

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?

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

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

Should 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

*Source: http://www.owasp.org/index.php/Top_10_2007

Web Leakage – Don't be next!

Home : **News** : Traffic : Weather : Sports : Business : WRAL-TV : 5 On Your Side

Local : State : Nation : World :

Public Records

Local News

ECU Mistakenly Posts Personal Info Online

Posted: Feb 9, 2007

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

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



Princeton Review, an organization that is responsible for leaking private information over the last seven weeks, some of the information that Princeton Review has been available for every address.

The organization has been hired to evaluate schools in Florida. The file that offered an overview of the school's performance was leaked.

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

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



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.

Scenario 1: Compromised 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 t
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.”**

Scenario 2: Vulnerabilities in Web Applications

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.”**

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.

Video

- [ECU Mistakenly Puts Personal Info Online](#)
- [WEB ONLY: ECU News Conference](#)

Scenario 2: Vulnerabilities in Web Applications

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 booking portal exposed confidential customer details.

“... 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 her name and details -- provided by Qantas for check-in for an upcoming flight. Doust's 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.

CENTER OF EXCELLENCE

INFRASTRUCTURE

» Outbound Email and Data Loss Prevention

This report shows the findings of a recent Proofpoint and

Scenario 2: Vulnerabilities in Web Applications

West Penn Hospital (Jan 2009)

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

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

“...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

Hospital Addresses Online Privacy

wpxi

- 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

Scenario 2: Vulnerabilities in Web Applications

Statutory Board A, Singapore

- SQL and source codes were leaked

URL is not shown

Error occurred while updating [redacted]-database, please inform [redacted], 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) "
```

Scenario 2: Vulnerabilities in Web Applications

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())
```

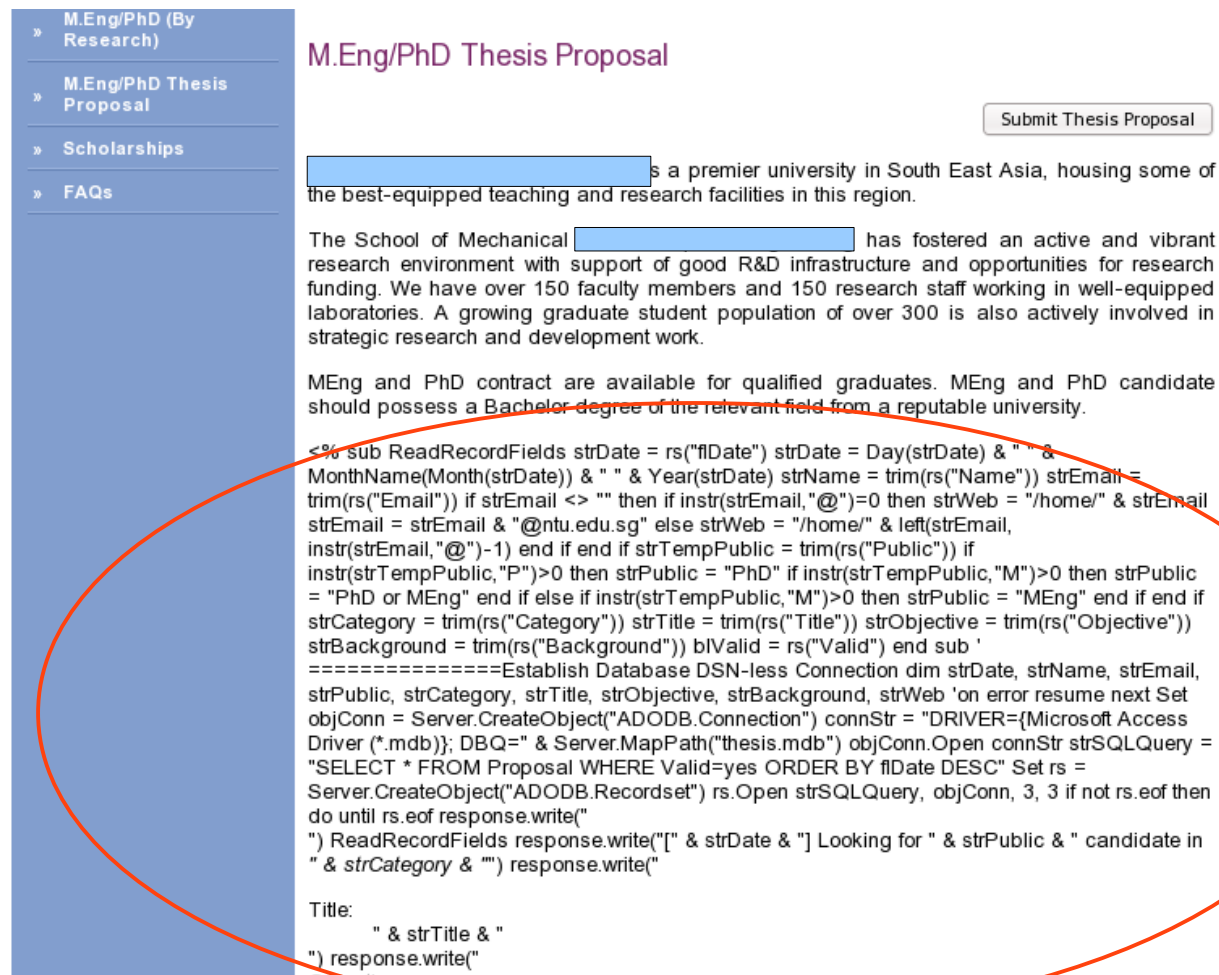
cannot find news

Scenario 2: Vulnerabilities in Web Applications

University A, Singapore

- SQL and source codes were leaked

URL is not shown



The screenshot displays a web application interface for submitting a thesis proposal. On the left is a blue sidebar with navigation links: » M.Eng/PhD (By Research), » M.Eng/PhD Thesis Proposal, » Scholarships, and » FAQs. The main content area is titled "M.Eng/PhD Thesis Proposal" and includes a "Submit Thesis Proposal" button. Below the title, there is a text input field and a paragraph of text: "_____ is a premier university in South East Asia, housing some of the best-equipped teaching and research facilities in this region." This is followed by another paragraph: "The School of Mechanical _____ has fostered an active and vibrant research environment with support of good R&D infrastructure and opportunities for research funding. We have over 150 faculty members and 150 research staff working in well-equipped laboratories. A growing graduate student population of over 300 is also actively involved in strategic research and development work." Below this, a paragraph states: "MEng and PhD contract are available for qualified graduates. MEng and PhD candidate should possess a Bachelor degree of the relevant field from a reputable university." The bottom section of the page contains source code for a VBScript function, which is circled in red. The code is as follows:

```
<% sub ReadRecordFields strDate = rs("flDate") strDate = Day(strDate) & " " &
MonthName(Month(strDate)) & " " & Year(strDate) strName = trim(rs("Name")) strEmail =
trim(rs("Email")) if strEmail <> "" then if instr(strEmail,"@")=0 then strWeb = "/home/" & strEmail
strEmail = strEmail & "@ntu.edu.sg" else strWeb = "/home/" & left(strEmail,
instr(strEmail,"@")-1) end if end if strTempPublic = trim(rs("Public")) if
instr(strTempPublic,"P")>0 then strPublic = "PhD" if instr(strTempPublic,"M")>0 then strPublic
= "PhD or MEng" end if else if instr(strTempPublic,"M")>0 then strPublic = "MEng" end if end if
strCategory = trim(rs("Category")) strTitle = trim(rs("Title")) strObjective = trim(rs("Objective"))
strBackground = trim(rs("Background")) bValid = rs("Valid") end sub '
=====Establish Database DSN-less Connection dim strDate, strName, strEmail,
strPublic, strCategory, strTitle, strObjective, strBackground, strWeb 'on error resume next Set
objConn = Server.CreateObject("ADODB.Connection") connStr = "DRIVER={Microsoft Access
Driver (*.mdb)}; DBQ=" & Server.MapPath("thesis.mdb") objConn.Open connStr strSQLQuery =
"SELECT * FROM Proposal WHERE Valid=yes ORDER BY flDate DESC" Set rs =
Server.CreateObject("ADODB.Recordset") rs.Open strSQLQuery, objConn, 3, 3 if not rs.eof then
do until rs.eof response.write("
") ReadRecordFields response.write("[ " & strDate & " ] Looking for " & strPublic & " candidate in
" & strCategory & " ") response.write("
Title:
" & strTitle & "
") response.write("
"
```


Scenario 2: Vulnerabilities in Web Applications

Polytechnic A, Singapore

- National IDs of 23 students were leaked

URL is not shown

The screenshot shows a web application interface for Polytechnic A, Singapore. The page is titled "Freshmen Orientation Tour 10 & 11 April". It displays a list of students for the tour, with columns for Full Name, Studen ID, NRIC/FIN, School, and Which session you are signing for?. A red oval highlights the NRIC/FIN column, which contains the National IDs of 23 students. The interface includes a sidebar with navigation links and a top navigation bar.

Full Name	Studen ID	NRIC/FIN	School	Which session you are signing for?
	85361	GO680881L	RP	10 April 12.00pm
	85738	S8674170I	RP	10 April 12.00pm
	85183	G0706932X	SIT	10 April 5.00pm
	85200	G0704337L	SEG	10 April 5.00pm
	85304	G0704332K	SEG	10 April 5.00pm
	85225	G0680863N	SEG	11 April 5.00pm
	85090	G0681443W	SIT	11 April 5.00pm
	85185	G0681576L	SCHOOL OF ENGINEERING	11 April 5.00pm
	85790	s8871459h	school of engineering	11 April 5.00pm
	85539	s7902117b	SHL	10 April 12.00pm
	85388	S8432610j	SIT	10 April 5.00pm
	85647	G0579665U	SEG	11 April 5.00pm
	85336	G0647511L	SEG	11 April 5.00pm
	85287	G7913436N	SEG	11 April 5.00pm
	85161	G0680022Q	RP	10 April 5.00pm

Scenario 2: Vulnerabilities in Web Applications

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[redacted]templates/bfbDetail.xhtml @219,70 rendered="#{empty comments}":  
//var/projects/josiah/view[redacted]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



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," 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

Scenario 3: Server Errors

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:     

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

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

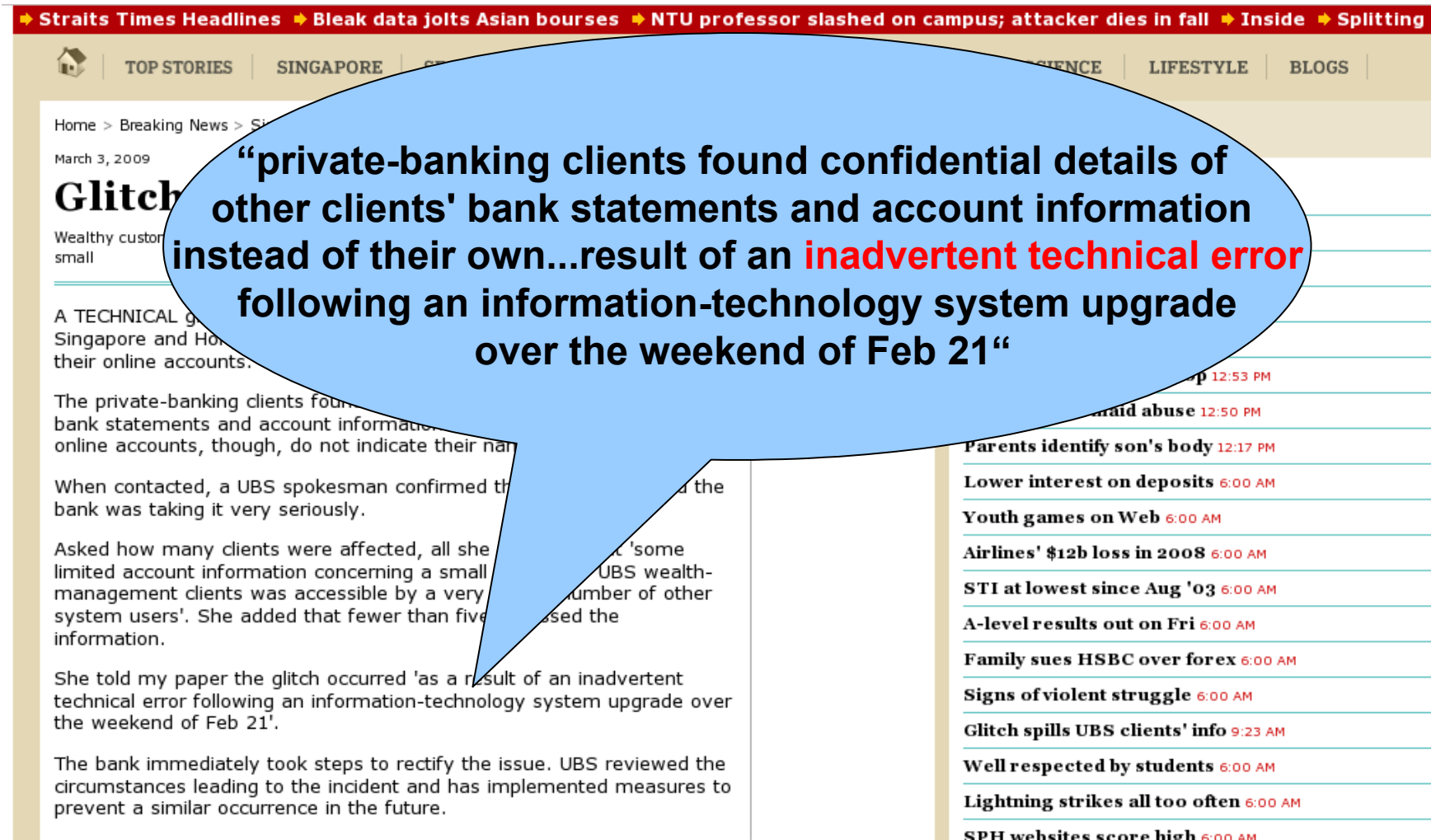
```
9 dir 117150 svn+ssh://tubbs/svnroot/tfb/releases/thefacebook-r116496-fb95/www/lb/display/privacy svn+ssh://tubbs/svnroot 2008-08-05T21:47:04.536211Z 114218 chad svn:special svn:externals svn:needs-lock 2c7ba8d8-a2f7-0310-a573-de162e16dc7 pages.php file 2008-08-18T18:50:32.000000Z
e69ad7884111ae71df858b23a4d356c 2008-08-05T21:47:04.536211Z 114218 chad 8328
month name), 'dtmay' => array('May', 'Non-abbreviated month name'), 'dtjune' => array('June', 'Non-abbreviated month name'), 'dtjuly' => array('July', 'Non-abbreviated month name'), 'dtaugust' => array('August', 'Non-abbreviated month name'), 'dtseptember' => array('September', 'Non-abbreviated month name'), 'dtoctober' =>
array('October', 'Non-abbreviated month name'), 'dtnovember' => array('November', 'Non-abbreviated month name'), 'dtdecember' => array('December', 'Non-abbreviated month name'), 'dtjan' => array('Jan', 'Abbreviated month name'), 'dtfeb' => array('Feb', 'Abbreviated month name'), 'dtmar' => array('Mar', 'Abbreviated month name'),
'dtapr' => array('Apr', 'Abbreviated month name'), 'dtmay' => array('May', 'Abbreviated month name'), 'dtjun' => array('Jun', 'Abbreviated month name'), 'dtjul' => array('Jul', 'Abbreviated month name'), 'dtaug' => array('Aug', 'Abbreviated month name'), 'dtsep' => array('Sep', 'Abbreviated month name'), 'dtoct' => array('Oct',
'Abbreviated month name'), 'dtnov' => array('Nov', 'Abbreviated month name'), 'dtdec' => array('Dec', 'Abbreviated month name'), 'dtmonday' => array('Monday', 'Day of the week'), 'dtuesday' => array('Tuesday', 'Day of the week'), 'dtwednesday' => array('Wednesday', 'Day of the week'), 'dtthursday' => array('Thursday', 'Day of the
week'), 'dtfriday' => array('Friday', 'Day of the week'), 'dtsaturday' => array('Saturday', 'Day of the week'), 'dtsunday' => array('Sunday', 'Day of the week'), 'dtmon' => array('Mon', 'Abbreviated day of the week'), 'dtTue' => array('Tue', 'Abbreviated day of the week'), 'dtWed' => array('Wed', 'Abbreviated day of the week'), 'dtThu' =>
array('Thu', 'Abbreviated day of the week'), 'dtFri' => array('Fri', 'Abbreviated day of the week'), 'dtsat' => array('Sat', 'Abbreviated day of the week'), 'dtsun' => array('Sun', 'Abbreviated day of the week'), 'dtoday' => array('Today', 'Time period'), 'dtyesterday' => array('Yesterday', 'Time period'), /** ***/ apiconfirmation.js ***/ 'ac01'
=> array('Granting access to information is required to use applications. If you are not willing to grant access to your information, do not use this application.'), 'ac02' => array('You must select the checkbox to grant these application privileges. If you do not wish to grant access, click Cancel.'), /** ***/ ads (create.js; admanager.js) ***/ 'ads01'
=> array('There was an error with the information you submitted.'), 'ads02' => array('Social Actions', 'Facebook feature'), 'ads03' => array('Social Actions) from (source) will automatically be added.', 'ad social action summary'), 'ads04' => array('If there was an error processing your action.'), 'ads05' => array('You have not finished creating
your ad. If you leave this page, your ad will not be saved.'), 'adprimary-link' => array('Make this your primary credit card.'), 'adsremove-link' => array('Remove this card from your account.'), 'adprimary-dialog-1' => array('This is your primary credit card. We will attempt to bill invoices against your '. primary credit card first. However, in the
event that a payment fails, we will '. attempt to bill other credit cards associated with your account.'), 'adprimary-dialog-2' => array('You cannot edit or remove your primary credit card. In order to remove this card, you '. must first make another verified credit card the primary card. To edit the billing details ', for this card, add it again and
then remove the original entry for the card.'), 'ads:close-dialog-1' => array('Are you sure you want to close your account? This action will pause all of your '. currently running campaigns and charge your credit card for any outstanding balance '. on your account. The credit cards on your account will be automatically removed after '. your
outstanding balance has been paid. It may take up to 2 business days for your '. account balance to be settled.'), 'ads:verified-dialog-1' => array('This is a verified credit card. The information you have provided has passed '. verification, so you can designate this credit card as your primary credit card.'), 'ads:verified-dialog-2' => array('If you
make this credit card your primary credit card, then invoices will attempt '. to bill against it first. However, if a payment were to fail, we would attempt '. to bill other credit cards associated with your account.'), 'ads:verified-dialog-3' => array('You cannot delete this credit card because it is the only verified credit card ', associated with
your account.'), 'ads:unverified-dialog-1' => array('This is an unverified credit card. The information that you have provided has not ', passed verification, so you cannot designate this credit card as your primary credit card.'), 'ads:unverified-dialog-2' => array('In order to pass verification, you must remove this credit card and add it back '. with the
correct information.'), 'ads:unverified-dialog-3' => array('You cannot remove this credit card because it is the only credit card associated with your '. your account. In order to pass verification, you will need to add a new credit card.'), 'ads:edit-action-add' => array('Add Credit Card'), 'ads:edit-action-add' => array('Save Credit Card'), 'ads:remove-title'
=> array('Remove Credit Card'), 'ads:remove-dialog' => array('Are you sure that you want to remove this card from your account?'), 'ads:primary-title' => array('Change Primary Credit Card'), 'ads:primary-action' => array('Make Primary'), 'adprimary-dialog' => array('Are you sure that you want to make this your primary card?'), 'ads:close-
title' => array('Close Ads Account'), 'ads:close-action' => array('Close My Account'), 'ads:info-title' => array('Credit Card Information'), 'ads:show-details' => array('Show Details', 'Link: shows credit card details'), 'ads:hide-details' => array('Hide details', 'Link: hides credit card details'), 'ads:cc-text' => array('A Card Security Code (CSC) is a
security feature of debit and credit cards that helps fight credit card fraud. The following graphic illustrates where to find the CSC code on your credit card.', 'description of Card Security Code (CSC)', 'business-critical', 'ads:cc-title' => array('What's a CSC code?', 'header: section describes what a credit card security code is'), 'ads:cc-
validation-title' => array('Why is CSC validation required?', 'header: section describes why we need to validate credit card security code for stored cards'), 'ads:cc-validation-text' => array('In order to fight credit card fraud, we have started to enforce CSC code validation in credit card payments. For credit cards we have stored before, this
means they will need to be CSC validated once for later uses. You will not be prompted in the future once the card gets validated.', 'explain why we need credit card security code for stored cards', 'business-critical', 'ads:cap-warning-title' => array('There is a chance that your ad's title may not meet our capitalization guidelines and could cause
your ad to be rejected. Your ad may not include excessive or incorrect capitalization. Acronyms, however, may be capitalized. If you believe your ad uses9 dir 117150 svn+ssh://tubbs/svnroot/tfb/releases/thefacebook-r116496-fb95/www/lb/display/puzzles svn+ssh://tubbs/svnroot 2008-08-14T18:24:46.740620Z 116087 jhsu svn:special
svn:needs-lock 2c7ba8d8-a2f7-0310-a573-de162e16dc7 puz1.html file 2008-08-18T18:50:32.000000Z 4ffeaec2f288a7f2d4460677c9c26f 2008-08-06T22:25:40.405254Z 105557 jhsu has-props 3954 puz2.html file 2008-08-18T18:50:32.000000Z 11b7b47b9ec069ff40dd223281351d1 2008-07-08T00:23:20.388784Z 108188
marcel has-props 2917 puz3.html file 2008-08-18T18:50:32.000000Z 05692949df703d10212e52cbda9ee95 2008-07-09T01:1:27:04.115817Z 108480 jhsu has-props 1222 puz4.html file 2008-08-18T18:50:32.000000Z f843dbba89c66fb50c54981288b32af 2008-08-06T18:17:15.798733Z 114488 dells 7752 puz5.html file
2008-08-18T18:50:32.000000Z bc3571f5bca400f1dd1a9d7c1214662 2008-08-14T18:24:46.740620Z 116087 jhsu 4932
dir 117150 svn+ssh://tubbs/svnroot/tfb/releases/thefacebook-r116496-fb95/www/lb/display/share svn+ssh://tubbs/svnroot 2008-08-13T11:54:53.583365Z 115810 eric svn:special svn:externals svn:needs-lock 2c7ba8d8-a2f7-0310-a573-de162e16dc7 share_stage.php file 2008-08-18T18:50:32.000000Z
2f04131e115b930904620f082c54189 2008-08-13T11:54:53.583365Z 115810 eric
'Dialog body for removing a publisher', 'fb95', 'apps:remove-composer-button' => array('Remove', 'Dialog button for removing a publisher', 'fb95'), 'apps:remove-composer-block-button' => array('Unblock', 'Button to unblock an app's publisher'), 'apps:remove-composer-block-title' => array('Unblock (App-name) Publisher', 'Dialog title for
prompt to unblock a publisher from the profile', 'fb95'), 'apps:remove-composer-block-body' => array('Are you sure you want to allow this application's publisher on your profile?', 'Dialog body for removing a block on a publisher', 'fb95'), /** ***/ applications/reviews/reviews.js ***/ 'arev:close-button' => array('Close', 'Review Application: close
review dialog'), 'arev:delete-button' => array('Delete', 'Review Application: delete a review'), 'arev:post-button' => array('Post', 'Review Application: submit a review'), 'arev:post-success' => array('Post successful', 'Review Application: submitted a review'), 'arev:required-fields' => array('You have not filled out all the required fields.', 'Review
Application: missing required information'), 'arev:no-rating' => array('You must choose a star rating', 'Review Application: missing star rating'), 'arev:update-review' => array('Update Review', 'Update a review'), /** ***/ html/js/lib/net/async.js ***/ 'async:error' => array('Something went wrong. We're working on getting this fixed as soon as we
can.'), 'You may be able to try again.', 'async:oops' => array('Oops', 'Dialog title for a warning message when something bad happened'), /** ***/ attachments.js ***/ 'at01' => array('Attach', 'Button: submits message attachment'), /** ***/ attachments.js ***/ 'base01' => array('more', 'Link: expands your left-hand nav to show more
applications'), 'base02' => array('less', 'Link: collapses your left-hand nav if you have it expanded'), /** ***/ business/mobile/service.js ***/ 'bizmob:messages' => array('Messages', 'Label: Messages (as in SMS or MMS messages)'), 'bizmob:pv' => array('Page Views', 'Label: Page Views (as in ')', 'bizmob:pmsg' => array('Page Views and
Messages', 'Label: Page Views and Messages.'), 'bizmob:dedup' => array('Note: this is the total number of de-duplicated unique users utilizing SMS, MMS, or WAP services.', 'Label: Explanation for the total unique de-duplicated number of users over SMS, MMS, and WAP services.'), /** ***/ beacon_manager.js ***/ 'bm:site-name' => array('['Site
Name'], 'label indicating 'Site Name' inside square brackets', 'beacon'), /** ***/ calendar.js ***/ 'cal:createSuccess' => array('['event_title has been created.', ' ', 'horizon'], 'cal:accept' => array('Accept', 'Button: accepts the current invitation', 'horizon'), 'cal:decline' => array('Decline', 'Button: declines the current invitation', 'horizon'),
'cal:newItem' => array('New Calendar Item', 'Label for a new item on user's calendar.', 'horizon'), 'cal:going' => array('You are going.', 'Event status text', 'horizon'), 'cal:unnotGoing' => array('You can add this.', 'Event status text', 'horizon'), 'cal:itemDetails' => array('Item Details', 'Title for calendar detailed popup dialog', 'horizon'),
'cal:svpAccepted' => array('['event-name'] has been added. <undo-link>', ' ', 'horizon'), 'cal:svpDeclined' => array('['event-name'] has been removed. <undo-link>', ' ', 'horizon'), 'cal:svpRequested' => array('['event-name'] has been set to undecided. <undo-link>', ' ', 'horizon'), 'cal:svpDefault' => array('Your RSVP status to '['event-name']'
has been changed. <undo-link>', ' ', 'horizon'), 'cal:deleteWarningTitle' => array('Delete Item?', 'Title of dialog asking if the user is sure they want to delete an item', 'horizon'), 'cal:deleteWarningMessage' => array('Are you sure that you want to delete this item? If you delete this item all of the attendees will be notified. This action CANNOT be
undone.', ' ', 'horizon'), 'cal:day_header' => array('week:day', ' (month)', 'Ex: Thursday, December 5', 'horizon'), 'cal:dateSelect' => array('month' (date)', 'year', 'MM/DD/YYYY', 'horizon'), 'cal:monthYear' => array('year' (month)', 'year', 'Example: October 2007', 'horizon'), 'cal:dateRange' => array('month' (date)', 'date' (date)', 'date2', '
Example: October 28 to December 5', 'horizon'), 'cal:savesChanges' => array('Save Changes', 'Button label to save changes to an event', 'horizon'), 'cal:inviteFriends' => array('Invite friends to come', 'Link that enables users to invite friends to attend an event', 'horizon'), 'cal:sendInvites' => array('Send Invites', 'Button label to send invites to
friends', 'horizon'), 'cal:add' => array('Add', 'Button: Adds something to a user's calendar', 'horizon'), 'cal:addToCalendar' => array('Add To Calendar', 'Title: Adds something to a user's calendar', 'horizon'), 'cal:itemDetails' => array('Item Details', 'Title describing the details of an item', 'horizon'), /** ***/ canvas.js ***/ 'can01' => array('Report',
'Link to report a bad application'), /** ***/ cards.js ***/ 'cd01' => array('Remove Card', 'Remove credit card from account header'), 'cd02' => array('Are you sure you want to remove this credit card from your account?', 'Remove credit card from account message'), 'cd03' => array('Remove', 'Button: Remove credit card from account'), /** ***/ chat/buddy_list.js ***/ 'chb01' => array('Could not load available friends.', 'Chat friends list error'), 'chb02' => array('Online Friends (number-available)', 'Number of available Chat friends'), 'chb03' => array('You (no one is available to chat.', 'Facebook Chat'), 'chb04' => array('('name)', 'status') (time)', 'Facebook Chat: Name and status listing in
available friends list'), 'chb05' => array('('idle)' - (name)', 'status') (time)', 'Facebook Chat: Name and status listing in available friends list for an idle friend'), 'chb06' => array('Could not find that friend online.', 'Facebook Chat search title'), 'chb07' => array('Idle', 'Facebook Chat Friend is Idle'), 'chb08' => array('Go offline to List', 'Ability for a
user to go offline to a particular friend list in Chat', 'chp-fri'), 'chb09' => array('You are offline to 'friend-list-name''), 'Notice to a user indicating being offline to a particular friendlist', 'chp-fri'), /** ***/ chat/chat_display.js ***/ 'chd01' => array('Chat', 'Facebook feature: Chat'), 'chd02' => array('Show/Hide (Chat) Window', 'Button label'),
'chd03' => array('Close (Chat) Window', 'Button label'), 'chd04' => array('Hide (Chat) Window', 'Button label'), 'chd05' => array('New message from (name)', 'Alert about new Chat message'), /** ***/ chat/status_control.js ***/ 'chd01' => array('Couldn't set (Chat)
availability', 'Chat error'), 'chd02' => array('Couldn't change that setting', 'Chat setting change error'), /** ***/ chat/tabs.js ***/ 'cht01' => array('Couldn't retrieve chat history', 'null'), 'cht02' => array('The message could not be sent.', 'Chat message error'), 'cht03' => array('Sending', 'Sending the Chat message'), 'cht05' => array('Send (name) a
message', 'Link'), 'cht06' => array('You are not online.', 'null'), 'cht07' => array('Clear (Chat) history', 'Link text'), 'cht09' => array('Couldn't clear (Chat) history', 'Chat error'), 'cht10' => array('('name) is online.', 'Message that someone is available in Chat'), 'cht11' => array('('send-
as-a-message)'), 'Part of sentence, prompts user to send a chat IM as a Facebook message.', 'send as a message is linked'), 'cht12' => array('Send as a message', 'Link: prompts user to send a chat IM as a Facebook message'), 'cht13' => array('You are online.', 'Message that user is online in Chat'), 'cht14' => array('('name) is no longer online.
The following were not sent', 'null'), /** ***/ confirmfriend.js ***/ 'cf:friend_title' => array('You have a friend request.', 'cf:ignore-button' => array('Ignore friend request', 'Button: Ignore friend request'), /** ***/ contact_importer.js ***/ 'ciuser-request' => array('This user will receive your friend request shortly.', 'contact importer message for one
friend request'), 'ciusers-request' => array('These users will receive your friend requests shortly.', 'contact importer message for more than 1 friend'), 'ciuser-success' => array('Success! A friend request will now be sent to your friend.'), 'Once your friend confirms your friendship, you will be able to see each other's profiles.', 'added a friend'),
'ciusers-success' => array('Success! Friend requests will now be sent to (number) friends.', 'Once they confirm your friendship, you will be able to see each other's profiles.', 'added multiple friends'), 'ciuser_error' => array('There was an error processing your request.', 'ciwl-password-disabled' => array('Password entered on Windows
Live', 'ciyh-password-disabled' => array('Password entered on Yahoo! login page'), 'ci:domain-list-desc' => array('We currently support the domains listed below. If you do not see your domain in the list but would like us to support it, please email info@facebook.com.'), /** ***/ contact_importer.js ***/ 'cioutlook-importer' => array('outlook importer (ie only) // Intro Text
'ci_v00' => array('You need to install the Outlook Importer ActiveX '. Control to continue', 'Prompts users that they need an ActiveX control to '. continue'), 'ci_v01' => array(' ', 'continue'), 'ci_v02' => array(' ', 'continue'), 'ci_v03' => array(' ', 'continue'), 'ci_v04' => array(' ', 'continue'), 'ci_v05' => array(' ', 'continue'), 'ci_v06' => array(' ', 'continue'), 'ci_v07' => array(' ', 'continue'), 'ci_v08' => array(' ', 'continue'), 'ci_v09' => array(' ', 'continue'), 'ci_v10' => array(' ', 'continue'), 'ci_v11' => array(' ', 'continue'), 'ci_v12' => array(' ', 'continue'), 'ci_v13' => array(' ', 'continue'), 'ci_v14' => array(' ', 'continue'), 'ci_v15' => array(' ', 'continue'), 'ci_v16' => array(' ', 'continue'), 'ci_v17' => array(' ', 'continue'), 'ci_v18' => array(' ', 'continue'), 'ci_v19' => array(' ', 'continue'), 'ci_v20' => array(' ', 'continue'), 'ci_v21' => array(' ', 'continue'), 'ci_v22' => array(' ', 'continue'), 'ci_v23' => array(' ', 'continue'), 'ci_v24' => array(' ', 'continue'), 'ci_v25' => array(' ', 'continue'), 'ci_v26' => array(' ', 'continue'), 'ci_v27' => array(' ', 'continue'), 'ci_v28' => array(' ', 'continue'), 'ci_v29' => array(' ', 'continue'), 'ci_v30' => array(' ', 'continue'), 'ci_v31' => array(' ', 'continue'), 'ci_v32' => array(' ', 'continue'), 'ci_v33' => array(' ', 'continue'), 'ci_v34' => array(' ', 'continue'), 'ci_v35' => array(' ', 'continue'), 'ci_v36' => array(' ', 'continue'), 'ci_v37' => array(' ', 'continue'), 'ci_v38' => array(' ', 'continue'), 'ci_v39' => array(' ', 'continue'), 'ci_v40' => array(' ', 'continue'), 'ci_v41' => array(' ', 'continue'), 'ci_v42' => array(' ', 'continue'), 'ci_v43' => array(' ', 'continue'), 'ci_v44' => array(' ', 'continue'), 'ci_v45' => array(' ', 'continue'), 'ci_v46' => array(' ', 'continue'), 'ci_v47' => array(' ', 'continue'), 'ci_v48' => array(' ', 'continue'), 'ci_v49' => array(' ', 'continue'), 'ci_v50' => array(' ', 'continue'), 'ci_v51' => array(' ', 'continue'), 'ci_v52' => array(' ', 'continue'), 'ci_v53' => array(' ', 'continue'), 'ci_v54' => array(' ', 'continue'), 'ci_v55' => array(' ', 'continue'), 'ci_v56' => array(' ', 'continue'), 'ci_v57' => array(' ', 'continue'), 'ci_v58' => array(' ', 'continue'), 'ci_v59' => array(' ', 'continue'), 'ci_v60' => array(' ', 'continue'), 'ci_v61' => array(' ', 'continue'), 'ci_v62' => array(' ', 'continue'), 'ci_v63' => array(' ', 'continue'), 'ci_v64' => array(' ', 'continue'), 'ci_v65' => array(' ', 'continue'), 'ci_v66' => array(' ', 'continue'), 'ci_v67' => array(' ', 'continue'), 'ci_v68' => array(' ', 'continue'), 'ci_v69' => array(' ', 'continue'), 'ci_v70' => array(' ', 'continue'), 'ci_v71' => array(' ', 'continue'), 'ci_v72' => array(' ', 'continue'), 'ci_v73' => array(' ', 'continue'), 'ci_v74' => array(' ', 'continue'), 'ci_v75' => array(' ', 'continue'), 'ci_v76' => array(' ', 'continue'), 'ci_v77' => array(' ', 'continue'), 'ci_v78' => array(' ', 'continue'), 'ci_v79' => array(' ', 'continue'), 'ci_v80' => array(' ', 'continue'), 'ci_v81' => array(' ', 'continue'), 'ci_v82' => array(' ', 'continue'), 'ci_v83' => array(' ', 'continue'), 'ci_v84' => array(' ', 'continue'), 'ci_v85' => array(' ', 'continue'), 'ci_v86' => array(' ', 'continue'), 'ci_v87' => array(' ', 'continue'), 'ci_v88' => array(' ', 'continue'), 'ci_v89' => array(' ', 'continue'), 'ci_v90' => array(' ', 'continue'), 'ci_v91' => array(' ', 'continue'), 'ci_v92' => array(' ', 'continue'), 'ci_v93' => array(' ', 'continue'), 'ci_v94' => array(' ', 'continue'), 'ci_v95' => array(' ', 'continue'), 'ci_v96' => array(' ', 'continue'), 'ci_v97' => array(' ', 'continue'), 'ci_v98' => array(' ', 'continue'), 'ci_v99' => array(' ', 'continue'), 'ci_v100' => array(' ', 'continue'), 'ci_v101' => array(' ', 'continue'), 'ci_v102' => array(' ', 'continue'), 'ci_v103' => array(' ', 'continue'), 'ci_v104' => array(' ', 'continue'), 'ci_v105' => array(' ', 'continue'), 'ci_v106' => array(' ', 'continue'), 'ci_v107' => array(' ', 'continue'), 'ci_v108' => array(' ', 'continue'), 'ci_v109' => array(' ', 'continue'), 'ci_v110' => array(' ', 'continue'), 'ci_v111' => array(' ', 'continue'), 'ci_v112' => array(' ', 'continue'), 'ci_v113' => array(' ', 'continue'), 'ci_v114' => array(' ', 'continue'), 'ci_v115' => array(' ', 'continue'), 'ci_v116' => array(' ', 'continue'), 'ci_v117' => array(' ', 'continue'), 'ci_v118' => array(' ', 'continue'), 'ci_v119' => array(' ', 'continue'), 'ci_v120' => array(' ', 'continue'), 'ci_v121' => array(' ', 'continue'), 'ci_v122' => array(' ', 'continue'), 'ci_v123' => array(' ', 'continue'), 'ci_v124' => array(' ', 'continue'), 'ci_v125' => array(' ', 'continue'), 'ci_v126' => array(' ', 'continue'), 'ci_v127' => array(' ', 'continue'), 'ci_v128' => array(' ', 'continue'), 'ci_v129' => array(' ', 'continue'), 'ci_v130' => array(' ', 'continue'), 'ci_v131' => array(' ', 'continue'), 'ci_v132' => array(' ', 'continue'), 'ci_v133' => array(' ', 'continue'), 'ci_v134' => array(' ', 'continue'), 'ci_v135' => array(' ', 'continue'), 'ci_v136' => array(' ', 'continue'), 'ci_v137' => array(' ', 'continue'), 'ci_v138' => array(' ', 'continue'), 'ci_v139' => array(' ', 'continue'), 'ci_v140' => array(' ', 'continue'), 'ci_v141' => array(' ', 'continue'), 'ci_v142' => array(' ', 'continue'), 'ci_v143' => array(' ', 'continue'), 'ci_v144' => array(' ', 'continue'), 'ci_v145' => array(' ', 'continue'), 'ci_v146' => array(' ', 'continue'), 'ci_v147' => array(' ', 'continue'), 'ci_v148' => array(' ', 'continue'), 'ci_v149' => array(' ', 'continue'), 'ci_v150' => array(' ', 'continue'), 'ci_v151' => array(' ', 'continue'), 'ci_v152' => array(' ', 'continue'), 'ci_v153' => array(' ', 'continue'), 'ci_v154' => array(' ', 'continue'), 'ci_v155' => array(' ', 'continue'), 'ci_v156' => array(' ', 'continue'), 'ci_v157' => array(' ', 'continue'), 'ci_v158' => array(' ', 'continue'), 'ci_v159' => array(' ', 'continue'), 'ci_v160' => array(' ', 'continue'), 'ci_v161' => array(' ', 'continue'), 'ci_v162' => array(' ', 'continue'), 'ci_v163' => array(' ', 'continue'), 'ci_v164' => array(' ', 'continue'), 'ci_v165' => array(' ', 'continue'), 'ci_v166' => array(' ', 'continue'), 'ci_v167' => array(' ', 'continue'), 'ci_v168' => array(' ', 'continue'), 'ci_v169' => array(' ', 'continue'), 'ci_v170' => array(' ', 'continue'), 'ci_v171' => array(' ', 'continue'), 'ci_v172' => array(' ', 'continue'), 'ci_v173' => array(' ', 'continue'), 'ci_v174' => array(' ', 'continue'), 'ci_v175' => array(' ', 'continue'), 'ci_v176' => array(' ', 'continue'), 'ci_v177' => array(' ', 'continue'), 'ci_v178' => array(' ', 'continue'), 'ci_v179' => array(' ', 'continue'), 'ci_v180' => array(' ', 'continue'), 'ci_v181' => array(' ', 'continue'), 'ci_v182' => array(' ', 'continue'), 'ci_v183' => array(' ', 'continue'), 'ci_v184' => array(' ', 'continue'), 'ci_v185' => array(' ', 'continue'), 'ci_v186' => array(' ', 'continue'), 'ci_v187' => array(' ', 'continue'), 'ci_v188' => array(' ', 'continue'), 'ci_v189' => array(' ', 'continue'), 'ci_v190' => array(' ', 'continue'), 'ci_v191' => array(' ', 'continue'), 'ci_v192' => array(' ', 'continue'), 'ci_v193' => array(' ', 'continue'), 'ci_v194' => array(' ', 'continue'), 'ci_v195' => array(' ', 'continue'), 'ci_v196' => array(' ', 'continue'), 'ci_v197' => array(' ', 'continue'), 'ci_v198' => array(' ', 'continue'), 'ci_v199' => array(' ', 'continue'), 'ci_v200' => array(' ', 'continue'), 'ci_v201' => array(' ', 'continue'), 'ci_v202' => array(' ', 'continue'), 'ci_v203' => array(' ', 'continue'), 'ci_v204' => array(' ', 'continue'), 'ci_v205' => array(' ', 'continue'), 'ci_v206' => array(' ', 'continue'), 'ci_v207' => array(' ', 'continue'), 'ci_v208' => array(' ', 'continue'), 'ci_v209' => array(' ', 'continue'), 'ci_v210' => array(' ', 'continue'), 'ci_v211' => array(' ', 'continue'), 'ci_v212' => array(' ', 'continue'), 'ci_v213' => array(' ', 'continue'), 'ci_v214' => array(' ', 'continue'), 'ci_v215' => array(' ', 'continue'), 'ci_v216' => array(' ', 'continue'), 'ci_v217' => array(' ', 'continue'), 'ci_v218' => array(' ', 'continue'), 'ci_v219' => array(' ', 'continue'), 'ci_v220' => array(' ', 'continue'), 'ci_v221' => array(' ', 'continue'), 'ci_v222' => array(' ', 'continue'), 'ci_v223' => array(' ', 'continue'), 'ci_v224' => array(' ', 'continue'), 'ci_v225' => array(' ', 'continue'), 'ci_v226' => array(' ', 'continue'), 'ci_v227' => array(' ', 'continue'), 'ci_v228' => array(' ', 'continue'), 'ci_v229' => array(' ', 'continue'), 'ci_v230' => array(' ', 'continue'), 'ci_v231' => array(' ', 'continue'), 'ci_v232' => array(' ', 'continue'), 'ci_v233' => array(' ', 'continue'), 'ci_v234' => array(' ', 'continue'), 'ci_v235' => array(' ', 'continue'), 'ci_v236' => array(' ', 'continue'), 'ci_v237' => array(' ', 'continue'), 'ci_v238' => array(' ', 'continue'), 'ci_v239' => array(' ', 'continue'), 'ci_v240' => array(' ', 'continue'), 'ci_v241' => array(' ', 'continue'), 'ci_v242' => array(' ', 'continue'), 'ci_v243' => array(' ', 'continue'), 'ci_v244' => array(' ', 'continue'), 'ci_v245' => array(' ', 'continue'), 'ci_v246' => array(' ', 'continue'), 'ci_v247' => array(' ', 'continue'), 'ci_v248' => array(' ', 'continue'), 'ci_v249' => array(' ', 'continue'), 'ci_v250' => array(' ', 'continue'), 'ci_v251' => array(' ', 'continue'), 'ci_v252' => array(' ', 'continue'), 'ci_v253' => array(' ', 'continue'), 'ci_v254' => array(' ', 'continue'), 'ci_v255' => array(' ', 'continue'), 'ci_v256' => array(' ', 'continue'), 'ci_v257' => array(' ', 'continue'), 'ci_v258' => array(' ', 'continue'), 'ci_v259' => array(' ', 'continue'), 'ci_v260' => array(' ', 'continue'), 'ci_v261' => array(' ', 'continue'), 'ci_v262' => array(' ', 'continue'), 'ci_v263' => array(' ', 'continue'), 'ci_v264' => array(' ', 'continue'), 'ci_v265' => array(' ', 'continue'), 'ci_v266' => array(' ', 'continue'), 'ci_v267' => array(' ', 'continue'), 'ci_v268' => array(' ', 'continue'), 'ci_v269' => array(' ', 'continue'), 'ci_v270' => array(' ', 'continue'), 'ci_v271' => array(' ', 'continue'), 'ci_v272' => array(' ', 'continue'), 'ci_v273' => array(' ', 'continue'), 'ci_v274' => array(' ', 'continue'), 'ci_v275' => array(' ', 'continue'), 'ci_v276' => array(' ', 'continue'), 'ci_v277' => array(' ', 'continue'), 'ci_v278' => array(' ', 'continue'), 'ci_v279' => array(' ', 'continue'), 'ci_v280' => array(' ', 'continue'), 'ci_v281' => array(' ', 'continue'), 'ci_v282' => array(' ', 'continue'), 'ci_v283' => array(' ', 'continue'), 'ci_v284' => array(' ', 'continue'), 'ci_v285' => array(' ', 'continue'), 'ci_v286' => array(' ', 'continue'), 'ci_v287' => array(' ', 'continue'), 'ci_v288' => array(' ', 'continue'), 'ci_v289' => array(' ', 'continue'), 'ci_v290' => array(' ', 'continue'), 'ci_v291' => array(' ', 'continue'), 'ci_v292' => array(' ', 'continue'), 'ci_v293' => array(' ', 'continue'), 'ci_v294' => array(' ', 'continue'), 'ci_v295' => array(' ', 'continue'), 'ci_v296' => array(' ', 'continue'), 'ci_v297' => array(' ', 'continue'), 'ci_v298' => array(' ', 'continue'), 'ci_v299' => array(' ', 'continue'), 'ci_v300' => array(' ', 'continue'), 'ci_v301' => array(' ', 'continue'), 'ci_v302' => array(' ', 'continue'), 'ci_v303' => array(' ', 'continue'), 'ci_v304' => array(' ', 'continue'), 'ci_v305' => array(' ', 'continue'), 'ci_v306' => array(' ', 'continue'), 'ci_v307' => array(' ', 'continue'), 'ci_v308' => array(' ', 'continue'), 'ci_v309' => array(' ', 'continue'), 'ci_v310' => array(' ', 'continue'), 'ci_v311' => array(' ', 'continue'), 'ci_v312' => array(' ', 'continue'), 'ci_v313' => array(' ', 'continue'), 'ci_v314' => array(' ', 'continue'), 'ci_v315' => array(' ', 'continue'), 'ci_v316' => array(' ', 'continue'), 'ci_v317' => array(' ', 'continue'), 'ci_v318' => array(' ', 'continue'), 'ci_v319' => array(' ', 'continue'), 'ci_v320' => array(' ', 'continue'), 'ci_v321' => array(' ', 'continue'), 'ci_v322' => array(' ', 'continue'), 'ci_v323' => array(' ', 'continue'), 'ci_v324' => array(' ', 'continue'), 'ci_v325' => array(' ', 'continue'), 'ci_v326' => array(' ', 'continue'), 'ci_v327' => array(' ', 'continue'), 'ci_v328' => array(' ', 'continue'), 'ci_v329' => array(' ', 'continue'), 'ci_v330' => array(' ', 'continue'), 'ci_v331' => array(' ', 'continue'), 'ci_v332' => array(' ', 'continue'), 'ci_v333' => array(' ', 'continue'), 'ci_v334' => array(' ', 'continue'), 'ci_v335' => array(' ', 'continue'), 'ci_v336' => array(' ', 'continue'), 'ci_v337' => array(' ', 'continue'), 'ci_v338' => array(' ', 'continue'), 'ci_v339' => array(' ', 'continue'), 'ci_v340' => array(' ', 'continue'), 'ci_v341' => array(' ', 'continue'), 'ci_v342' => array(' ', 'continue'), 'ci_v343' => array(' ', 'continue'), 'ci_v344' => array(' ', 'continue'), 'ci_v345' => array(' ', 'continue'), 'ci_v346' => array(' ', 'continue'), 'ci_v347' => array(' ', 'continue'), 'ci_v348' => array(' ', 'continue'), 'ci_v349' => array(' ', 'continue'), 'ci_v350' => array(' ', 'continue'), 'ci_v351' => array(' ', 'continue'), 'ci_v352' => array(' ', 'continue'), 'ci_v353' => array(' ', 'continue'), 'ci_v354' => array(' ', 'continue'), 'ci_v355' => array(' ', 'continue'), 'ci_v356' => array(' ', 'continue'), 'ci_v357' => array(' ', 'continue'), 'ci_v358' => array(' ', 'continue'), 'ci_v359' => array(' ', 'continue'), 'ci_v360' => array(' ', 'continue'), 'ci_v361' => array(' ', 'continue'), 'ci_v362' => array(' ', 'continue'), 'ci_v363' => array(' ', 'continue'), 'ci_v364' => array(' ', 'continue'), 'ci_v365' => array(' ', 'continue'), 'ci_v366' => array(' ', 'continue'), 'ci_v367' => array(' ', 'continue'), 'ci_v368' => array(' ', 'continue'), 'ci_v369' => array(' ', 'continue'), 'ci_v370' => array(' ', 'continue'), 'ci_v371' => array(' ', 'continue'), 'ci_v372' => array(' ', 'continue'), 'ci_v373' => array(' ', 'continue'), 'ci_v374' => array(' ', 'continue'), 'ci_v375' => array(' ', 'continue'), 'ci_v376' => array(' ', 'continue'), 'ci_v377' => array(' ', 'continue'), 'ci_v378' => array(' ', 'continue'), 'ci_v379' => array(' ', 'continue'), 'ci_v380' => array(' ', 'continue'), 'ci_v381' => array(' ', 'continue'), 'ci_v382' => array(' ', 'continue'), 'ci_v383' => array(' ', 'continue'), 'ci_v384' => array(' ', 'continue'), 'ci_v385' => array(' ', 'continue'), 'ci_v386' => array(' ', 'continue'), 'ci_v387' => array(' ', 'continue'), 'ci_v388' => array(' ', 'continue'), 'ci_v389' => array(' ', 'continue'), 'ci_v390' => array(' ', 'continue'), 'ci_v391' => array(' ', 'continue'), 'ci_v392' => array(' ', 'continue'), 'ci_v393' => array(' ', 'continue'), 'ci_v394' => array(' ', 'continue'), 'ci_v395' => array(' ', 'continue'), 'ci_v396' => array(' ', 'continue'), 'ci_v397' => array(' ', 'continue'), 'ci_v398' => array(' ', 'continue'), 'ci_v399' => array(' ', 'continue'), 'ci_v400' => array(' ', 'continue'), 'ci_v401' => array(' ', 'continue'), 'ci_v402' => array(' ', 'continue'), 'ci_v403' => array(' ', 'continue'), 'ci_v404' => array(' ', 'continue'), 'ci_v405' => array(' ', 'continue'), 'ci_v406' => array(' ', 'continue'), 'ci_v407' => array(' ', 'continue'), 'ci_v408' =&gt
```


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



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

TOP STORIES | SINGAPORE | SCIENCE | LIFESTYLE | BLOGS

Home > Breaking News > Singapore

March 3, 2009

Glitch

Wealthy customers' bank statements spilled

A TECHNICAL glitch at UBS on Monday allowed private-banking clients in Singapore and Hong Kong to see confidential details of other clients' bank statements and account information on their online accounts.

The private-banking clients found that they could see bank statements and account information of other clients' online accounts, though, do not indicate their names.

When contacted, a UBS spokesman confirmed that the bank was taking it very seriously.

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

12:53 PM
12:50 PM
12:17 PM
6:00 AM
6:00 AM
6:00 AM
6:00 AM
6:00 AM
6:00 AM
6:00 AM
6:00 AM
6:00 AM
6:00 AM
6:00 AM

Parents identify son's body
Lower interest on deposits
Youth games on Web
Airlines' \$12b loss in 2008
STI at lowest since Aug '03
A-level results out on Fri
Family sues HSBC over forex
Signs of violent struggle
Glitch spills UBS clients' info
Well respected by students
Lightning strikes all too often
SPH websites score high

Scenario 4: Sensitive Information Left on Web Server

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 Review
response
sex
The
Florida
ethnicities and

“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 “

students' skills in mathematics, reading, science, and writing. The data also included other sensitive information regarding learning disabilities, or whether students were bilingual or not.

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

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

Scenario 4: Sensitive Information Left on Web Server

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	

Scenario 4: Sensitive Information Left on Web Server

Ministry B, Singapore

- Locations of friendly foreign armed forces units in Singapore were leaked.

URL is not shown

Previous Entity Registration No	Entity Name	Registered Address Street Name
Issuance Agency	Entity Type	UEN
<u>Mindef</u>	FM	T08FM0001E
<u>Mindef</u>	FM	T08FM0002A
<u>Mindef</u>	FM	T08FM0003H
<u>Mindef</u>	FM	T08FM0004D
<u>Mindef</u>	FM	T08FM0005L
<u>Mindef</u>	FM	T08FM0006G

Previous

Entity Name

ROYAL AUSTRALIAN NAVY (RAN)

AUSTRALIAN DEFENCE FORCE

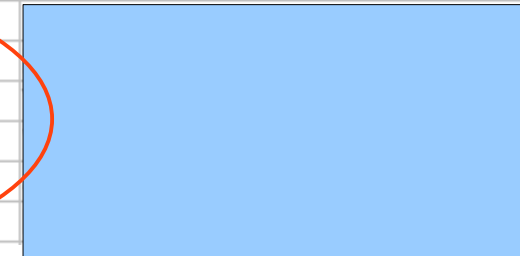
DEFENCE FUELS GROUP

NEW ZEALAND DEFENCE SUPPORT UNIT (SEA)

FISC DETACHMENT SINGAPORE

NAVY REGION CENTER SINGAPORE (NRCS)

Registered Address Street Name



Scenario 4: Sensitive Information Left on Web Server

Polytechnic A, Singapore

- Private information of 53 students were leaked.

URL is not shown

New Approvals from Sean								
ID	Name	Contact	NRIC	Email	Sup_Doc_Rec		Remar	
282		92704847	S8039798D	50361@	Approved	50361		
252		67521219	S8716561B	50406@	Approved	50406		
409		67604603	S8832950C	51097@	Approved	51097		
278		94505231	S8622886F	51418@	Approved	51418		
297		91432246	S8702820H	51611@	Approved	51611		
349		91874897	S8319872I	52014@	Approved	52014		
348		65870972	S8713281A	52075@	Approved	52075		
347		65602371	S8605561I	51648@	Approved	51648		
ID		Contact	NRIC	Email	Sup_Doc_Rec	UserID	Remar	
232		94311584	S8812558D	50835@	Approved	50835	Paid \$.	
235		81398095	G0339247W	50086@	Approved	50086	paid \$.	
236		91294047	S8723133Z	50455@	Approved	50455	Paid \$.	
238		67954374	S8809559F	50795@	Approved	50795	Paid \$.	
239		81004593	S8327283Z	50362@	Approved	50362	Paid \$.	
245		67824968	S8805838J	50734@	Approved	50734	Paid \$.	
254		93805712	S8731801Z	50539@	Approved	50539	paid \$.	
255		63630161	S8823042F	50973@	Approved	50973	Paid \$.	
257		65697545	S8743357I	50633@	Approved	50633	Paid \$.	
268		91738425	S8816010Z	51906@	Approved	51906	Decline	
		mobile						
269		94742839	S8730896J	50527@	Approved	50527	paid \$.	
279		63672712	S8822329B	50965@	Approved	50965	Paid \$.	

Scenario 4: Sensitive Information Left on Web Server

High School A, Singapore

- National ID for 44 secondary students were leaked.

URL is not shown

[REDACTED]													
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	[REDACTED]	S9570431Z		23/05/08									
2	[REDACTED]	S9527958I		23/05/08									
3	[REDACTED]	S9524379G		23/05/08				07/11/08					
4	[REDACTED]	S9501671E		23/05/08									
5	[REDACTED]	S9543949G		11/07/08									
6	[REDACTED]	S9570194I		23/05/08									
7	[REDACTED]	S9533923I		23/05/08				07/11/08					
8	[REDACTED]	S9531990D		23/05/08									
9	[REDACTED]	S9514429B		23/05/08									
10	[REDACTED]	S9527320C		23/05/08									
11	[REDACTED]	S9590023B		23/05/08									
12	[REDACTED]	S9533159I		23/05/08				07/11/08					
13	[REDACTED]	S9571436F		23/05/08									
14	[REDACTED]	S9540695E		23/05/08									

Scenario 4: Sensitive Information Left on Web Server

High School B, Singapore

- National ID for 20 secondary students were leaked.

URL is not shown

TRINITY MUSIC CENTRE					
(Singapore Representative for Music / Speech & Drama)					
Date Of Exam : 13 November 2007 (Tue)					
Venue Of Exam : [REDACTED]					
Time	Candidates' Name	Grade	Subject	Reg. No.	NRIC
9.00 - 9.20	[REDACTED]	4	Communication Skills		S9221677B
9.20 - 9.40		4	Communication Skills		S9214584J
9.40 - 10.00		4	Communication Skills		F2796956U
10.00 - 10.20		5	Communication Skills		S9212065A
10.20 - 10.40		5	Communication Skills		S9217344E
10.40 - 11.00		B R E A K			
11.00 - 11.20	ELANEYOGANVINO	5	Communication Skills		S9212065A

Scenario 4: Sensitive Information Left on Web Server

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		LIU WEN QIANG VINCENT	S9116041B	5/7/1991

Scenario 4: Sensitive Information Left on Web Server

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_it@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
		kennytbd@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
		chua06@singnet.com.sg	97972940	03S15	15/08/86	S8622355D
		jambrianfu@hotmail.com	97264784	03S1A	08/06/86	S8616016A
		johathanley@hotmail.com	97879631	03S13	17/07/86	S8619089C
		khoochwee05@hotmail.com	98475015	03S32	21/07/86	S8619880J

Scenario 4: Sensitive Information Left on Web Server

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	[REDACTED]
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?

Scenario 4: Sensitive Information Left on Web Server

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

Scenario 4: Sensitive Information Left on Web Server

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

Scenario 4: Sensitive Information Left on Web Server

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

Scenario 4: Sensitive Information Left on Web Server

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		

Scenario 4: Sensitive Information Left on Web Server

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	Please arrange to reimburse		
\$0.00			
\$0.00	NRIC / FIN No.	S83059381	
\$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

Scenario 4: Sensitive Information Left on Web Server

Research Institute A, Singapore

- Entire list of 375 staff were leaked.

URL is not shown

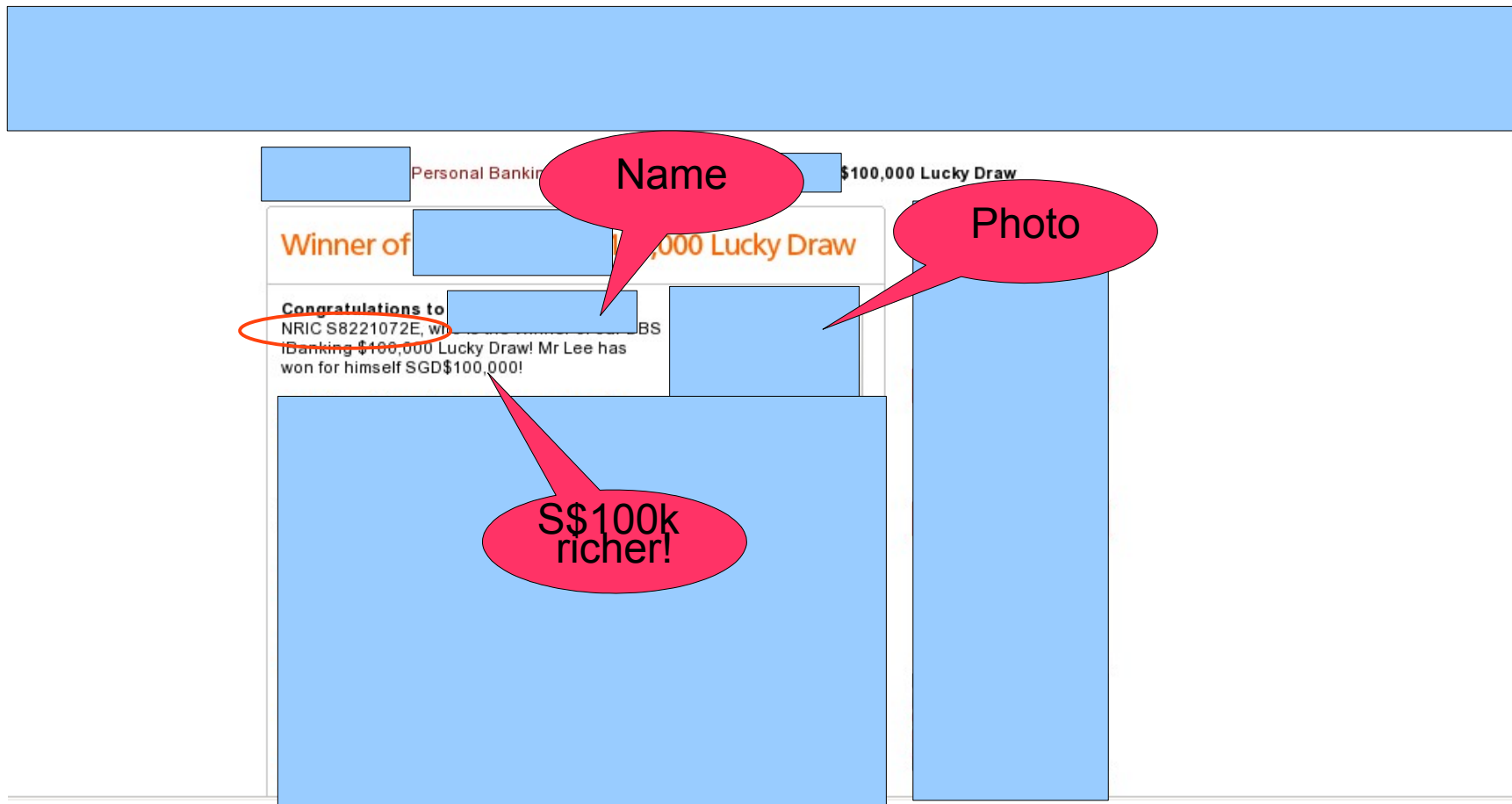
Mail	Name	SN	givenName	Phone	Title
sflee@ri.a.gov.sg	Lee Siew Fong	Lee	Siew Fong	67938235	Snr An
Lynn@ri.a.gov.sg	Au Lynn	Au	Lynn	67938240	Snr An
larry@ri.a.gov.sg	Lim Seow Yam Larry	Lim	Seow Yam	67938241	Snr An
hhyo@ri.a.gov.sg	Yong Hock Hung	Yong	Hock Hung	67938237	Progr
kcwo@ri.a.gov.sg	Wong Kam Choy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

Scenario 4: Sensitive Information Left on Web Server

Bank A, Singapore

- National ID of a lucky draw winner was leaked.

URL is not shown



Scenario 4: Sensitive Information Left on Web Server

Polytechnic B, Singapore

- Administrator password was leaked.

URL is not shown

OPAC [redacted] -- More Searches -- [Help](#)

[Basic Search](#) [Advanced Search](#) [Previous Search](#) [Results List](#) [Basket](#) [User](#)

[Add to Basket](#) | [Email / Save Record](#)

Full Record No. 1 out of 1 [Back to Result List](#)

[Previous Record](#) [Next Record](#)

Call Number	LB1044.7 JET
Title	Learning, media and technology.
Prev. Title	Journal of educational media ISSN:1358-1651
Availability	All items [redacted]
Frequency	Quarterly 2006-
Former Frequency	Three issues a year 2005-2005
Publication Date	Vol. 30, no. 1 (Mar. 2005)-
Publisher	Basingstoke : Routledge, c2005-
Description	v. : ill. ; 25 cm.
Electronic Location	View online on campus only View online via SwetsWise on campus only { Click on IP authentication within SwetsWise }
Notes	Title from cover.
Notes	Administrator id=jamilah, password=1633[redacted]
Subject Heading	Educational technology -- Periodicals

Scenario 4: Sensitive Information Left on Web Server

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/caweb site/CAowntownspace.txt"; String filename = "e:\\home01\\docs\\cudd\\caweb site  
\\CAowntownspace.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!

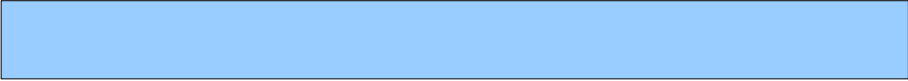
LOADING IN PROGRESS ...

Scenario 4: Sensitive Information Left on Web Server

Statutory Board E, Singapore

- Directory listing exposed files and source codes

URL is not shown

		/einfo/
[To Parent Directory]		
Tuesday, September 23, 2003 11:03 AM	<dir>	_private
Tuesday, September 23, 2003 11:03 AM	<dir>	_ScriptLibrary
Monday, December 20, 2004 3:00 PM	636937	290305GUIcontrol.asp
Tuesday, March 18, 2003 5:09 PM	2583	addKeyword.asp
Tuesday, October 15, 2002 1:31 PM	2565	addKeywordOLD.asp
Friday, July 13, 2007 5:43 PM	<dir>	Admin
Tuesday, June 22, 2004 9:52 AM	<dir>	AdminDocs
Friday, April 11, 2003 3:48 PM	2153	ado_upload.asp
Friday, April 11, 2003 3:48 PM	2102	ado_upload_admin.asp
Tuesday, September 30, 2003 5:54 PM	5922	AR_LoginMenu.js
Tuesday, September 30, 2003 5:54 PM	5922	AR_LoginMenu13122004.js
Monday, April 28, 2003 12:29 PM	5915	AR_LoginMenuold.js
Tuesday, September 23, 2003 11:03 AM	<dir>	asp
Friday, April 04, 2003 4:46 PM	1411	ASPPage1.asp
Tuesday, September 23, 2003 11:03 AM	<dir>	AuthFiles
Thursday, August 08, 2002 7:21 AM	120	backbutton.gif
Tuesday, September 23, 2003 11:03 AM	<dir>	
Saturday, December 01, 2001 5:55 AM	86967	.xsl
Thursday, September 27, 2001 2:50 AM	86671	20011130.xsl
Friday, January 25, 2002 2:22 AM	92951	25Jan02.xsl
Thursday, December 06, 2007 2:50 PM	<dir>	TS
Friday, November 10, 2000 10:46 AM	3706	BDRRefresh.asp
Monday, October 27, 2003 2:25 PM	1423	broadcast.html
Friday, June 22, 2007 5:01 PM	<dir>	BROADCASTER
Tuesday, June 25, 2002 3:59 AM	1695	BUT.gif
Thursday, December 27, 2001 9:56 AM	11546	CatalogProperties.xml
Friday, October 01, 2004 11:17 AM	13598	CheckCir.asp
Wednesday, August 14, 2002 1:23 AM	13526	CheckCiroid.asp
Saturday, August 03, 2002 8:14 AM	16336	Checknews.asp
Tuesday, January 09, 2007 12:34 PM	24771	circular_listing_bakup_4Jul07.asp
Friday, July 13, 2007 5:56 PM	24898	circular_listing.asp
Wednesday, January 25, 2006 3:41 PM	20525	circular_listing_bakup_30Nov06.asp
Wednesday, July 04, 2007 10:24 AM	24832	circular_listing_bakup_5Jul07.asp

Scenario 4: Sensitive Information Left on Web Server

ISP A, Singapore

- SQL file was exposed.

URL is not shown

```
-- Script Name: [REDACTED]
-- Created 28/05/2001 by Koh Seow Boon
-- Script to be run by csapp
-- Purpose: This is for the new [REDACTED] 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 [REDACTED]
-- in June 2001. Authenticates dial-in password and redirects
-- to the free trial [REDACTED] website.
--
-- Koh Seow Boon 28/05/2001
-----
-- Version 1.01
--
-- Changes paths of gif files from [REDACTED] 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 [REDACTED] as

    Procedure login
        (mstatus in varchar2 default Null);

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

End;
/
show errors
```

Scenario 4: Sensitive Information Left on Web Server

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[REDACTED].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 [REDACTED] 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;
```

Scenario 4: Sensitive Information Left on Web Server

Naga City, Philippines

- Database password and username were leaked.

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

```
<?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**