Web Application Security

Basic SQL injection
Basic Click Jacking

OWASP
11th August, 2012

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

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.
$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 10000 miles underground, and surrounded by 10000 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. Of course, 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.
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
Foreign reporters' Gmail hacked in China
Claims follow similar attacks against e-mail of human rights activists

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 compromised.
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
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 which the Administration Kit will be installed on?

Kaspersky Support

- 5.0.24: support@usa.kaspersky-labs.com:kaspersky
Gmail hacked by Cyber hackers of China | Phishing 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 “Phishing” 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.

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 Phishing 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
Sony Hacked Again; 25 Million Entertainment Users’ Info at Risk

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

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
Zuckerberg's Facebook page hacked

(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?"


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
Yahoo hacked, 450,000 passwords posted online

By Doug Gross, CNN

July 12, 2012 -- Updated 16:21 GMT (00:21 HKT) | Filed under: Web
Network process to application
6. Presentation
Data representation and encryption
5. Session
Interhost communication
4. Transport
End-to-end connections and reliability
3. Network
Path determination and logical addressing
2. Data link
End-to-end addressing
1. Physical
Physical addressing

- DNS, WWW/HTTP
- P2P, EMAIL/POP, SMTP
- Telnet, FTP
- Recognizing data
- HTML, DOC, JPEG, MP3, AVI
- Sockets, Session establishment in TCP, SIP, RTP
- RPC - Named pipes, TCP, UDP, SCTP, SSL, TLS
- IP, IPsec, ICMP, IGMP, OSPF
- Ethernet, 802.11, MAC/LLC, VLAN, ATM, HDP
- Fibre Channel, Frame Relay, HDLC, PPP, Q.921, Token Ring, ARP
- RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11
Attacks shifted its focus from Outer layers to Inner layers of the OSI Model
SOMETHING, SOMEWHERE WENT TERRIBLY WRONG.
```
Famous Last Words

"I think there is a world market for maybe five computers."
-- Thomas Watson, 1943 (President of IBM)

"640K RAM ought to be enough for anybody for life time"
-- Bill Gates, 1981 (Founder of M$)

"32 bits should be enough address space for Internet"
-- Vint Cerf, 1977 (Father of internet)
```
Top 10 ATTACKS

- Be Happy for being a elite crowd, why?
### Top 10 attacks (Injection stays at top)

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

HTTP request (cleartext or SSL)

HTTP reply (HTML, Javascript, VBscript, etc)

Web Client

Web Server

Web app

Web app

Web app

Firewall

SQL Database

Web app

Web app

Web app

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

Database connection:
- ADO,
- ODBC, etc.

Apache

IIS

Netscape etc…
Steel Wheels

Login to Steel Wheels

Username
joe

Password

Login
How it works?

Example:

```
select * from Users where user_id = 'infySEC' and password = 'infySEC123'
```
How it works?

Example:

```sql
User-Id: admin
Password: ' or '1' = '1

select * from Users where user_id='admin' and password='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?

The right way
To answer true and false questions

True
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
Intro

- ERROR Based SQL injection
- Blind SQL Injection
- LDAP injection
- XML Path Injection
### Other vectors than Top 10

#### Popular Tests

<table>
<thead>
<tr>
<th>Incubated vulnerability - Incubated vulnerability</th>
<th>Testing for SQL Wildcard Attacks - SQL Wildcard vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Testing for HTTP Splitting/Smuggling - HTTP Splitting, Smuggling</td>
<td>Locking Customer Accounts - Locking Customer Accounts</td>
</tr>
<tr>
<td>SSI Injection - SSI Injection</td>
<td>Testing for DoS Buffer Overflows - Buffer Overflows</td>
</tr>
<tr>
<td>XPath Injection - XPath Injection</td>
<td>User Specified Object Allocation - User Specified Object Allocation</td>
</tr>
<tr>
<td>IMAP/SMTP Injection - IMAP/SMTP Injection</td>
<td>User Input as a Loop Counter - User Input as a Loop Counter</td>
</tr>
<tr>
<td>Code Injection - Code Injection</td>
<td>Writing User Provided Data to Disk - Writing User Provided Data to Disk</td>
</tr>
<tr>
<td>OS Commanding - OS Commanding</td>
<td>Failure to Release Resources - Failure to Release Resources</td>
</tr>
<tr>
<td>Buffer overflow - Buffer overflow</td>
<td>Storing too Much Data in Session - Storing too Much Data in Session</td>
</tr>
<tr>
<td>Incubated vulnerability - Incubated vulnerability</td>
<td>WS Information Gathering - N.A.</td>
</tr>
<tr>
<td>Testing for HTTP Splitting/Smuggling - HTTP Splitting, Smuggling</td>
<td>Testing WSDL - WSDL Weakness</td>
</tr>
<tr>
<td>Testing for File Extensions Handling - File extensions handling</td>
<td>XML Structural Testing - Weak XML Structure</td>
</tr>
<tr>
<td>Old, backup and unreferenced files - Old, backup and unreferenced files</td>
<td>XML content-level Testing - XML content-level</td>
</tr>
<tr>
<td>Infrastructure and Application Admin Interfaces - Access to Admin interfaces</td>
<td>HTTP GET parameters/REST Testing - WS HTTP GET parameters/REST</td>
</tr>
<tr>
<td>Testing for HTTP Methods and XST</td>
<td>Naughty SOAP attachments - WS Naughty SOAP attachments</td>
</tr>
<tr>
<td>Credentials transport over an encrypted channel</td>
<td>Replay Testing - WS Replay Testing</td>
</tr>
<tr>
<td>Testing for user enumeration - User enumeration</td>
<td>AJAX Vulnerabilities - N.A.</td>
</tr>
<tr>
<td>Testing for Guessable (Dictionary) User Account</td>
<td>AJAX Testing - AJAX weakness</td>
</tr>
<tr>
<td>Brute Force Testing - Credentials Brute forcing</td>
<td>Testing for Reflected Cross Site Scripting - Reflected XSS</td>
</tr>
<tr>
<td>Testing for bypassing authentication schema</td>
<td>Testing for Stored Cross Site Scripting - Stored XSS</td>
</tr>
</tbody>
</table>
### Other vectors than Top 10

#### Popular Tests

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

The Best Part in ones life IS DOING WHAT PEOPLE SAY YOU CANNOT DO

- Vino

Flow our blog at :


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