Indian Computer Emergency Response Team
Department of Information Technology
Ministry of Communications & Information Technology
(Government of India)

CCAOI™
Representing the ecosystem of Internet -Bharat Model

Security Newsletter 15th March, 2011

As internet is becoming an integral part of our lives, it is important that we are aware of the threats we face in the Cyberspace. Cybercrime is on the rise as is evident from the number of cases that are reported in the media. The need of the hour is to be aware and adequately equipped to protect ourselves online.

Looking at the gravity of the situation, with the support of Indian Computer Emergency Response Team (Cert IN), Department of Information Technology, VeriSign India and Sify Technologies Ltd, we are releasing this edition of our Security Newsletter.

eCommerce Sites : Attacks and Preventive Measures

Attacks against eCommerce Sites are on the rise and practically every month, there is an announcement of an attack on a major Web site where sensitive information is obtained. The low cost of entry to an e-Commerce site, and unimaginable payoffs of a successful attack attracts the criminal population.

Hackers today attack the users of eCommerce sites in various ways. Few of them are discussed below:

- **Tricking the Shopper**. Collecting data of the user and getting to know their shopping behavior, or getting information from the user in some pretext like calling them up as representatives of the site or through phishing schemes.

- **Monitoring the Network**. In such a scenario the attacker monitors the data between the shopper's computer and the server. He collects data about the shopper or steals personal information, such as credit card numbers.

- **Guessing the User's Password**. This can be either manual or automated. Manual attacks are laborious, and only successful if the attacker knows something about the shopper. Automated attacks have a higher likelihood of success, because the probability of guessing a user ID/password becomes more significant as the number of tries increases.

- **Denial of service Attack**. The denial of service attack is one of the best examples of impacting site availability. It involves getting the server to perform a large number of mundane tasks, exceeding the capacity of the server to cope with any other task.

- **Using Server Bugs**. Here the attacker first analyzes the site and then based on the vulnerabilities identified attacks the areas which are vulnerable. The sophisticated attacker finds a weakness in a similar type of software, and tries to use that to exploit the system. This is a simple, but effective attack.

- **Gaining Access to the Servers**. This is the most coveted type of exploit because the possibilities are limitless. When you attack a shopper or his computer, you can only affect one individual. With a root exploit, you gain control of the merchants and all the shoppers' information on the site. There are two main types of root exploits: buffer overflow attacks and executing scripts against a server.

Despite the existence of hackers and crackers, eCommerce remains a safe and secure activity. All the eCommerce companies take steps to make it as secure as possible. However it is the responsibility of all the users of the system to keep it as secure as possible and educating the users and the all stakeholders to take **appropriate precautions**:

- Install personal firewalls for the client machines.
- Store confidential information in encrypted form.
- Encrypt the stream using the Secure Socket Layer (SSL) protocol to protect information flowing between the client and the e-Commerce Web site.
- Use appropriate password policies, firewalls, and routine external security audits.

- Use threat model analysis, strict development policies, and external security audits to protect ISV software running the Web site.

The following checklist could help you to protect yourself online while using any eCommerce Site

- When you login to an eCommerce site and register or enter any kind of private information and credit card details ensure the site is secure using SSL
- Do not shop at a site when the browser does not recognize the server's SSL certificate. This check is done by your browser the first time your URL becomes HTTPS for the site. If the certificate is not recognized, then your browser presents a pop-up message to inform you.
- Always have a password which has atleast 6 characters, and includes numeric and special characters
- Avoid reusing the same user ID and password at multiple Web sites.
- Always logoff after you finish
- Use a credit card for online purchases. Most credit card companies will help you with non-existent or damaged products.

CCAOI, 258 Okhla Industrial Estate, Phase III, New Delhi – 110020. Visit us online at: www.ccaoi.in
For any comments/suggestions email: info@ccaoi.in