Web Application Security

Basic SQL injection
Basic Click Jacking

Vinod Senthil T
Director
infySEC
vinod@infysec.com
044-42611142/43

OWASP
11th August, 2012

The OWASP Foundation
http://www.owasp.org

$whoami

Vinod T Senthil - Information security consultant/researcher for infySEC. By Qualification he is a **Computer Science engineer, MBA in IT** along with a **Diploma in Cyber crime.**

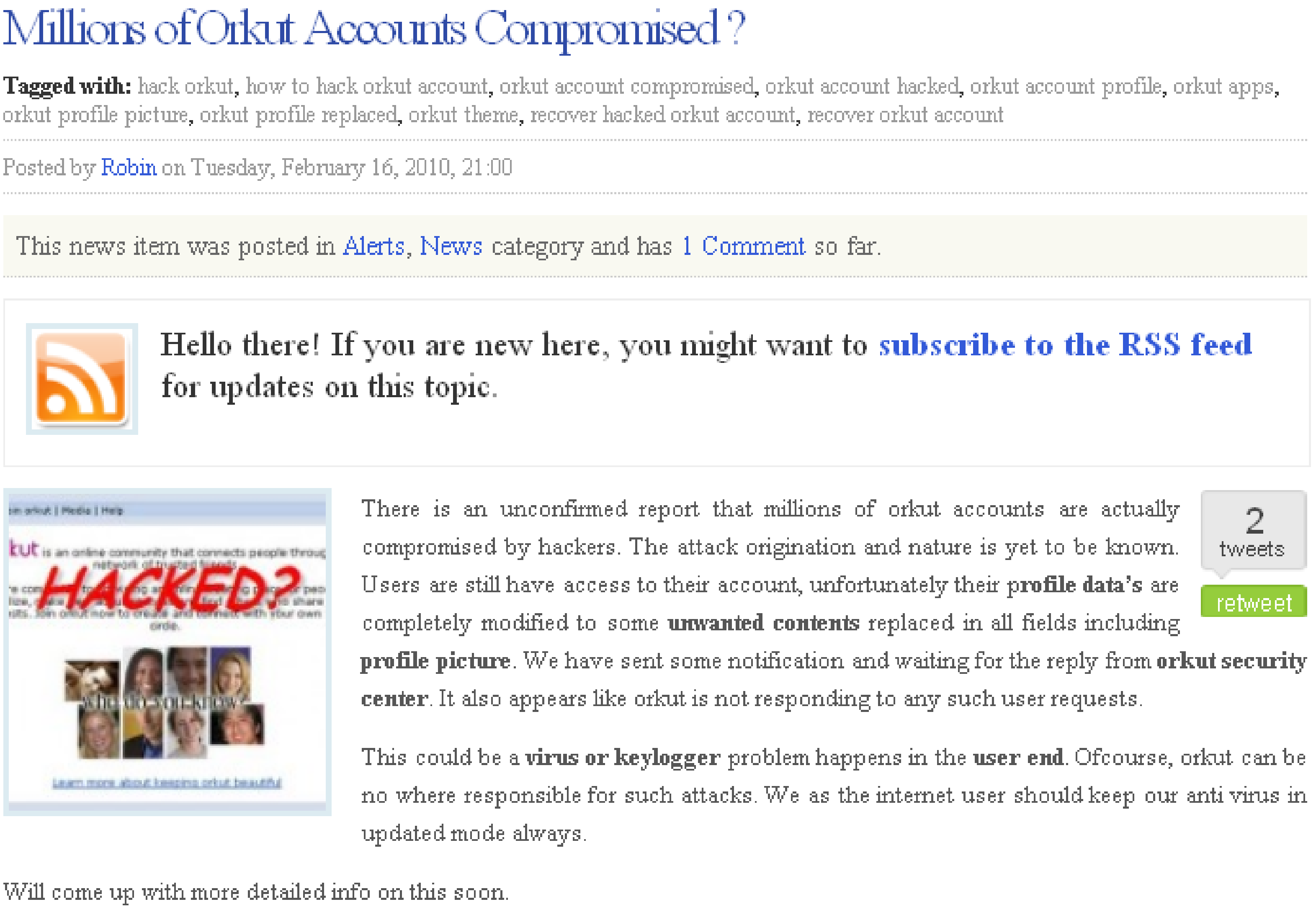
Also posses some certifications such as

- SANS Certified Intrusion Analyst – GCIA
- Certified Ethical Hacker (CEH)
- Certified Hacker Forensics Investigator (CHFI)
- Checkpoint Certified Security Administrator (CCSA)
- Oracle Certified Associate (OCA)
- Microsoft Certified Professional (MCP)
- IT Infrastructure Library (ITIL V3)
- Cisco Certified Network Administrator (CCNA)

What is the ‘Worlds MOST Secured System’ ?

The worlds most secured system is a system, That is dug 10ooo miles underground, and surrounded by 10ooo volts of electrified fences and filled with toxic nitrous gas on all sides , with a bunch of trained army men, and still it stays to be one of the most vulnerable piece of a code.

Little of History



Millions of Orkut Accounts Compromised ?

Tagged with: hack orkut, how to hack orkut account, orkut account compromised, orkut account hacked, orkut account profile, orkut apps, orkut profile picture, orkut profile replaced, orkut theme, recover hacked orkut account, recover orkut account

Posted by Robin on Tuesday, February 16, 2010, 21:00

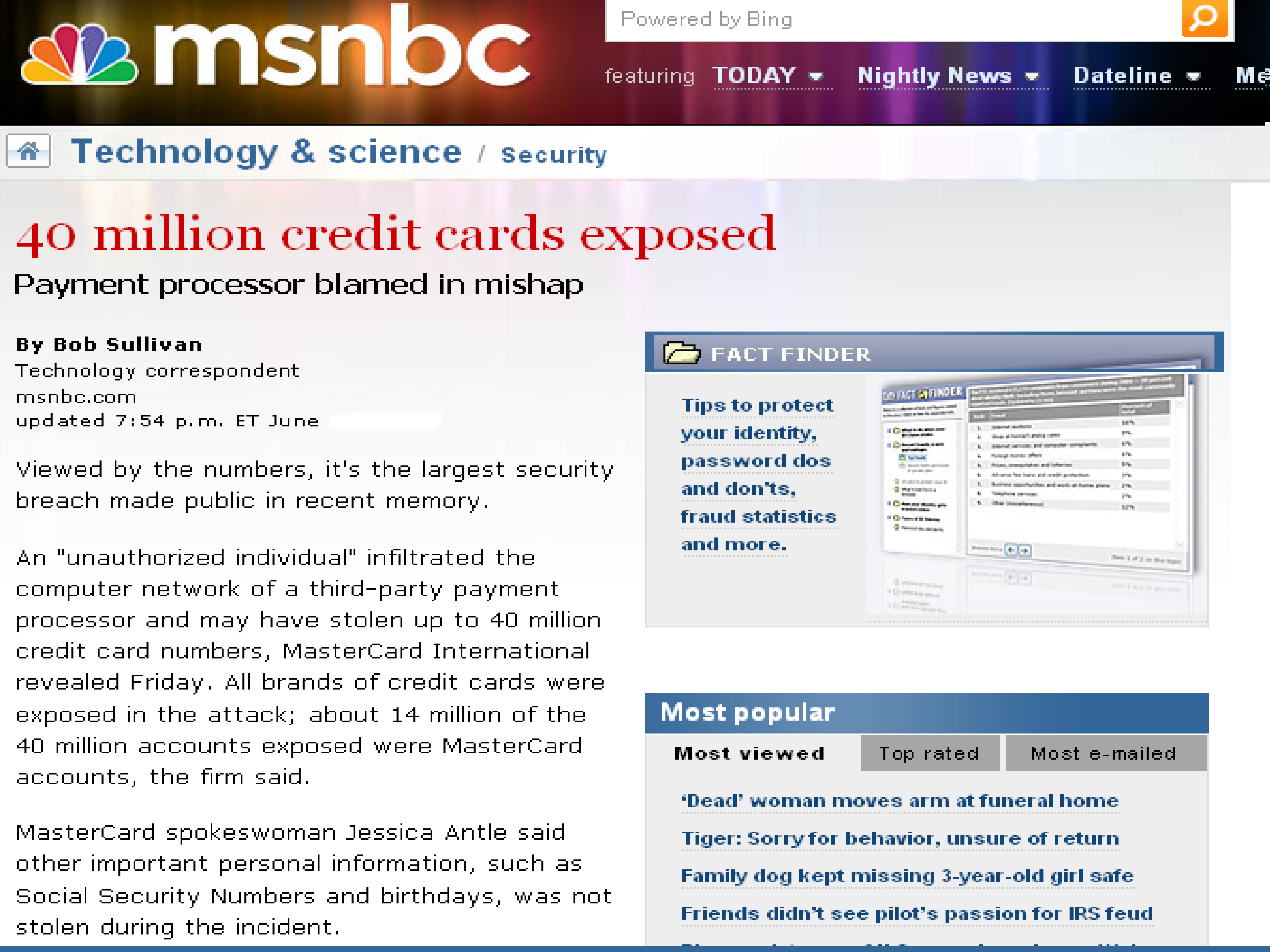
This news item was posted in Alerts, News category and has 1 Comment so far.

Hello there! If you are new here, you might want to **subscribe to the RSS feed** for updates on this topic.

There is an unconfirmed report that millions of orkut accounts are actually compromised by hackers. The attack origination and nature is yet to be known. Users are still have access to their account, unfortunately their **profile data's** are completely modified to some **unwanted contents** replaced in all fields including **profile picture**. We have sent some notification and waiting for the reply from **orkut security center**. It also appears like orkut is not responding to any such user requests.

This could be a **virus or keylogger** problem happens in the **user end**. Ofcourse, orkut can be no where responsible for such attacks. We as the internet user should keep our anti virus in updated mode always.

Will come up with more detailed info on this soon.



40 million credit cards exposed

Payment processor blamed in mishap

By Bob Sullivan
Technology correspondent
msnbc.com
updated 7:54 p.m. ET June

Viewed by the numbers, it's the largest security breach made public in recent memory.

An "unauthorized individual" infiltrated the computer network of a third-party payment processor and may have stolen up to 40 million credit card numbers, MasterCard International revealed Friday. All brands of credit cards were exposed in the attack; about 14 million of the 40 million accounts exposed were MasterCard accounts, the firm said.

MasterCard spokeswoman Jessica Antle said other important personal information, such as Social Security Numbers and birthdays, was not stolen during the incident.

FACT FINDER

Tips to protect your identity, password dos and don'ts, fraud statistics and more.

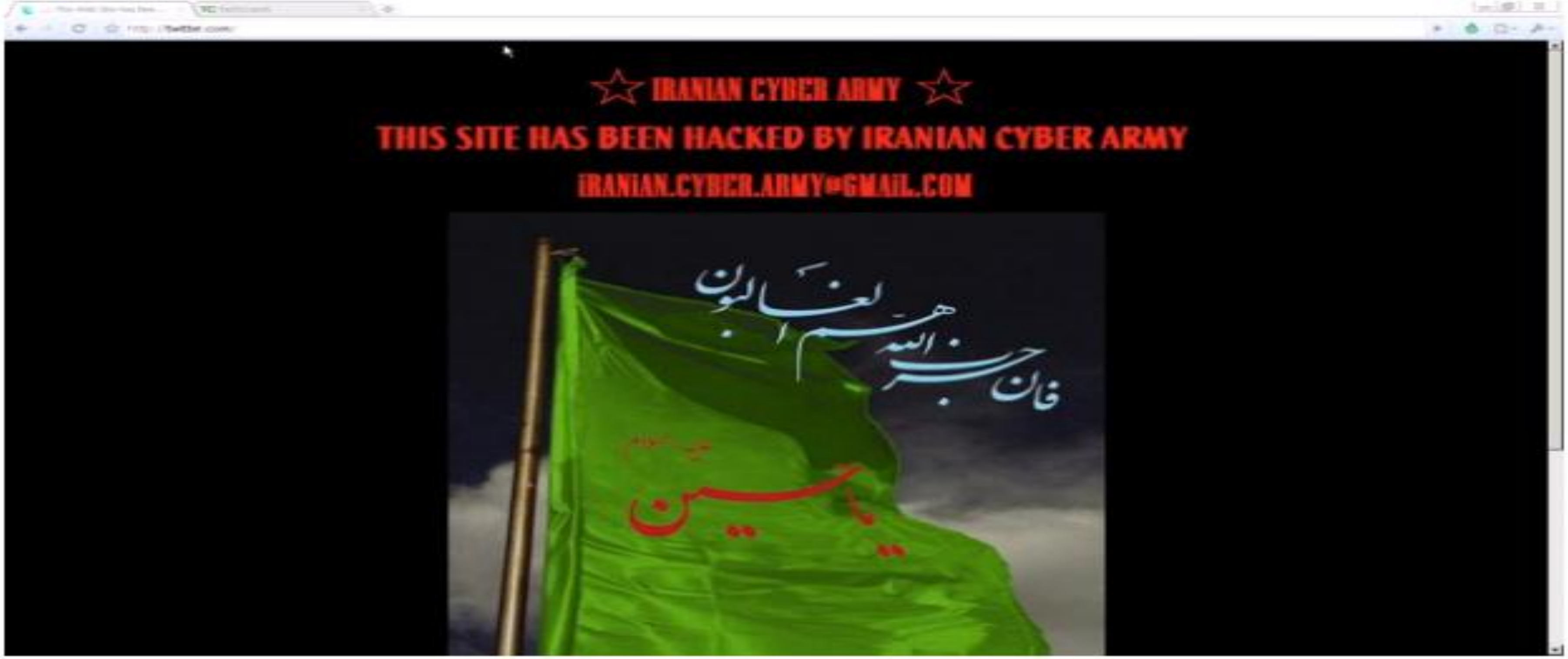
Most popular

Most viewed | Top rated | Most e-mailed

'Dead' woman moves arm at funeral home
Tiger: Sorry for behavior, unsure of return
Family dog kept missing 3-year-old girl safe
Friends didn't see pilot's passion for IRS feud

Twitter Hacked, Defaced By "Iranian Cyber Army"

by **Michael Arrington** on Dec   **785 Comments** **4136** retweet **Share** 2828 **Buzz it**



☆ IRANIAN CYBER ARMY ☆

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

iRANiAN.CYBER.ARMY@GMAIL.COM

We've received multiple tips right around 10 pm that **Twitter** was hacked and defaced with the message below. The site was offline for a while.

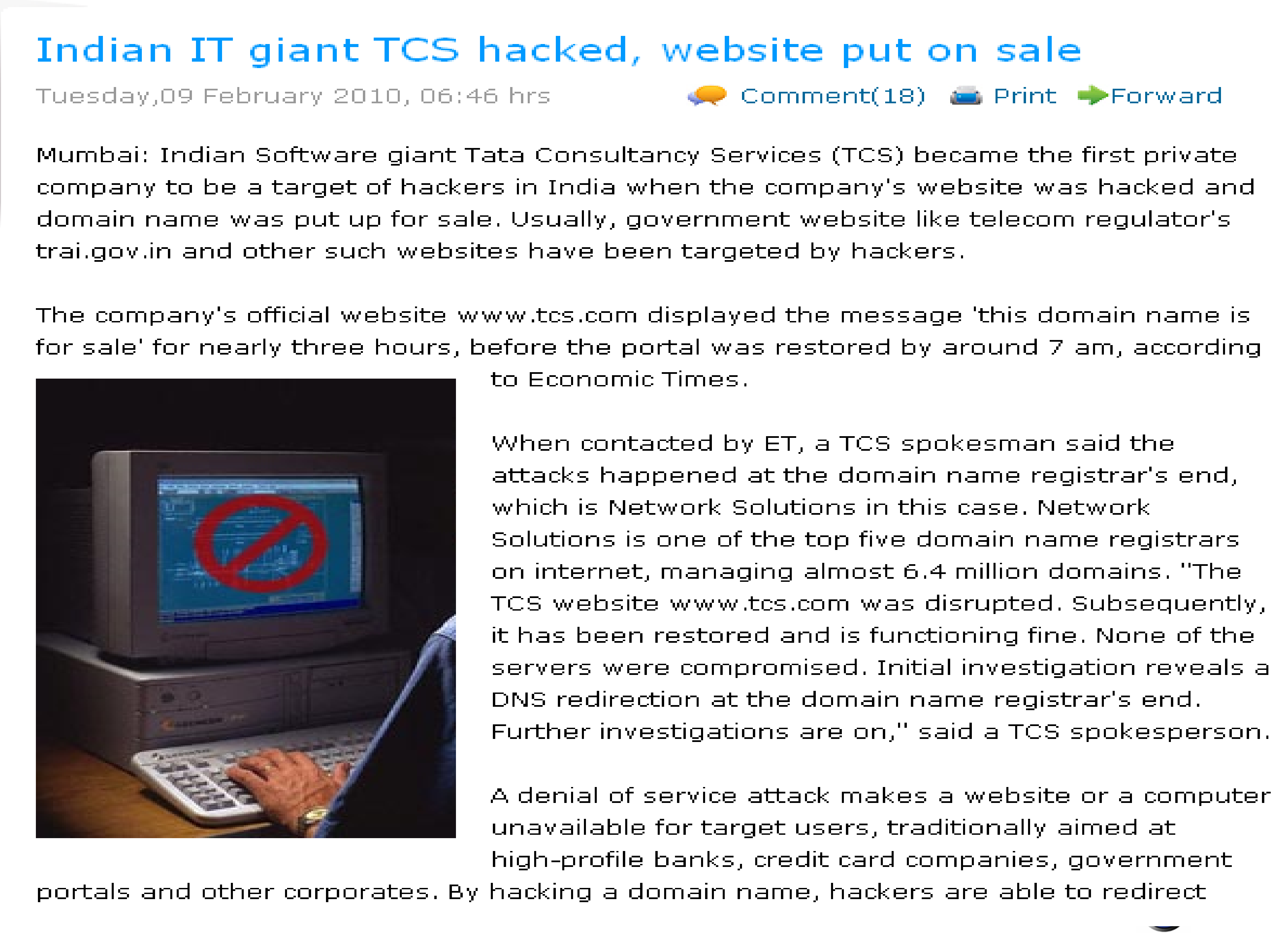
We're looking into this and awaiting on a response from Twitter.

The message read:

Iranian Cyber Army

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

iRANiAN.CYBER.ARMY@GMAIL.COM



Indian IT giant TCS hacked, website put on sale

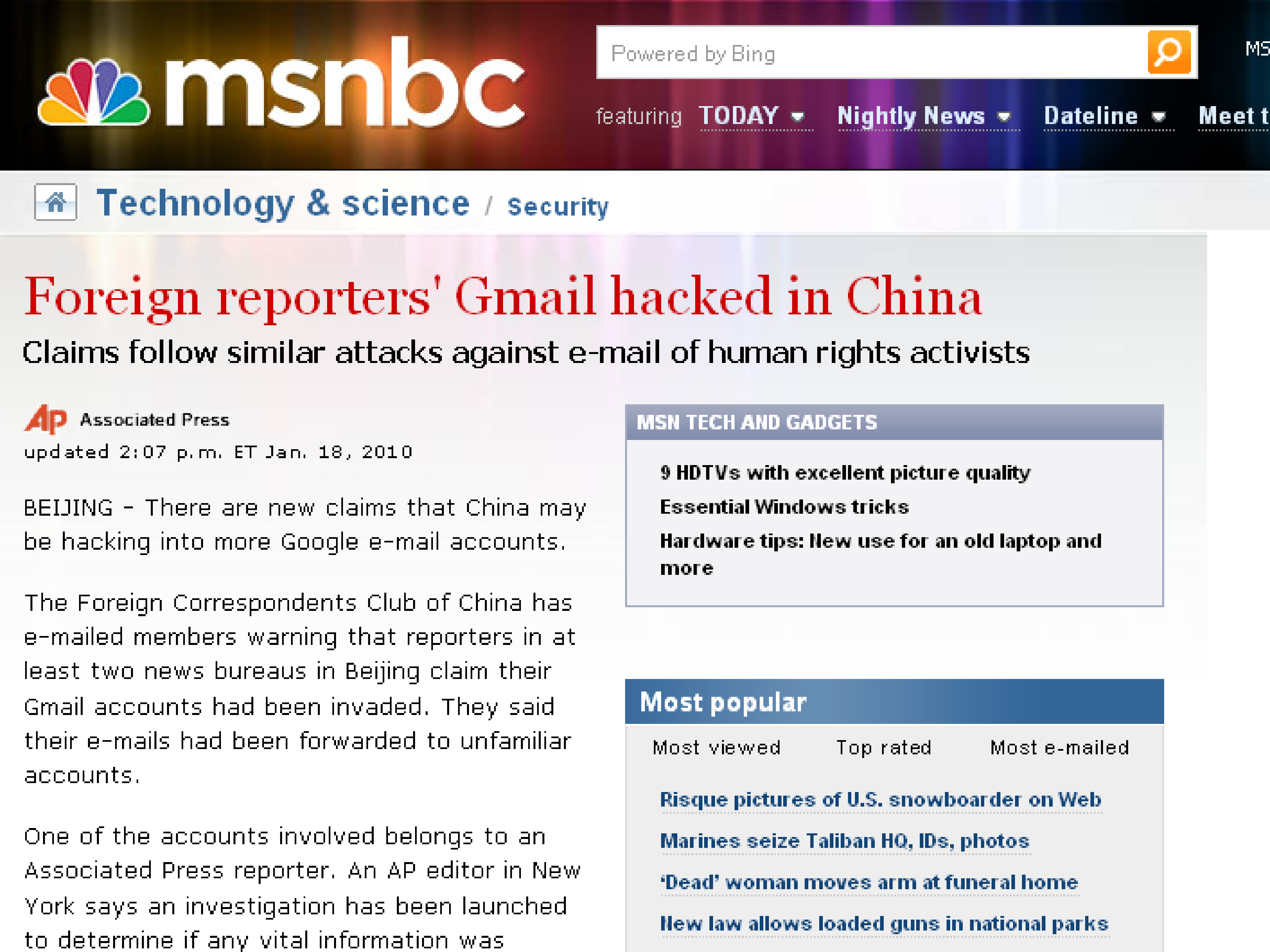
Tuesday,09 February 2010, 06:46 hrs

Mumbai: Indian Software giant Tata Consultancy Services (TCS) became the first private company to be a target of hackers in India when the company's website was hacked and domain name was put up for sale. Usually, government website like telecom regulator's trai.gov.in and other such websites have been targeted by hackers.

The company's official website www.tcs.com displayed the message 'this domain name is for sale' for nearly three hours, before the portal was restored by around 7 am, according to Economic Times.

When contacted by ET, a TCS spokesman said the attacks happened at the domain name registrar's end, which is Network Solutions in this case. Network Solutions is one of the top five domain name registrars on internet, managing almost 6.4 million domains. "The TCS website www.tcs.com was disrupted. Subsequently, it has been restored and is functioning fine. None of the servers were compromised. Initial investigation reveals a DNS redirection at the domain name registrar's end. Further investigations are on," said a TCS spokesperson.

A denial of service attack makes a website or a computer unavailable for target users, traditionally aimed at high-profile banks, credit card companies, government portals and other corporates. By hacking a domain name, hackers are able to redirect



Technology & science / Security

Foreign reporters' Gmail hacked in China

Claims follow similar attacks against e-mail of human rights activists

Associated Press
updated 2:07 p.m. ET Jan. 18, 2010

BEIJING - There are new claims that China may be hacking into more Google e-mail accounts.

The Foreign Correspondents Club of China has e-mailed members warning that reporters in at least two news bureaus in Beijing claim their Gmail accounts had been invaded. They said their e-mails had been forwarded to unfamiliar accounts.

One of the accounts involved belongs to an Associated Press reporter. An AP editor in New York says an investigation has been launched to determine if any vital information was

Most popular

Most viewed Top rated Most e-mailed

Risque pictures of U.S. snowboarder on Web

Marines seize Taliban HQ, IDs, photos

'Dead' woman moves arm at funeral home

New law allows loaded guns in national parks

Symantec Online Store Hacked

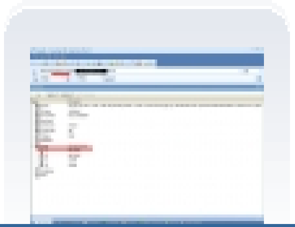
Adjust text size: A- A+

November 23rd, 2009, 11:51 GMT| By **Lucian Constantin**

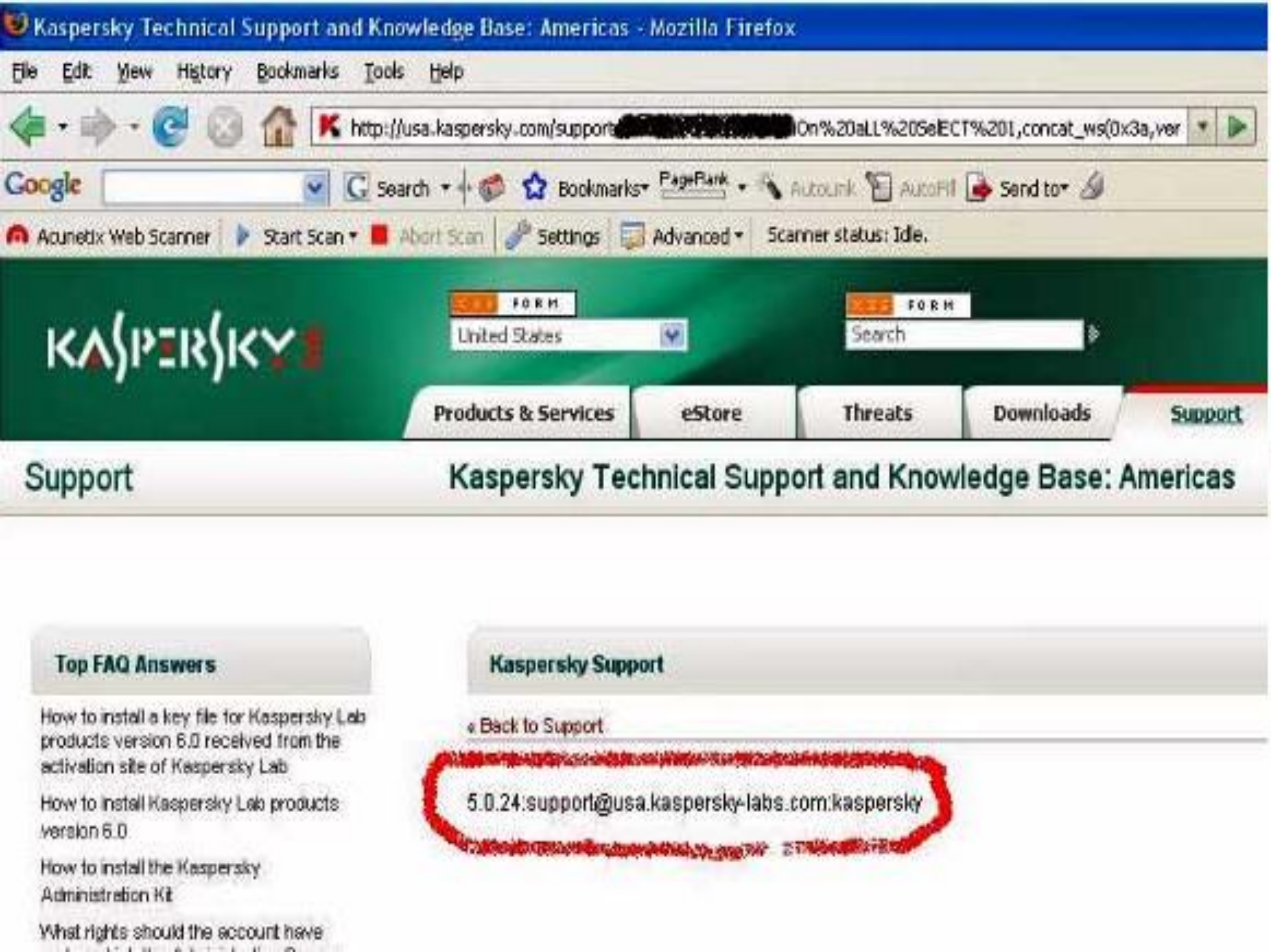
A self-proclaimed grey-hat hacker has located a critical SQL injection vulnerability in a website belonging to security giant Symantec. The flaw can be leveraged to extract a wealth of information from the database including customer and admin login credentials, product serial numbers, and possibly credit card information.

The flaw was found by a Romanian hacker going by the online handle of Unu, according to whom an insecure parameter of a script from the pcd.symantec.com website, allows for a blind SQL injection (SQLi) attack to be performed. In such an attack, the hacker obtains read and/or write permission to the underlying database of the vulnerable website.

During a regular SQLi attack, the result of a rogue SQL query is displayed inside the browser instead of the normal web page output. Meanwhile, in a blind SQL injection, the query executes, but the website continues to display normally, making it much more difficult to extract information.



The content of the pcd.symantec.com website is written in Japanese, but from what we could determine, it serves a product called Norton PC Doctor. Accessing most of the website's sections requires authentication, and in order to exploit the



http://usa.kaspersky.com/support[redacted]0n%20aLL%20SelECT%201,concat_ws(0x3a,ver

Support

Kaspersky Technical Support and Knowledge Base: Americas

Top FAQ Answers

How to install a key file for Kaspersky Lab products version 6.0 received from the activation site of Kaspersky Lab

How to install Kaspersky Lab products version 6.0

How to install the Kaspersky Administration Kit

What rights should the account have

Kaspersky Support

« Back to Support

[redacted]

5.0.24:support@usa.kaspersky-labs.com:kaspersky

[redacted]

Gmail hacked by Cyber hackers of China | Pishing Hacking Attack

June 2, 2011

By admin

Google Officials gave the statement over the gmail hacking that the Google Gmail Accounts are being hacked by Cyber hackers of china. Thousands of Gmail accounts password been hacked under this acts know as "Pishing" it is also stated that some of the US officials, Military Persons Gmail account were also targeted. Officials say that this hacking done from Jinan, China.

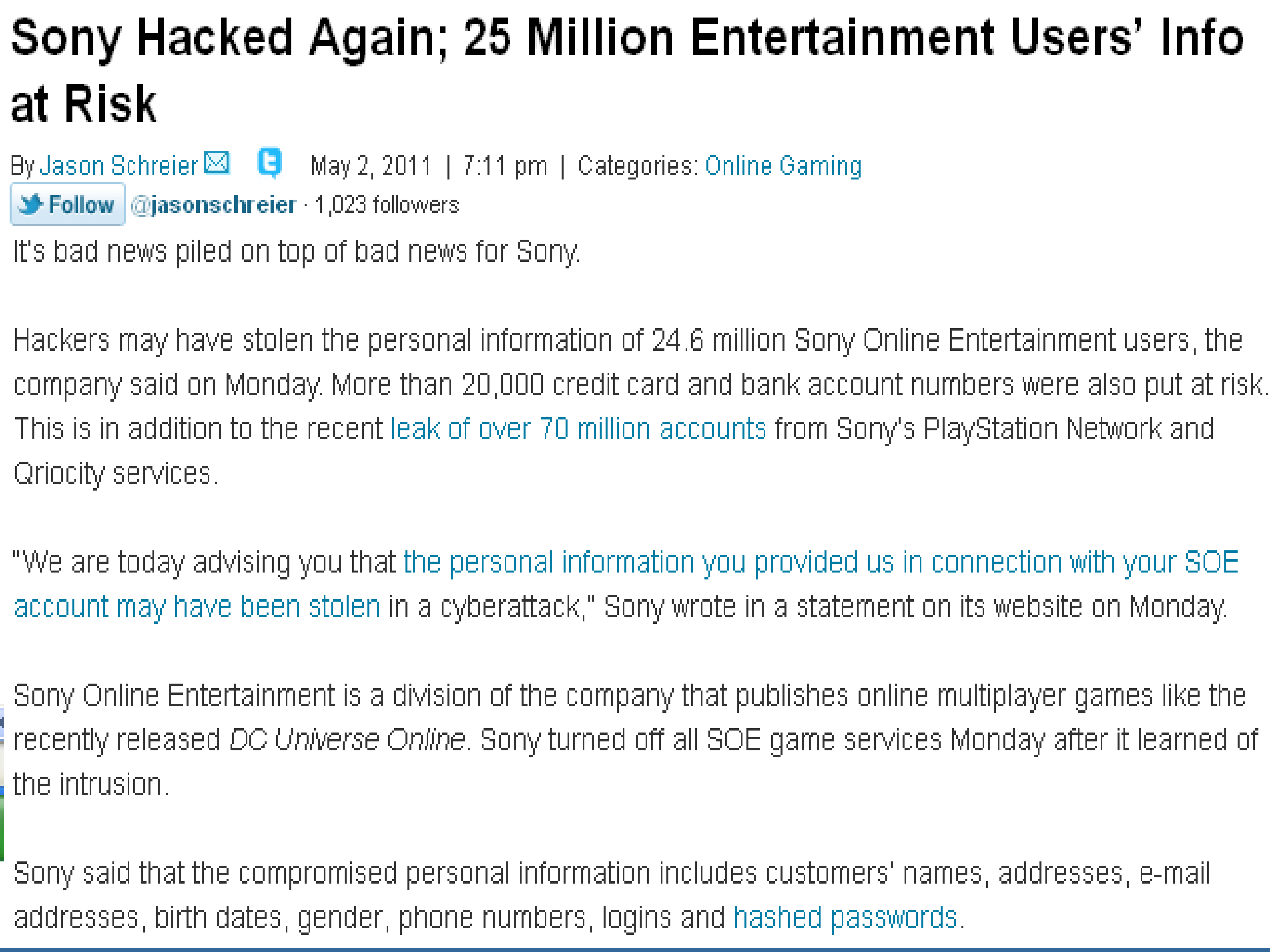
Sign in to Gmail with your
Google Account
ername:
ssword:
Remember me on this compu
Sign in
I cannot access my account
HACKED

This cyber space hacking games between china and US is running since long time at various ways and now hacking of Google Gmail is one of them. This hacking controversy could be the linked with the restrictions on Google operation in the china while according to the Google statement our huge number of employee working under Google china.

Chinese officials rejects the Pishing Hacking allegation news and said we have no any report of any Chinese official involvement in this cyber attack and we did not accept such type of allegation put over china. As for as Hacking concerned China is the biggest victim of Hackers belong to US. We don't support any kind of hacking.

Hacking Of Sony Playstation May Affect 75 Million People

MoxNewsDotCom 6,627 videos Subscribe



Sony Hacked Again; 25 Million Entertainment Users' Info at Risk

By Jason Schreier ✉ May 2, 2011 | 7:11 pm | Categories: Online Gaming

@jasonschreier · 1,023 followers

It's bad news piled on top of bad news for Sony.

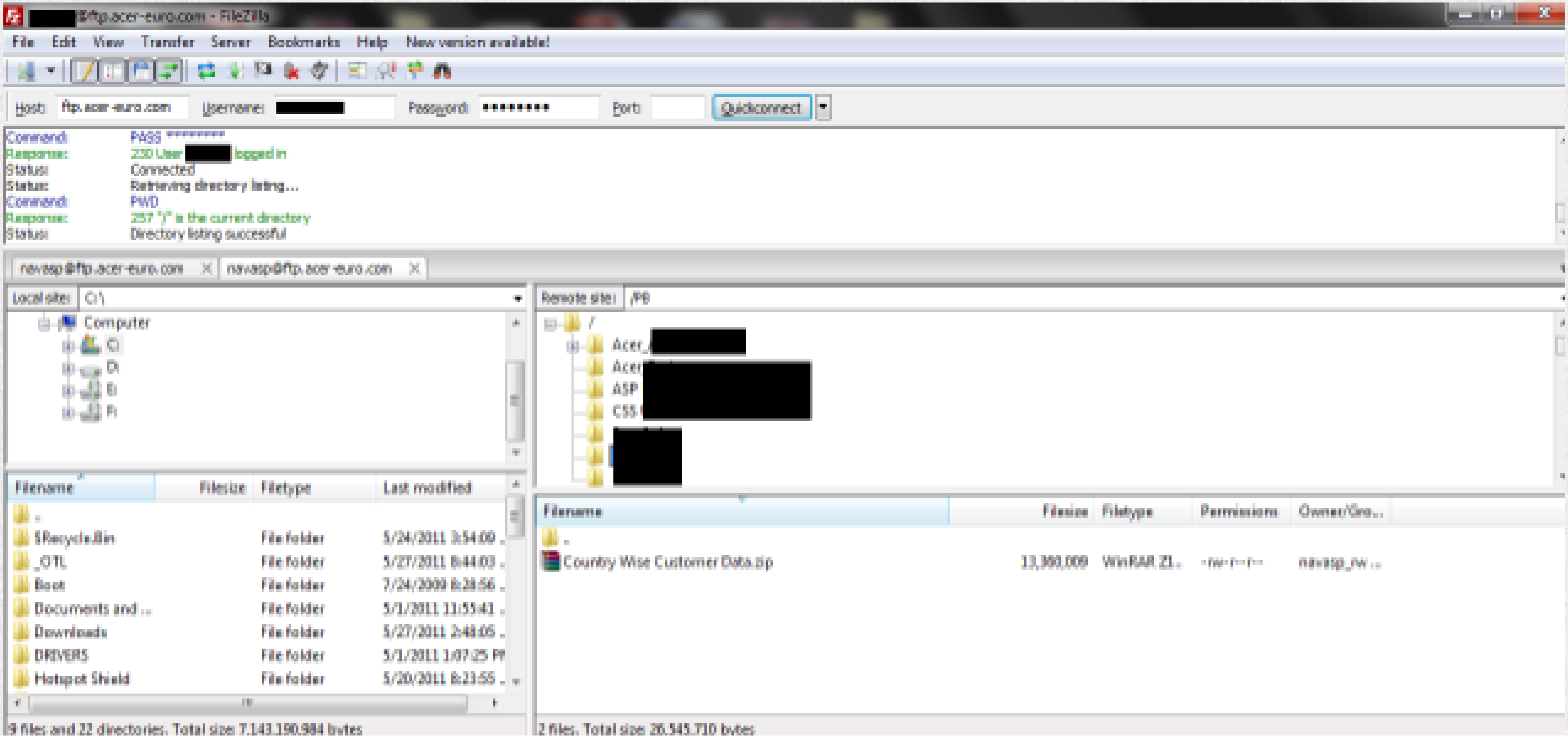
Hackers may have stolen the personal information of 24.6 million Sony Online Entertainment users, the company said on Monday. More than 20,000 credit card and bank account numbers were also put at risk. This is in addition to the recent leak of over 70 million accounts from Sony's PlayStation Network and Qriocity services.

"We are today advising you that the personal information you provided us in connection with your SOE account may have been stolen in a cyberattack," Sony wrote in a statement on its website on Monday.

Sony Online Entertainment is a division of the company that publishes online multiplayer games like the recently released *DC Universe Online*. Sony turned off all SOE game services Monday after it learned of the intrusion.

Sony said that the compromised personal information includes customers' names, addresses, e-mail addresses, birth dates, gender, phone numbers, logins and hashed passwords.

2.) FTP Access on acer-euro.com


[redacted]@ftp.acer-euro.com - FileZilla
File Edit View Transfer Server Bookmarks Help New version available!
Quickconnect

Host: ftp.acer-euro.com Username: [redacted] Password: ••••••••• Port:

```
Command:    PASS *********
Response:   230 User [redacted] logged in
Status:     Connected
Status:     Retrieving directory listing...
Command:    PWD
Response:   257 "/" is the current directory
Status:     Directory listing successful
```

navasp@ftp.acer-euro.com | navasp@ftp.acer-euro.com

Local site: C:\

- Computer
  - C:
  - D:
  - E:
  - F:

Remote site: /PB

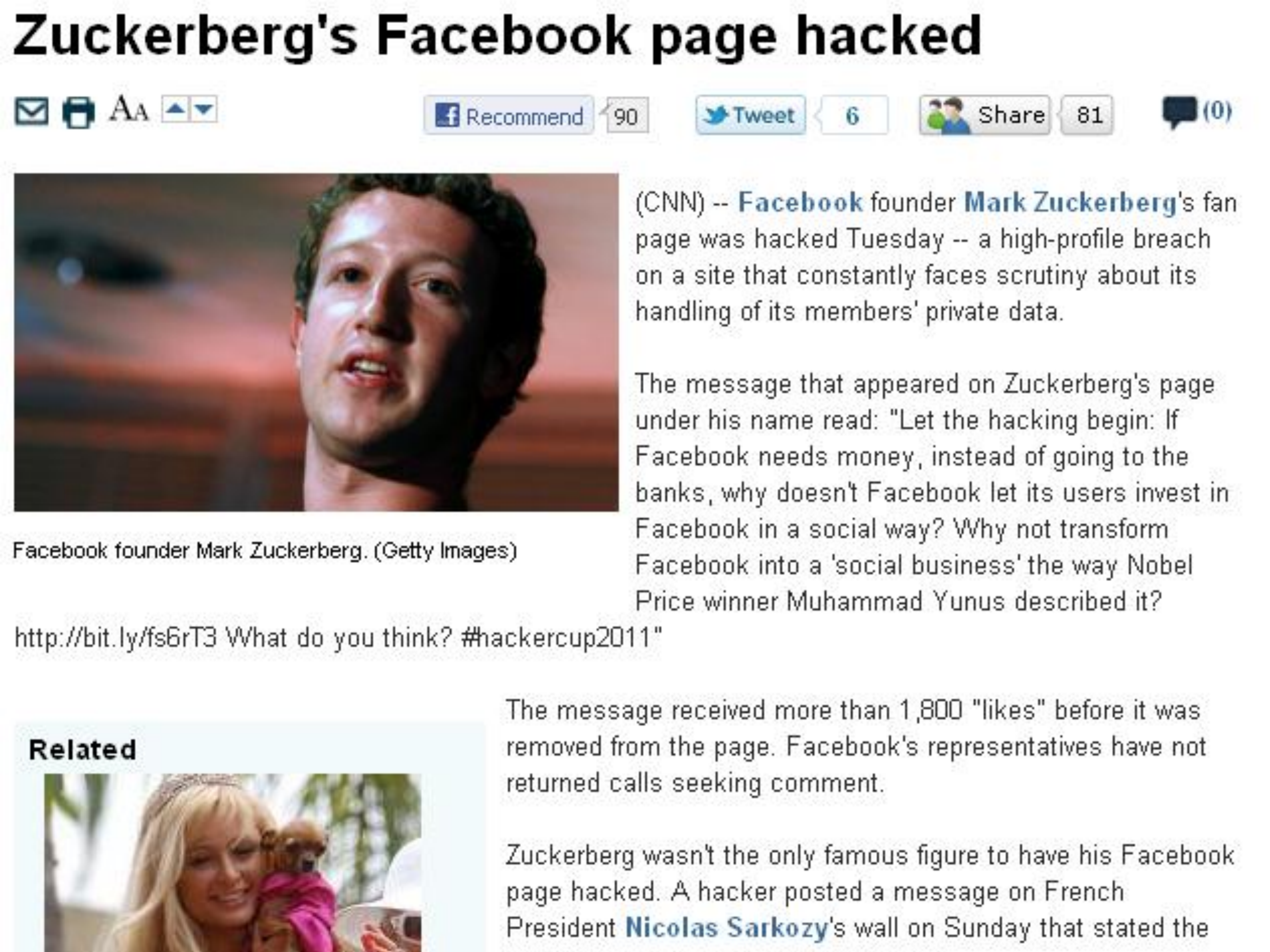
- /
  - Acer_[redacted]
  - Acer [redacted]
  - ASP
  - CSS
  - [redacted]

Filename	Filesize	Filetype	Last modified
..			
$Recycle.Bin		File folder	5/24/2011 3:54:09 ...
_OTL		File folder	5/27/2011 8:44:03 ...
Boot		File folder	7/24/2009 8:28:56 ...
Documents and ...		File folder	5/1/2011 11:55:41 ...
Downloads		File folder	5/27/2011 2:48:05 ...
DRIVERS		File folder	5/1/2011 1:07:25 PM
Hotspot Shield		File folder	5/20/2011 8:23:55 ...

9 files and 22 directories. Total size: 7,143,190,984 bytes

Filename	Filesize	Filetype	Permissions	Owner/Gro...
..				
Country Wise Customer Data.zip	13,300,009	WinRAR ZI...	-rw-r--r--	navasp_rw ...

2 files. Total size: 26,545,710 bytes



Zuckerberg's Facebook page hacked

Facebook founder Mark Zuckerberg. (Getty Images)

(CNN) -- Facebook founder Mark Zuckerberg's fan page was hacked Tuesday -- a high-profile breach on a site that constantly faces scrutiny about its handling of its members' private data.

The message that appeared on Zuckerberg's page under his name read: "Let the hacking begin: If Facebook needs money, instead of going to the banks, why doesn't Facebook let its users invest in Facebook in a social way? Why not transform Facebook into a 'social business' the way Nobel Price winner Muhammad Yunus described it? http://bit.ly/fs6rT3 What do you think? #hackercup2011"

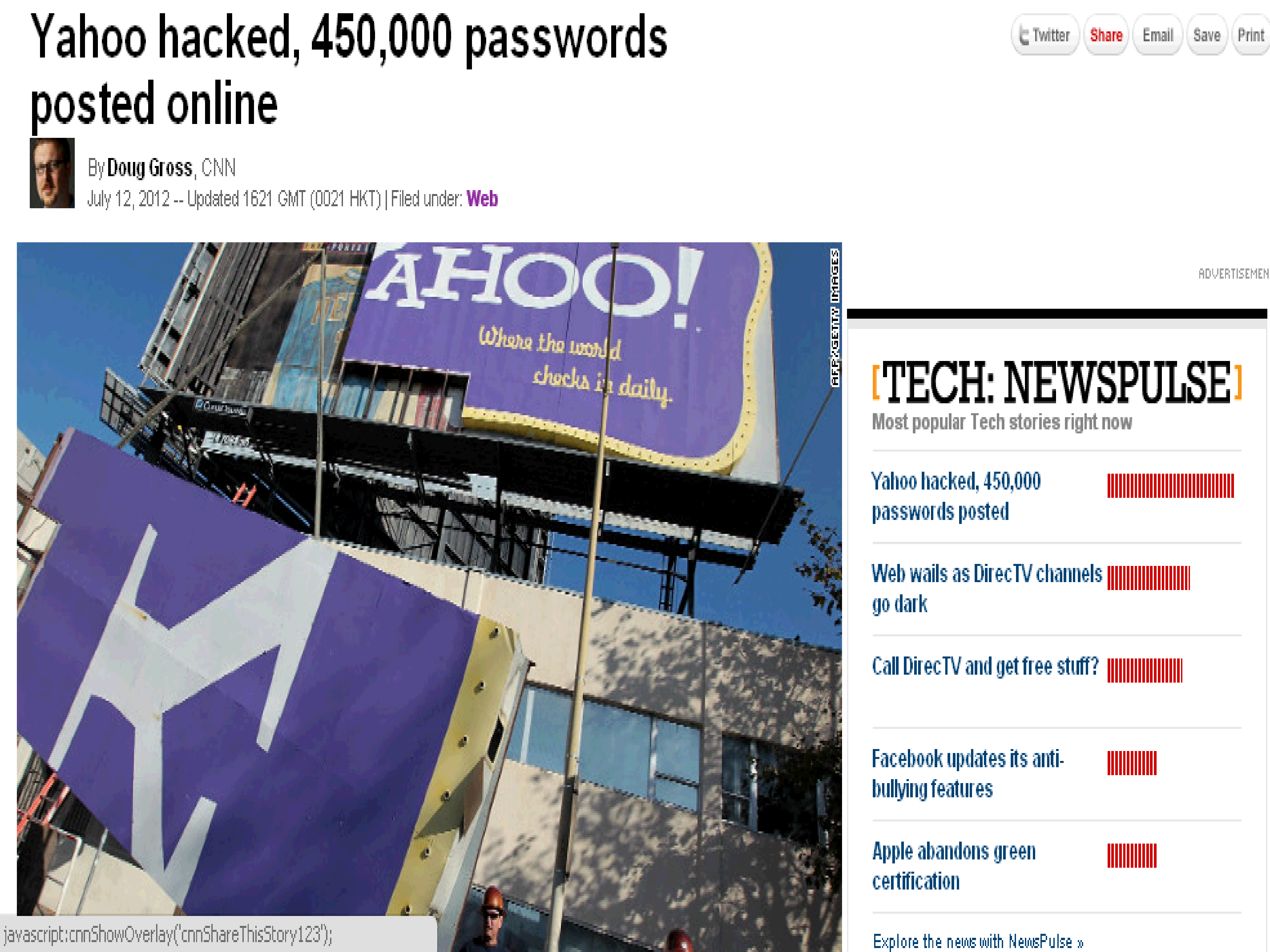
Related

The message received more than 1,800 "likes" before it was removed from the page. Facebook's representatives have not returned calls seeking comment.

Zuckerberg wasn't the only famous figure to have his Facebook page hacked. A hacker posted a message on French President Nicolas Sarkozy's wall on Sunday that stated the

6.4 Million Passwords Reportedly Stolen From LinkedIn Website

LinkedIn
World's Largest Professiona
Favorites
Home
What
World's Largest Professional Network | LinkedIn
http://www.linkedin.com/
File Edit View Favorites Tools Help



Yahoo hacked, 450,000 passwords posted online

By **Doug Gross**, CNN

July 12, 2012 -- Updated 1621 GMT (0021 HKT) | Filed under: **Web**

AFP/GETTY IMAGES

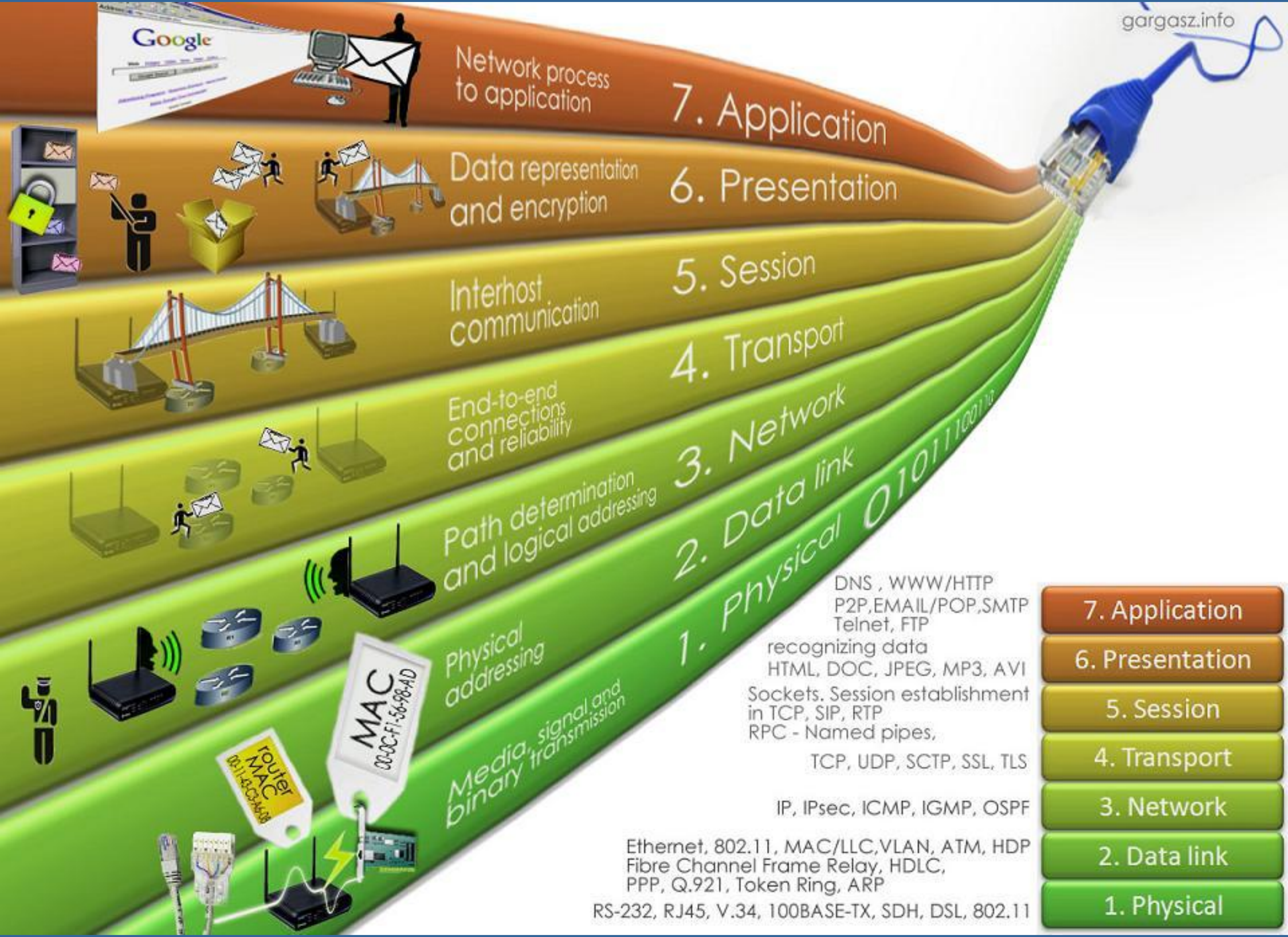
[TECH: NEWSPULSE]

Most popular Tech stories right now

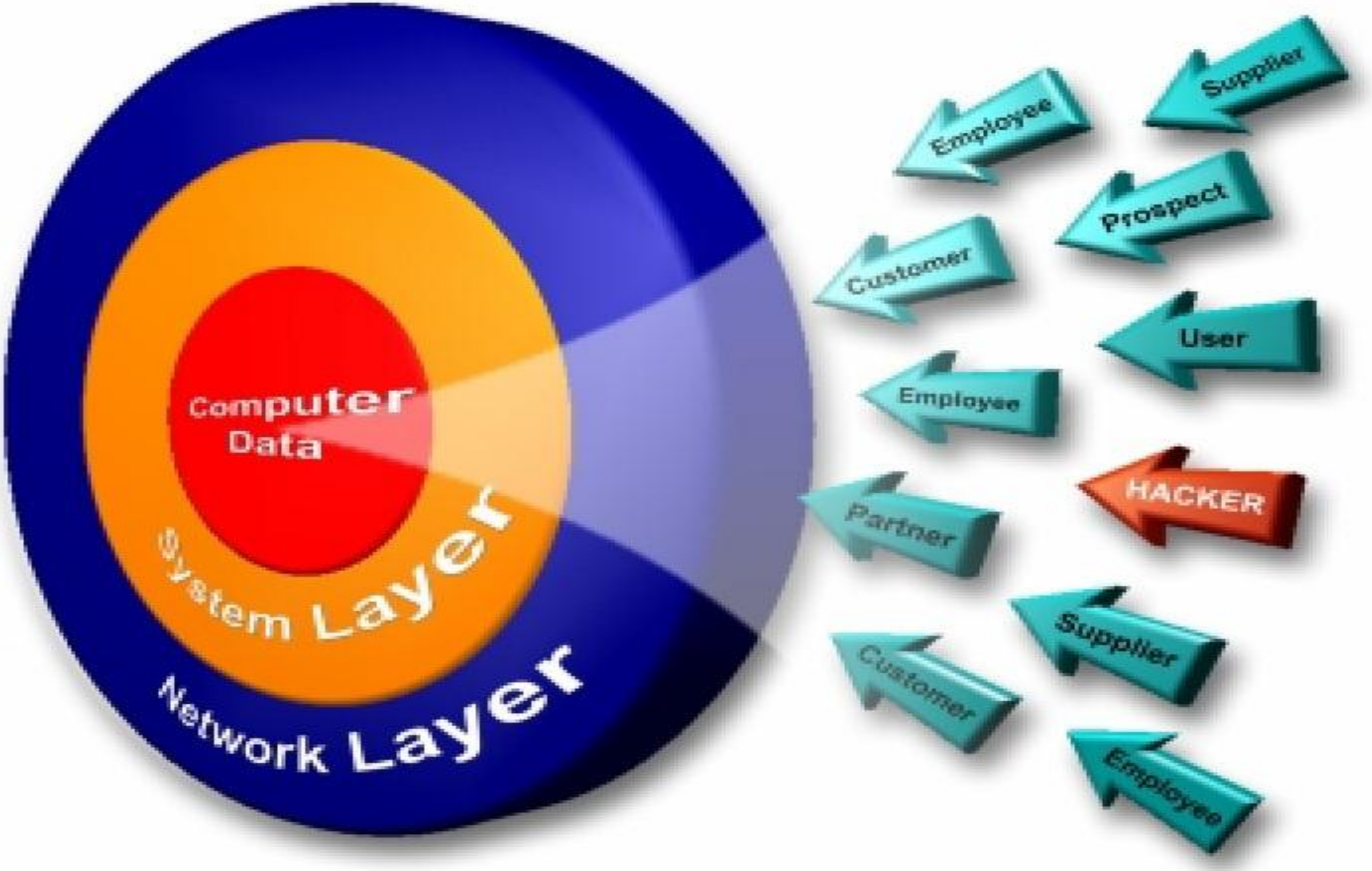
- Yahoo hacked, 450,000 passwords posted
- Web wails as DirecTV channels go dark
- Call DirecTV and get free stuff?
- Facebook updates its anti-bullying features
- Apple abandons green certification

Explore the news with NewsPulse »

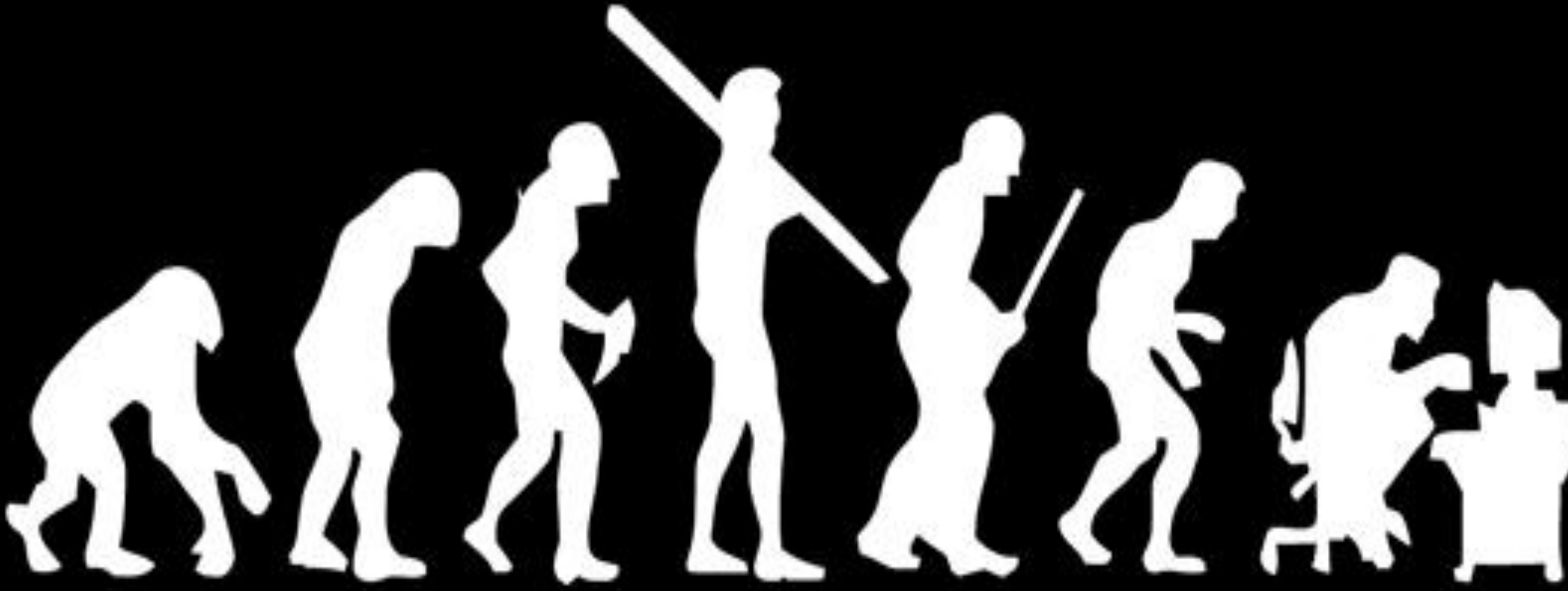
javascript:cnnShowOverlay('cnnShareThisStory123');


gargasz.info
Google
Network process to application
7. Application
Data representation and encryption
6. Presentation
Interhost communication
5. Session
End-to-end connections and reliability
4. Transport
Path determination and logical addressing
3. Network
Physical addressing
2. Data link
Media, signal and binary transmission
1. Physical 0101111001110
MAC 00-0C-F1-56-98-AD
router MAC 00-11-43-C3-A6-08

DNS , WWW/HTTP P2P,EMAIL/POP,SMTP Telnet, FTP	7. Application
recognizing data HTML, DOC, JPEG, MP3, AVI	6. Presentation
Sockets. Session establishment in TCP, SIP, RTP RPC - Named pipes,	5. Session
TCP, UDP, SCTP, SSL, TLS	4. Transport
IP, IPsec, ICMP, IGMP, OSPF	3. Network
Ethernet, 802.11, MAC/LLC,VLAN, ATM, HDP Fibre Channel Frame Relay, HDLC, PPP, Q.921, Token Ring, ARP	2. Data link
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11	1. Physical



Attacks shifted its focus from Outer layers to Inner layers of the OSI Model



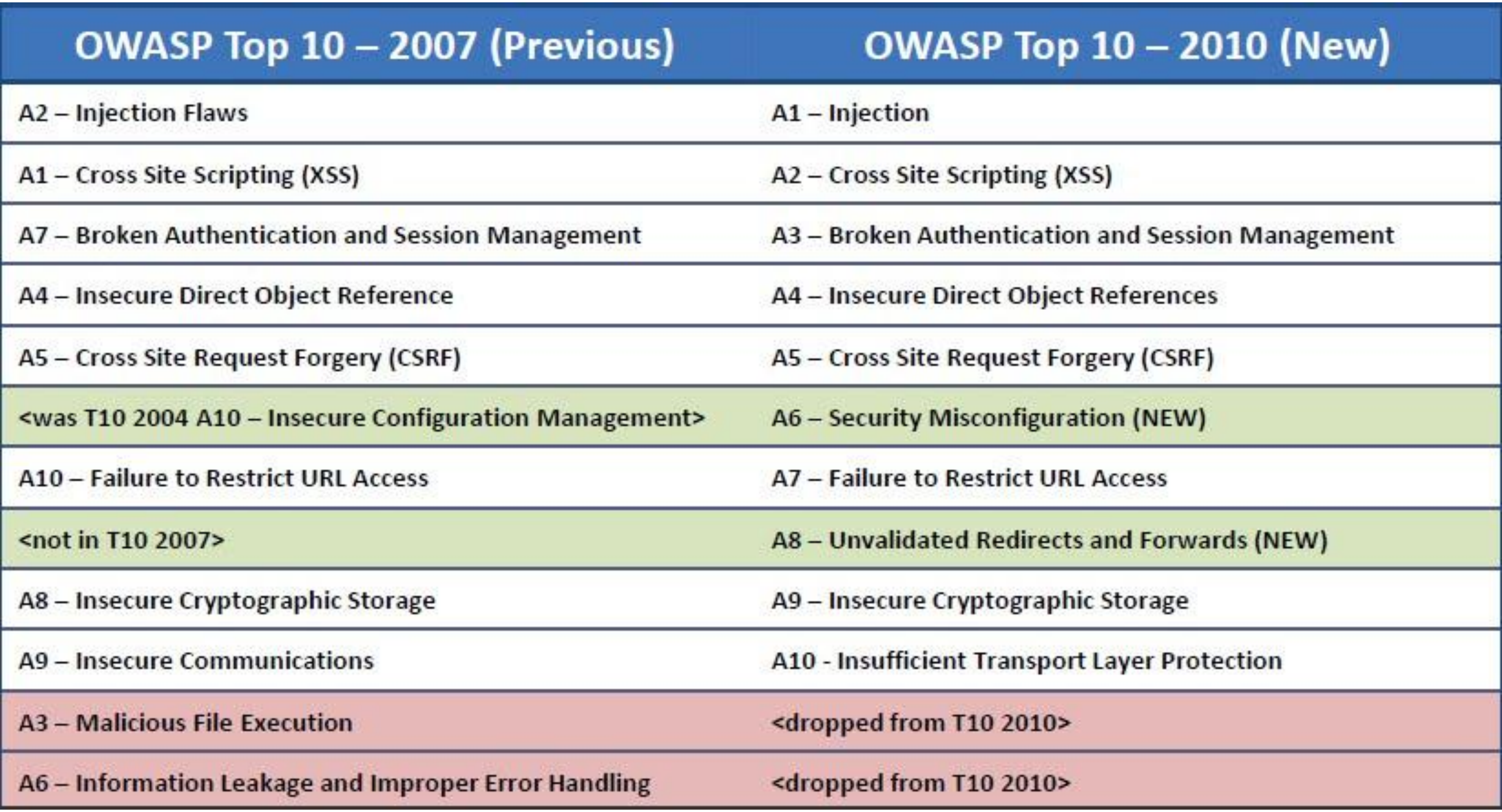
SOMETHING, SOMEWHERE WENT TERRIBLY WRONG.

You are
Wrong
sign
house
asedancy
road
time
reason
ryhme
day
week
method
technique
mix
jeans
night
place
tendencies

Top 10 ATTACKS

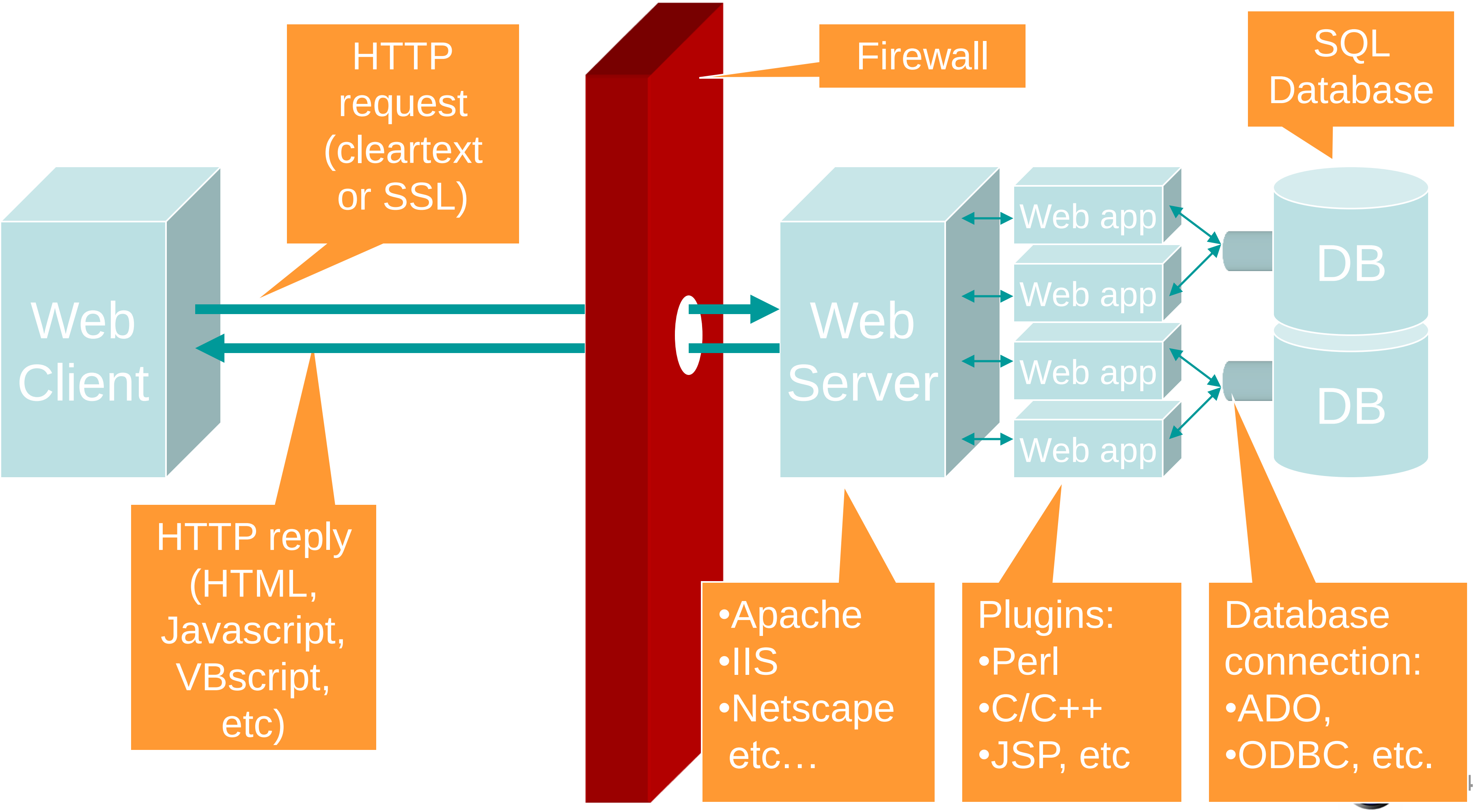
- Be Happy for being a elite crowd , why ?

Top 10 attacks (Injection stays at top)



OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	A7 – Failure to Restrict URL Access
<not in T10 2007>	A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	A10 - Insufficient Transport Layer Protection
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>

Typical Web Application Setup



HTTP request (cleartext or SSL)

Firewall

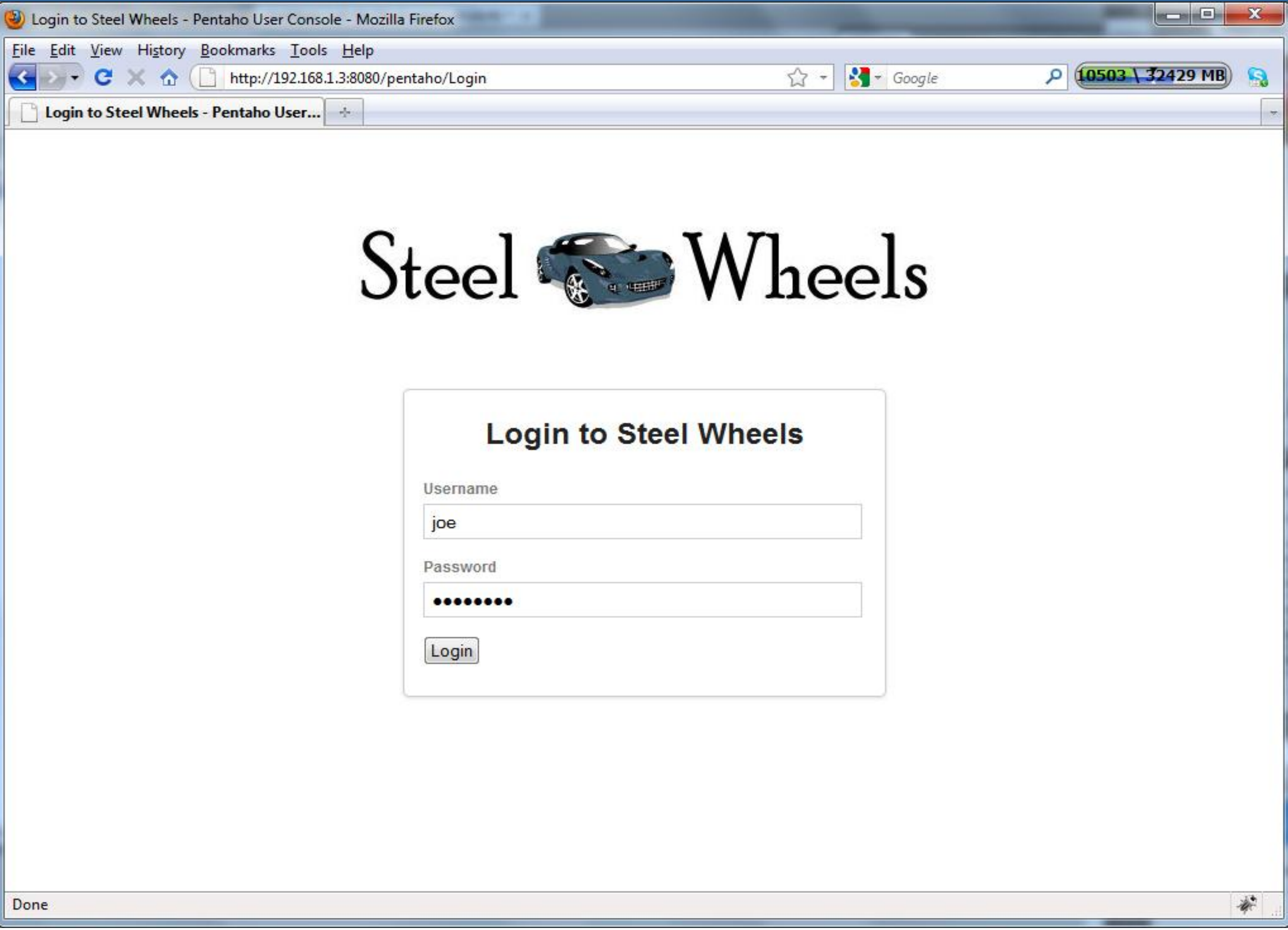
SQL Database

HTTP reply (HTML, Javascript, VBscript, etc)

- Apache
- IIS
- Netscape etc…

Plugins:
- Perl
- C/C++
- JSP, etc

Database connection:
- ADO,
- ODBC, etc.



Login to Steel Wheels - Pentaho User Console - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.3:8080/pentaho/Login
Google
10503 \ 32429 MB
Login to Steel Wheels - Pentaho User...
Steel Wheels

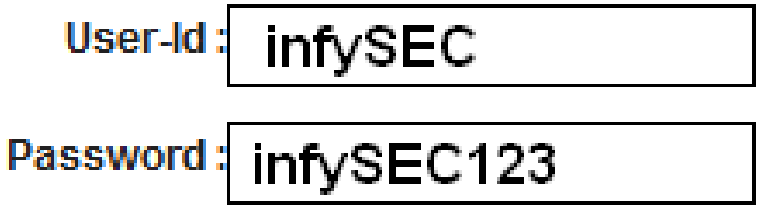
Login to Steel Wheels

Username: joe

Password: ●●●●●●●●●

How it works ?

Example :



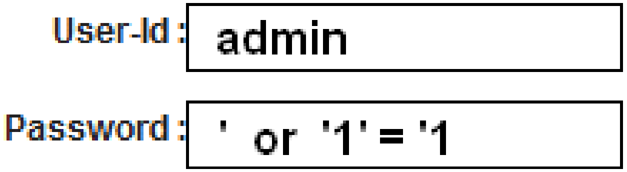
User-Id : infySEC

Password : infySEC123

```
select * from Users where user  id= ' infySEC ' and password = ' infySEC123 '
```

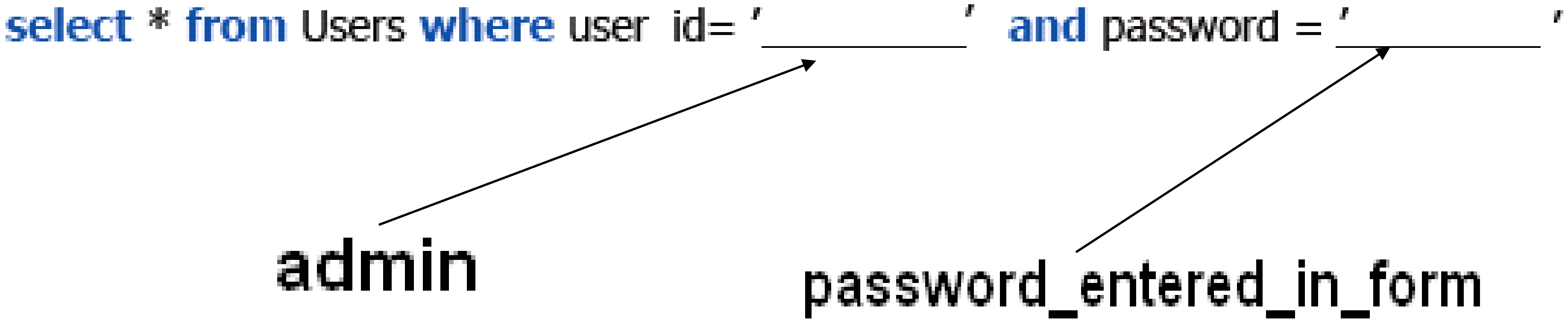
How it works ?

- Example :



User-Id : admin

Password : ' or '1' = '1



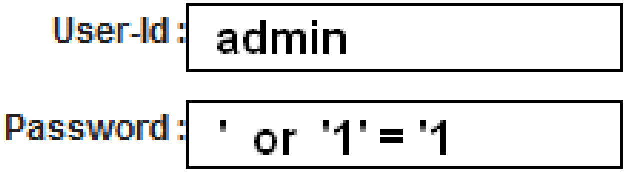
select * from Users where user id= '__________' and password = '__________'

admin

password_entered_in_form

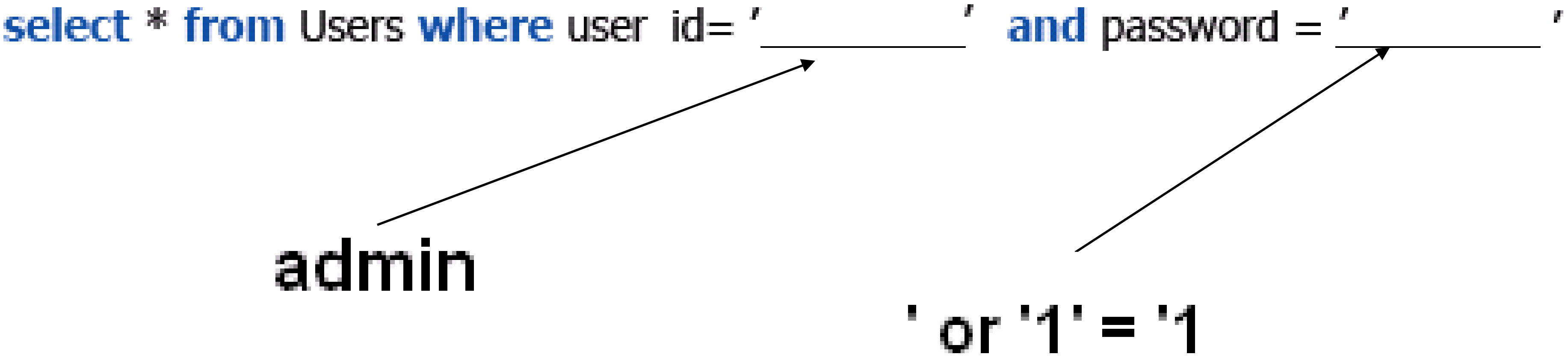
How it works ?

- Example :



User-Id : admin

Password : ' or '1' = '1

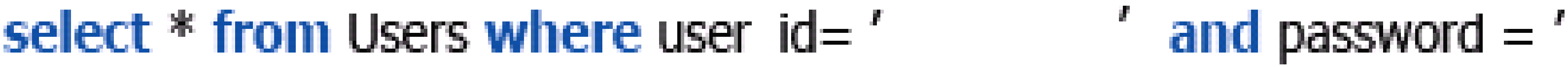


select * from Users where user id= '__________' and password = '__________'

admin

' or '1' = '1

Examining



```
select * from Users where user  id= '                    '  and password = '
```

- AND STATEMENT

(I love TRISHA) AND (I LOVE JENILIA) = TRUE

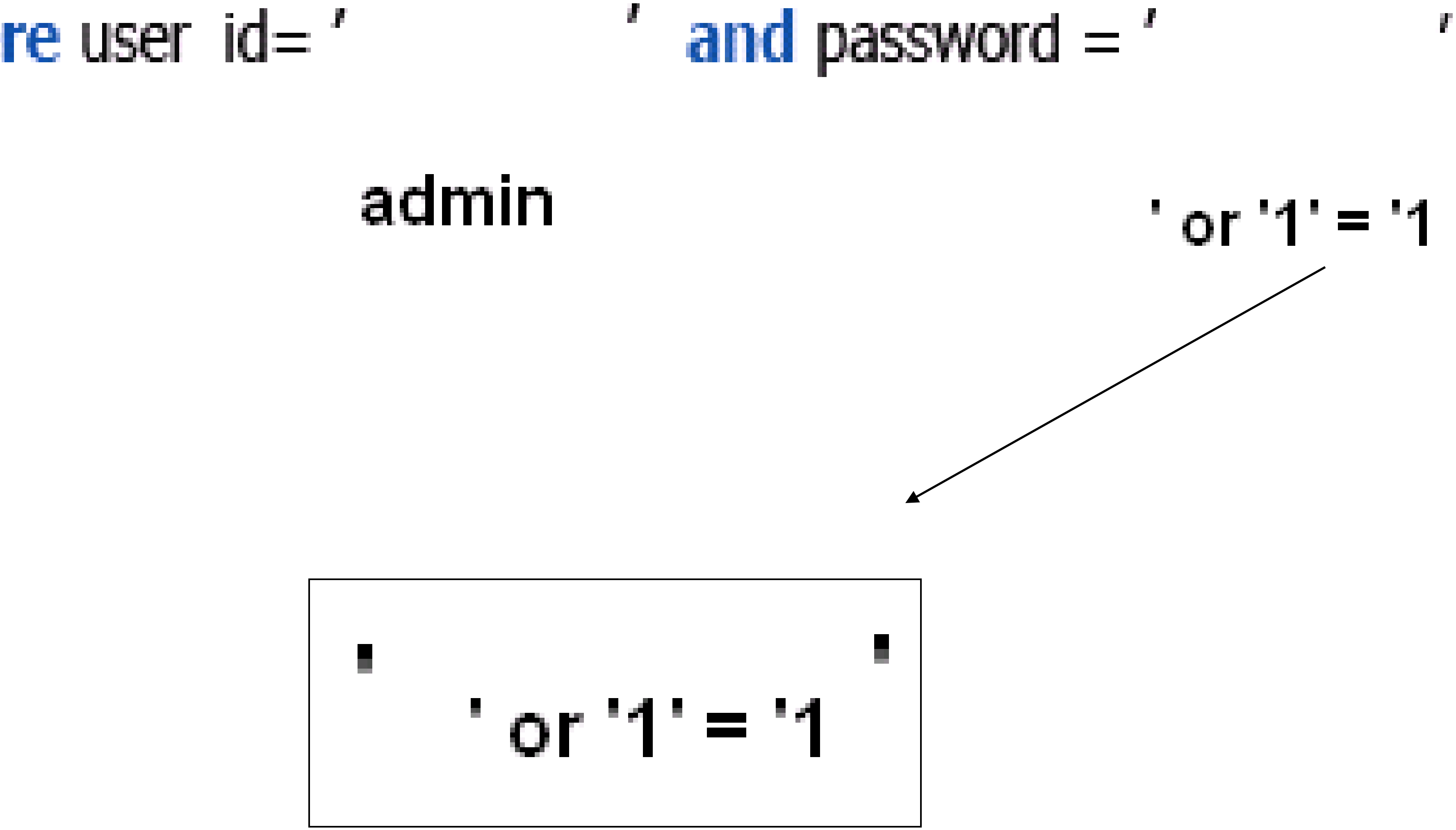
(I love SANTHANAM) AND (I love JENILIA) = FALSE

- OR STATEMENT

(I love TRISHA) OR (I LOVE JENILIA) = FALSE

(I love SANTHANAM) OR (I love JENILIA) = TRUE

Examining



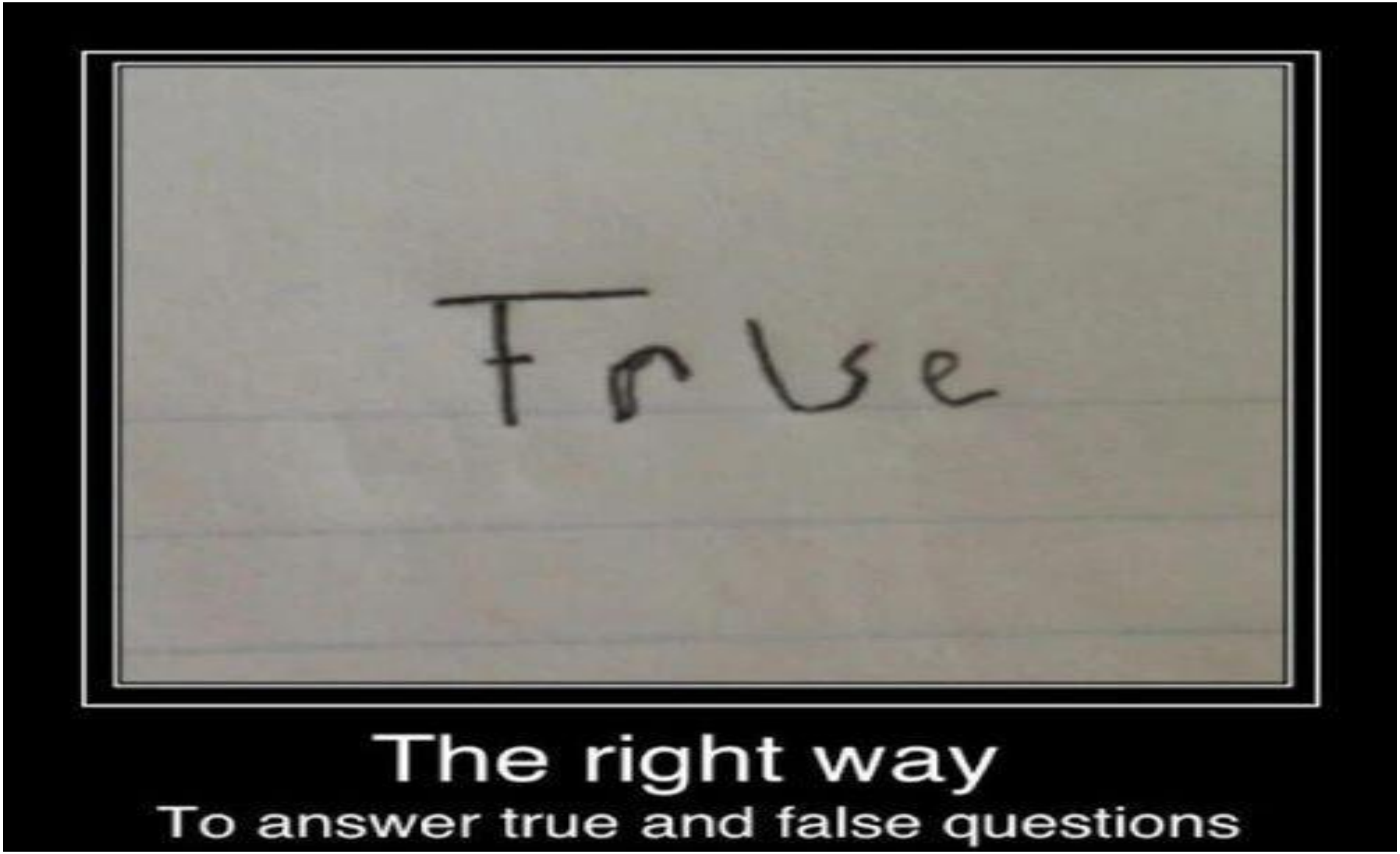
```
re user  id= '                    '   and password = '                   '
```

admin

' or '1' = '1

```
'        ' or '1' = '1        '
```

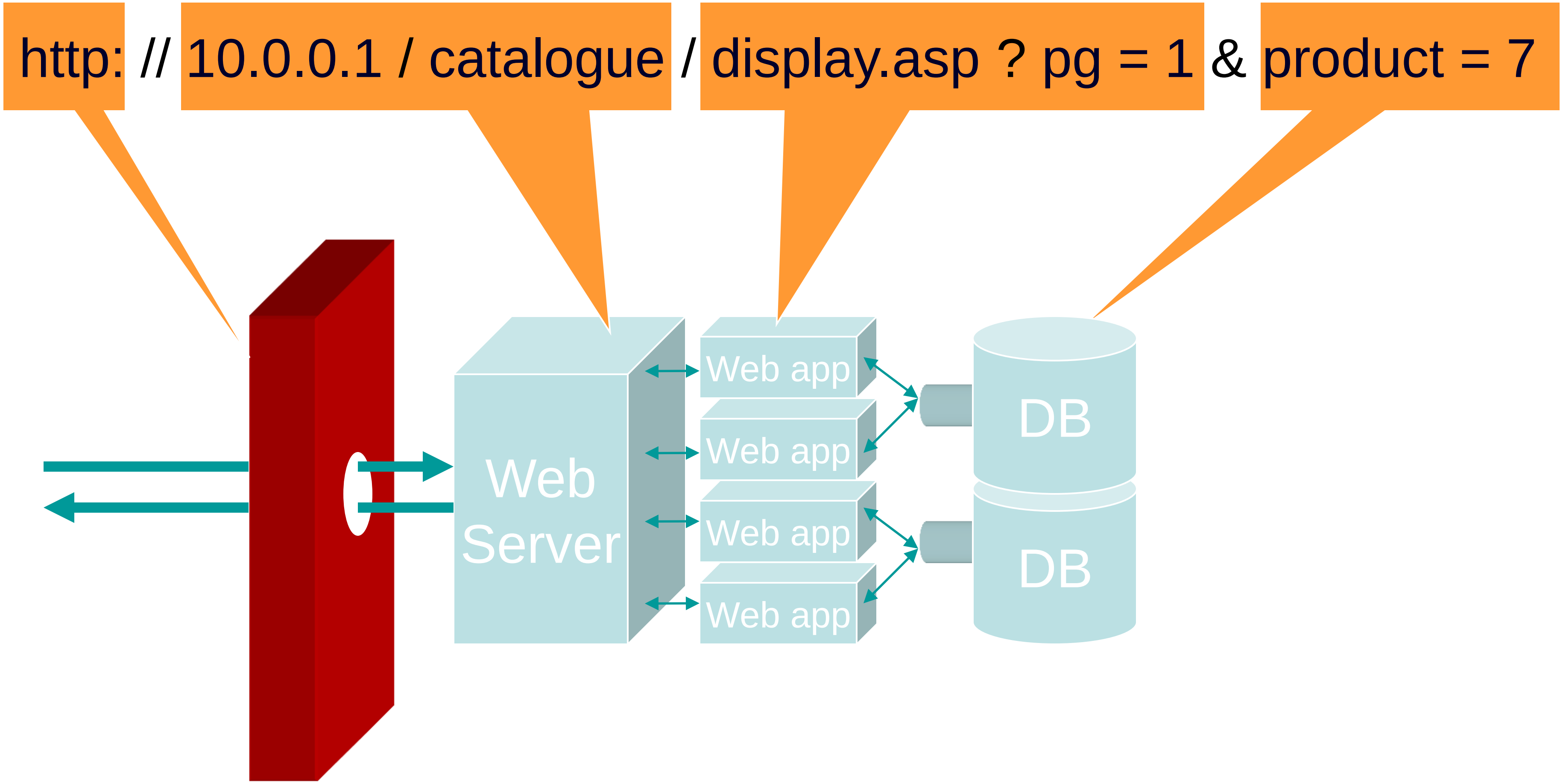
Question ?



What is Click Jacking & Tab Nabbing ?

- Want to hear from you ☺

The Cruise-Missile Structure


http: // 10.0.0.1 / catalogue / display.asp ? pg = 1 & product = 7
Web Server
Web app
Web app
Web app
Web app
DB
DB

Intro

- ERROR Based SQL injection
- Blind SQL Injection

- LDAP injection
- XML Path Injection

Other vectors than Top 10

Popular Tests	
Incubated vulnerability - Incubated vulnerability	Testing for SQL Wildcard Attacks - SQL Wildcard vulnerability
Testing for HTTP Splitting/Smuggling - HTTP Splitting, Smuggling	Locking Customer Accounts - Locking Customer Accounts
SSI Injection - SSI Injection	Testing for DoS Buffer Overflows - Buffer Overflows
XPath Injection - XPath Injection	User Specified Object Allocation - User Specified Object Allocation
IMAP/SMTP Injection - IMAP/SMTP Injection	User Input as a Loop Counter - User Input as a Loop Counter
Code Injection - Code Injection	Writing User Provided Data to Disk - Writing User Provided Data to Disk
OS Commanding - OS Commanding	Failure to Release Resources - Failure to Release Resources
Buffer overflow - Buffer overflow	Storing too Much Data in Session - Storing too Much Data in Session
Incubated vulnerability - Incubated vulnerability	WS Information Gathering - N.A.
Testing for HTTP Splitting/Smuggling - HTTP Splitting, Smuggling	Testing WSDL - WSDL Weakness
Testing for File Extensions Handling - File extensions handling	XML Structural Testing - Weak XML Structure
Old, backup and unreferenced files - Old, backup and unreferenced files	XML content-level Testing - XML content-level
Infrastructure and Application Admin Interfaces - Access to Admin interfaces	HTTP GET parameters/REST Testing - WS HTTP GET parameters/REST
Testing for HTTP Methods and XST	Naughty SOAP attachments - WS Naughty SOAP attachments
Credentials transport over an encrypted channel	Replay Testing - WS Replay Testing
Testing for user enumeration - User enumeration	AJAX Vulnerabilities - N.A.
Testing for Guessable (Dictionary) User Account	AJAX Testing - AJAX weakness
Brute Force Testing - Credentials Brute forcing	Testing for Reflected Cross Site Scripting - Reflected XSS
Testing for bypassing authentication schema	Testing for Stored Cross Site Scripting - Stored XSS

Other vectors than Top 10

Popular Tests	
Testing for vulnerable remember password and pwd reset	Testing for DOM based Cross Site Scripting - DOM XSS
Testing for Logout and Browser Cache Management	Testing for Cross Site Flashing - Cross Site Flashing
Testing for CAPTCHA - Weak Captcha implementation	SQL Injection - SQL Injection
Testing Multiple Factors Authentication	LDAP Injection - LDAP Injection
Testing for Race Conditions - Race Conditions vulnerability	ORM Injection - ORM Injection
Testing for Session Management Schema	XML Injection - XML Injection
Testing for Cookies attributes	SSI Injection - SSI Injection
Testing for Session Fixation	XPath Injection - XPath Injection
Testing for Exposed Session Variables	IMAP/SMTP Injection - IMAP/SMTP Injection
Testing for CSRF	Code Injection - Code Injection
Testing for Path Traversal	OS Commanding - OS Commanding
Testing for bypassing authorization schema	Buffer overflow - Buffer overflow
Testing for Privilege Escalation - Privilege Escalation	Spiders, Robots and Crawlers
Testing for Business Logic - Bypassable business logic	Search Engine Discovery/Reconnaissance
Testing for Reflected Cross Site Scripting - Reflected XSS	Identify application entry points
Testing for Stored Cross Site Scripting - Stored XSS	Testing for Web Application Fingerprint
Testing for DOM based Cross Site Scripting - DOM XSS	Application Discovery
Testing for Cross Site Flashing - Cross Site Flashing	Analysis of Error Codes
SQL Injection - SQL Injection	SSL/TLS Testing
LDAP Injection - LDAP Injection	DB Listener Testing - DB Listener weak
ORM Injection - ORM Injection	XML Injection - XML Injection

Thank you

The Best Part in ones life IS

DOING WHAT PEOPLE SAY YOU CANNOT DO

- Vino

Flow our blog at :

http://www.infysec.com/news-and-blog/

infySEC

Demystifying Innovations

vinod@infysec.com
http://linkedin.com/in/vino007