Web Server Information Leakage - How to Stop Web Servers from Leaking

Information Leakage Detection & Protection
For Web Servers

Presented By: Wong Onn Chee
12 March 2009

Overview

- Web Leakage Today – Size and Scale

- Reasons why web leakages may occur

- "Best practices" during development

- "Best practices" at production maintenance

Web Leakages is a Serious Risk Today!

Figures exclude leakages from end points or tapes.

Industry	# U.S. Records Lost (2005-2008)
Government	2,269,656
Education	588,846
Healthcare	529,034
Financial	114,745
Manufacturing	46,000
Retail	22,735
Real Estate	13,000
Security	5,878
Utilities	3,000
Internet	2,750
Legal	530
Logistics	465

Source: http://www.privacyrights.org/ar/ChronDataBreaches.htm

Type of information	"Street Value" of malicious usage (USD)
Payment Card Info	$2 - $5 per record
Full Account Info	$200 - $300 per record
Zero-day Malware	$2500 - $4000 per incident

Source: The Aegenis group , USENIX 2008

There is a demand for your sensitive information

Can you risk providing the supply?

RESOLVO

Web Leakages is a Serious Risk Today!

Item	Advertised Price (in US Dollars)
United States-based credit card with card verification value	$1–$6
United Kingdom-based credit card with card verification value	$2–$12
An identity (including US bank account, credit card, date of birth, and government issued identification number)	$14–$18
List of 29,000 emails	$5
Online banking account with a $9,900 balance	$300
Yahoo Mail cookie exploit—advertised to facilitate full access when successful	$3
Valid Yahoo and Hotmail email cookies	$3
Compromised computer	$6–$20
Phishing Web site hosting—per site	$3–5
Verified PayPal account with balance (balance varies)	$50–$500
Unverified PayPal account with balance (balance varies)	$10–$50
Skype account	$12
World of Warcraft account—one month duration	$10

Table 3. Advertised prices of items traded on underground economy servers
Source: Symantec Corporation

RESOLVO

Applicable regulations on the area of web information leakage

The following regulations apply to web servers too, in requiring them not to leak any sensitive information, especially private personal information.

1.	EU Data Protection Directive – Security Safeguards Principle 11
2.	Sarbanes-Oxley Act (2002)
3.	HIPAA (1996)
4.	Gramm-Leach Bliley Act (GLBA)
5.	California SB1386 (2003)
6.	Personal Information Protection Act – Japan
7.	Data Protection Act – UK
8.	IDA IM8 Instruction Manual – Singapore

*See Back Up slides for full listing of regulatory requirements

Applicable OWASP's Top 10

Interesting, the even-numbered OWASP Top 10* items are applicable too:

A2	Injection Flaws

Should protect against SELECT SQL injection flaws which may result in a leakage of sensitive information stored in databases

A4	Insecure Direct Object Reference

Shoould protect against unwanted direct object references, such as a file, directory, database record, or key, as a URL or form parameter

A6	Information Leakage and Improper Error Handling

Should protect against application loopholes that unintentionally leak information about their configuration, internal workings, or violate privacy through application problems

A8	Insecure Cryptographic Storage

Should protect against leakages of information, such as credit card numbers, if not properly encrypted or masked

A10	Failure to restrict URL Access

Should protect against leakages of information through unwanted direct URL accesses by hackers

Web Leakage – Don't be next!

Home : **News** : **Traffic** : **Weather** : **Sports** : **Business** : **WRAL-TV** : **5 On Y...**

Local : State : Nation : World :

: Public Records

Local News

ECU Mistakenly Posts Personal Info Online

Posted: Feb 9, 2007

GREENVILLE, N.C. — East Carolina
plans to notify about 65,000 students
and staff members about a security breach that
could put them at risk for identity theft.

Facebook Source Code Leak Raises Security Questions

Examining the leaked code reveals vulnerabilities in Facebook's applications that could be exploited, a developer said.

By **K.C. Jones**
InformationWeek
August 14, 2007 02:25 PM

Facebook source code has been leaked on the Web, and that's raising some serious issues about the site's security and data privacy.

Source code from the social networking site's main index page appeared on a blog called Facebook

Student Private Information Leaked
Preparatory Firm Website

Princeton Review published confidential data by ac...

Princeton Review, an organization that
responsible for leaking private inform
seven weeks, some of the informatio
Review, has been available for every
address.

The organization has been hired to ev
Florida. The file that offered an over

➔ Straits Times Headlines ➔ Bleak data jolts Asian bourses ➔ NTU professor slashed on campus; attacker dies in fall ➔ Inside ➔ Splitting

| TOP STORIES | SINGAPORE | SE ASIA | ASIA | WORLD | MONEY | SPORT | TECH & SCIENCE | LIFESTYLE | BLOGS |

Home > Breaking News > Singapore > Story

March 3, 2009

Glitch spills UBS clients' info

Wealthy customers saw details of others' online accounts, but bank says number affected is small

A TECHNICAL glitch at Swiss bank UBS gave its wealthy customers in Singapore and Hong Kong a shock last week when they logged on to their online accounts.

The private-banking clients found confidential details of other clients' bank statements and account information instead of their own. Clients' online accounts, though, do not indicate their names.

When contacted, a UBS spokesman confirmed the incident and said the bank was taking it very seriously.

Asked how many clients were affected, all she said was that 'some limited account information concerning a small number of UBS wealth-management clients was accessible by a very limited number of other system users'. She added that fewer than five accessed the information.

She told my paper the glitch occurred 'as a result of an inadvertent technical error following an information-technology system upgrade over the weekend of Feb 21'.

The bank immediately took steps to rectify the issue. UBS reviewed the circumstances leading to the incident and has implemented measures to prevent a similar occurrence in the future.

email
print
larger
smaller
discuss

singapore

He lost his scholarship 3:23 PM
Outpouring of sympathy 3:09 PM
Cheaper Arts Fest tickets 2:27 PM
Serial predator gets 42 yrs 2:33 PM
2 fined for obscene act 1:26 PM
Jailed for obstructing cop 12:53 PM
Charged with maid abuse 12:50 PM
Parents identify son's body 12:17 PM
Lower interest on deposits 6:00 AM
Youth games on Web 6:00 AM
Airlines' $12b loss in 2008 6:00 AM
STI at lowest since Aug '03 6:00 AM
A-level results out on Fri 6:00 AM
Family sues HSBC over forex 6:00 AM
Signs of violent struggle 6:00 AM
Glitch spills UBS clients' info 9:23 AM
Well respected by students 6:00 AM
Lightning strikes all too often 6:00 AM
SPH websites score high 6:00 AM

4 main reasons why information leaks from web servers

1. ## Compromised web servers
Infected web servers can cause information to be leaked out.

2. ## Vulnerabilities in web applications
Poorly written applications can result in more information than necessary being shown.

3. ## Server errors
Malfunctioned or misconfigured web servers can display too much information.

4. ## Sensitive Information left on web servers
Backup copies of source codes, SQL files, CSV files containing customer records can be left on web servers.

Auction.co.kr (Apr 2008)

· 10.81 million customer records.
http://english.chosun.com/w21data/html/news/200804/200804180010.html

Home> Biz/Tech

Concerns M

The personal
Korea's larg
February, i
of user info

Experts fear
the leaked inform
addresses, telephone
credit card numbers.

According to the results of
Agency's Cyber Terror R   Center, a user with the name "fuckkr"
may have hacked into the company's website using a computer worm
from an overseas IP address. Existing computer anti-virus services
were unable to detect the worm.

What is perhaps more shocking is that the company was at a loss as
to what to do about the attack until information on more than 10
million, or 60 percent of 18 million subscribers, was leaked. With the
extent of the damage now revealed, Auction will likely face its most
serious crisis since its founding.

(englishnews@chosun.com)

> " hacked into the company's website using a **computer worm** from an overseas IP address. Existing computer anti-virus services were **unable to detect the worm**."

East Carolina University (Feb 2007)

· 65,000 student records. http://www.wral.com/news/local/story/1198897/

"A **programming error** on the school's OnePass Web site created files that made it possible for anyone to view personal information of thousands of students, former students and faculty members. The information included names, addresses, Social Security numbers and, in some cases, credit card numbers."

Qantas (Nov 2008)

· Other customer records were shown in online booking portal.

http://www.cio.com/article/465089/Confidential_Customer_Details_Exposed_on_Qantas_Site

Confidential Customer Details Exposed on Qantas Site

Qantas' online b~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~nal
detail~~~

"... revealed the privacy breach to Australian PC World...
unearthed the error while attempting to access the company's secure booking site.
Doust's initial attempt to access her flight and booking information failed.
She attempted to log-in again,
only to be presented with the personal details of two other Qantas customers."

to access the

She accessed the details using he~~~~~~~~~~~~~~~
and details -- provided by Qantas~~~~~~~~~~~~~~e
check-in for an upcoming flight. Dous~~~~~~~~pt to
access her flight and booking informat~~~~iled. She
attempted to log-in again, only to be presented with the
personal details of two other Qantas customers.

CENTER OF EXCELLENCE

INFRASTRUCTURE

» Outbound Email and Data Loss Prevention
This report shows the findings of a recent Proofpoint and

West Penn Hospital (Jan 2009)

· Other patient records were shown in online bill payment portal.

http://www.wpxi.com/target11/18449490/detail.html

Hospital Addresses Online Privacy

wpxi

> "...she was able to view information on 85 other patients.
> That information included the patient's name, address, medical procedure and costs....
> ...blamed the problem on a temporary data translation error
> involving a third-party billing partner."

"I was... the privacy iss... people realize that other...

DeMarco said she sent two e-mails alerting the...

DeMarco then contacted Target Eleven.

When Earle contacted the hospital, hospital officials b... investigation.

A hospital spokesman blamed the problem on a temporary data translation error involving a third-party billing partner.

"We immediately disabled the online bill payment service to complete a full audit of the system. We are working to institute additional safeguards and cross-checks with out third party service to ensure that this issues is completely

...ake
...o Died On
...r Patients Have
...MC

· Judge Sentences Local Man After 12th DUI

· Some Notice Mysterious Charge On Bank Statement

· Online Comments Lead To Privacy Complaint

· Target 11 Investigates Crime At Pittsburgh Area Malls

Statutory Board A, Singapore

- SQL and source codes were leaked

URL is not shown

```
Error occurred while updating      -database, please inform      , unable to continue.
"); echo("
[Back]

"); echo("unable to connect to database!!!"); exit; } $language = "MALAY"; $accessDate ; $hitCount = 0;
$hitCountQuery = "SELECT MAX(HIT_COUNT) FROM cleancard_hitcounter WHERE language='MALAY'
and to_date(Access_Date,'dd/mm/yyyy')=to_date(SYSDATE,'dd/mm/yyyy')"; //echo("hitCountQuery is
".$hitCountQuery); $hitCountStatement = OCIParse($connection,$hitCountQuery);
if($hitCountStatement == false) { echo ("Error in ociparse!"); echo OCIError($hitCountStatement)."
" ; exit; } OCIDefineByName($hitCountStatement,"MAX(HIT_COUNT)",&$hitCount);
OCIExecute($hitCountStatement); OCIFetch($hitCountStatement); //$hitCount =
OCIFetch($hitCountStatement); OCIFreeStatement($hitCountStatement); //echo('Initial $hitCount is
.... '.$hitCount)."
"; $hitCountIncrementQuery = "insert into cleancard_hitcounter(language,Access_Date,Hit_Count)
values('MALAY',SYSDATE,1)"; //echo('hitCountIncrementQuery in insert is '.$hitCountIncrementQuery);
$hitCountIncrementStatement = OCIParse($connection,$hitCountIncrementQuery);
if($hitCountIncrementStatement == false) { echo ("Error in ociparse!"); echo
OCIError($hitCountIncrementStatement)."
" ; exit; } $incrementSuccess = OCIExecute($hitCountIncrementStatement);
OCIFreeStatement($hitCountIncrementStatement); //echo('incrementSuccess in 0 block is
'.$incrementSuccess)."
" ; /*if($hitCount > 0) { $hitCountIncrementQuery = "update cleancard_hitcounter set Hit_Count=
(Hit_Count)+1 where language='MALAY' and to_date(Access_Date,'dd/mm/yyyy')=to_date(SYSDATE,'DD
/MM/YYYY')"; //echo('hitCountIncrementQuery in update is '.$hitCountIncrementQuery);
$hitCountIncrementStatement = OCIParse($connection,$hitCountIncrementQuery);
if($hitCountIncrementStatement == false) { echo ("Error in ociparse!"); echo
OCIError($hitCountIncrementStatement)."
" ; exit; } $incrementSuccess = OCIExecute($hitCountIncrementStatement);
OCIFreeStatement($hitCountIncrementStatement); commit; // echo('incrementSuccess in >0 block is
' $incrementSuccess) "
```

13

Statutory Board B, Singapore

- SQL code was leaked
URL is not shown

```
Warning: Query error in channel 'bf_prod/blog'.
SQL Error: You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server version for
the right syntax to use near ''no','no','no',10,10,3,3,'no','no','yes','yes','no',0,'grant re
in /home/user/ctown/ctx/class/api.inc on line 314

Query was -
insert into bf_prod.blog(name,owner__id,category,approve,mail_alert,post_per_page,comment_per_page,home_recentarticle,home_recentcomment,home_cat
valid-user
grant comment
valid-user
grant write admin
owner',now())

cannot find news
```

University A, Singapore

- SQL and source codes were leaked

URL is not shown

Polytechnic A, Singapore

· National IDs of 23 students were leaked

URL is not shown

Statutory Board C, Singapore

· Debug message is overly verbose and exposes system information
URL is not shown

An Error Occurred:

javax.el.ELException: //var/projects/josiah/view▮▮▮/templates/bfbDetail.xhtml @219,70 rendered="#{empty comments}":
//var/projects/josiah/view▮▮▮templates/bfbDetail.xhtml @214,94 value="#
{JosiahCommentManager.getCommentList(commentGroup)}": java.lang.NullPointerException

+ Stack Trace

+ Component Tree

- Scoped Variables

Request Parameters

Name	Value
articleTitle	trace
catname	others
page	bfb_detail
parentName	entertainment

Request Attributes

Name	Value
JosiahGamesRating	com.mavenlab.josiah.games.GamesRating@12049d9
JosiahPointManager	com.mavenlab.josiah.point.PointManager@d0796d

Scenario 3: Server Errors

Facebook (July 2007)

- Source codes were leaked out during a maintenance run.

http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=201800144

Facebook Source Code Leak Raises Security Questions

Examining the leaked code reveals vulnerabilities in Facebook's applications that could be exploited

"From just this single page of source code, a lot can be said and extrapolated about the rest of the Facebook application and platform. At a quick glance, I know that I can see some obvious things in the code that both reveal certain hidden aspects of the platform and give a potential attacker a good head start."

» IronPort 2008
Malware Trends Report

Videos

...son
...promise

...a TechCrunch blog posting that
...erabilities in Facebook's applications
that could be ex...

"From just this single pag... ...ce code, a lot can be said and extrapolated about the rest of ...acebook application and platform," he said. "At a quick glance, I know that I can see some obvious things in the code that both reveal certain hidden aspects of the platform and

18

Facebook (June 2008)

• Source codes were leaked AGAIN!

http://www.foxnews.com/story/0,2933,293115,00.html

FOXNEWS.COM HOME > SCITECH

Facebook Source Code Leaked Onto Internet

Wednesday, June 25, 2008

By Jonathan Richards

THE TIMES

E-Mail | Print

Share: [icons]

Facebook users on Monday were left contemplating the security of private details stored on the social-networking site after part of its source code was leaked onto the Internet.

The site on Monday acknowledged that a section of its code had been copied and published on a blog, but stressed that none of the personal details of its 52 million users had been compromised.

Over the weekend, a blog called **Facebook Secrets** published details of part of Facebook's source code, the set of commands which determine the way the site appears when it is viewed by users.

• Click here to visit FOXNews.com's Cybersecurity Center.

• Click here for FOXNews.com's Personal Technology Center.

Facebook said that a fraction of its code had been "exposed to a small number of users as a result of a single, misconfigured Web server" but that the problem was "fixed immediately."

RELATED

"It was not a security breach and did not compromise user data in any way," the company said in a statement released

19

Scenario 3: Server Errors

Facebook (June 2008)

- Here is a screenshot of the source code

http://www.codeandcoffee.com/wp-content/uploads/2008/08/facebook-home_1219773725753.png
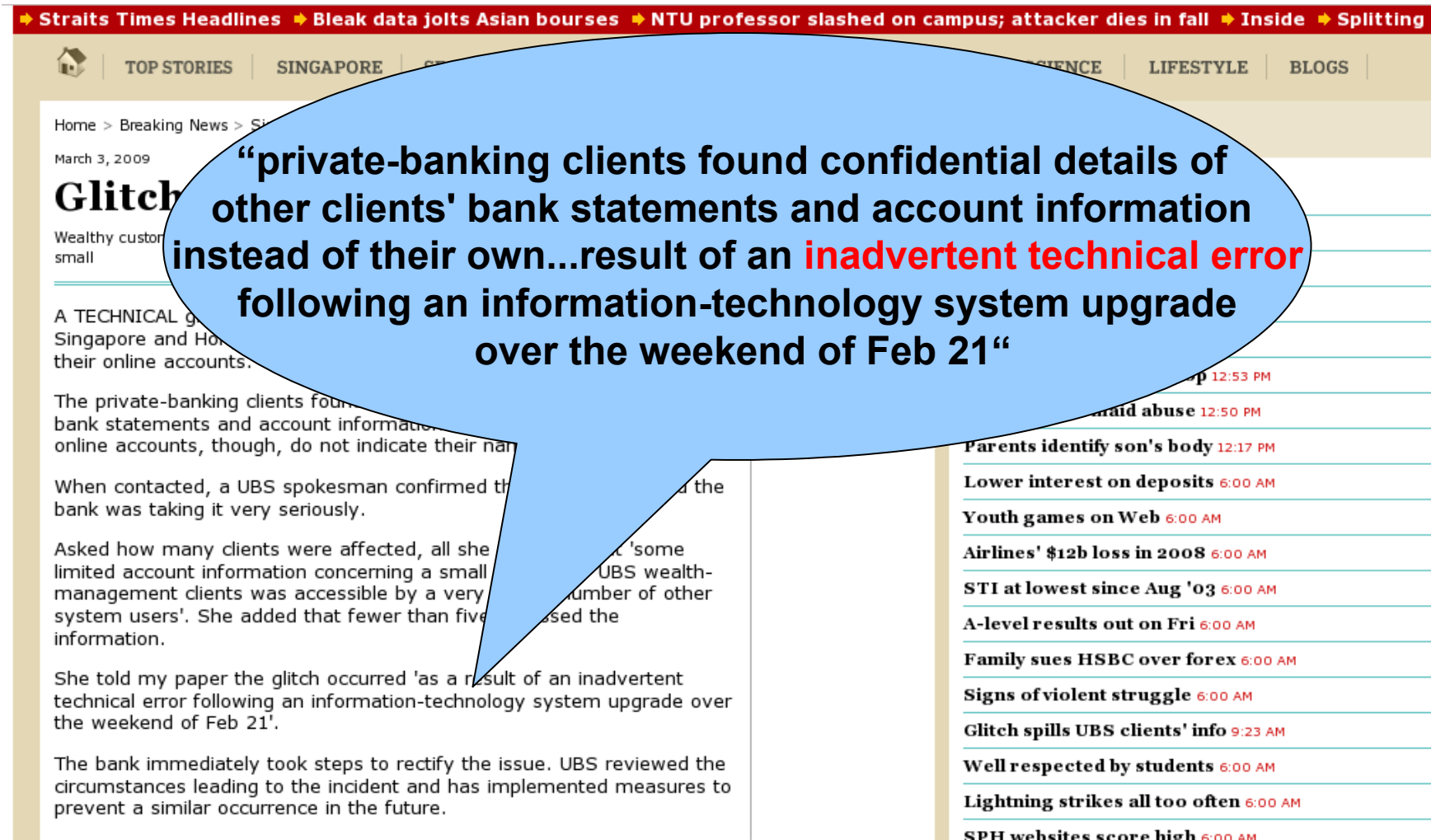
9 dir 117150 svn+ssh://tubbs/svnroot/tfb/releases/thefacebook-r116496-fb95/www/lib/display/privacy svn+ssh://tubbs/svnroot 2008-08-05T21:47:04.536211Z 114218 chad svn:special svn:externals svn:needs-lock 2c7ba8d8-a2f7-0310-a573-de162e16dcc7 pages.php file 2008-08-18T18:50:32.000000Z
e69ad78841111ae71df858b23a4d356c 2008-08-05T21:47:04.536211Z 114218 chad 8328

Scenario 3: Server Errors

UBS (February 2009)

- Customer records were leaked during system upgrade

http://www.straitstimes.com/Breaking%2BNews/Singapore/Story/STIStory_345246.html

Princeton Review (Aug 2008)

- 108,000 student records.

http://news.softpedia.com/news/Student-Private-Information-Leaked-on-Preparatory-Firm-Website-92103.shtml

Student Private Information Leaked on Preparatory Firm Website
Princeton Review published confidential data by accident

By **Denisa Ilascu**, Internet / SEO News Editor
19th of August 2008, 12:28 GMT

Adjust text size: A- **A+**

Princeton Revi...
respon...
se...

The...
Florida...
ethnicities and...

students' skills in mathematics, reading, scien... ...g with other sensitive information regarding learning disabilities, or wh... ...er language or not.

The schools in Sarasota were not the only ones affected by the... ...urity system of Princeton Review. The names and birthdays of approximately 74,000 students from the public... ...ax County, Virginia, were revealed in the same way.

"Some of the information is said to have been accessible t... search engines like Google. You have to wonder - if companies are making it this easy to discover information ab... ndividuals, why do identity thieves go to all that effort of writing spyware?" **commented** Senior Technology Consultant... the security company Sophos, Graham Cluley.

The most intriguing thing about the incident was that it was discovered by another preparatory firm, as it was performing a survey to see how competition was doing. When finding that all the data, which were not supposed to ever be made public, were available on the Princeton Review website, the institution, on the condition of being allowed anonymity, broke the story to the Washington Post.

> "The most intriguing thing about the incident was that it was discovered by **another preparatory firm**, as it was performing a survey to see how competition was doing... broke the story to the **Washington Post** "

Ministry A, Singapore

- National ID of 23 citizens were leaked.

URL is not shown

S/No	NRIC No (Fin No For Non-S'poreans Only)	Name
1	S9609875H	
2	S9672728C	
3	S9637560C	
4	S9603642F	
5	S9605493I	
6	S9618238D	
7	S9638427J	
8	S9610678E	
9	S9603163G	
10	S9637592A	
11	S9601869Z	
12	S9644176B	
13	S9631997E	
14	S9643158I	
15	S9610720D	

Ministry B, Singapore

- Locations of friendly foreign armed forces units in Singapore were leaked.
URL is not shown

Previous Entity Registration No Mappings					Registered Address Street Name
Issuance Agency	Entity Type	UEN	Previous	Entity Name	
Mindef	FM	T08FM0001E		ROYAL AUSTRALIAN NAVY (RAN)	
Mindef	FM	T08FM0002A		AUSTRALIAN DEFENCE FORCE	
Mindef	FM	T08FM0003H		DEFENCE FUELS GROUP	
Mindef	FM	T08FM0004D		NEW ZEALAND DEFENCE SUPPORT UNIT (SEA)	
Mindef	FM	T08FM0005L		FISC DETACHMENT SINGAPORE	
Mindef	FM	T08FM0006G		NAVY REGION CENTER SINGAPORE (NRCS)	
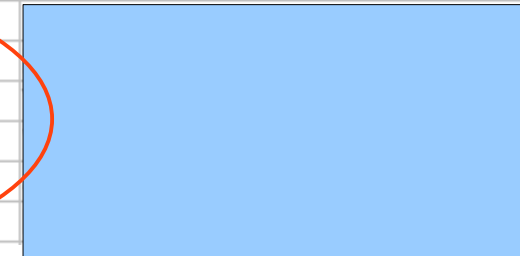
Polytechnic A, Singapore

- Private information of 53 students were leaked.

URL is not shown

High School A, Singapore

- National ID for 44 secondary students were leaked.

URL is not shown

NATIONAL POLICE CADET CORPS
SECONDARY 1 SQUAD 2008
CADET PROFILE MANAGEMENT SYSTEM

No.	Name	NRIC	CD	CP	CSS	Drill/1	Drill/2	Drill/3	HFS	LS	MM	NH
1		S9570431Z		23/05/08								
2		S9527958I		23/05/08								
3		S9524379G		23/05/08			07/11/08					
4		S9501671E		23/05/08								
5		S9543949G		11/07/08								
6		S9570194I		23/05/08								
7		S9533923I		23/05/08			07/11/08					
8		S9531990D		23/05/08								
9		S9514429B		23/05/08								
10		S9527320C		23/05/08								
11		S9590023B		23/05/08								
12		S9533159I		23/05/08			07/11/08					
13		S9571436F		23/05/08								
14		S9540695E		23/05/08								

High School B, Singapore

- National ID for 20 secondary students were leaked.

URL is not shown

High School C, Singapore

• National ID, birth dates and phone numbers for 55 secondary students were leaked.

URL is not shown

Leadership Training Camp 2005-2006
Calling System

Class	Name	NRIC No.	Date of Birth (M/D/Y)	Phone Number
Squad One				
2A		S9100358I	1/9/1991	67835663
2I		S9127160E	8/5/1991	64429323
2I		S9107848A	2/15/1991	64476159
2G		S9120716H	5/30/1991	65850018
2F		S9132166A	9/18/1991	64587073
2D		S9111580H	3/29/1991	65837686
2C		S9107998D	3/11/1991	67448726
2G		S9101653B	1/13/1991	65827766
2A		S9017930F	5/31/1990	67432998
Squad Two				
2I		S9134531E	9/23/1991	67463408
2I		S9113098Z	4/2/1991	64759161
2G		S9131931D	9/11/1991	64493973
2F		S9134699J	9/22/1991	65815036
2D		S9145513G	12/14/1991	67871694
2D		S9108515A	3/6/1991	62837426
2C		S9129329C	8/16/1991	63483750
2C	LIM WEN QIANG VINCENT	S9116041B	5/7/1991	67852163

Junior College A, Singapore

• Home address, national ID, email addresses, birth dates and phone numbers for 23 junior college students were leaked.
URL is not shown

Name	Address	Email	Hp No.	Class	D.O.B	NRIC
		the_raider@hotmail.com	98633617	04S36	30/12/87	S8742976A
		conanad@hotmail.com	91558670	04S36	14/03/87	S8708018H
		twinlance@hotmail.com	97986388	04S15	14/12/87	S8740827B
		esky2806@hotmail.com	97200480	04S43	06/11/87	S8736022I
		jellybean_fun@hotmail.com	97959140	04S61	13/03/87	S8727801H
		joleneho87@hotmail.com	97399119	04S17	19/03/87	S8706655Z
		q_jt@hotmail.com	91901629	04S12	22/03/87	S8706897H
		josephz1987@hotmail.com	90663731	04A51	10/10/87	S8731692J
		kenorms@hotmail.com	97979616	04S36	08/07/87	S8719655J
		kennytxd@hotmail.com	91724261	04S35	26/02/87	S8704039I
		zaerkkahn@hotmail.com	98232806	04S43	01/10/87	S8732374I
		zyn5152@hotmail.com	90041685	04S12	21/06/87	S8772433F
		stasia846@hotmail.com	98464409	03S1A	20/06/86	S8617293C
		chua86@singnet.com.sg	97972940	03S15	15/08/86	S8622355D
		iambrianfu@hotmail.com	97264784	03S1A	08/06/86	S8616016A
		jonathanley@hotmail.com	97879631	03S13	17/07/86	S8619089C
		khoonwee05@hotmail.com	98475015	03S32	21/07/86	S8619880J

High School D, Singapore

- National ID for 22 high school students were leaked.

URL is not shown

SUCCESSFUL APPEALS for YEAR 1, 2009	
NRIC NO.	NAME OF STUDENT
S9624801F	
S9636359A	
S9620678Z	
S9611751E	
S9648599Z	
S9624388Z	
S9607380A	
S9633822H	
S9600829E	
S9603525Z	
F2873500Q	
S9602436C	
S9633868F	
S9615390B	
S9607294E	
S9622959C	
S9637351A	
S9638269C	
S9606524H	
S9622909B	
S9643527D	
S9618526Z	

Should the school expose identities of students who initially failed to enroll based on their primary school scores?

Primary School A, Singapore

• National ID for 59 primary school students were leaked.

URL is not shown

FORM TEACHER	CLASS	NO	NAME	NRIC NO
MR TAN JING HWA	ES4P	1		S9219430B
		2		S9209547I
		3		S9335679I
		4		S9349236F
		5		S9319589B
		6		S9350508E
		7		S9223511D
		8		S9220336J
		9		S9137280J
		10		S9143760J
		11		S9337245Z
		12		S9244665D
		13		G0480394P
		14		G0428701R
		15		S9075116F
MR LOH AH BAH	MS4P	1		S9313953D
		2		S9229128F
		3		S9310570B
		4		S9174016H
		5		S9221236Z
		6		G0474824M
		7		S9226595A
		8		S9122028H
		9		S9208765D

High School E, Singapore

• National ID for 34 school volunteers were leaked.

URL is not shown

S/N	Name	Area(s) of Contribution	NRIC	Institution/JC
1	Cynthia Chua	Teacher		
2	Joyce Chong	Teacher		
3	Steven Ong	Teacher		
4		Befriender	S9234374Z	
5		Befriender	S9214365A	
6		Befriender	S9223279D	
7		Befriender	S9370013I	
8		Befriender	S9217264C	
9		Befriender	S9233069I	
10		Befriender	S9051179C	NYP
11		Befriender/Church TGC	S90154322	Si Mei ITE
12		Befriender	S9234502E	
13		Befriender	S9104143Z	NYJC
14		Befriender	S9132267F	YJC
15		Befriender	S9147091H	MI
16		Befriender/Church TGC/band	S8770934E	Church
17		Befriender/Church TGC/band	S8514005A	
18		Befriender/Church TGC/band	S8705622H	NTU
19		Befriender/Church TGC/band	S8730752B	SP
20		Befriender/IC	S9041825D	RP
21		Befriender	S8839289B	NTU
22		Befriender	S9371585C	
23		Befriender	S9137451Z	IJC
24		Befriender	S9010616C	NYP
25		Befriender	S9127701H	IJC
26		Befriender/Church AMK	S8815467C	NP
27		Befriender/Church AMK	S9005988H	SP

University B, Singapore

- Full personal details of a staff were leaked in a web-based file storage facility

URL is not shown

EPT REGISTRATION FORM

	(ENTER INFORMATION HERE)
Test Date: (DD/MM/YYYY) (Please refer to the list of test dates)	05/08/2008 (Please mail in this form and payment during the registration period only)
***Title :** (Mr/Mrs/Miss)	Mrs
Full Name : (As shown in NRIC / Passport)	
Sex : (Male / Female)	Female
NRIC/Passport Number : (For foreigner please use passport number)	S7185692E
Date of birth : (DD/MM/YYYY)	10/11/1971
Address : eg.BLK 1 ABC ROAD, AVE 2, ST 3 #01-234 SINGAPORE 123456	(This address is for correspondence, please provide an address in Singapore only) Blk 540 Bukit Batok ST 52 #09-519 Singapore 650540

University B, Singapore

• National ID of 8 applicants to access a military organisation were leaked in an extra worksheet in a publicly available staff directory spreadsheet.
URL is not shown

Record for DSO Security Pass

No.	Name	NRIC No.	Collected by (Name)	Signature and Date
27		S7732185c		
28		F2843898L		
29		E1867448		
30		S7161135C		
31		S7927015F		
32		S7625928C		
33		S7201312C		
34		S0019335F		

University A, Singapore

• National ID and home address of a student were leaked by a student organisation

URL is not shown

REIMBURSEMENT FORM

Cost Centre: S 9 1 1 0 0 2 0 0

Date	7-Sep-2005	
Attn	Office Of Finance	
Dear Sir,		

Amount Less GST		
$0.00	Please arrange to reimburse	
$0.00		
$0.00	NRIC / FIN No.	S8305938I
$0.00		
$0.00	Matric number	044398G04
$0.00		
$0.00	Address	Blk 18 Toa Payoh Lor 7 #08-238 S(310018)
$0.00		
$0.00	an amount of dollars	$0.00	for the purpose
$0.00		
$0.00	of	0
$0.00		
$0.00	The expenses incurred are to be debited as follows:	
$0.00		
$0.00	General Ledger		Gross Amount	Amount

Research Institute A, Singapore

- Entire list of 375 staff were leaked.

URL is not shown

Mail	Name	SN	givenName	Phone	Title
sflee	Lee Siew Fong	Lee	Siew Fong	67938235	Snr An
Lynn	Au Lynn	Au	Lynn	67938240	Snr An
larry	Lim Seow Yam Larry	Lim	Seow Yam	67938241	Snr An
hhyo	Yong Hock Hung	Yong	Hock Hung	67938237	Progr
kcwo	Wong Kam Choy Jack	Wong	Kam Choy	67938239	Snr An
franci	Tay Francis	Tay	Francis	67938228	Snr Mg
klng	Ng Khoon Leong	Ng	Khoon Leong	67938232	Snr Pr
gctan	Tan Gak Chee	Tan	Gak Chee	67938993	Snr R.
nzhan	Zhang NengSheng, Dr	Zhang	NengSheng	67938303	R. Sc.
splee	Lee Siew Poh	Lee	Siew Poh	67938413	Snr An
pstan	Tan Puay Siew	Tan	Puay Siew	67938377	DGM
lqzhu	Zhuang Liqun	Zhuang	Liqun	67938405	Snr R.
jhzha	Zhao Jianhong, Dr	Zhao	Jianhong	67938595	Snr Sc
sklau	Lau Soo Khim, Dr	Lau	Soo Khim	67938434	R. Sc
tcng	Ng Teck Chew	Ng	Teck Chew	67938261	Snr R.
wlin	Lin Wei, Dr	Lin	Wei	67938254	Snr Sc
yllee	Lee Yeng Lang	Lee	Yeng Lang	67938234	Progr
ewlee	Lee Eng Wah, Dr	Lee	Eng Wah	67938349	GM
rama	Ramasamy S/O Valliappan	Valliappan	Ramasamy	67938971	Snr R.
tktan	Tan Toh Khoong William	Tan	Toh Khoong	67938207	R. Offi
tmlim	Lim Tao Ming	Lim	Tao Ming	67932215	R. Eng
bytay	Tay Bee Yen, Dr	Tay	Bee Yen	67933545	R. Scie
alicek	Koh Theng Hong Alice	Koh	Theng Hong	67938249	Officer
jltan	Tan Joo Lett	Tan	Joo Lett	67938497	Snr R.
lily@S	Chew Lily	Chew	Lily	67938250	Asst M
angie	Yip Angie	Yip	Mei Ling	67938268	Snr Ex
devi	Vasantha Devi D/O K Krishnamurthi	K Krishnamurthi	Vasantha Devi	67938388	Snr Ex

Bank A, Singapore

- National ID of a lucky draw winner was leaked.
  URL is not shown
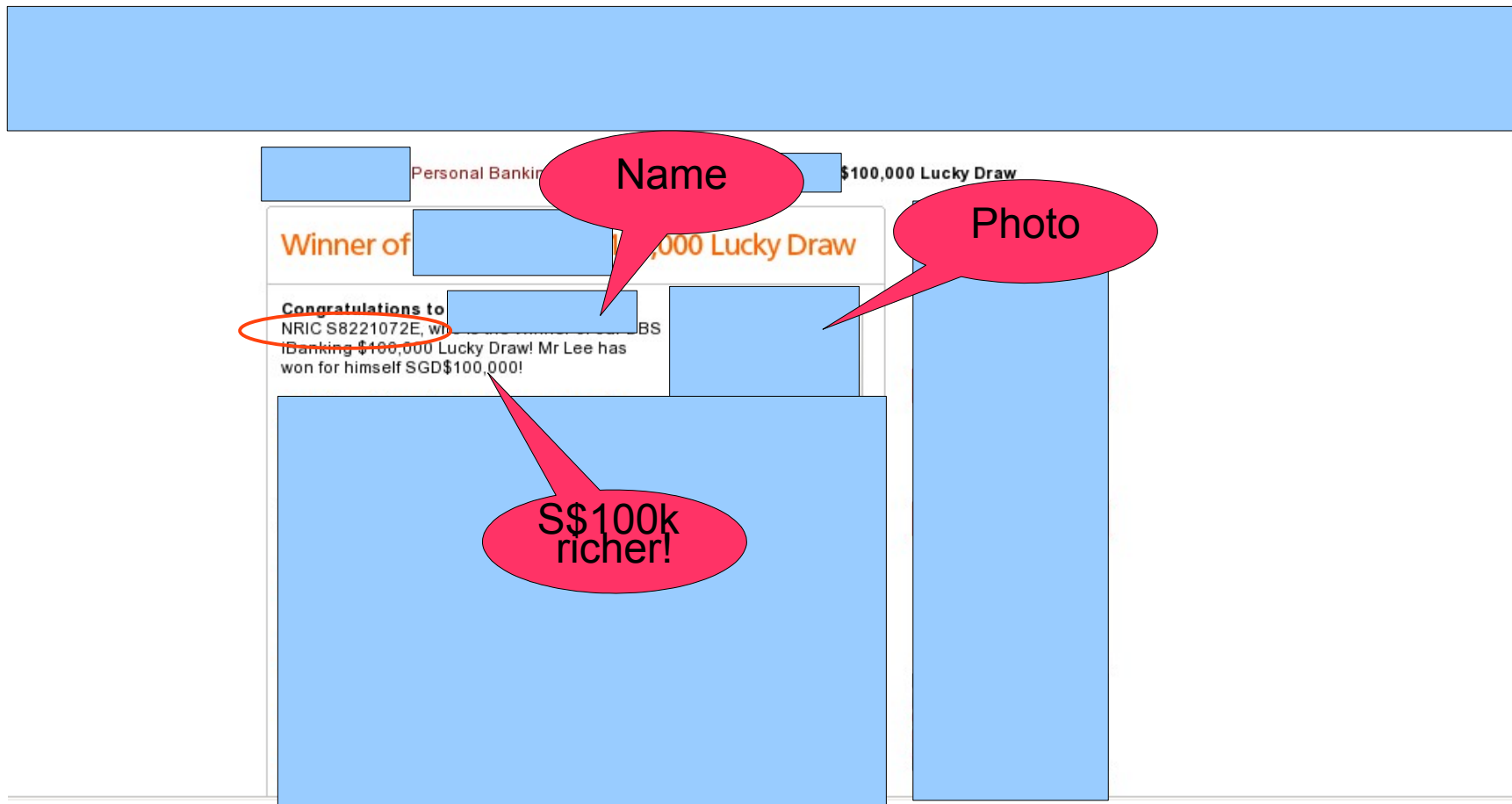
Polytechnic B, Singapore

- Administrator password was leaked.
URL is not shown

Statutory Board D, Singapore

- Partial source code was leaked
URL is not shown

```
<%@ page language="java" import="java.io.*;"%> <% int theCounter = 0; try{ String result; // String filename =
"/home01/docs/cudd/cawebsite/CAdowntownspace.txt"; String filename = "e:\\home01\\docs\\cudd\\cawebsite
\\CAdowntownspace.txt"; FileReader r = new FileReader(filename); BufferedReader br= new BufferedReader (r);
result=br.readLine(); br.close(); int intres=Integer.parseInt(result); intres=intres+1; result=""+intres; FileWriter
w=new FileWriter(filename); BufferedWriter bo = new BufferedWriter(w); bo.write(result); bo.flush(); bo.close();
//out.println("you are the " + intres + " person to hit this page"); theCounter = intres; } catch(Exception e) {
out.println("Exception"+e); } %>
```

OUR CITY CENTRE
A great place to Live, Work & Play!
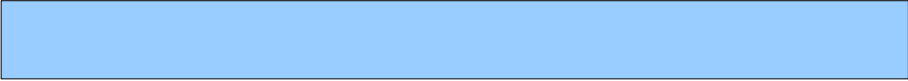
LOADING IN PROGRESS ...

Statutory Board E, Singapore

· Directory listing exposed files and source codes

URL is not shown

ISP A, Singapore

- SQL file was exposed.

URL is not shown

```
-- Script Name: [        ]
-- Created 28/05/2001 by Koh Seow Boon
-- Script to be run by csapp
-- Purpose: This is for the new [    ] service. This package
--          will register customers who wish to apply for this
--          service. This also authenticates the customer
--          before redirecting to the partner (M2B) site.
------------------------------------------------------------
-- Version 1.0
--
-- First production version for launch of free trial of[    ]
-- in June 2001. Authenticates dial-in password and redirects
-- to the free trial [    ] website.
--
-- Koh Seow Boon 28/05/2001
------------------------------------------------------------
-- Version 1.01
--
-- Changes paths of gif files from[            ] to local
-- server after gif files are copied to local server. The gif
-- files are bg_top.gif, pix_logo.gif, empty.gif & box.gif.
--
-- Koh Seow Boon 15/06/2001
------------------------------------------------------------

set scan off

Create or Replace Package [    ]as

  Procedure login
    (mstatus  in varchar2 default Null);

  Procedure display
    (musername   in varchar2 default Null,
     mpassword   in varchar2 default Null);

End;
/
show errors
```

Statutory Board F, Singapore

- Complete source code was leaked

URL is not shown

```
/*<applet code=App_Ordh_Qry.class width=585 height=200>
<PARAM name="session_id" value="145">
<PARAM name="activity" value="Select">
<PARAM name="pathplsql" value="http://highflyer____.gov.sg:8088/sfrsph2/plsql/">
<PARAM name="venue" value="Select">
<PARAM name="date" value="Select">
<PARAM name="timeslot" value="Select">
<PARAM name="placeofcall" value="B">
</applet>*/

/* -*-Java-*-
* @(#)App_Ordh_Qry
*  $Id:$
*
* Copyright (c) 1998 Singapore [        ], Singapore. All Rights Reserved
*
* CopyrightVersion 0.1
*
*/
/*
|-----|--------|-------|--------------------|----------|
|    |Who      |Date of|Brief Description of |Reference |
|S.No.|Changed |Change |    Change          |   No.    |
|-----|--------|-------|--------------------|----------|
*/

import java.awt.*;
import java.applet.AppletContext;
import java.io.*;
import java.net.*;
import java.awt.Font;
import java.util.Date;
import java.lang.String;
import java.awt.event.*;

import CalendarFrame;
import RecordRow1;
```

Naga City, Philippines

- Database password and username were leaked.

http://www.naga.gov.ph/~jessie/erpts_standard/includes/web/local.inc.bak

```php
<?php
/*
 * Session Management for PHP3
 *
 * Copyright (c) 1998-2000 NetUSE AG
 *                         Boris Erdmann, Kristian Koehntopp
 *
 * $Id: local.inc,v 1.1.1.1 2003/06/13 03:44:41 ravage Exp $
 *
 */
class DB_address extends DB_Sql{
    var $Host     = "localhost";
    var $Database = "nccMaster";
    var $User     = "nmuser";
    var $Password = "nccgov";
}

class DB_Report extends DB_Transaction{
    var $Host     = "localhost";
    var $Database = "erpts";
    var $User     = "root";
    var $Password = "";
    var $Halt_On_Error = "no"; //extension property

    function DB_Report($dbName){
        $curr = getcwd();
        $folders = explode("/",$curr);
        foreach ($folders as $folder) {
            if (substr($folder,0,5) == "erpts") break;
        }
        $this->Database = $folder;
    }
}
```

"Best Practices" - Development Phase

During development:

1. Block all SQL injection attacks to prevent SELECT SQL injection attacks.

2. Always make use of server-side validation. Do not rely only on client-side validation.

3. Use an index value or a reference map to avoid exposing direct object references.

4. Ensure proper error handling to avoid displaying of verbose error messages.

5. When errors occur, display a generic, user-friendly error message to users. An error code can be used for easy escalation, but the error code should be known only to the organisation and should help user to draw any references.

6. Ensure proper authentication and authorisation is required for access to sensitive data.

7. Never store any password in source codes.

8. Do not use persistent cookies. If cookies are to be used, encrypt the information to be stored in the cookies.

"Best Practices" - Development Phase

During development:

9. Passwords or other confidential information should never be stored in clear text, especially in configuration files, even if access is restricted.

10. Use strong hashing or encryption algorithms, such as SHA-256 or AES-256, to protect sensitive data during storage.

11. Never use personal information, such as NRIC, as system identifiers.

12. Educate all developers about the importance of information leakage. Use personal examples to gain greater empathy, by asking "What will you do if your and your family personal information is at stake here?"

13. Hold the development lead, not information security team, accountable for information leakage arising from applications.

14. Include checks for information leakage during QA testing.

"Best Practices" - Production Phase

During production maintenance and configuration:

1. Disable verbose debugging or error messages in server configuration.

2. Use HTTPS for all login pages.

3. Allow only authorised file types to be served from web server. Request for unknown or unauthorised file types should not be entertained. A web application firewall may be used.

4. Disable directory listing.

5. Redirect all HTTP errors to a standard, sanitised error page.

6. Remove any environment checking scripts.

7. Remove all default documentation or example scripts.

8. Harden the robots.txt to avoid search engines from crawling sensitive or private areas on your web server.

"Best Practices" - Production Phase

During production maintenance and configuration:

9. Restrict access to upload content to web server. Implement a "maker-checker" procedure where any upload of files is duly checked and verified.

10. Hold the webmaster, not information security team, accountable for any leakage arising from static content on the web server.

11. Remove all unwanted or obsolete documents from web server.

12. Perform regular monitoring and audit of your web server for information leakages.

13. Implement a host-based monitoring system that alerts administrators when non-compliant changes are made to the web server.

14. Implement a comprehensive web security system, comprising of protection against inbound attacks and outbound leakages.

Thank You

for

Your Attention