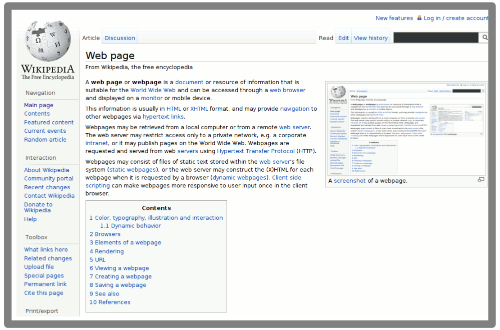
Hardening WebKit2

Thiago Marcos P. Santos
Intel Corporation

TIZEN™
DEVELOPER
CONFERENCE
2013
SAN FRANCISCO

example.com



New features Log in / create account

Article Discussion Read Edit View history

WIKIPEDIA
The Free Encyclopedia

Navigation

- Main page
- Contents
- Featured content
- Current events
- Random article

Interaction

- About Wikipedia
- Community portal
- Recent changes
- Contact Wikipedia
- Donate to Wikipedia
- Help

Toolbox

- What links here
- Related changes
- Upload file
- Special pages
- Permanent link
- Cite this page

Print/export

Web page

From Wikipedia, the free encyclopedia

A **web page** or **webpage** is a document or resource of information that is suitable for the World Wide Web and can be accessed through a web browser and displayed on a monitor or mobile device.

This information is usually in HTML or XHTML format, and may provide navigation to other webpages via hypertext links.

Webpages may be retrieved from a local computer or from a remote web server. The web server may restrict access only to a private network, e.g. a corporate intranet, or it may publish pages on the World Wide Web. Webpages are requested and served from web servers using Hypertext Transfer Protocol (HTTP).

Webpages may consist of files of static text stored within the web server's file system (static webpages), or the web server may construct the (X)HTML for each webpage when it is requested by a browser (dynamic webpages). Client-side scripting can make webpages more responsive to user input once in the client browser.

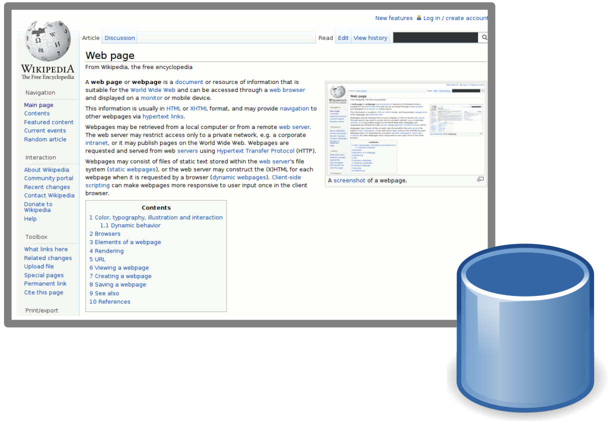
A screenshot of a webpage.

Contents

1 Color, typography, illustration and interaction
    1.1 Dynamic behavior
2 Browsers
3 Elements of a webpage
4 Rendering
5 URL
6 Viewing a webpage
7 Creating a webpage
8 Saving a webpage
9 See also
10 References

Images source: Wikimedia.org

example.com



Web page

From Wikipedia, the free encyclopedia

A **web page** or **webpage** is a document or resource of information that is suitable for the World Wide Web and can be accessed through a web browser and displayed on a monitor or mobile device.

This information is usually in HTML or XHTML format, and may provide navigation to other webpages via hypertext links.

Webpages may be retrieved from a local computer or from a remote web server. The web server may restrict access only to a private network, e.g. a corporate intranet, or it may publish pages on the World Wide Web. Webpages are requested and served from web servers using Hypertext Transfer Protocol (HTTP).

Webpages may consist of files of static text stored within the web server's file system (static webpages), or the web server may construct the (X)HTML for each webpage when it is requested by a browser (dynamic webpages). Client-side scripting can make webpages more responsive to user input once in the client browser.

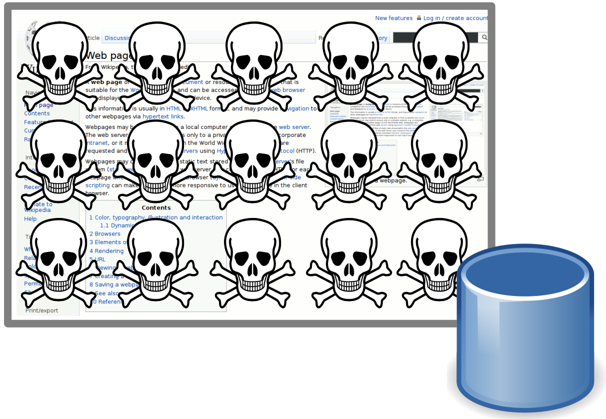
Contents

1 Color, typography, illustration and interaction
    1.1 Dynamic behavior
2 Browsers
3 Elements of a webpage
4 Rendering
5 URL
6 Viewing a webpage
7 Creating a webpage
8 Saving a webpage
9 See also
10 References

A screenshot of a webpage.

Images source: Wikimedia.org

example.com

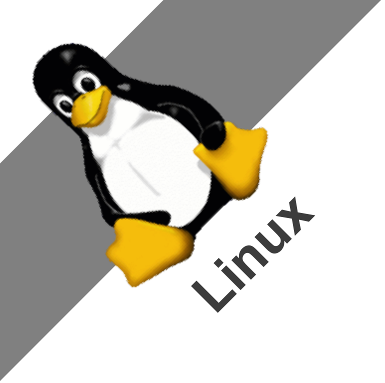


Images source: Wikimedia.org

Images source: Wikimedia.org
Trademarks and logos belong to their respective owners.

WebKit2

Trademarks and logos belong to their respective owners.

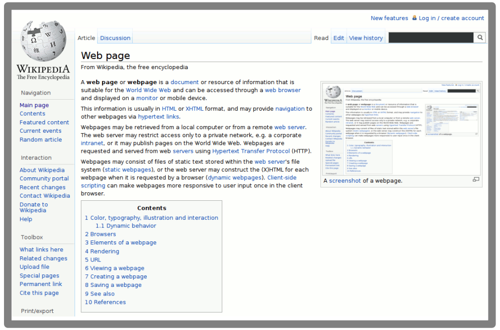


Trademarks and logos belong to their respective owners.

Trademarks and logos belong to their respective owners.

IPC

UIProcess



New features Log in / create account

Article Discussion Read Edit View history

WIKIPEDIA
The Free Encyclopedia

Navigation

- Main page
- Contents
- Featured content
- Current events
- Random article

Interaction

- About Wikipedia
- Community portal
- Recent changes
- Contact Wikipedia
- Donate to Wikipedia
- Help

Toolbox

- What links here
- Related changes
- Upload file
- Special pages
- Permanent link
- Cite this page

Print/export

Web page

From Wikipedia, the free encyclopedia

A **web page** or **webpage** is a document or resource of information that is suitable for the World Wide Web and can be accessed through a web browser and displayed on a monitor or mobile device.

This information is usually in HTML or XHTML format, and may provide navigation to other webpages via hypertext links.

Webpages may be retrieved from a local computer or from a remote web server. The web server may restrict access only to a private network, e.g. a corporate intranet, or it may publish pages on the World Wide Web. Webpages are requested and served from web servers using Hypertext Transfer Protocol (HTTP).

Webpages may consist of files of static text stored within the web server's file system (static webpages), or the web server may construct the (X)HTML for each webpage when it is requested by a browser (dynamic webpages). Client-side scripting can make webpages more responsive to user input once in the client browser.

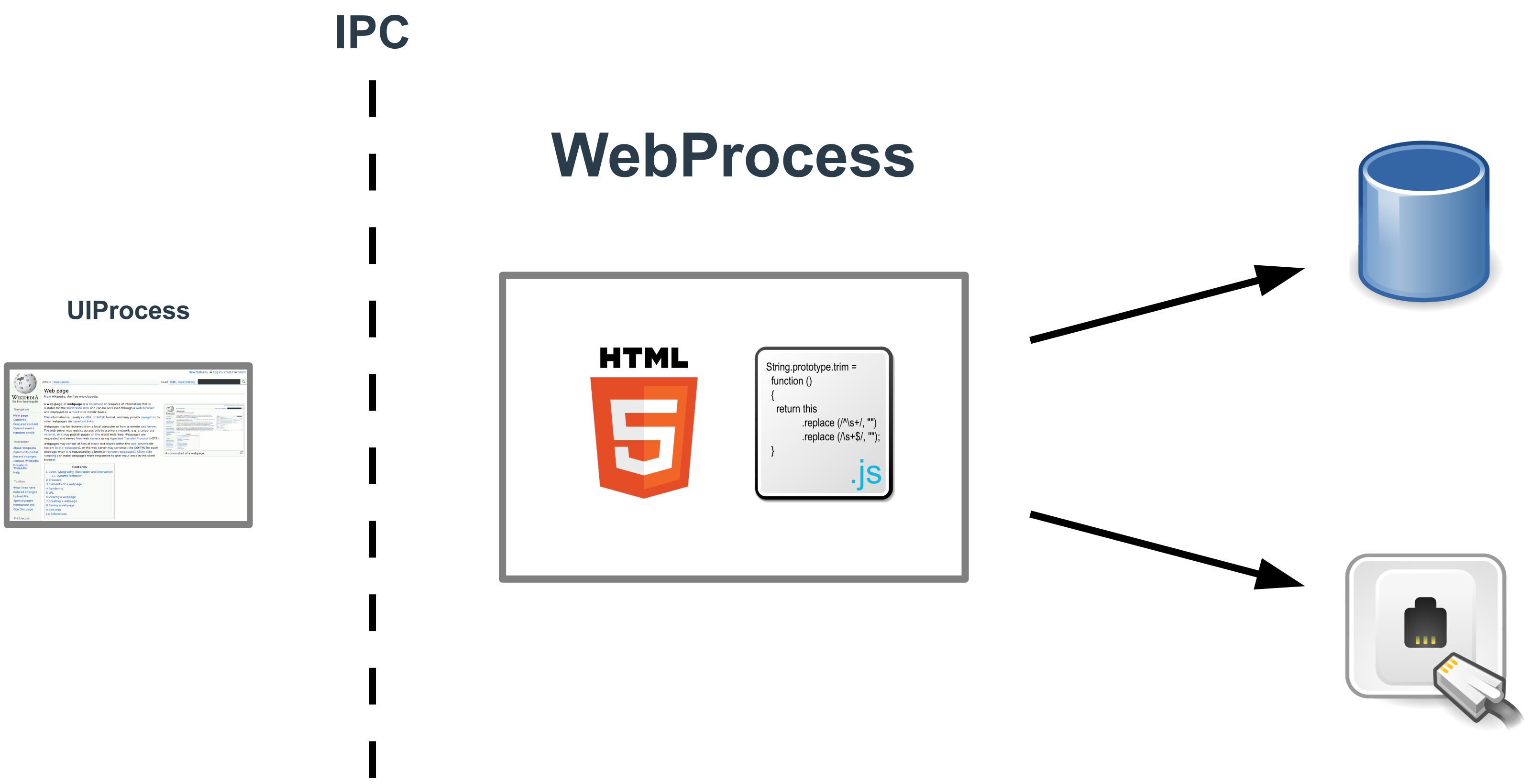
A screenshot of a webpage.

Contents

WebProcess

```
String.prototype.trim =
  function ()
  {
    return this
              .replace (/^\s+/, "")
              .replace (/\s+$/, "");
  }
```

Images source: Wikimedia.org



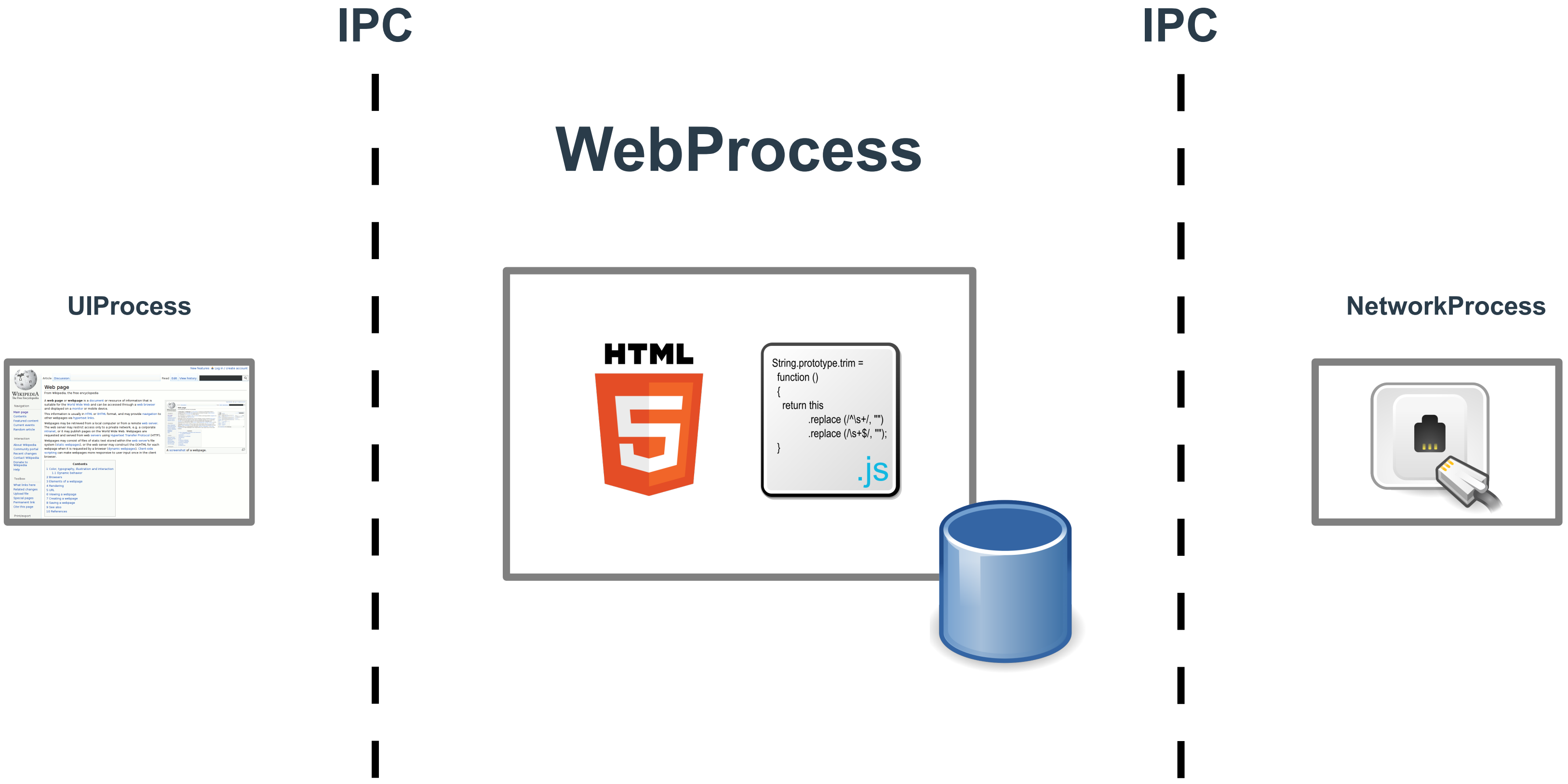
IPC

WebProcess

UIProcess

```
String.prototype.trim =
 function ()
 {
  return this
        .replace (/^\s+/, "")
        .replace (/\s+$/, "");
 }
```

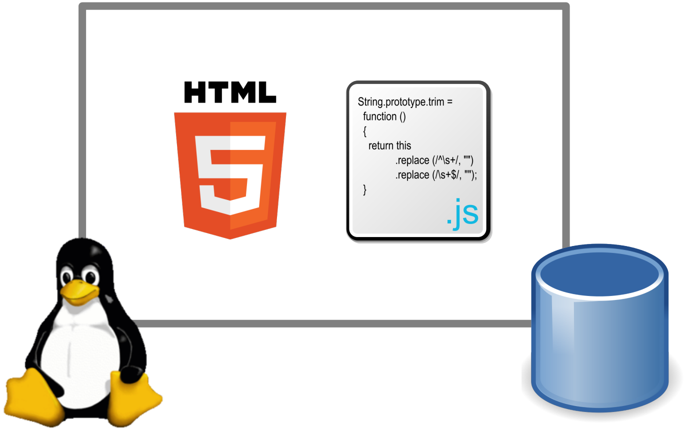
Images source: Wikimedia.org



```
String.prototype.trim =
  function ()
  {
    return this
          .replace (/^\s+/, "")
          .replace (/\s+$/, "");
  }
```

Images source: Wikimedia.org

WebProcess



```
String.prototype.trim =
 function ()
 {
  return this
         .replace (/^\s+/, "")
         .replace (/\s+$/, "");
 }
```

Images source: Wikimedia.org
Trademarks and logos belong to their respective owners.

WebProcess

```
String.prototype.trim =
  function ()
  {
    return this
            .replace (/^\s+/, "")
            .replace (/\s+$/, "");
  }
```

Images source: Wikimedia.org
Trademarks and logos belong to their respective owners.

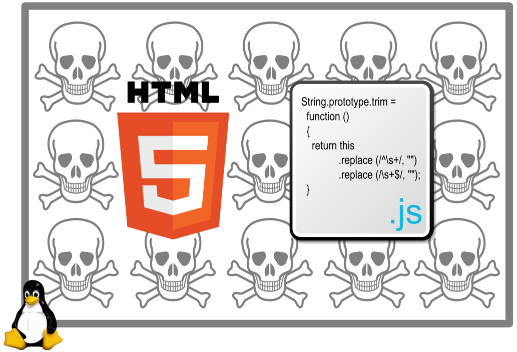
WebProcess

```
String.prototype.trim =
  function ()
  {
    return this
            .replace (/^\s+/, "")
            .replace (/\s+$/, "");
  }
```

Images source: Wikimedia.org
Trademarks and logos belong to their respective owners.

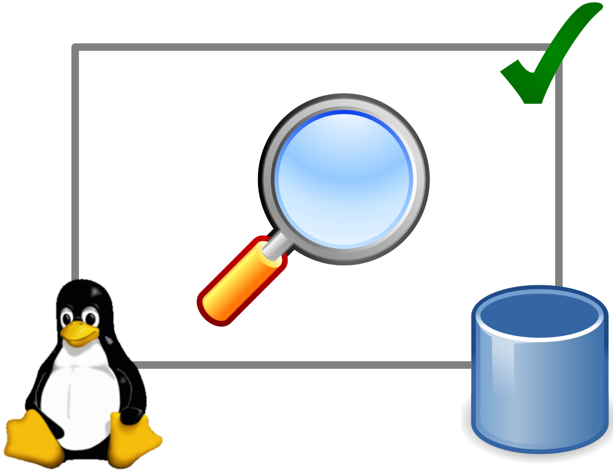
IPC

WebProcess



```
String.prototype.trim =
  function ()
  {
    return this
             .replace (/^\s+/, "")
             .replace (/\s+$/, "");
  }
```

BrokerProcess

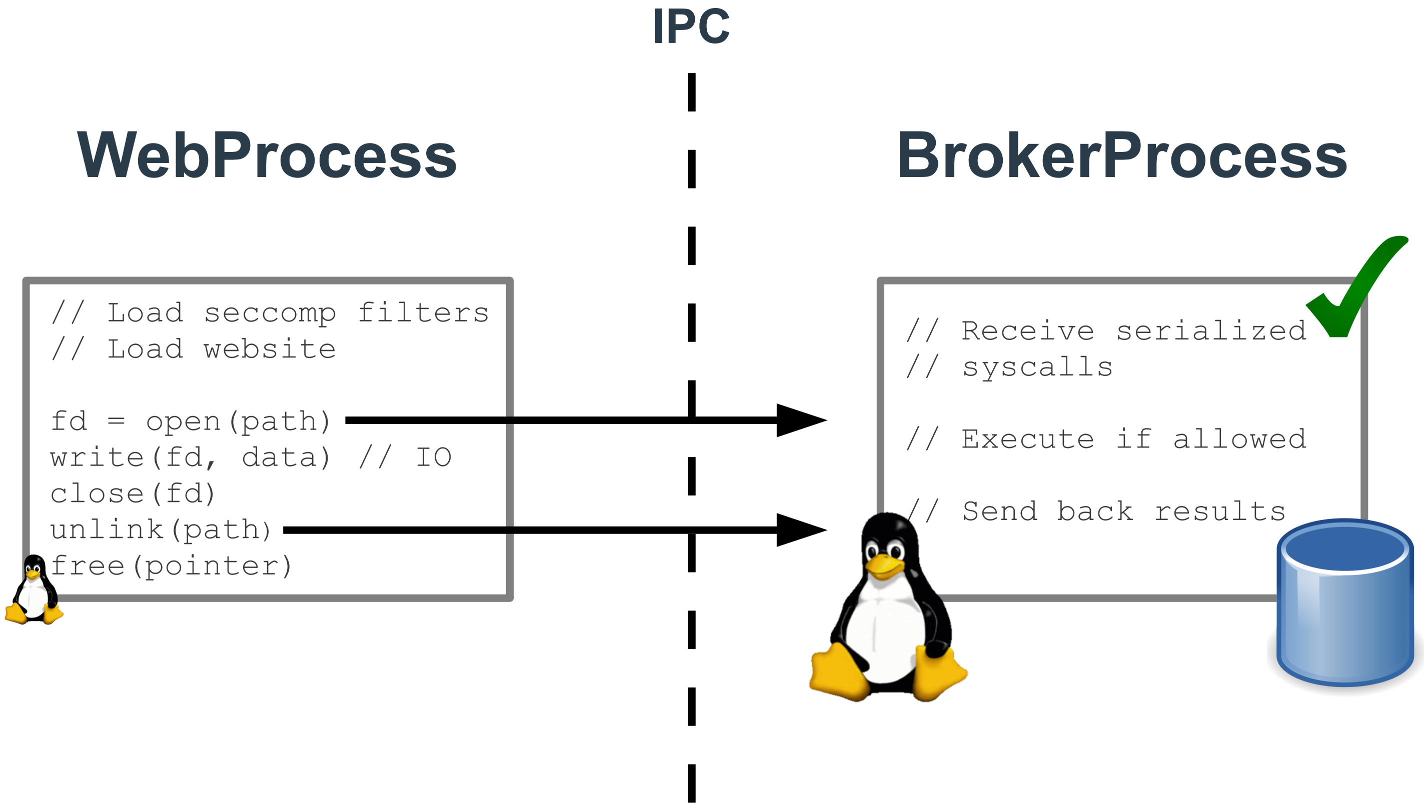


```
$HOME/.browser/example.com/*  (rw)
$HOME/.browser/defaults.conf  (r)
/usr/share/fonts/* (r)
/* (not allowed)
```

Images source: Wikimedia.org
Trademarks and logos belong to their respective owners.

Seccomp Filters

- Linux Kernel 3.5
- Ubuntu 12.04
- Whitelist syscalls
- Blacklist syscalls
- Trap syscalls and inspect its parameters
- Make it possible to emulate a syscall
- ~370 syscalls: libseccomp for the rescue



```
// Load seccomp filters
// Load website

fd = open(path)
write(fd, data) // IO
close(fd)
unlink(path)
free(pointer)
```

```
// Receive serialized
// syscalls

// Execute if allowed

// Send back results
```

Images source: Wikimedia.org
Trademarks and logos belong to their respective owners.

Additional information

- **Performance implications**
  - open() ~28x slower
  - 15.000 open()'s in ~590ms

- **Source code**

```
# ls Source/WebKit2/Shared/linux/SeccompFilters/*
```

- **How to build**

```
# ./Tools/Scripts/build-webkit --efl -2 --seccomp-filters
```

- **Documentation**

  http://tinyurl.com/seccompwk2

Questions?

TIZEN™

DEVELOPER CONFERENCE

2013

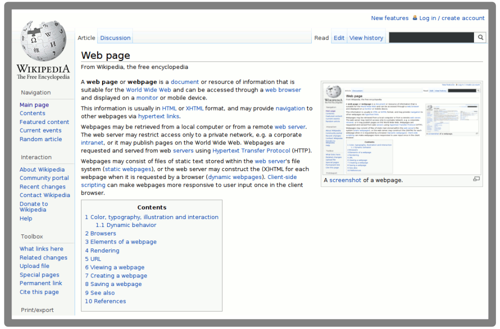
SAN FRANCISCO

WebKit

IPC

UIProcess

WebProcess



New features Log in / create account

Article Discussion Read Edit View history

Wikipedia
The Free Encyclopedia

Navigation
- Main page
- Contents
- Featured content
- Current events
- Random article

Interaction
- About Wikipedia
- Community portal
- Recent changes
- Contact Wikipedia
- Donate to Wikipedia
- Help

Toolbox
- What links here
- Related changes
- Upload file
- Special pages
- Permanent link
- Cite this page

Print/export

Web page

From Wikipedia, the free encyclopedia

A **web page** or **webpage** is a document or resource of information that is suitable for the World Wide Web and can be accessed through a web browser and displayed on a monitor or mobile device.

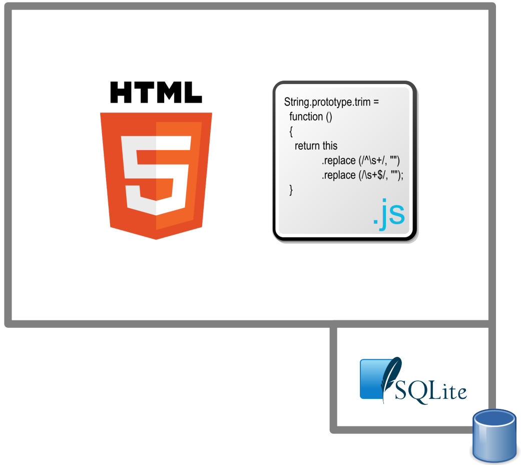
This information is usually in HTML or XHTML format, and may provide navigation to other webpages via hypertext links.

Webpages may be retrieved from a local computer or from a remote web server. The web server may restrict access only to a private network, e.g. a corporate intranet, or it may publish pages on the World Wide Web. Webpages are requested and served from web servers using Hypertext Transfer Protocol (HTTP).

Webpages may consist of files of static text stored within the web server's file system (static webpages), or the web server may construct the (X)HTML for each webpage when it is requested by a browser (dynamic webpages). Client-side scripting can make webpages more responsive to user input once in the client browser.

A screenshot of a webpage.

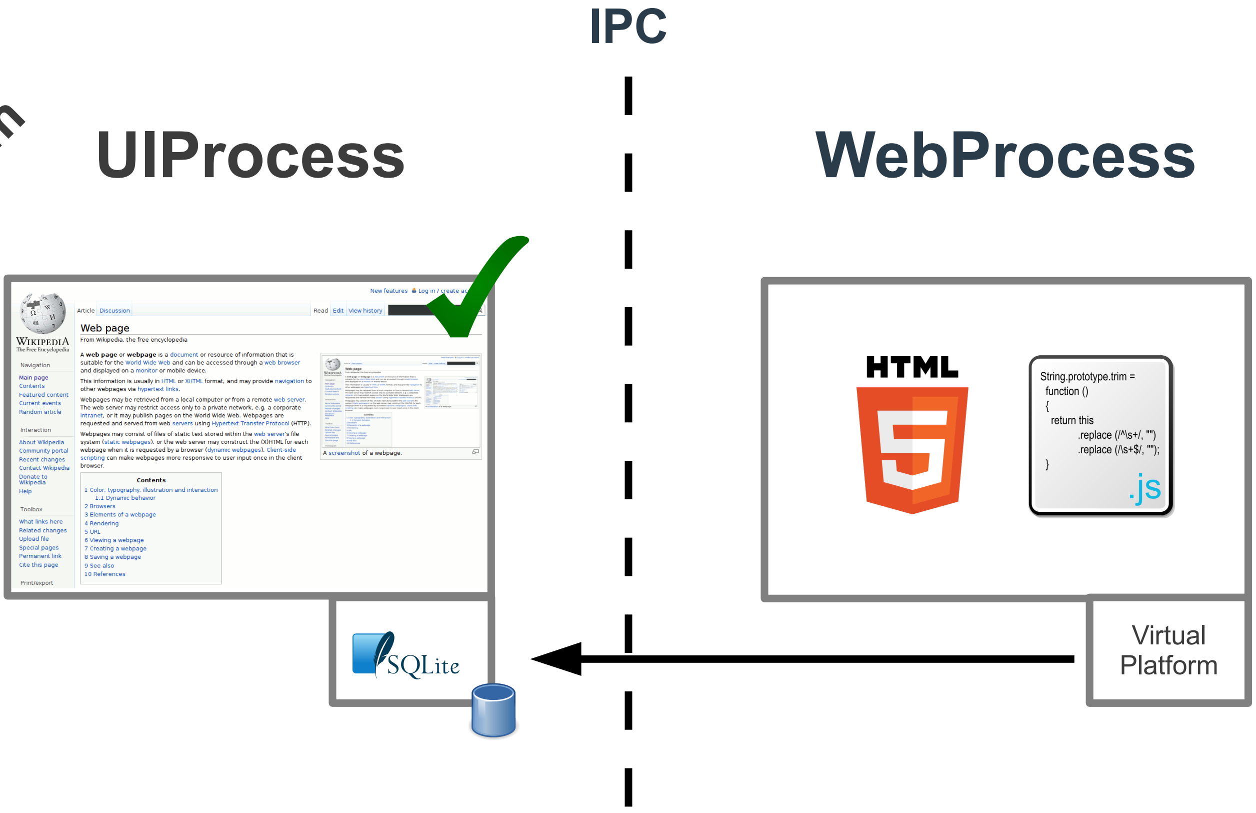
Contents



```
String.prototype.trim =
  function ()
  {
    return this
              .replace (/^\s+/, "")
              .replace (/\s+$/, "");
  }
```

Images source: Wikimedia.org
Trademarks and logos belong to their respective owners.

Chromium



New features Log in / create ac

Article Discussion Read Edit View history

WIKIPEDIA
The Free Encyclopedia

Navigation
- Main page
- Contents
- Featured content
- Current events
- Random article

Interaction
- About Wikipedia
- Community portal
- Recent changes
- Contact Wikipedia
- Donate to Wikipedia
- Help

Toolbox
- What links here
- Related changes
- Upload file
- Special pages
- Permanent link
- Cite this page

Print/export

Web page

From Wikipedia, the free encyclopedia

A **web page** or **webpage** is a document or resource of information that is suitable for the World Wide Web and can be accessed through a web browser and displayed on a monitor or mobile device.

This information is usually in HTML or XHTML format, and may provide navigation to other webpages via hypertext links.

Webpages may be retrieved from a local computer or from a remote web server. The web server may restrict access only to a private network, e.g. a corporate intranet, or it may publish pages on the World Wide Web. Webpages are requested and served from web servers using Hypertext Transfer Protocol (HTTP).

Webpages may consist of files of static text stored within the web server's file system (static webpages), or the web server may construct the (X)HTML for each webpage when it is requested by a browser (dynamic webpages). Client-side scripting can make webpages more responsive to user input once in the client browser.

A screenshot of a webpage.

Contents

```
String.prototype.trim =
  function ()
  {
   return this
          .replace (/^\s+/, "")
          .replace (/\s+$/, "");
  }
```

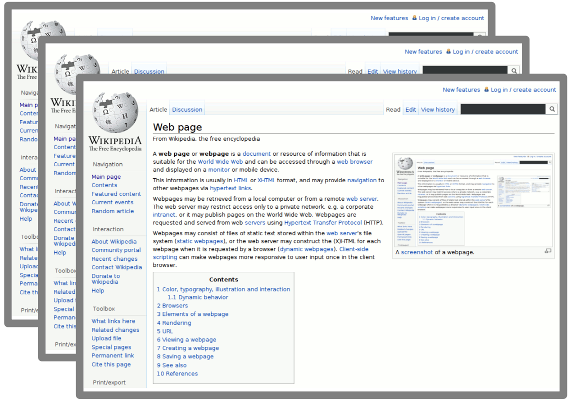
.js

Images source: Wikimedia.org
Trademarks and logos belong to their respective owners.

WebKit

IPC

UIProcess



New features Log in / create account

Article Discussion Read Edit View history

WIKIPEDIA
The Free Encyclopedia

Navigation
- Main page
- Contents
- Featured content
- Current events
- Random article

Interaction
- About Wikipedia
- Community portal
- Recent changes
- Contact Wikipedia
- Donate to Wikipedia
- Help

Toolbox
- What links here
- Related changes
- Upload file
- Special pages
- Permanent link
- Cite this page

Print/export

Web page

From Wikipedia, the free encyclopedia

A **web page** or **webpage** is a document or resource of information that is suitable for the World Wide Web and can be accessed through a web browser and displayed on a monitor or mobile device.

This information is usually in HTML or XHTML format, and may provide navigation to other webpages via hypertext links.

Webpages may be retrieved from a local computer or from a remote web server. The web server may restrict access only to a private network, e.g. a corporate intranet, or it may publish pages on the World Wide Web. Webpages are requested and served from web servers using Hypertext Transfer Protocol (HTTP).

Webpages may consist of files of static text stored within the web server's file system (static webpages), or the web server may construct the (X)HTML for each webpage when it is requested by a browser (dynamic webpages). Client-side scripting can make webpages more responsive to user input once in the client browser.

Contents
1 Color, typography, illustration and interaction
  1.1 Dynamic behavior
2 Browsers
3 Elements of a webpage
4 Rendering
5 URL
6 Viewing a webpage
7 Creating a webpage
8 Saving a webpage
9 See also
10 References

A screenshot of a webpage.

WebProcess

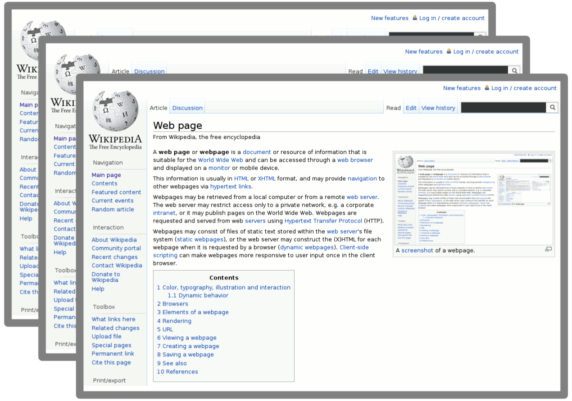
```
String.prototype.trim =
  function ()
  {
    return this
               .replace (/^\s+/, "")
               .replace (/\s+$/, "");
  }
```

Images source: Wikimedia.org
Trademarks and logos belong to their respective owners.

Chromium

IPC

UIProcess



New features Log in / create account

WIKIPEDIA
The Free Encyclopedia

Navigation
Main page
Contents
Featured content
Current events
Random article

Interaction
About Wikipedia
Community portal
Recent changes
Contact Wikipedia
Donate to Wikipedia
Help

Toolbox
What links here
Related changes
Upload file
Special pages
Permanent link
Cite this page

Print/export

Article Discussion Read Edit View history

Web page

From Wikipedia, the free encyclopedia

A **web page** or **webpage** is a document or resource of information that is suitable for the World Wide Web and can be accessed through a web browser and displayed on a monitor or mobile device.

This information is usually in HTML or XHTML format, and may provide navigation to other webpages via hypertext links.

Webpages may be retrieved from a local computer or from a remote web server. The web server may restrict access only to a private network, e.g. a corporate intranet, or it may publish pages on the World Wide Web. Webpages are requested and served from web servers using Hypertext Transfer Protocol (HTTP).

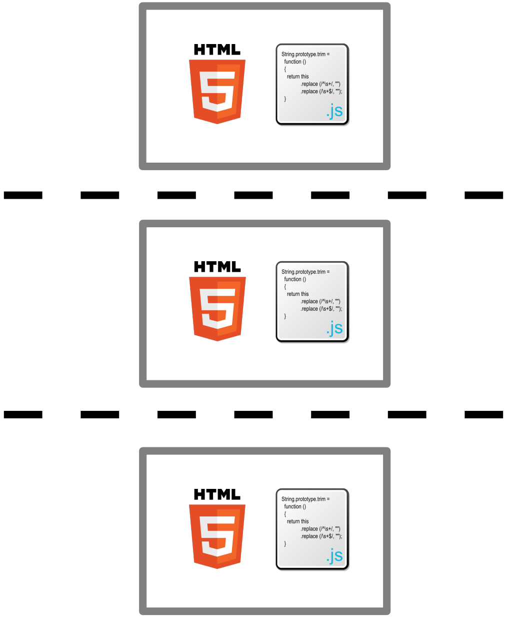
Webpages may consist of files of static text stored within the web server's file system (static webpages), or the web server may construct the (X)HTML for each webpage when it is requested by a browser (dynamic webpages). Client-side scripting can make webpages more responsive to user input once in the client browser.

A screenshot of a webpage.

Contents

1 Color, typography, illustration and interaction
    1.1 Dynamic behavior
2 Browsers
3 Elements of a webpage
4 Rendering
5 URL
6 Viewing a webpage
7 Creating a webpage
8 Saving a webpage
9 See also
10 References

WebProcess



```
String.prototype.trim =
 function ()
 {
  return this
         .replace (/^\s+/, "")
         .replace (/\s+$/, "");
 }
```

HTML
5

```
String.prototype.trim =
 function ()
 {
  return this
         .replace (/^\s+/, "")
         .replace (/\s+$/, "");
 }
```

.js

HTML
5

```
String.prototype.trim =
 function ()
 {
  return this
         .replace (/^\s+/, "")
         .replace (/\s+$/, "");
 }
```

.js

Images source: Wikimedia.org
Trademarks and logos belong to their respective owners.