IFRAMES

Iframes come with their own set of issues

Clickjacking

Display malicious content

Webpage redirection

malware

interference

IFRAMES

Example17-iframes-embedded.php

IFRAMES

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Iframes - embedded</title>
</head>
<body>
  <iframe src = "http://nytimes.com" height="400px" width="600px"
          scrolling="yes" frameborder="0">
  </iframe>
  <iframe src = "Example17-iframes-annoying.php" height="400px" width="600px"
          scrolling="yes" frameborder="0">
  </iframe>
</body>
</html>
```

This page is pretty annoying - look carefully

IFRAMES

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Iframes - embedded</title>
</head>
<body>
  <iframe src = "http://nytimes.com" height="400px" width="600px"
          scrolling="yes" frameborder="0">
  </iframe>
  <iframe src = "Example17-iframes-annoying.php" height="400px" width="600px"
          scrolling="yes" frameborder="0">
  </iframe>
</body>
</html>
```

Here is an embedded iframe displaying the front page of the NYT

IFRAMES

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Iframes - embedded</title>
</head>
<body>
  <iframe src = "http://nytimes.com" height="400px" width="600px"
          scrolling="yes" frameborder="0">
  </iframe>
  <iframe src = "Example17-iframes-annoying.php" height="400px" width="600px"
          scrolling="yes" frameborder="0">
  </iframe>
</body>
</html>
```

And another local page - now this local page could do a bunch of stuff to annoy users

IFRAMES

```html
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>Iframes – annoying iframe</title>
</head>
<body>
  <h3> This is a pretty annoying iframe </h3>
  <script>
    window.onload = function() {
      setTimeout(function() { alert("Hello – am I annoying you yet? "); }, 3000);
    }
  </script>
</body>
</html>
```

IFRAMES

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>Iframes - annoying iframe</title>
</head>
<body>
  <h3> This is a pretty annoying iframe </h3>
  <script>
    window.onload = function() {
      setTimeout(function() { alert("Hello - am I annoying you yet? "); }, 3000);
    }
  </script>
</body>
</html>
```

This one displays a popup every 3 seconds

IFRAMES

We need a way to allow iframes to do stuff without interfering with our site

The principle of least privilege

using the `sandbox` attribute

IFRAMES

using the `sandbox` attribute

This allows you to specify what exactly your iframe **can** and **cannot** do

You have very **granular** control over the privileges of the iframe

IFRAMES

using the `sandbox` attribute

This attribute allows us to have the advantage of using iframes while having greater control over what they can do!

IFRAMES

using the sandbox attribute

```
<iframe
    src="https://platform.twitter.com/widgets/tweet_button.html"
    style="border: 0; width:80px; height:20px;”
    sandbox="">
</iframe>
```

Embed the Twitter tweet button on your page using an iframe

IFRAMES

```
<iframe
    src="https://platform.twitter.com/widgets/tweet_button.html"
    style="border: 0; width:80px; height:20px;”
    sandbox="">
</iframe>
```

This attribute indicates that this iframe is fully sandboxed and a whole bunch of restrictions apply to it

IFRAMES restrictions

```
<iframe
    src="https://platform.twitter.com/widgets/tweet_button.html"
    style="border: 0; width:80px; height:20px;"
        sandbox="">
</iframe>
```

No Javascript execution

No JS in script tags, no inline event handlers, no javascript: URLs

No Javascript execution

IFRAMES restrictions

```
<iframe
    src="https://platform.twitter.com/widgets/tweet_button.html"
    style="border: 0; width:80px; height:20px;”
         sandbox="" >
</iframe>
```

Unique origin

This means that all same-origin checks will fail for that frame, unique origins match no other origin

No access to cookies, DBs of any origin

No Javascript execution
Unique origin

IFRAMES restrictions

```
<iframe
    src="https://platform.twitter.com/widgets/tweet_button.html"
    style="border: 0; width:80px; height:20px;"
            sandbox="" >
</iframe>
```

No new windows or dialogs

The iframe cannot use `window.open` or `target="_blank"`

No Javascript execution
Unique origin
No new windows or dialogs

IFRAMES restrictions

```
<iframe
    src="https://platform.twitter.com/widgets/tweet_button.html"
    style="border: 0; width:80px; height:20px;"
            sandbox="" >
</iframe>
```

No forms or plugins

You cannot submit forms on the iframe nor include any new plugins

IFRAMES restrictions

No Javascript execution

Unique origin

No new windows or dialogs

No forms or plugins

```
<iframe
    src="https://platform.twitter.com/widgets/tweet_button.html"
    style="border: 0; width:80px; height:20px;"
        sandbox="">
</iframe>
```

No parent navigation

The iframe can only navigate itself, not it's top-level parent

IFRAMES restrictions

- No Javascript execution
- Unique origin
- No new windows or dialogs
- No forms or plugins
- No parent navigation

```
<iframe
    src="https://platform.twitter.com/widgets/tweet_button.html"
    style="border: 0; width:80px; height:20px;"
            sandbox="">
</iframe>
```

No auto-triggered features

No autoplaying of videos, auto focusing of form elements

IFRAMES restrictions

```
<iframe
    src="https://platform.twitter.com/widgets/tweet_button.html"
    style="border: 0; width:80px; height:20px;"
        sandbox="" >
</iframe>
```

No Javascript execution

Unique origin

No new windows or dialogs

No forms or plugins

No parent navigation

No auto-triggered features

IFRAMES

```
<iframe
    src="https://platform.twitter.com/widgets/tweet_button.html"
    style="border: 0; width:80px; height:20px;"
            sandbox="" >
</iframe>
```

No JavaScript execution

Unique origin

No new windows/dialogs

No forms/plugins

No parent navigation

No auto-triggered features

Pretty draconian set of restrictions

IFRAMES

```
<iframe
    src="https://platform.twitter.com/widgets/tweet_button.html"
    style="border: 0; width:80px; height:20px;"
            sandbox=""  >
</iframe>
```

No Javascript execution

Unique origin

No new windows or dialogs

No forms or plugins

No parent navigation

No auto-triggered features

These might be fine for embedding static pages but we have to loosen these when we work with dynamic content

IFRAMES

```
<iframe
    src="https://platform.twitter.com/widgets/tweet_button.html"
    style="border: 0; width:80px; height:20px;"
        sandbox="" >
</iframe>
```

No Javascript execution

Unique origin

No new windows or dialogs

No forms or plugins

No parent navigation

No auto-triggered features

IFRAMES

Example18-iframes-sandbox.php

IFRAMES

```html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Iframes - sandbox</title>
</head>
<body>
<iframe src="http://nytimes.com" height="400px" width="600px"
        scrolling="yes" frameborder="0">
</iframe>
<br>
<iframe sandbox="allow-same-origin allow-scripts allow-popups allow-forms"
        src="https://platform.twitter.com/widgets/tweet_button.html"
        style="border: 0; width:80px; height:20px;">
</iframe>
</body>
</html>
```

IFRAMES

The Tweet button is embedded using an iframe

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Iframes - sandbox</title>
</head>
<body>
<iframe src="http://nytimes.com" height="400px" width="600px"
        scrolling="yes" frameborder="0">
</iframe>
<br>
<iframe sandbox="allow-same-origin allow-scripts allow-popups allow-forms"
        src="https://platform.twitter.com/widgets/tweet_button.html"
        style="border: 0; width:80px; height:20px;">
</iframe>
</body>
</html>
```

It requires a bunch of permissions to work

IFRAMES

Insert video of how Tweet button works

IFRAMES

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Iframes - sandbox</title>
</head>
<body>
<iframe src="http://nytimes.com" height="400px" width="600px"
        scrolling="yes" frameborder="0">
</iframe>
<br>
<iframe sandbox="allow-same-origin allow-scripts allow-popups allow-forms"
        src="https://platform.twitter.com/widgets/tweet_button.html"
          style="border: 0; width:80px; height:20px;">
</iframe>
</body>
</html>
```

This is the URL for the Tweet button

IFRAMES

```
</head>
<body>
<iframe src="http://nytimes.com" heig[illegible]00px"
        scrolling="yes" frameborder="[illegible]">
</iframe>
<br>
<iframe sandbox="allow-same-origin allow-scripts allow-popups allow-forms"
        src="https://platform.twitter.com/widgets/tweet_button.html"
        style="border: 0; width:80px; height:20px;">
</iframe>
</body>
</html>
```

These are the permissions that the iframe needs

IFRAMES

```
<body>
<iframe src="http://nytimes.com" height="400px" width="600px"
        scrolling="yes" frameborder="0">
</iframe>
<br>

<iframe sandbox="allow-same-origin allow-scripts allow-popup
forms"
        src="https://platform.twitter.com/widgets/tweet_button.html"
        style="border: 0; width:80px; height:20px;">
</iframe>
</body>
</html>
```

Allows the document in the frame to **maintain** its origin

This page is loaded from Twitter and will be able to access Twitter's data such as cookies

IFRAMES

```
e src="http://nytimes.com" height="400px" width="600px"
  scrolling="yes" frameborder="0">
me>

me sandbox="allow-same-origin allow-scripts allow-popups allow-
s"
  src="https://platform.twitter.com/widgets/tweet_button.html"
  style="border: 0; width:80px; height:20px;">
me>
>
>
```

Allows the frame to **run Javascript** and allows features to trigger automatically e.g. onFocus

The button implements Javascript to get data from Twitter to display a form

IFRAMES

```
times.com" height="400px" width="600px"
' frameborder="0">

llow-same-origin allow-scripts allow-popups allow-forms"
latform.twitter.com/widgets/tweet_button.html"
 0; width:80px; height:20px;">
```

Allows `window.open()`, `showModalDialog()`, `target=“_blank”` etc

The Twitter form opens up in a new dialog

IFRAMES

```
t="400px" width="600px"
">

igin allow-scripts allow-popups allow-forms"
com/widgets/tweet_button.html"
eight:20px;">
```

Allows the tweeting form to be submittable to Twitter

IFRAMES

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Iframes - sandbox</title>
</head>
<body>
<iframe src="http://nytimes.com" height="400px" width="600px"
        scrolling="yes" frameborder="0">
</iframe>
<br>
<iframe sandbox="allow-same-origin allow-scripts allow-popups allow-forms"
        src="https://platform.twitter.com/widgets/tweet_button.html"
        style="border: 0; width:80px; height:20px;">
</iframe>
</body>
</html>
```

There are other directives to sandbox as well, but these are the most common!