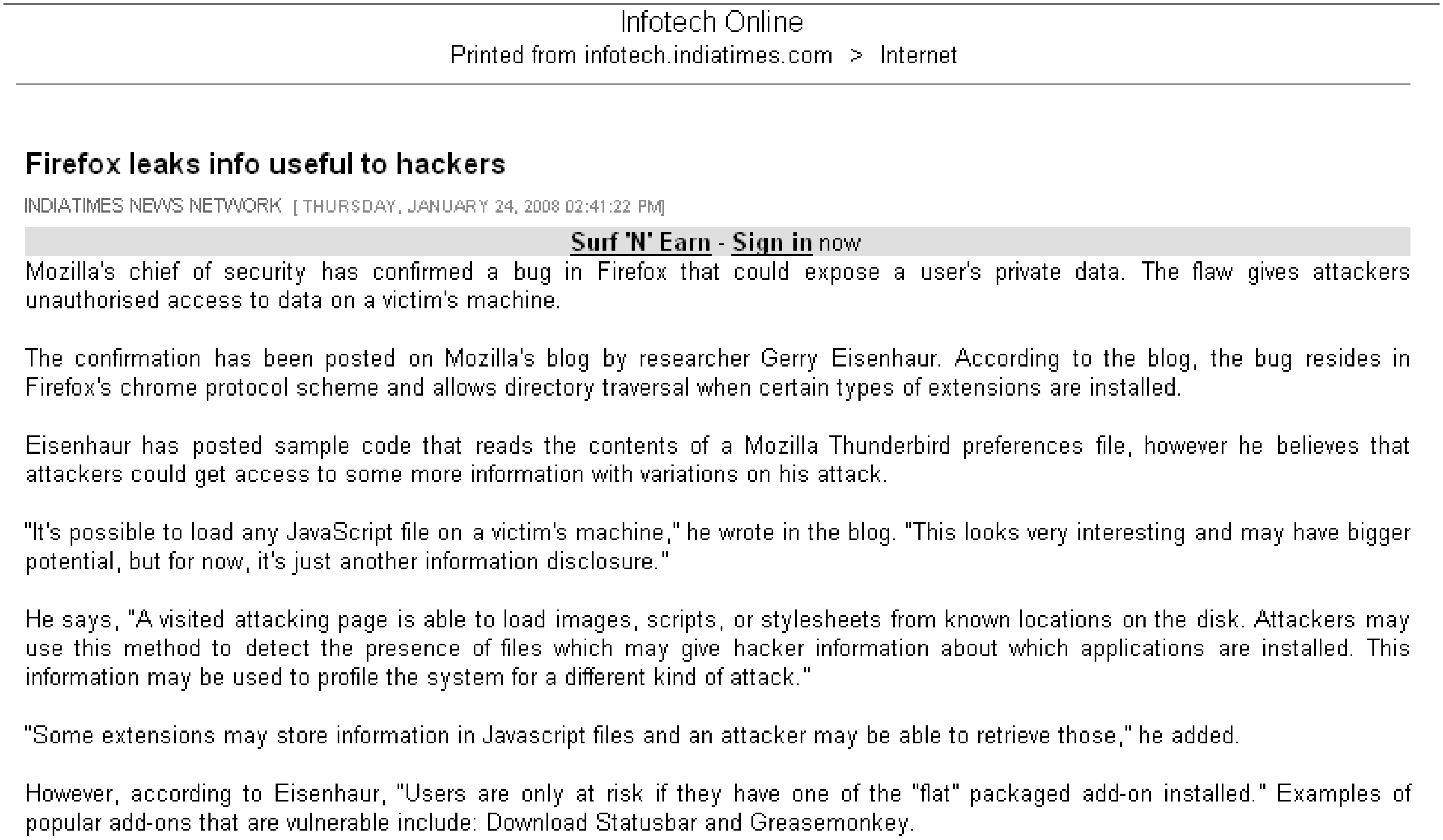
Ethical Hacking and Countermeasures

Version 6

Module LIII

Hacking Web Browsers

News



Infotech Online
Printed from infotech.indiatimes.com > Internet

Firefox leaks info useful to hackers

INDIATIMES NEWS NETWORK [THURSDAY, JANUARY 24, 2008 02:41:22 PM]

Mozilla's chief of security has confirmed a bug in Firefox that could expose a user's private data. The flaw gives attackers unauthorised access to data on a victim's machine.

The confirmation has been posted on Mozilla's blog by researcher Gerry Eisenhaur. According to the blog, the bug resides in Firefox's chrome protocol scheme and allows directory traversal when certain types of extensions are installed.

Eisenhaur has posted sample code that reads the contents of a Mozilla Thunderbird preferences file, however he believes that attackers could get access to some more information with variations on his attack.

"It's possible to load any JavaScript file on a victim's machine," he wrote in the blog. "This looks very interesting and may have bigger potential, but for now, it's just another information disclosure."

He says, "A visited attacking page is able to load images, scripts, or stylesheets from known locations on the disk. Attackers may use this method to detect the presence of files which may give hacker information about which applications are installed. This information may be used to profile the system for a different kind of attack."

"Some extensions may store information in Javascript files and an attacker may be able to retrieve those," he added.

However, according to Eisenhaur, "Users are only at risk if they have one of the "flat" packaged add-on installed." Examples of popular add-ons that are vulnerable include: Download Statusbar and Greasemonkey.

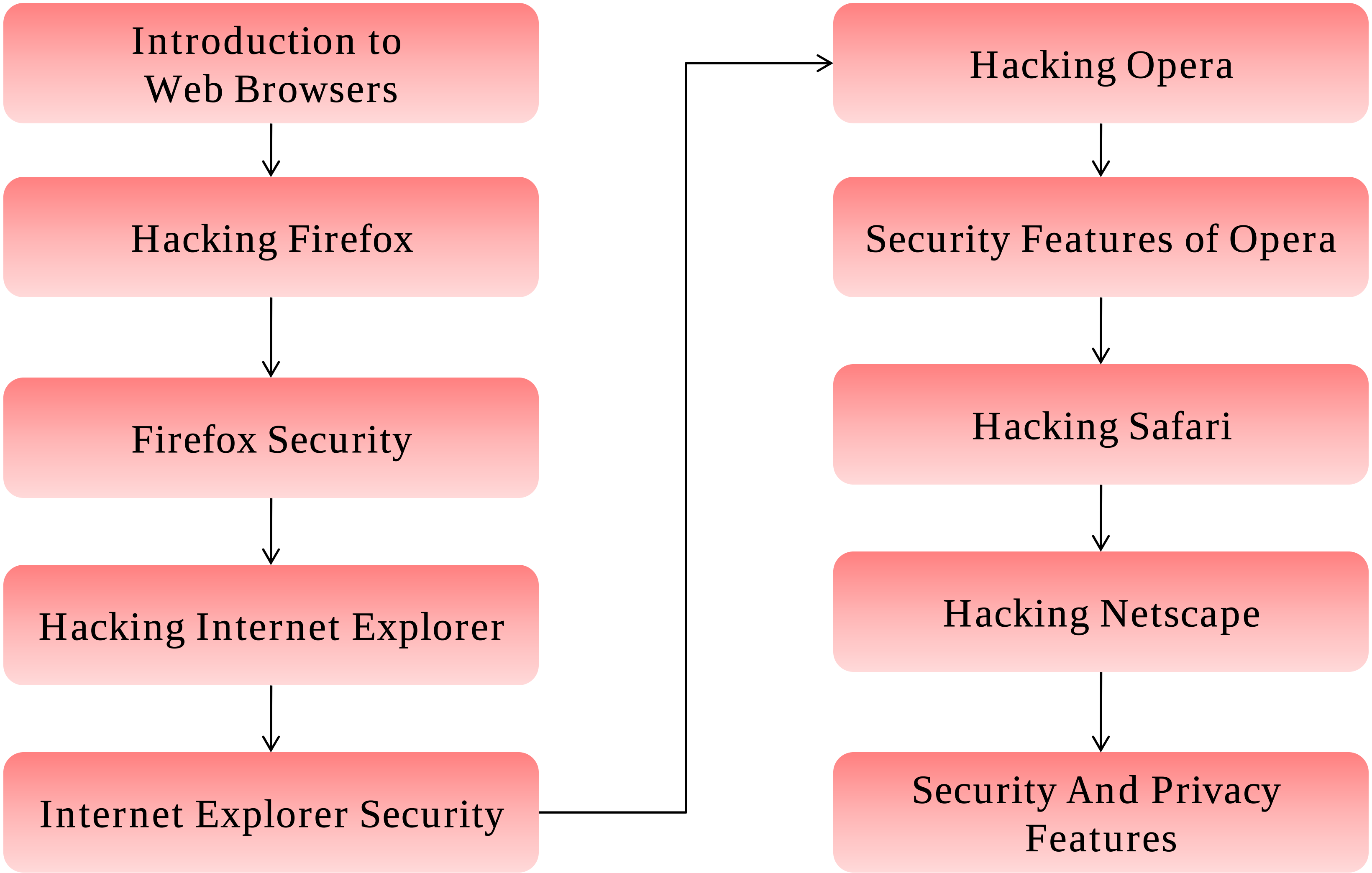
Source: *http://infotech.indiatimes.com/*

Module Objective

This module will familiarize you with:

- Introduction to Web Browsers
- Hacking Firefox
- Firefox Security
- Hacking Internet Explorer
- Internet Explorer Security
- Hacking Opera
- Security Features of Opera
- Hacking Safari
- Hacking Netscape
- Security And Privacy Features

Module Flow



Introduction to Web Browsers

Hacking Firefox

Firefox Security

Hacking Internet Explorer

Internet Explorer Security

Hacking Opera

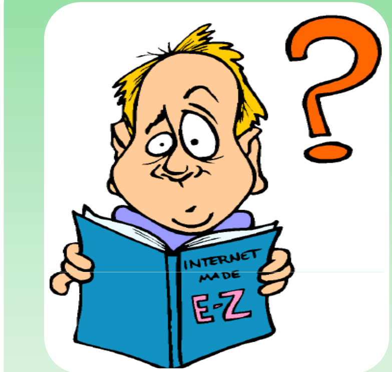
Security Features of Opera

Hacking Safari

Hacking Netscape

Security And Privacy Features

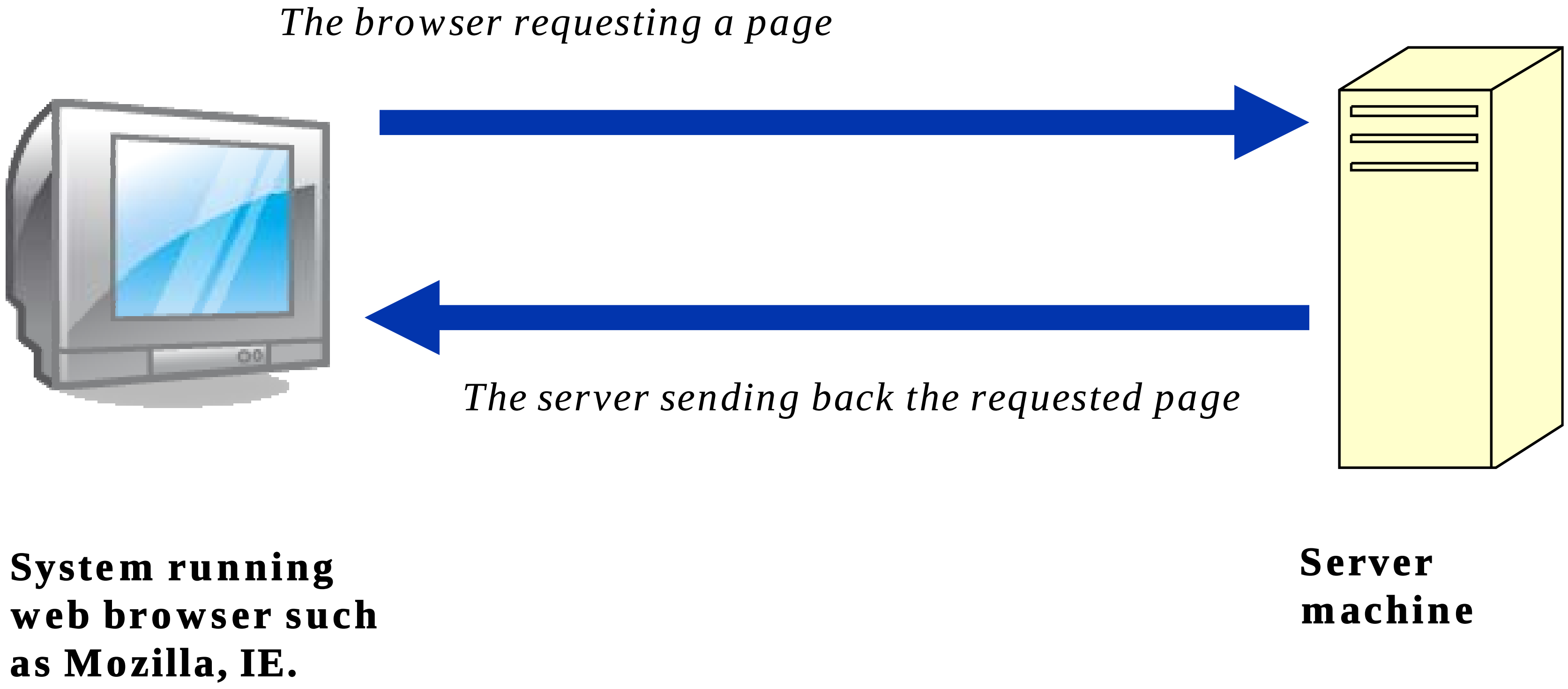
Introduction



Most of the people consider Web browser as the vital key for interacting with the Internet, which connects them to global web sites and helps them to consume online services and provides everything from booking flights to banking services to online shopping

This reality makes browsers a key tool when evaluating the security experience of users as the browser interprets Web content and programs delivered from around the world

How Web Browsers Work



The browser requesting a page

The server sending back the requested page

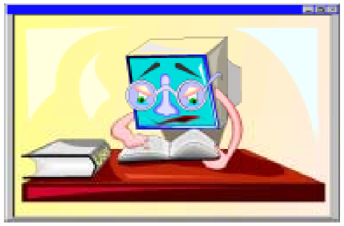
System running web browser such as Mozilla, IE.

Server machine

How Web Browsers Access HTML Documents

When an URL is entered in the URL field of browser the browser goes through the following three basic steps:

- The browser determines what protocol to use
- It looks up and contacts the server at the address specified
- The browser requests the specific document (including its path statement) from the server computer



Protocols for an URL

The following table shows some of the other protocols that can be part of an URL

Protocol	Accesses
http://	HTML documents
https://	Some "secure" HTML documents
file://	HTML documents on your hard drive
ftp://	FTP sites and files
gopher://	Gopher menus and documents
news://	UseNet newsgroups on a particular news server
news:	UseNet newsgroups
mailto:	E-mail messages
telnet:	Remote Telnet (login) session

Hacking Firefox

C|EH™ Certified Ethical Hacker

Firefox Proof of Concept Information Leak Vulnerability

Firefox leaks information that can allow an attacker to load any JavaScript file on a machine

Technically, it is a chrome protocol directory transversal

When a chrome package is “flat” rather than contained in a .jar, the directory traversal allows the extensions directory to escape and files to be read in a predictable location on the disk

A visited attacking page is able to load images, scripts, or stylesheets from known locations on the disk

Attackers may use this method to detect the presence of files which may give an attacker information about which applications are installed

CEH™ Certified Ethical Hacker

Firefox Spoofing Vulnerability

A flaw has been discovered in Firefox which could be used to trick a user into believing that they are actually visiting a trusted web site

Mozilla's latest version fails to sanitize single quotation marks and spaces in the "Realm" value of an authentication header

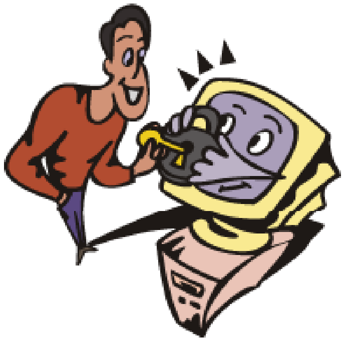
This makes it possible for an attacker to create a specially crafted Realm value which will look as if the authentication dialog came from a trusted site

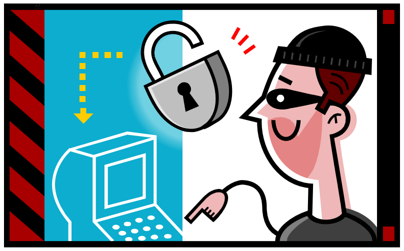
Exploiting this vulnerability, an attacker might be able to lure a user into providing his/her username, password, or other sensitive information

Password Vulnerability

Firefox contains a password management vulnerability that can allow malicious Web sites to steal user passwords

If you have JavaScript enabled and allow Firefox to remember your passwords, you are at risk from this flaw





Concerns With Saving Form Or Login Data

Firefox has the ability to store commonly used form elements and login credentials

To access the settings for form or login data, open the Options window, and access the Privacy settings (Tools ->Options)

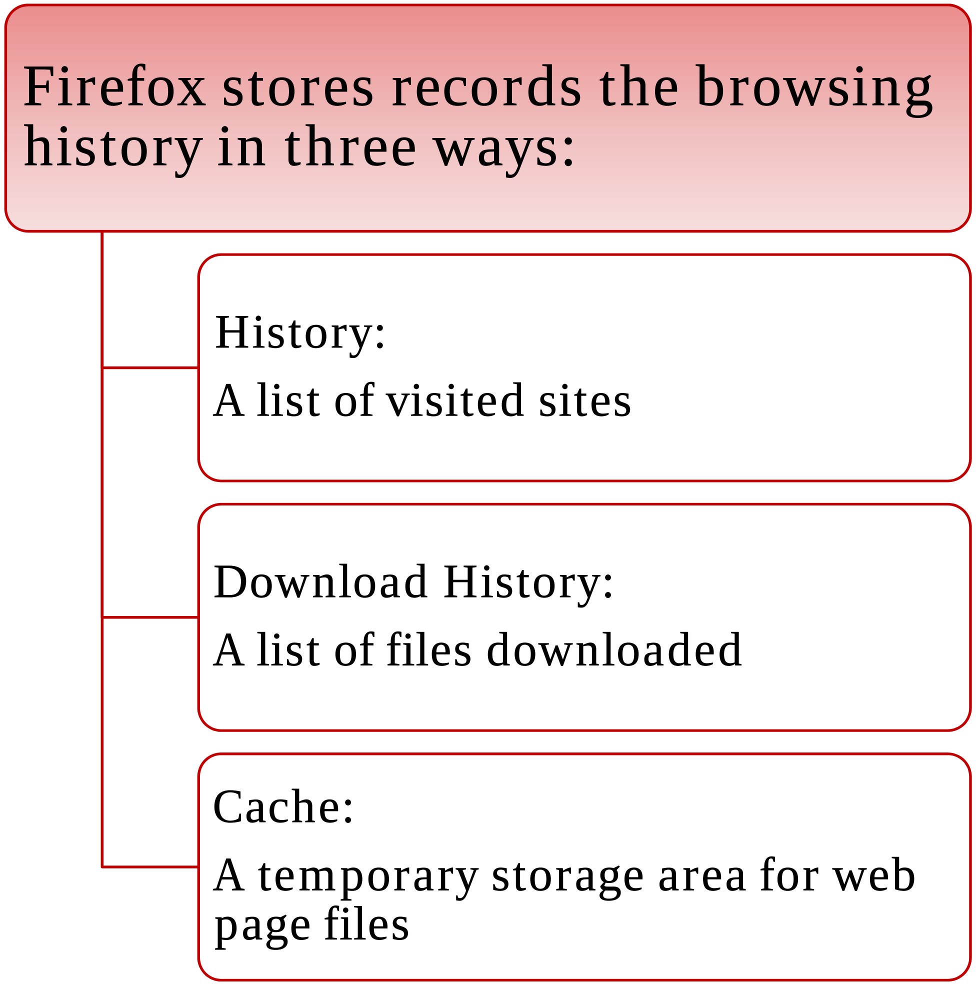
To prevent Firefox from saving any sort of form data in the future, uncheck "Save information I enter in web page forms and the Search Bar"

To prevent Firefox from saving any login credentials, uncheck "Remember Passwords"

Password Manager allows for fine-grained management of passwords

Password Manager allows to view any passwords that are previously saved by Firefox

Cleaning Up Browsing History



Firefox stores records the browsing history in three ways:

History:

A list of visited sites

Download History:

A list of files downloaded

Cache:

A temporary storage area for web page files

Cookies

Cookies are little pieces of information that are left on computer by web sites

Cookies have legitimate uses

Message boards use them so that a forum member does not have to log in every single time he/she visits

Merchant sites use cookies to keep track of what is being added to shopping carts

Cookies can also store a database session or some other piece of information that allows the web site to know what has transpired previously

"For the originating web site only" feature should probably be turned on, this will block web bugs from setting cookies and will allay many privacy concerns

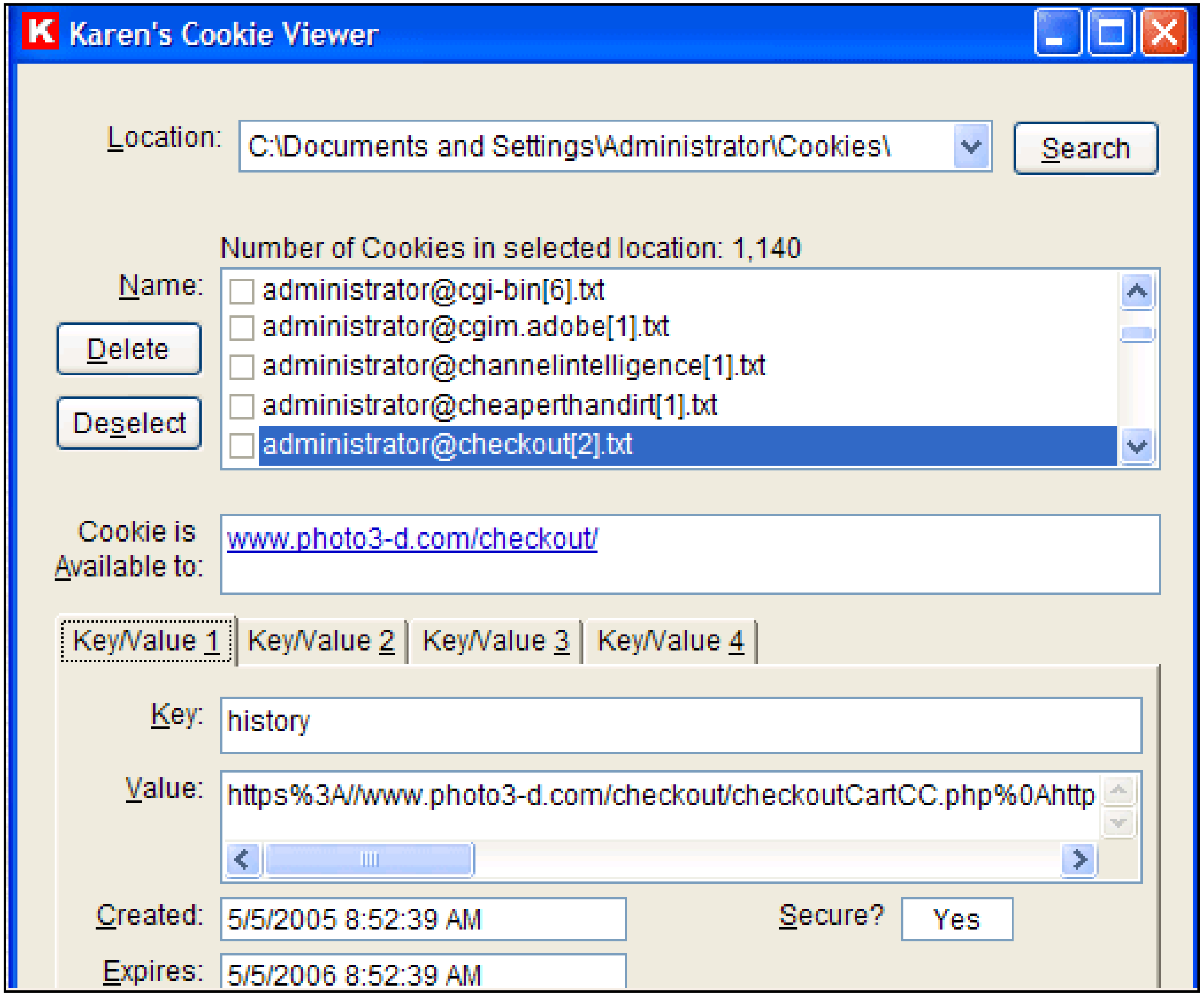
Internet History Viewer: Cookie Viewer

Cookie Viewer discovers the information that web sites store on users computer

It automatically scans your computer, looking for "cookies" created by Microsoft's Internet Explorer, Netscape's Navigator, and Mozilla Project's FireFox web browsers

It can also delete any unwanted cookies stored by these browsers

Cookie Viewer: Screenshot



Location: C:\Documents and Settings\Administrator\Cookies\

Number of Cookies in selected location: 1,140

Name:

- □ administrator@cgi-bin[6].txt
- □ administrator@cgim.adobe[1].txt
- □ administrator@channelintelligence[1].txt
- □ administrator@cheaperthandirt[1].txt
- □ administrator@checkout[2].txt

Cookie is Available to: www.photo3-d.com/checkout/

Key: history

Value: https%3A//www.photo3-d.com/checkout/checkoutCartCC.php%0Ahttp

Created: 5/5/2005 8:52:39 AM

Secure? Yes

Expires: 5/5/2006 8:52:39 AM

Firefox Security

Blocking Cookies Options

Firefox can flush cookies every time the browser closes down, or users can set the date on which they want the cookies to expire

Like JavaScript, cookies can be disabled entirely but many sites require cookies to function properly

It is easy enough to set few sites as exceptions

This involves low-maintenance and is less intrusive than addressing each individual cookie specifically

Tools For Cleaning Unwanted Cookies

There is a built-in tool for cookie removal in Firefox

There is a problem to clear out some cookies and save some others

The sites for which the cookies are to be saved must be highlighted

"Don't allow sites that set removed cookies to set future cookies" must be selected before clearing cookies

CookieCuller is a modified version of the Cookie Manager built into the Firefox browser

Tool: CookieCuller

CookieCuller protects the wanted cookies and quickly delete the unwanted

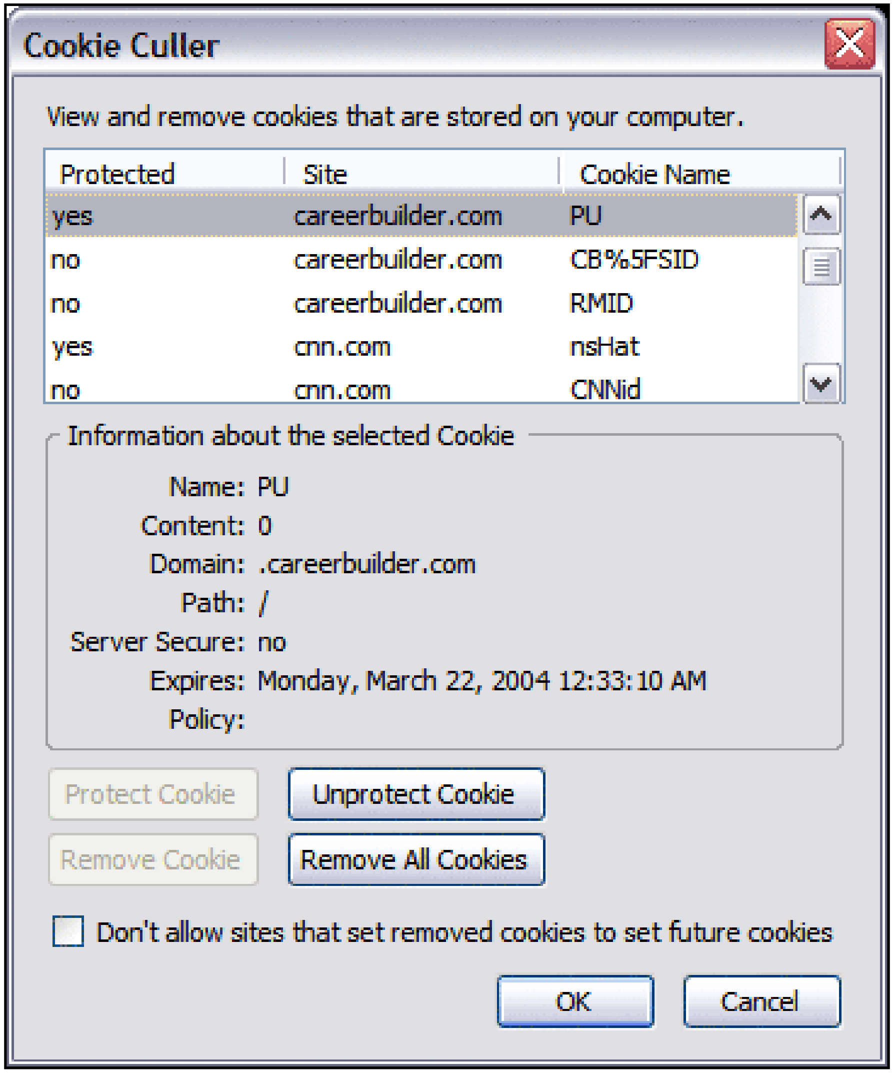
Gives quick access to the CookieCuller dialog using a custom toolbar button

Optionally deletes unprotected cookies on browser startup

Right Click on any toolbar icon and select Customize

Drag the CookieCuller icon to a position on the toolbar where it needs to be placed

CookieCuller: Screenshot



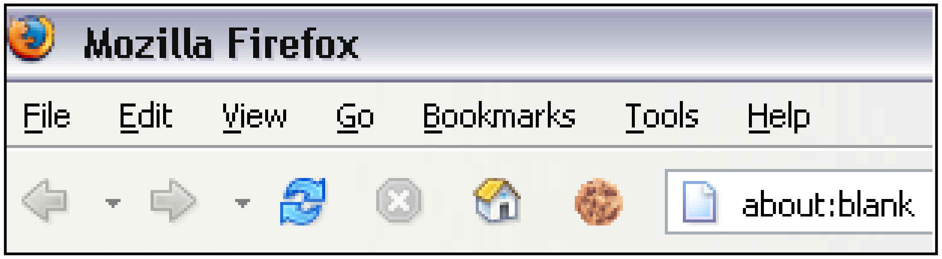
View and remove cookies that are stored on your computer.

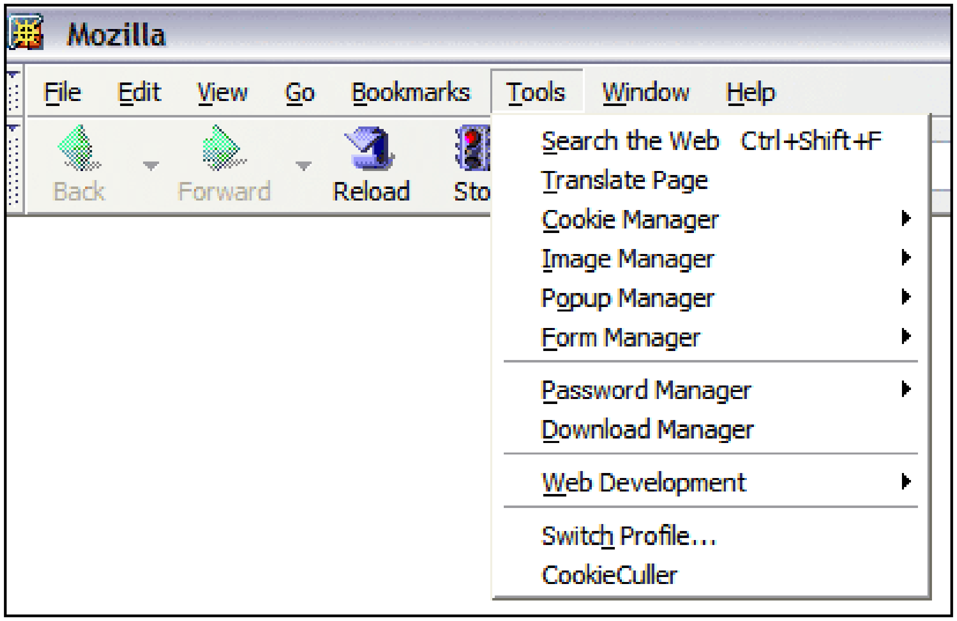
Protected	Site	Cookie Name
yes	careerbuilder.com	PU
no	careerbuilder.com	CB%5FSID
no	careerbuilder.com	RMID
yes	cnn.com	nsHat
no	cnn.com	CNNid

Information about the selected Cookie

Name: PU
Content: 0
Domain: .careerbuilder.com
Path: /
Server Secure: no
Expires: Monday, March 22, 2004 12:33:10 AM
Policy:

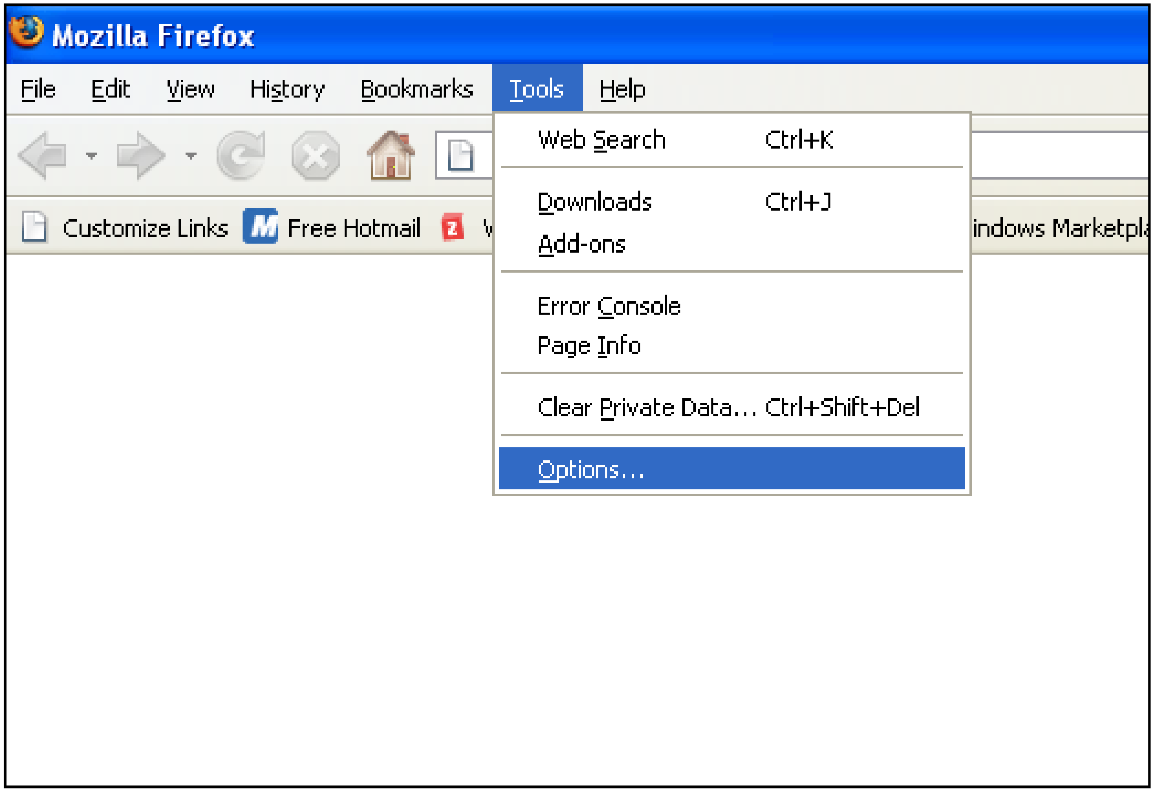
□ Don't allow sites that set removed cookies to set future cookies





Getting Started

To edit the settings for Mozilla Firefox, select Tools, then Options

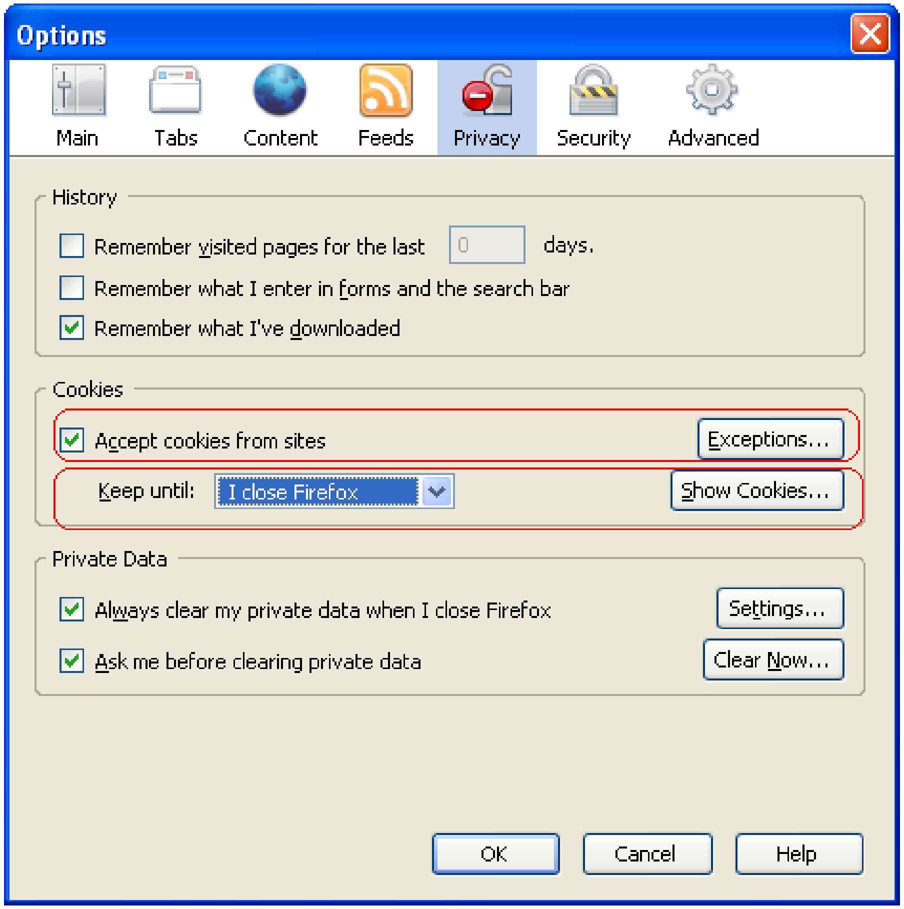

Mozilla Firefox
File Edit View History Bookmarks Tools Help
Customize Links Free Hotmail
indows Marketpl
Web Search Ctrl+K
Downloads Ctrl+J
Add-ons
Error Console
Page Info
Clear Private Data... Ctrl+Shift+Del
Options...

Privacy Settings

Under privacy section there is an option for setting cookies

Cookies can be accepted for few sites and rest will be left by mentioning sites address in Exceptions

Cookies can be kept un till they expire or browser is running



History

☐ Remember visited pages for the last 0 days.

☐ Remember what I enter in forms and the search bar

☑ Remember what I've downloaded

Cookies

☑ Accept cookies from sites

Keep until: I close Firefox

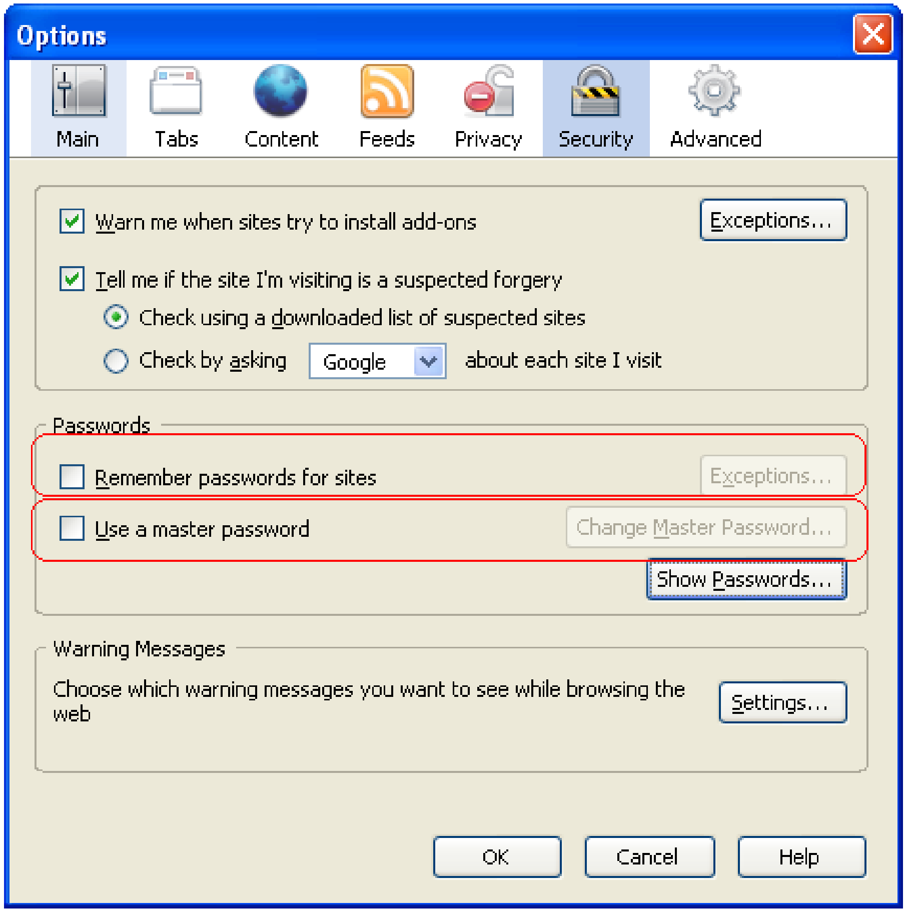
Private Data

☑ Always clear my private data when I close Firefox

☑ Ask me before clearing private data

C|EH™ Certified Ethical Hacker

Security Settings



☑ Warn me when sites try to install add-ons

☑ Tell me if the site I'm visiting is a suspected forgery

● Check using a downloaded list of suspected sites

○ Check by asking Google about each site I visit

Passwords

□ Remember passwords for sites

□ Use a master password

Warning Messages

Choose which warning messages you want to see while browsing the web

Under security settings passwords settings can be changed

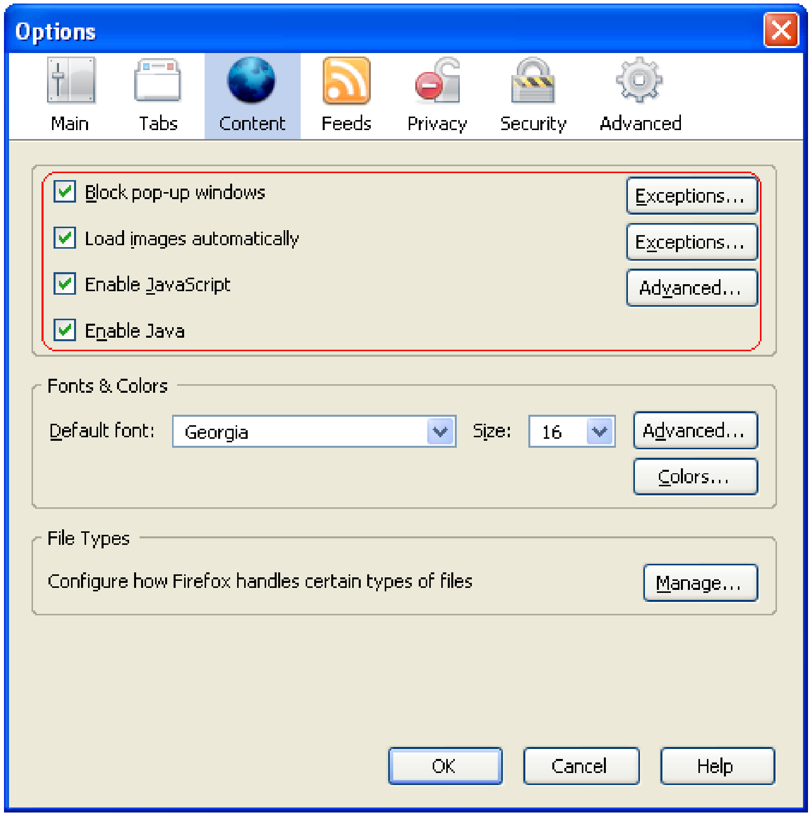
Passwords can be remembered by browser with some exceptions

Master password is also set to browser in order to manage passwords

Content Settings

Pop ups, images and java script can be enabled and disabled under content tab in options

Pop ups and images can be enabled for few sites with exceptions



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

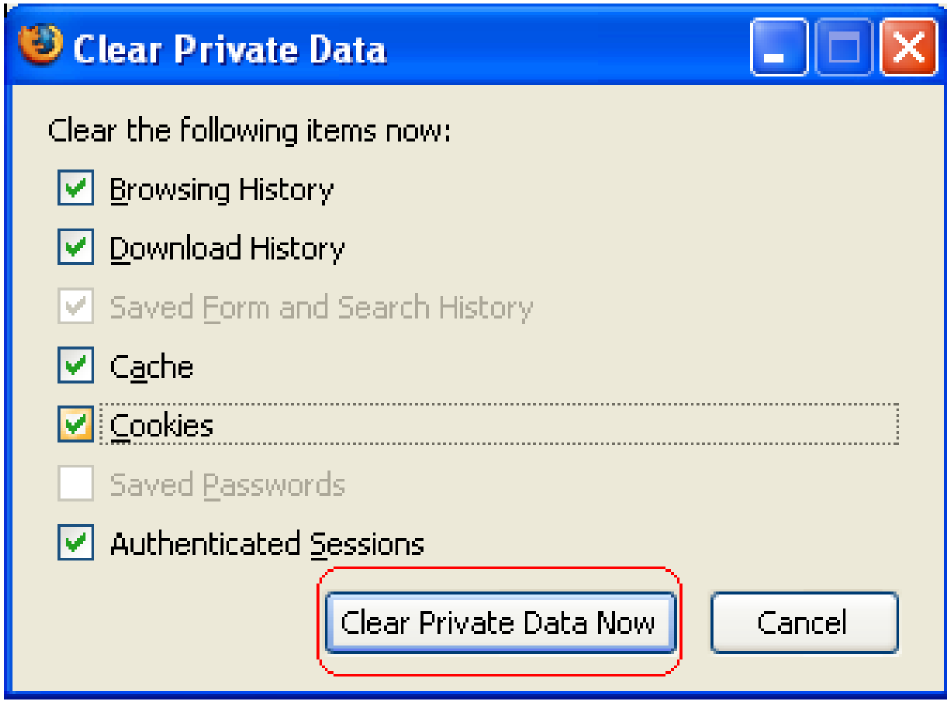
Fonts & Colors

Default font: Georgia Size: 16

File Types

Configure how Firefox handles certain types of files

Clear Private Data



Clear Private Data

Clear the following items now:

☑ Browsing History

☑ Download History

☑ Saved Form and Search History

☑ Cache

☑ Cookies

□ Saved Passwords

☑ Authenticated Sessions

Clear private data option is selected under tools tab in menu bar

It will clear all the private data including browsing history, cookies, cache, passwords and all

Mozilla Firefox Security Features

Firefox includes built-in controls to block pop-ups

Firefox does not support VBScript and ActiveX Controls, which are often the source of attacks and vulnerabilities within IE

Way of handling secure Web sites, such as e-commerce or online banking sites

- When visiting a secure site, Firefox highlights the address bar's URL in yellow and shows the Lock icon
- If you click the Lock icon, you can review the site's security information and decide whether to continue
- The domain name of the site you are visiting is also listed in the right-hand corner of secure windows, so you know the true source of every page
- A criminal hacker might be able to spoof the location bar address, but he/she will not be able to spoof this secondary address display

Adblock extension blocks flash advertising from Web sites

Hacking Internet Explorer

Redirection Information Disclosure Vulnerability

The vulnerability is caused due to an error in the handling of redirections for URLs with the "mhtml:" URI handler

This can be exploited to access documents served from another web site

Attacker can disclose potentially sensitive information using this vulnerability

Solution:

- Apply patches

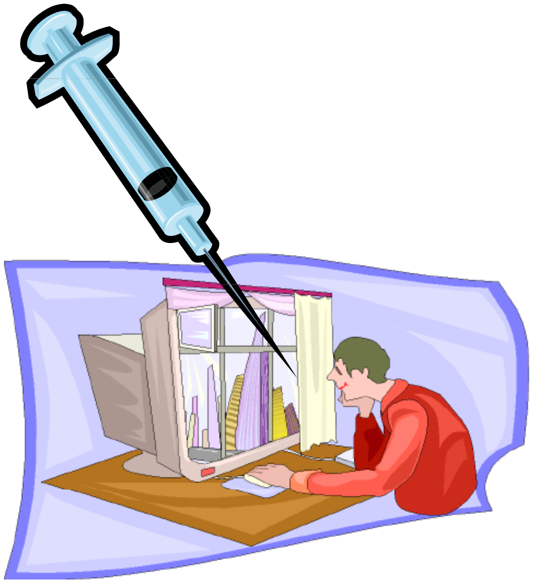
Window Injection Vulnerability

This vulnerability can be exploited by an attacker to spoof the content of websites

The problem is that a website can inject content into another site's window if the target name of the window is known

Solution:

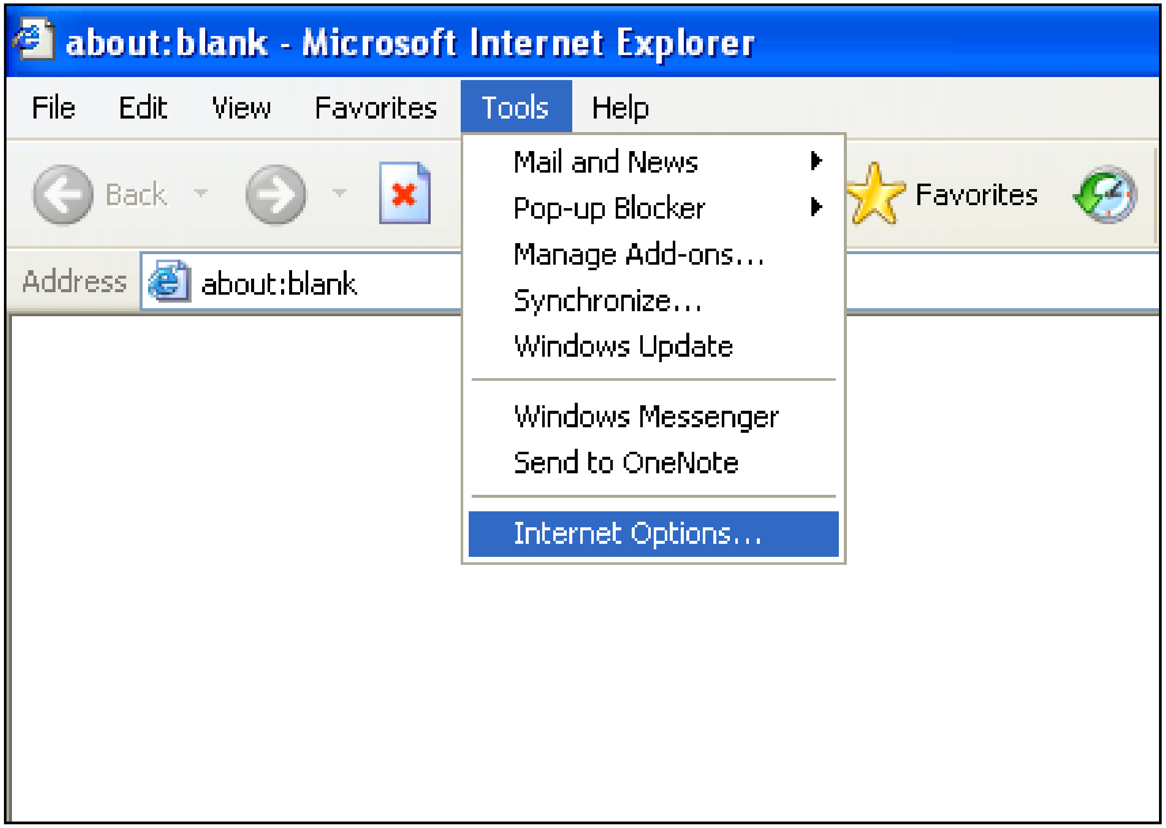
- Do not browse untrusted sites while browsing trusted sites



Internet Explorer Security

Getting Started

To get started, Tools > Internet Options



Security Zones

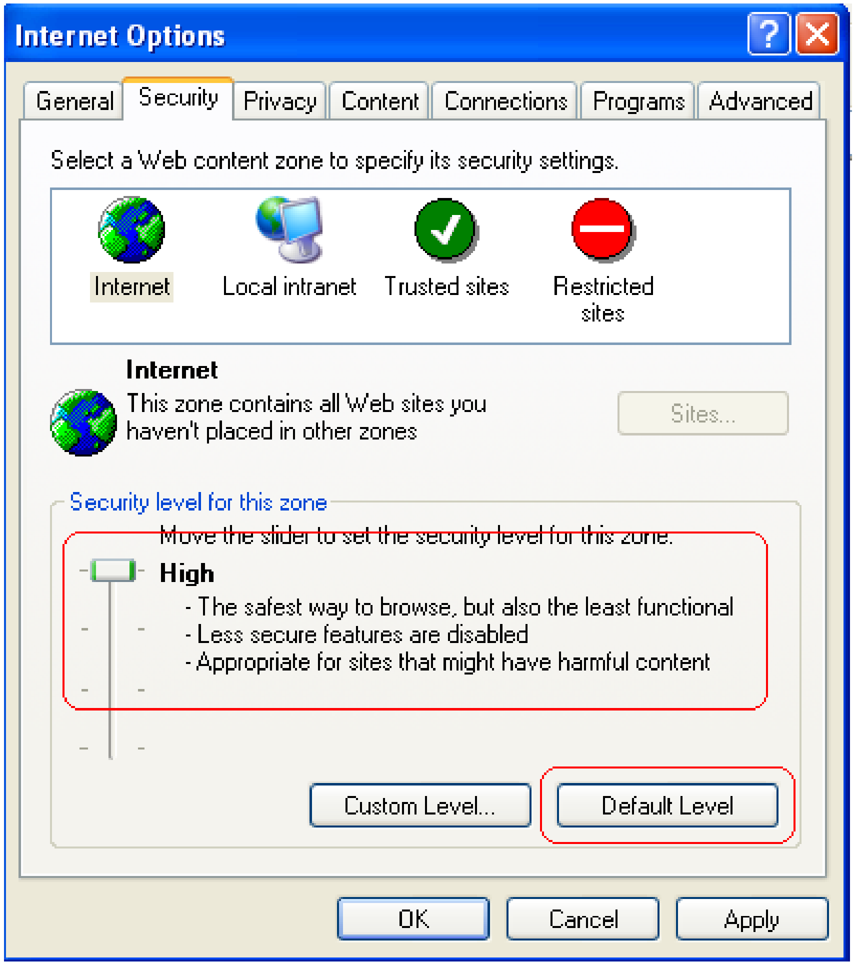
Click on the Security tab that shows the various IE security zones

Internet zone is where all sites initially start out

High security setting should be applied for Internet zone

By selecting the High security setting, several features including ActiveX, Active scripting, and Java will be disabled

With these features disabled, the browser will be more secure



Select a Web content zone to specify its security settings.

Internet

This zone contains all Web sites you haven't placed in other zones

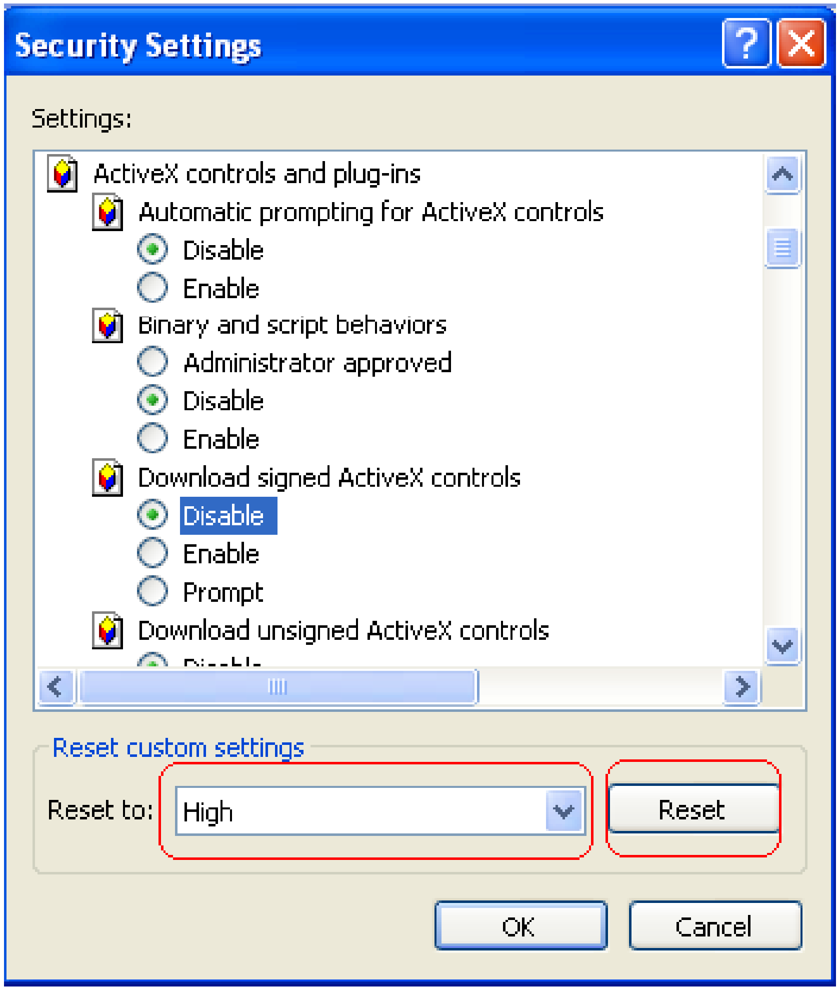
Security level for this zone

Move the slider to set the security level for this zone.

High

- The safest way to browse, but also the least functional
- Less secure features are disabled
- Appropriate for sites that might have harmful content

Custom Level



Security Settings

Settings:

- ActiveX controls and plug-ins
  - Automatic prompting for ActiveX controls
    - ● Disable
    - ○ Enable
  - Binary and script behaviors
    - ○ Administrator approved
    - ● Disable
    - ○ Enable
  - Download signed ActiveX controls
    - ● Disable
    - ○ Enable
    - ○ Prompt
  - Download unsigned ActiveX controls

Clicking on the Custom Level button displays more granular control over what features are allowed in the zone

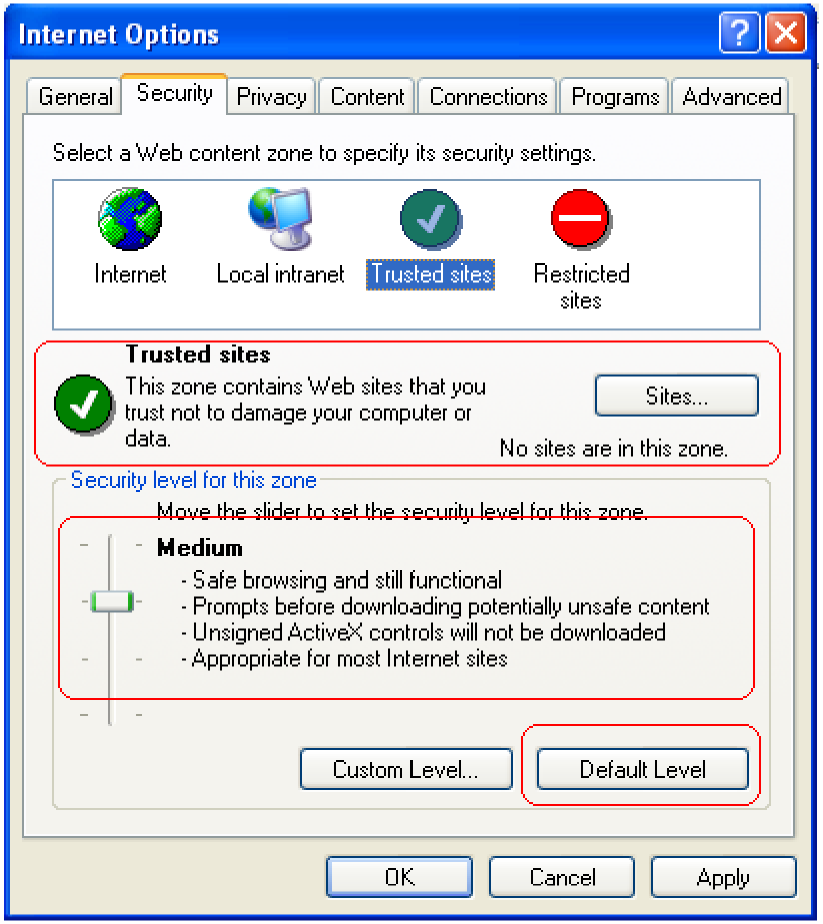
Default values for the High security setting can be selected by choosing High and clicking the Reset button to apply the changes

Trusted Sites Zone

Trusted sites are a security zone for web sites which are securely designed and contain trustworthy content

They can be added by clicking sites button

It is recommended to set the security level for the Trusted sites zone to Medium when Internet zone is set to high



Select a Web content zone to specify its security settings.

Trusted sites

This zone contains Web sites that you trust not to damage your computer or data.

No sites are in this zone.

Security level for this zone

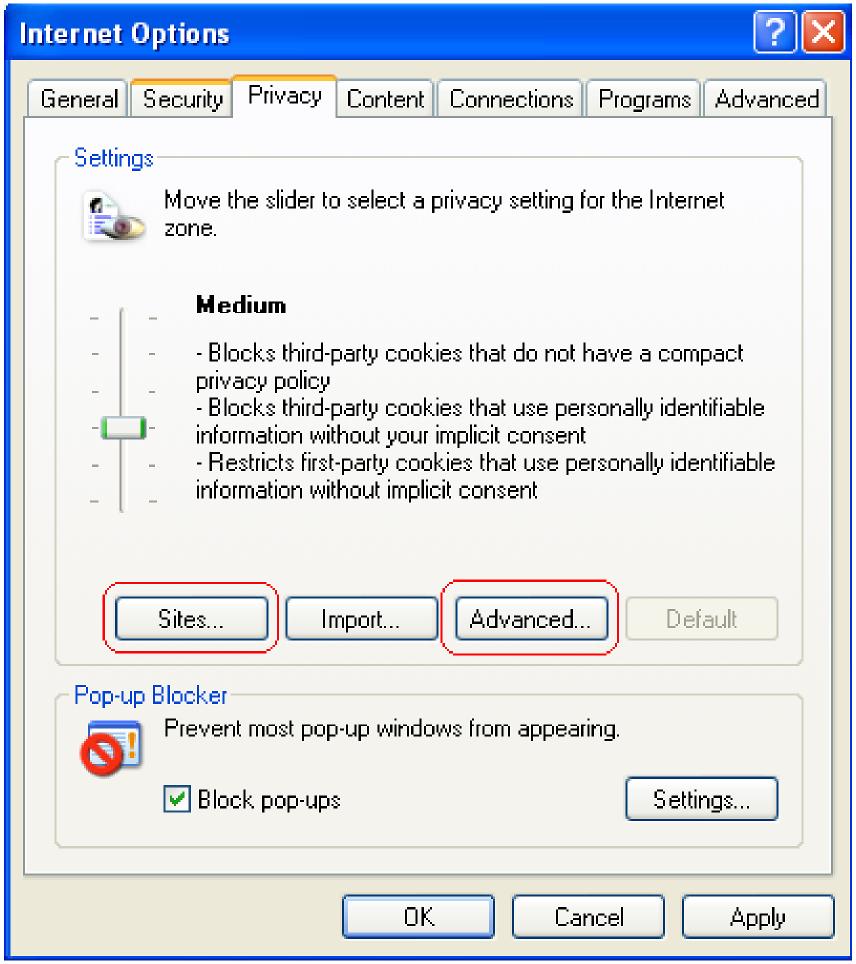
Move the slider to set the security level for this zone.

Medium

- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

EC-Council

Privacy



Settings

Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Pop-up Blocker

Prevent most pop-up windows from appearing.

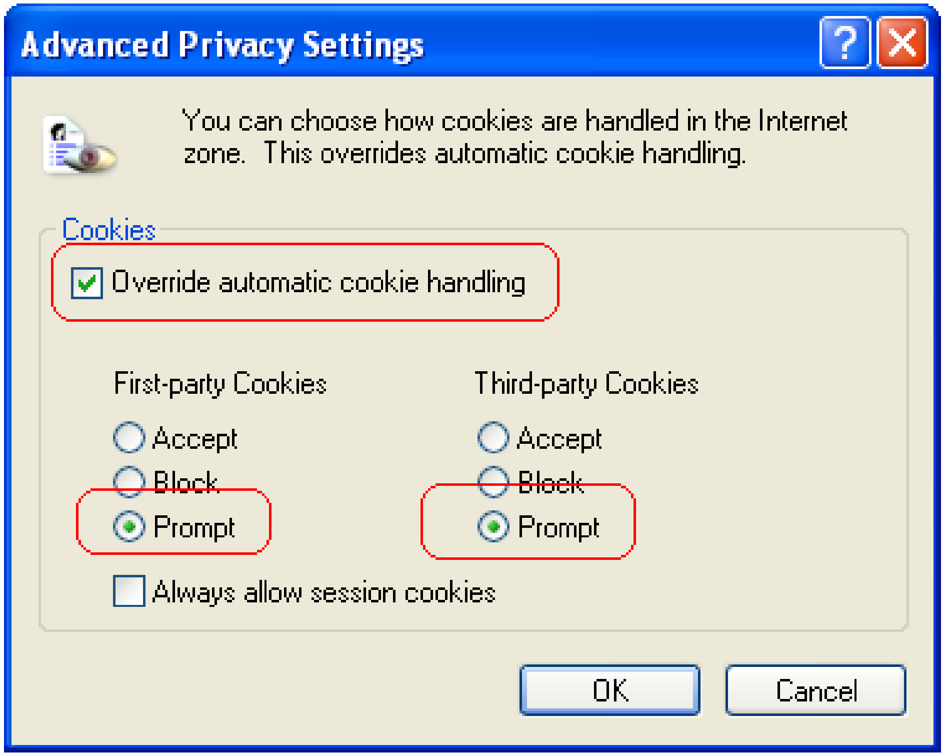
☑ Block pop-ups

In the Privacy tab, settings for configuring cookies are made

It is recommended to select the Advanced button and select Override automatic cookie handling

Overwrite Automatic Cookie Handling

Select Prompt for both first and third-party cookies; this will prompt each time a site tries to place a cookie on computer



You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

Cookies

☑ Override automatic cookie handling

First-party Cookies

○ Accept
○ Block
● Prompt

Third-party Cookies

○ Accept
○ Block
● Prompt

□ Always allow session cookies

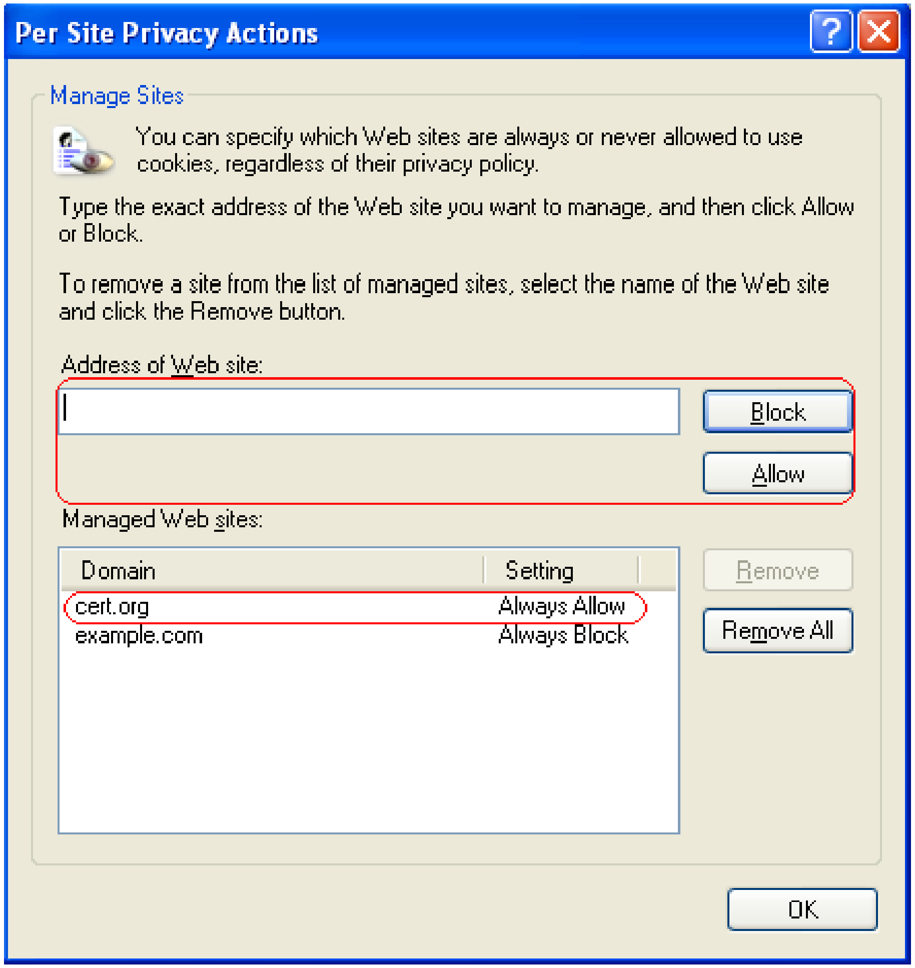
Per Site Privacy Actions

Cookie settings for specific sites can be managed by selecting the "Sites" button

Sites can be added and removed

Bottom section of this window will specify the domain of the site

It specifies action to be taken when that site wants to place a cookie on that computer



You can specify which Web sites are always or never allowed to use cookies, regardless of their privacy policy.

Type the exact address of the Web site you want to manage, and then click Allow or Block.

To remove a site from the list of managed sites, select the name of the Web site and click the Remove button.

Address of Web site:

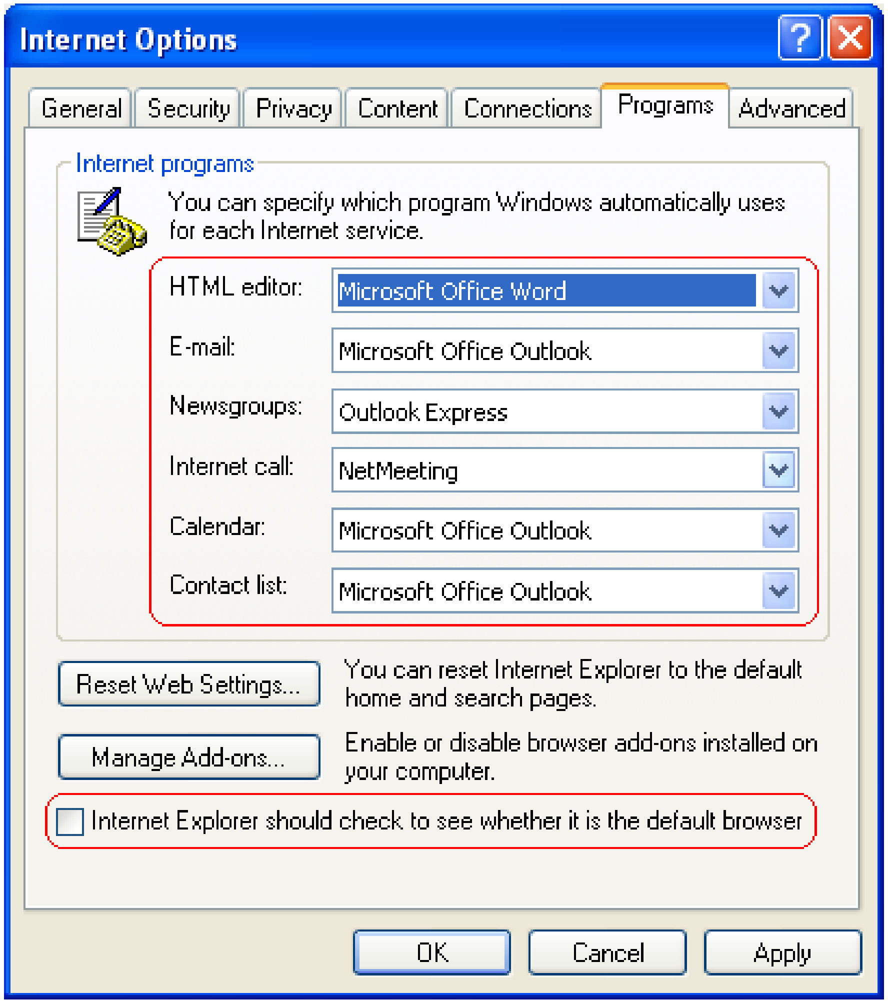
Managed Web sites:

Domain	Setting
cert.org	Always Allow
example.com	Always Block

Specify Default Applications

Under the Programs tab, speciation can be made for default applications for viewing Web sites, e-mails, and other network related tasks

Internet Explorer can prevent showing the message asking to be the default Web browser


Internet Options

Internet programs

You can specify which program Windows automatically uses for each Internet service.

HTML editor: Microsoft Office Word

E-mail: Microsoft Office Outlook

Newsgroups: Outlook Express

Internet call: NetMeeting

Calendar: Microsoft Office Outlook

Contact list: Microsoft Office Outlook

Reset Web Settings... You can reset Internet Explorer to the default home and search pages.

Manage Add-ons... Enable or disable browser add-ons installed on your computer.

□ Internet Explorer should check to see whether it is the default browser

Internet Explorer Security Features

1. • Default protection from potentially dangerous Active X controls
2. • Per-zone control of Active X opt-in
3. • Site and zone locking for Active X controls
4. • Protection against phishing
5. • Cross-domain security
6. • Locked down security zones
7. • Better SSL/TLS notification and digital certificate info
8. • Privacy protection features
9. • Has Address bars
10. • International character alert

Hacking Opera

JavaScript Invalid Pointer Vulnerability

A vulnerability has been reported in Opera, which potentially can be exploited by malicious people to compromise a users system

It is caused due to an unspecified error when processing JavaScript code and can result in a virtual function call using an invalid pointer

This can be exploited to execute arbitrary code by tricking the user into visiting a malicious website

BitTorrent Header Parsing Vulnerability

The vulnerability is caused due to Opera using already freed memory when parsing BitTorrent headers and can lead to an invalid object pointer being dereferenced

This can be exploited to execute arbitrary code, when the user is tricked into clicking on a specially crafted BitTorrent file and then removes it via a right-click from the download pane

Torrent File Handling Buffer Overflow Vulnerability

The vulnerability is caused due to a boundary error in the handling of certain keys in torrent files

It can be exploited to cause a stack-based buffer overflow when a user right-clicks a malicious torrent entry in the transfer manager

Successful exploitation allows execution of arbitrary code

Certified Ethical Hacker

Security Features of Opera

Security and Privacy Features

Encryption

- Opera supports Secure Socket Layer (SSL) versions 2 and 3, and TLS and offers automatic 256-bit encryption

Cookie control

- Opera gives detailed control of what cookies to accept and reject, such as allowing for different set-ups for different servers

Fraud protection

- Operas advanced fraud protection protects user against web sites that try to steal personal information

Security and Privacy Features (cont'd)

Delete private data

- Opera can be configured to clear the history and cache when exiting, to protect your privacy. Any kind of private data can easily be erased

Security bar

- Opera displays security information inside the address bar. By clicking on the yellow security bar user can get access to more information about the validity of the certificate

Hacking Safari

Safari Browser Vulnerability

The Safari browser automatically opens "safe" files such as movies, pictures, sounds, PDFs, text files, disk images and other archived files

It is possible for malicious files disguised as these safe files to automatically download, open, and infect Mac

To switch off the Open "safe" files after downloading:

- Open the Safari browser
- Click on Safari – Preferences – General
- Click to remove the checkmark next to Open "safe" files after downloading

iPhone Safari Browser Memory Exhaustion Remote Dos Vulnerability

This vulnerability target v1.1.2 firmware handsets

Once a malicious website is accessed, it will generate a memory hog in iPhone's Safari browser and freezes the iPhone

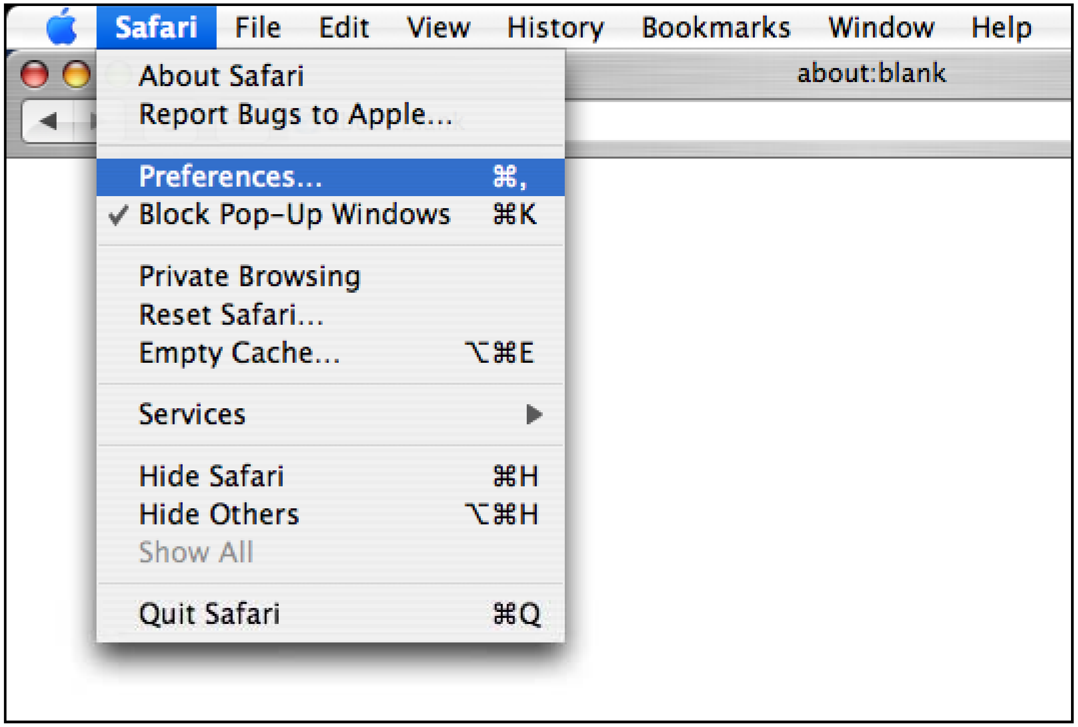
Securing Safari

EC-Council

Getting started

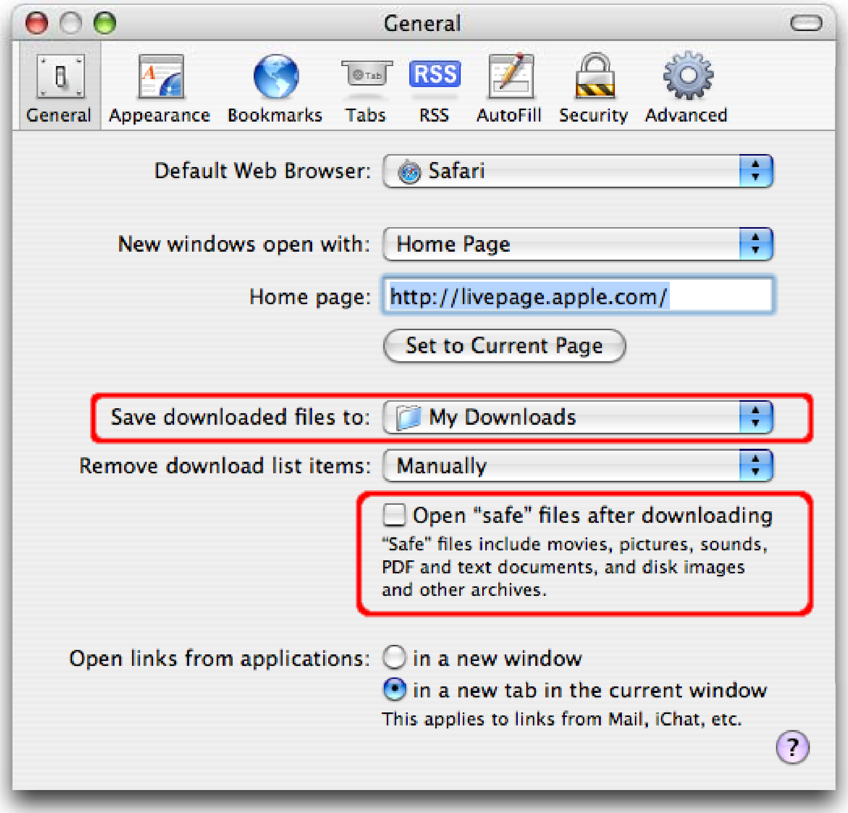
In order to change settings, select Safari and then select Preferences

Pop up windows also can be blocked using the setting “Block Pop-up Windows”



Preferences

General tab under Preferences has many options Save downloaded files to: and Open “safe” files after downloading, but it is not recommended to select this option



Default Web Browser: Safari

New windows open with: Home Page

Home page: http://livepage.apple.com/

Set to Current Page

Save downloaded files to: My Downloads

Remove download list items: Manually

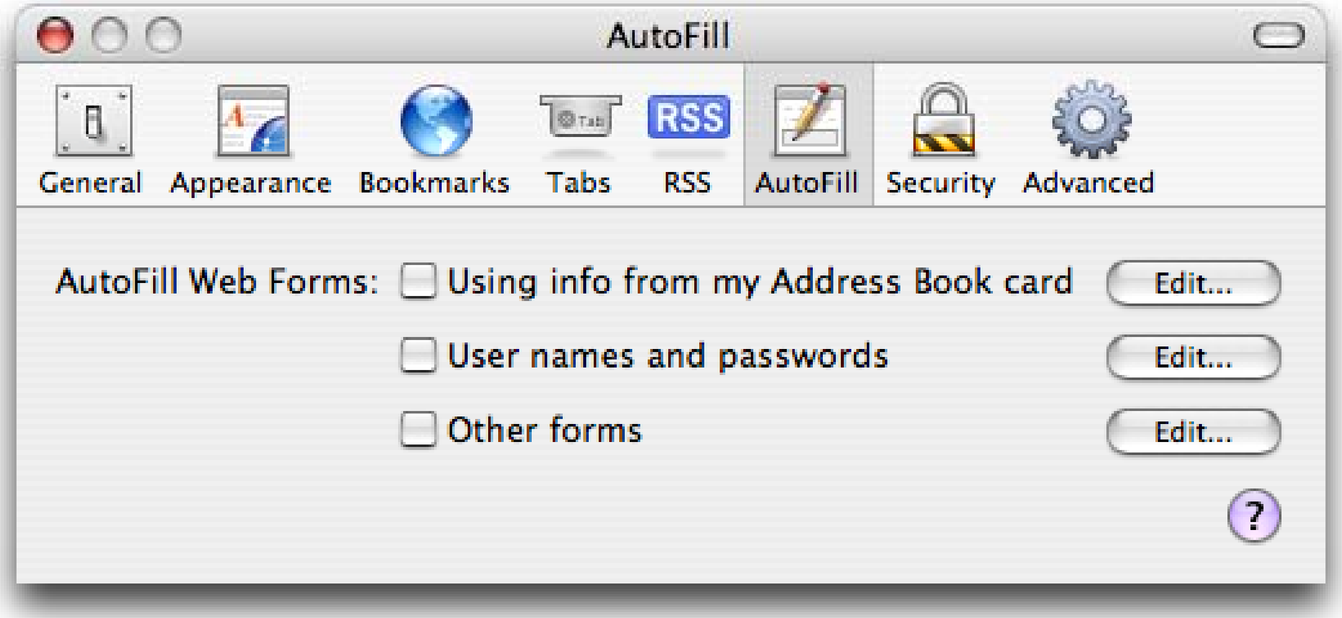
□ Open "safe" files after downloading
"Safe" files include movies, pictures, sounds, PDF and text documents, and disk images and other archives.

Open links from applications: ○ in a new window
● in a new tab in the current window
This applies to links from Mail, iChat, etc.

AutoFill

AutoFill is an another option under Preferences menu

What types of forms browser needs to fill in automatically should be selected in this option



AutoFill Web Forms: □ Using info from my Address Book card [Edit...]

□ User names and passwords [Edit...]

□ Other forms [Edit...]

CEH™ Certified Ethical Hacker

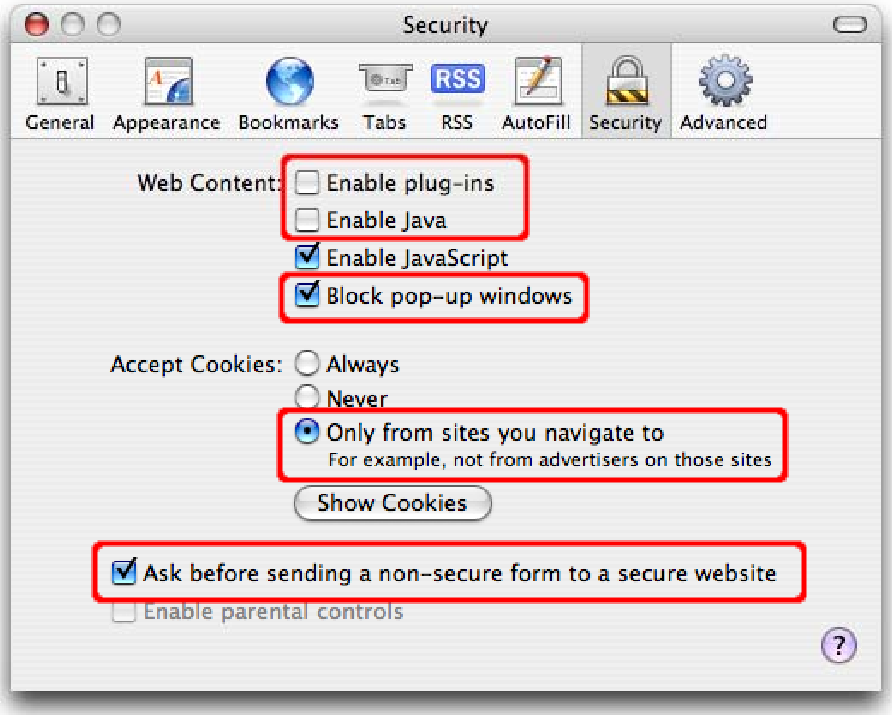
Security Features

Under security tab web content and cookie options can be changed

The Web Content section permits to enable or disable various forms of scripting and active content

Cookies should be accepted from few sites only

It is recommended to select the option “Ask before a non-secure form to a secure website”



Web Content: □ Enable plug-ins
□ Enable Java
☑ Enable JavaScript
☑ Block pop-up windows

Accept Cookies: ○ Always
○ Never
● Only from sites you navigate to
For example, not from advertisers on those sites

☑ Ask before sending a non-secure form to a secure website
□ Enable parental controls

Hacking Netscape

C|EH™ Certified Ethical Hacker

Netscape Navigator Improperly Validates SSL Sessions

This vulnerability includes information CERT/CC would not ordinarily publish, including specific site names and exploit information

The flaw effectively disables one of the two basic SSL functionalities

Using this flaw, the attacker can make users send secret information (like credit card data and passwords) to his web server rather than the real one

Solution:

- Netscape has provided a Navigator Add-on called Personal Security Manager. Installation of PSM corrects this flaw

Netscape Navigator Security Vulnerability

This vulnerability may allow a Web site operator to retrieve known files from the hard disks of visiting users by mimicking the submission of a form

To access a file on the hard drive the Web site operator would need to know the exact name and location of the file

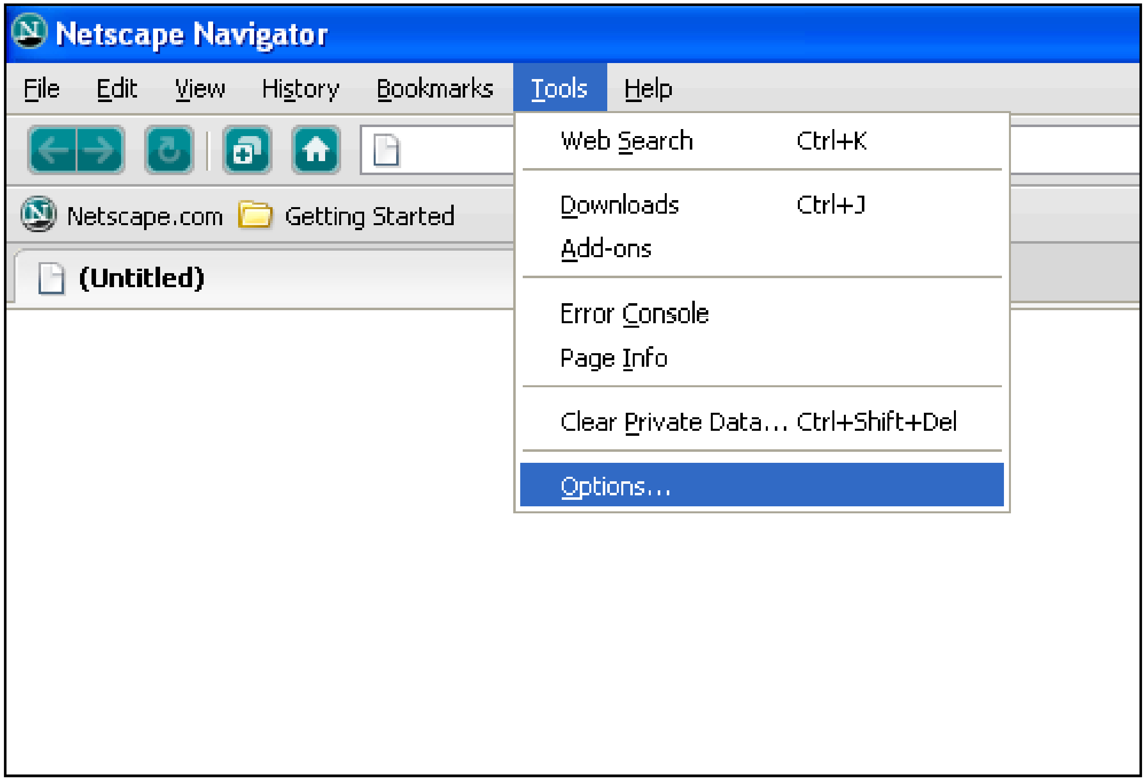
Solution:

- Security Advisor is opened by selecting the lock in the toolbar. “Sending Unencrypted Information to a Site" is selected under Navigator to enable that warning dialog box

Securing Netscape

Getting Started

To edit the security settings for Netscape, select Tools, then Options

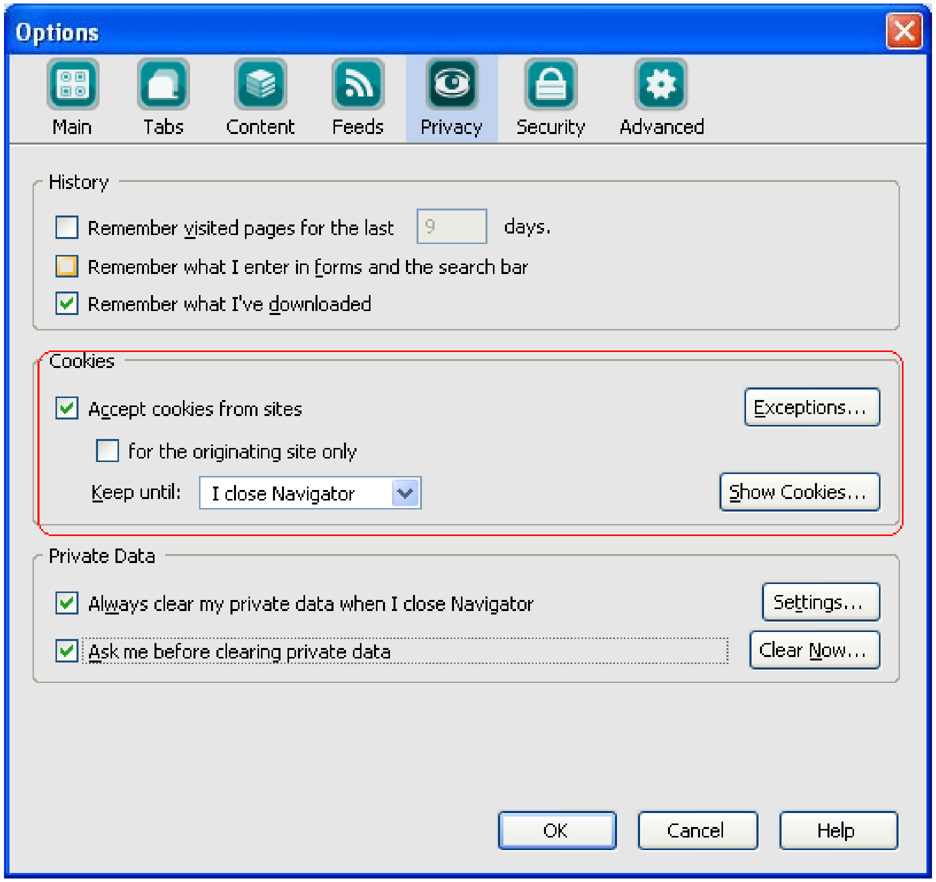


Privacy Settings

Under privacy section there is an option for setting cookies

Cookies can be accepted for few sites and rest will be left by mentioning sites address in Exceptions

Cookies can be kept un till they expire or browser is running



History

☐ Remember visited pages for the last 9 days.

☐ Remember what I enter in forms and the search bar

☑ Remember what I've downloaded

Cookies

☑ Accept cookies from sites

☐ for the originating site only

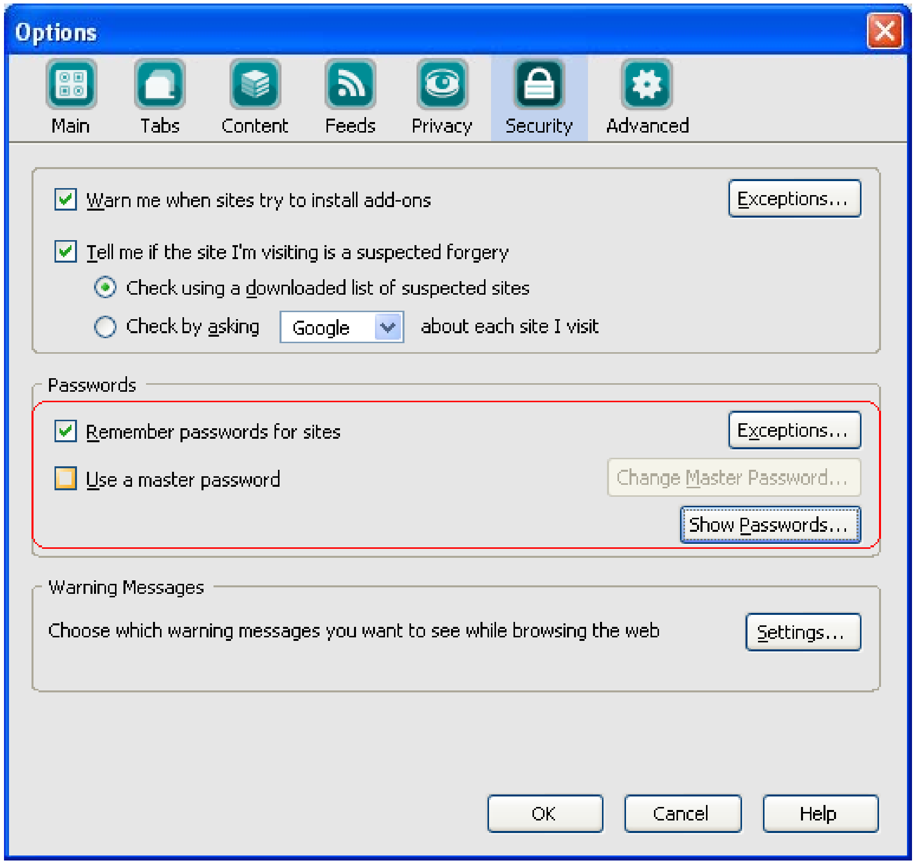
Keep until: I close Navigator

Private Data

☑ Always clear my private data when I close Navigator

☑ Ask me before clearing private data

Security Settings



Options

☑ Warn me when sites try to install add-ons [Exceptions...]

☑ Tell me if the site I'm visiting is a suspected forgery

● Check using a downloaded list of suspected sites

○ Check by asking [Google] about each site I visit

Passwords

☑ Remember passwords for sites [Exceptions...]

□ Use a master password [Change Master Password...]

[Show Passwords...]

Warning Messages

Choose which warning messages you want to see while browsing the web [Settings...]

Under security settings passwords settings can be changed

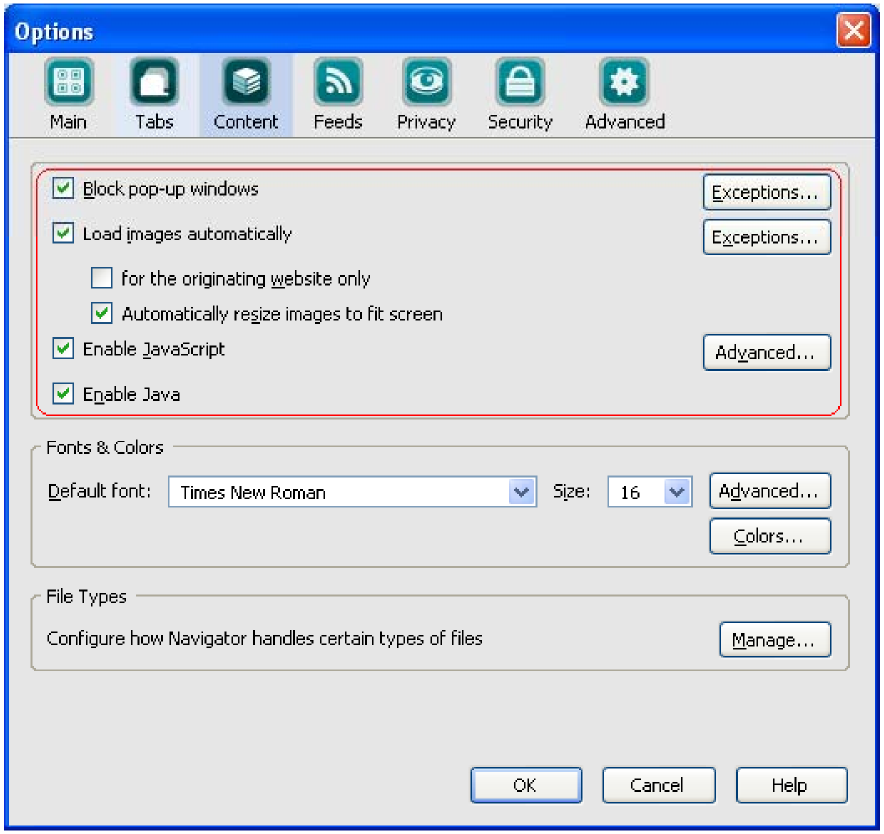
Passwords can be remembered by browser with some exceptions

Master password is also set to browser in order to manage passwords

Content Settings

Pop ups, images and java script can be enabled and disabled under content tab in options

Pop ups and images can be enabled for few sites with exceptions



☑ Block pop-up windows

☑ Load images automatically

□ for the originating website only

☑ Automatically resize images to fit screen

☑ Enable JavaScript

☑ Enable Java

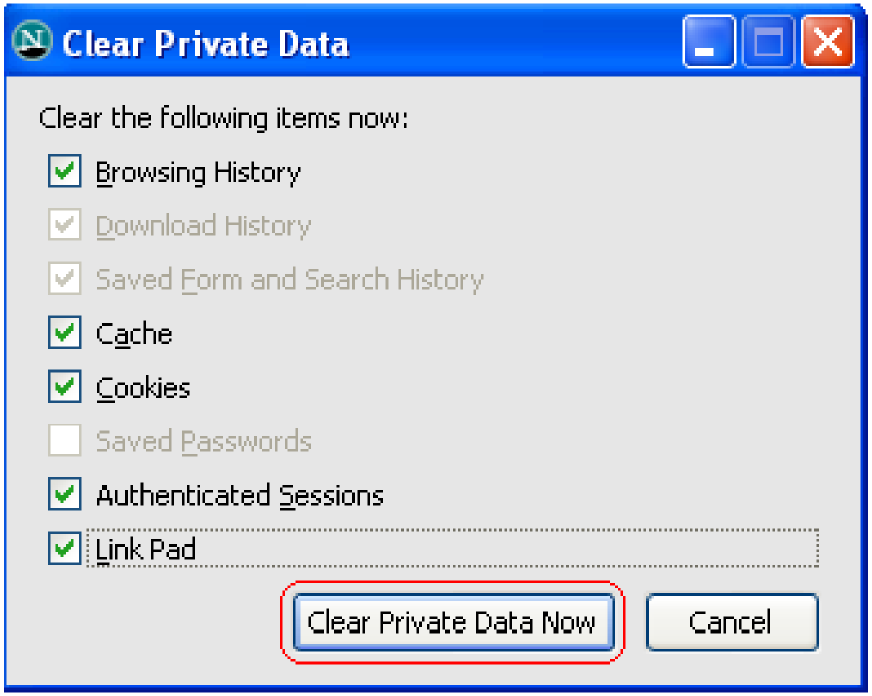
Fonts & Colors

Default font: Times New Roman Size: 16

File Types

Configure how Navigator handles certain types of files

Clear Private Data



Clear the following items now:

- ☑ Browsing History
- ☑ Download History
- ☑ Saved Form and Search History
- ☑ Cache
- ☑ Cookies
- ☐ Saved Passwords
- ☑ Authenticated Sessions
- ☑ Link Pad

Clear private data option is selected under tools tab in menu bar

It will clear all the private data including browsing history, cookies, cache, passwords and all

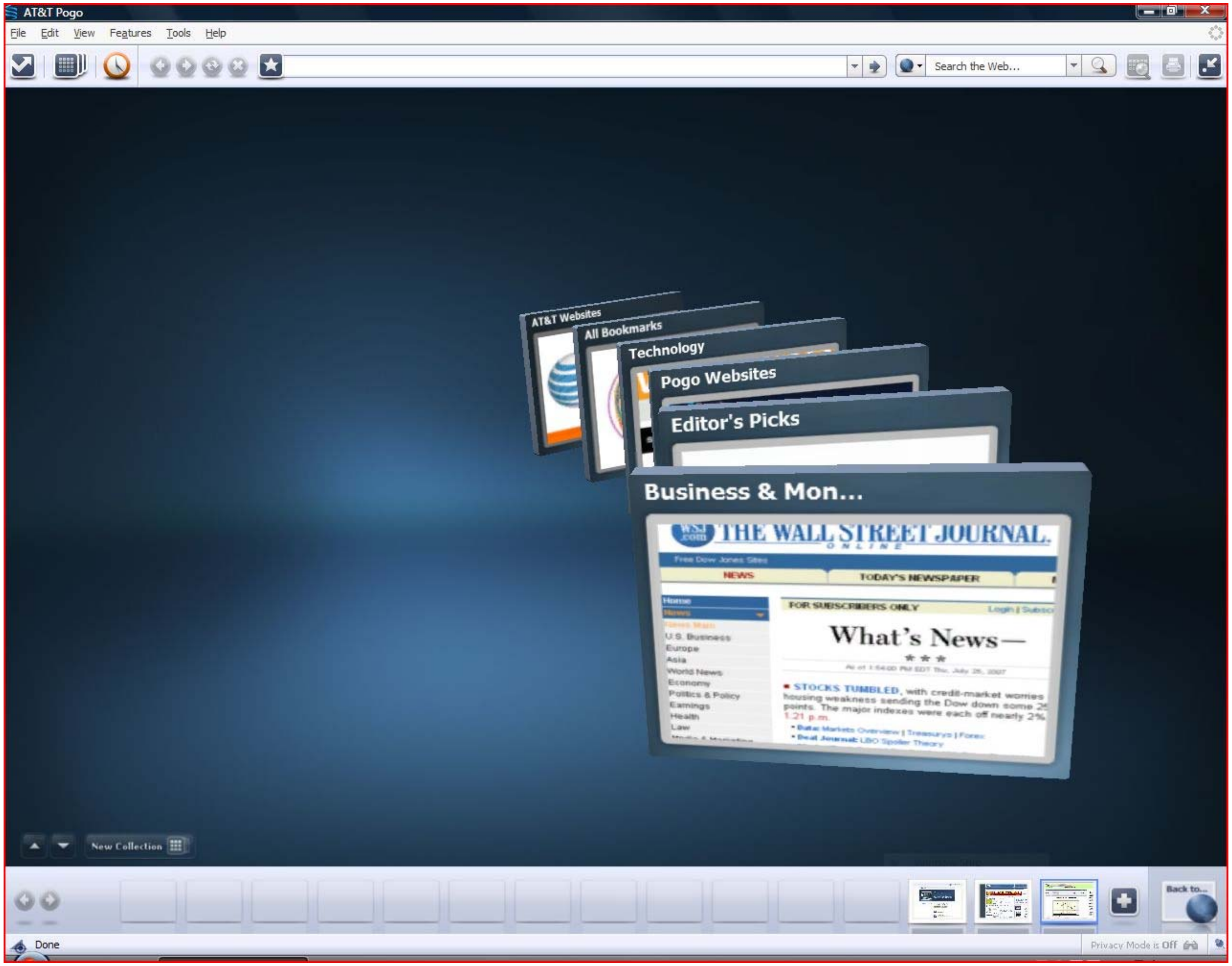
Pogo Browser

Pogo, a new 3D web browser, allows users to visually manage their online experience, offering a better UI while leveraging the Mozilla codebase for safe, secure and standardized browsing

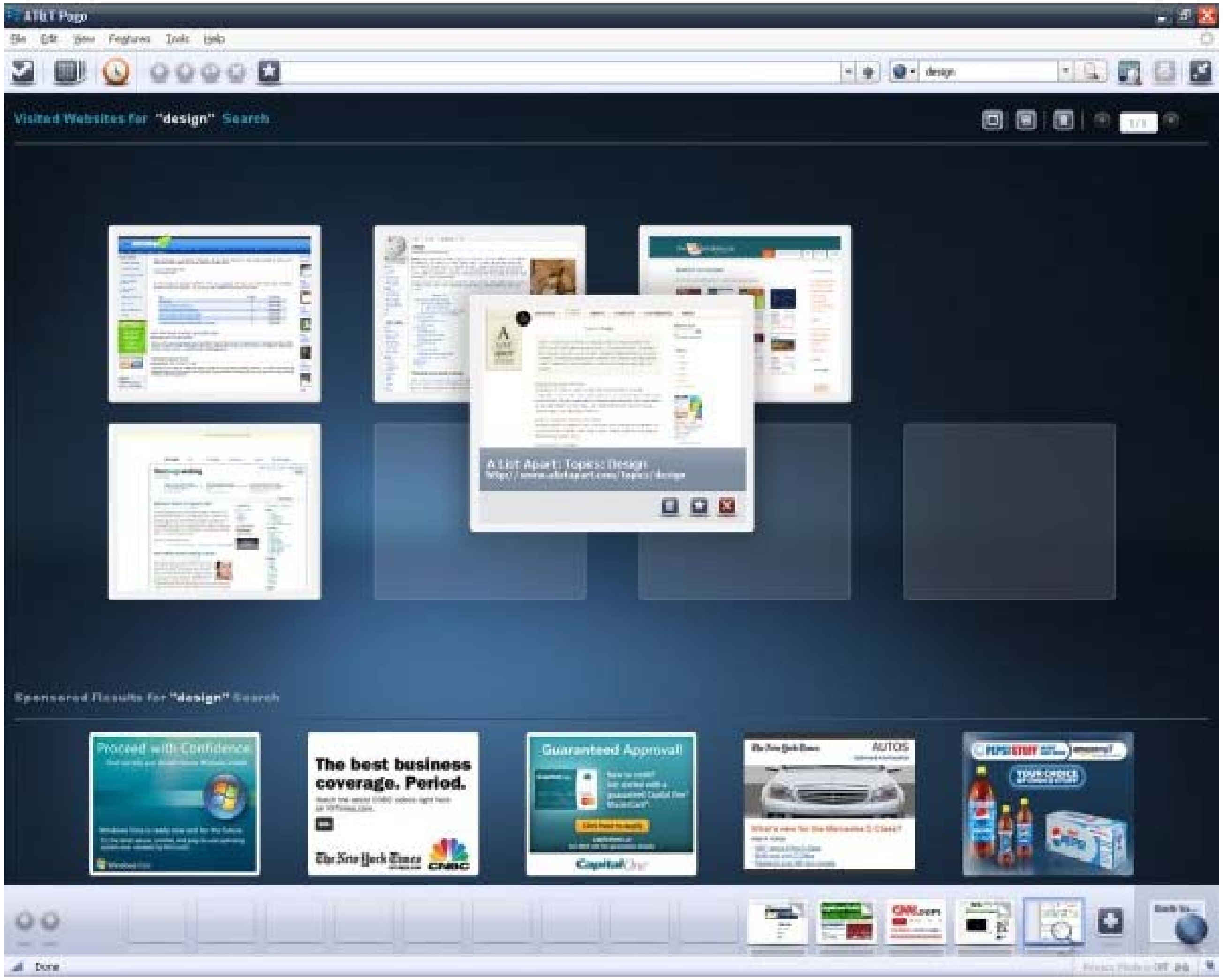
Pogo works like a regular browser, but it manages pages more visually

Instead of tabs, it has a scrollable strip on the bottom that shows a thumbnail image of each site you have visited during your session

Pogo Browser: Screenshot 1



Pogo Browser: Screenshot 2


AT&T Pogo
File Edit View Features Tools Help
design
Visited Websites for "design" Search
1/1
A List Apart: Topics: Design
http://www.alistapart.com/topics/design
Sponsored Results for "design" Search
Proceed with Confidence
The best business coverage. Period.
Guaranteed Approval!
AUTOS
Done

Summary

The browser requests the specific document (including its path statement) from the server computer

Firefox contains a password management vulnerability that can allow malicious Web sites to steal user passwords

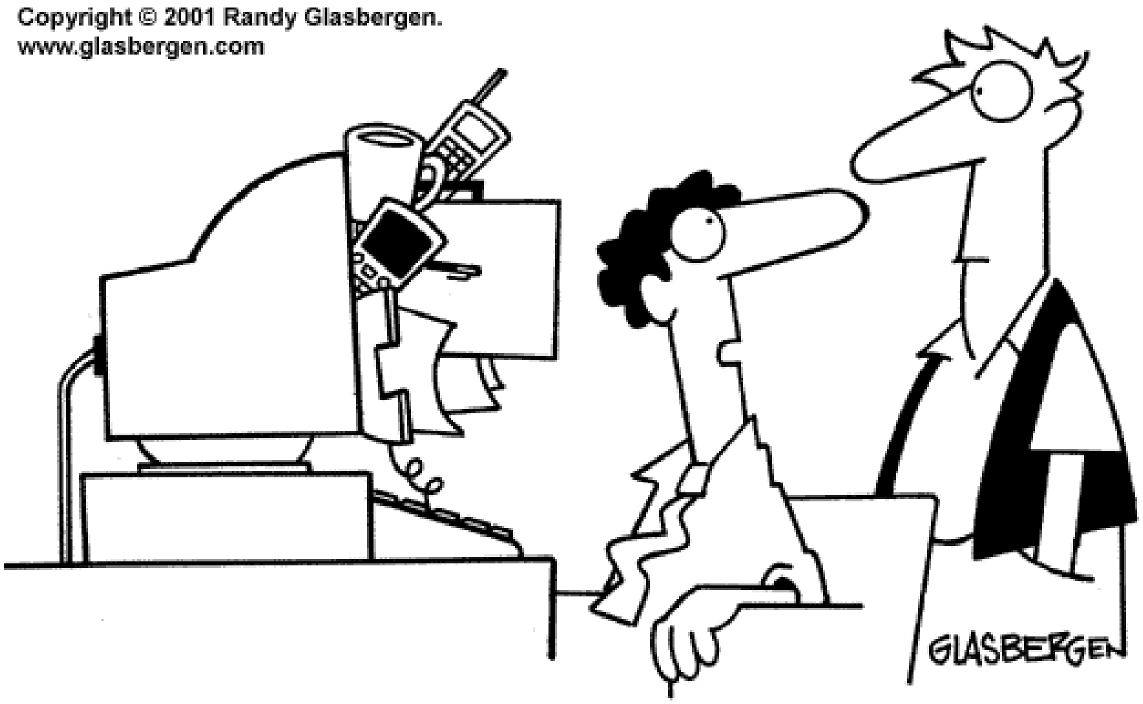
Firefox does not support VBScript and ActiveX Controls, which are often the source of attacks and vulnerabilities within IE

Opera supports Secure Socket Layer (SSL) versions 2 and 3, and TLS and offers automatic 256-bit encryption

The Safari browser automatically opens "safe" files such as movies, pictures, sounds, PDFs, text files, disk images and other archived files

Netscape vulnerability includes information CERT/CC would not ordinarily publish, including specific site names and exploit information

"Customers aren't impressed by our web site anymore. We need to put the 'gee' back in 'technologee'!"



"You made our web site too sticky."