



Fig 1: Types of Attacks Reported, and the Dollar Value of Related Losses, in the 2003 CSI/FBI Survey

1.2 Major Actors in e-commerce

In a typical e-Commerce system, a shopper proceeds to a Web site to browse a product catalogue and proceed for a purchase. This simple activity shows the four major players in e-Commerce security. One player is the shopper who uses his browser to locate the site. The site is usually operated by a merchant, also a player, whose business is to sell merchandise to make a profit. As the vendor business is selling goods online, not building software, he usually purchases most of the software to run his site from third-party software vendors. The software vendor is the last of the three legitimate players. The attacker is the player whose goal is to exploit the other three players for illegitimate gains. Figure 2. shows the players in a shopping experience[3].

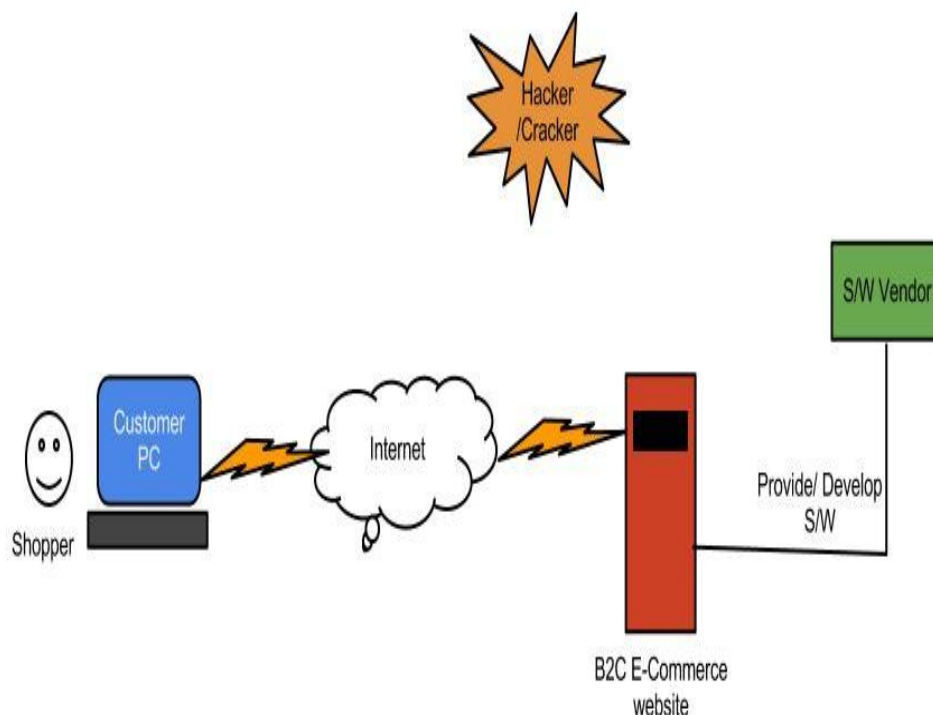


Fig.2: Actors in E-commerce transaction

1.3 Cyber Crime : This term depicts for any illegal activity that uses a computer as its primary means of commission, cyber crimes includes crimes that have been made possible by computers. The intensity of cyber crime in the recent years can be seen through Highlights of the results of the 2002 CSI/FBI Computer Crime and Security Survey, are presented in Table 2.

Security Breaches	Penetration levels	- 90% of respondents detected computer security breaches - 74% report their Internet connection as a frequent point of attack - 33% report internal systems as a frequent point of attack
	Type of Attacks	- 40% experienced a system penetration from the outside - 20% report theft of proprietary information - 12% report financial fraud
WWW	Web Presence	- 98% of respondents have www sites - 52% conduct e-commerce on their sites
	Penetration Level	- 38% suffered unauthorized access or misuse (another 21% didn't know), of which: - 25% report 1 incident - 27% report 2 to 5 incidents - 39% report 10 or more incidents
	Type of Attacks	- 70% of sites suffered from vandalism attacks - 12% included theft of transaction information - 6% financial fraud

Table 2: Highlights of the 2002 CSI/FBI Computer Crime and Security Survey

The paper is organised as below:

The second section deals with vulnerabilities

The third section describes the various attacks on web sites

The fourth section explains the countermeasure

Lastly we conclude the results.

2.0 Vulnerabilities

Vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.[1] To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness

2.1 Software life cycle not secure.

Over the years, efforts to enhance software development life cycle (SDLC) practices have been shown to improve software quality, reliability, and fault-tolerance. Now a days strategies to improve the security of software in organizations such as Microsoft, Oracle, and Motorola have resulted in software products with less vulnerabilities and greater dependability, trustworthiness, and robustness.

As per the SANS Institute's Top 20 list of security vulnerabilities, the MITRE Common Vulnerabilities and Exposures (CVE) site, the US-CERT Technical Cyber Security Alerts site, and the Microsoft Security Advisory site show that common software defects are the leading cause of security vulnerabilities (buffer overflows have been the most common software defect leading to security vulnerabilities).

Some of the things that can be incorporated in SDLC are:

1. Software should be installed using security defaults
2. A software patch management process should be there.

2.2 Vulnerabilities due to input validations:

Buffer Overflow : A buffer overflow condition occurs when a program attempts to copy more data in a buffer than it can hold. Buffer overflow is probably the best known form of software security vulnerability. At the code level, buffer overflow vulnerabilities usually involve the violation of a programmer's assumptions. Hackers use buffer overflows to corrupt the execution stack of a web application. Buffer overflow flaws can be present in both the web server or application server products that serve the static and dynamic aspects of the site. Buffer overflows generally resulted in to crashes. Other type of attacks will create the situation like lack of availability are possible, including putting the program into an infinite loop [7].

2.3 Log Forging : Writing unvalidated user input to log files can give access to attacker for forging log entries or injecting malicious content into the logs. Log forging vulnerabilities occur in following conditions:

- i) Data copied to an application from an unreliable source.
- ii) The data is copied to an application or system log file.

Applications uses log file to store a history of events for later review and record, statistics gathering, or debugging. Analysis of the log files may be misdirected if an attacker can supply inappropriate data to the application. In the most common case, an attacker may be able to insert false entries into the log file by providing the application with input that includes appropriate characters. If the log file is processed automatically, the attacker can render the file unusable by corrupting the format of the file or injecting unexpected characters. A more dangerous attack might involve changing the log file statistics.

2.4 Missing XML Validation: Failure to implement validation when parsing XML gives an attacker the way to supply malicious input. By accepting an XML document without validating it against a DTD or XML schema, the programmer gives chance to attackers to copy unexpected, unreasonable, or malicious input. It is not possible for an XML parser to validate all aspects of a document's content; a parser cannot understand the complete semantics of the data. However, a parser can do a complete and thorough job of checking the document's structure and therefore guarantee to the code that processes the document that the content is well-formed [9].

2.4 Validation checks in client: Performing validation check in client side code, mostly JavaScript, provides no protection for server-side code. An attacker can simply disable JavaScript, use telnet, or use a security testing proxy to bypass the client side validation. Client-side validation is widely used, but is not security relevant.

2.5 Vulnerabilities in database servers: There are various techniques to attack a database. External attacks may exploit configuration weaknesses that expose the database server. Also weak and insecure Web application can be used to exploit the database. An application with excess privilege in the database can put database at risk [3]. The main threats to a database server are:

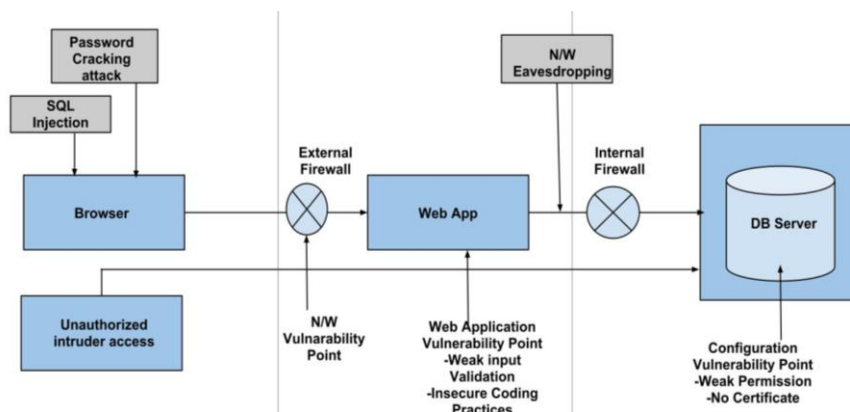


Fig 3: Main threats to a database server

- SQL injection: Technique used to attack database through website entry fields.
- Network eavesdropping: It is a network level attack consisting of capturing packets from the networked computers.
- Unauthorized server access: Attacked made unauthorised access through various loopholes in the system such as O/S, non availability of firewall etc.
- Password cracking: Technique of recovering password from data stored in computer.

2.6 Vulnerabilities in TCP/IP Protocols used for communications

TCP/IP is very popular and known to every one, IP – (Internet Protocol) that handles routing packets of data from one computer to another or from one router to another. TCP, (Transmission Control Protocol) , deals with ensuring that the data packets are delivered in a reliable manner from one computer to another [3] ,[9].

2.6.1 Major causes of vulnerabilities

- Dependency on IP source address for authentication
- Minimal/no authentication in network control mechanisms, e.g. routing protocol, congestion control, flow control, ICMP messages, etc.

2.6.2 Vulnerabilities in firewall: A firewall vulnerability is defined as an error made during firewall design, implementation, or configuration, that can be exploited to attack the trusted network that the firewall is supposed to protect [8]. For example, common firewall vulnerabilities and improper configurations include:

- (1) ICMP allowed, e.g., the firewall can be *ping*-ed;
- (2) Provides the attacker with additional information, or improves the speed of the attacker's port scan by doing Denial rather than drop of traffic to ports by the firewall suppose to block;
- (3) Misconfiguration that allows a TCP ping of internal hosts with Internet-routable IP addresses (e.g., in-bound TCP 80 is not restricted to the web server);
- (4) Trust or unrestricted access to certain IP addresses;
- (5) Availability of extra/ non required services on the firewall;
- (6) Unnecessarily open TCP and UDP ports;

2.6.3 Vulnerability in IPS: The main functions of intrusion prevention systems is to identify malicious activity, log information about malicious activity, attempt to block/stop activity, and report activity. Some of the IPS Vulnerabilities are as follows:

- (1) Under estimation of security capabilities, including information gathering, logging, detection, and prevention.
- (2) Focus on Performance rather than security, including maximum capacity and performance features.

- (3) Non defined Management policies, including design and implementation (e.g., reliability, interoperability, scalability, product security), operation and maintenance (including software updates), and training, documentation, and technical support.

2.6.4 Vulnerability loopholes of the users:

(1) Tolerating weak passwords: weak passwords are arguably the most nonsensical, yet simplest security flaws to fix.

(2) Connecting to unsecured WiFi hotspots : Many people don't think twice about logging onto a random (and unprotected) wireless network just to get some work done. That's all it takes for someone with ill intent to capture a user's login credentials and work his way onto your wireless network.

(3) Ignorance in encrypting hard drives and USB storage disks.

Simply encrypting computer hard drives can eliminate a huge portion of information risks.

(4) Assuming that patches are under control :There are typically hundreds of missing patches on both workstations and servers. In many situations, admins are unaware of specific patches to be installed.

(5) Not balancing security with convenience

Unintended acts , security controls often get in the way of users, who then find ways around it. General habit of writing passwords on sticky notes is just the beginning.

3.0 Types of e-commerce attacks.

Web based attacks are considered to be the greatest threat to the online business as it is related to confidentiality, availability, and integrity. The motive behind e-commerce attack is significantly different then other attacks; Web based attacks focus on an application itself and functions on layer 7 of the OSI. Following are types of attacks on e-commerce.

3.1 Fraudulent Email: Email is an important medium for communication in most companies, both among employees, and between employees and the outside world. It is thus one possible source of data from which potential problems can be detected [2].Examples include

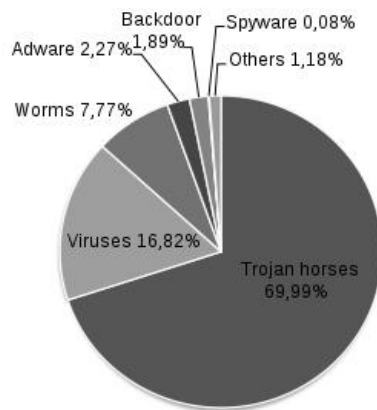
- A statement that there is a problem with user account at a financial institute . The email ask s recipient to visit a web site to correct the problem using deceptive link in email.

3.2 Pharming: Pharming attacks focuses on DNS system. This type of attack affects the routing system of internet by interfering in the lookup process of domain name. Example: customer enter desired site name such as www.ebay.in and gets diverted to similar look and feel site without realizing it.

3.3 Snooping the shopper's computer

An easy way to get entry into the shopper's system is to use a tool, such as SATAN, to perform port scans that detect entry points into the computer. Based on the opened ports found, the attacker can use various techniques to gain entry into the user's system. Upon entry, they scan shoppers file system for personal information, such as passwords.

3.4 Malware: Malicious Software, is a program (code, scripts, active content, and other software) created to disrupt , gather information that leads to loss of privacy, gain unauthorized access to system resources [5].



Malware by categories

March 16, 2011

Fig. 4: Malware by categories [5]

3.5 Man in the Middle attack : This technique uses a packet sniffer to tap the communication between client and the server. Packet sniffer comes in two categories: Active and Passive sniffers. Passive sniffers monitors and sniffs packet from a network having same collision domain i.e. network with a hub, as all packets are broadcasted on each port of hub. Active sniffers works with Switched LAN network by ARP spoofing. Once the hijacker reads the TCP header, he can know the sequence number expected by the server , the acknowledgement number, the ports and the protocol numbers ; so that hijacker can forge the packet and send it to the server before the client does so. Another way of doing so is to change the default gateway of the client’s machine so that it will route its packets via the hijacker’s machine. This can be done by ARP spoofing (i.e. by sending malicious ARP packets mapping its MAC address to the

3.6 CSS (Cross Site Scripting) : In Cross Site Scripting malicious scripts are injected in to the trusted website. Three distinct classes of XSS attacks exist: i) DOM-based attacks, ii) stored attacks, iii) reflected attacks [10].

i) In a DOM-based attack, the vulnerability is based on the Document Object Model (DOM) of the page. Such an attack can happen if the JavaScript in the page accesses a URL parameter and uses this information to write HTML to the page.

ii) In a stored XSS attack, the malicious JavaScript code is permanently stored on the target server (e.g., in a database, in a message forum, or in a guestbook).

iii) In a reflected XSS attack, the injected code is “reflected” off the web server, such as in an error message or a search result that may include some or all of the input sent to the server as part of the request. Reflected XSS attacks are delivered to the victims via e-mail messages or links embedded on other web pages. When a user clicks on a malicious link or submits a specially created form, the injected code travels to the vulnerable web application and is reflected back to the victim’s browser.

3.7 Password Attacks: An attempt to steal passwords using a password cracking program. Hackers widely use password cracking tools and techniques to steal online data. Following are the types of the most widely used attacks.

- i) **Password Guessing :** This is a very common type of attack, hackers can guess passwords locally or remotely using either a manual or automated approach. There are many tools available which can automate the process of typing password after password. Some common password guessing tools are Hydra [12] for guessing all sorts of passwords, including HTTP, Telnet, and Windows logons.
- ii) **Password Resetting :** Easier way to attackers to reset passwords than to guess them. Many password cracking programs are actually password resetters. Most

password resetters contain a bootable version of Linux that can mount NTFS volumes and can help you locate and reset the Administrator's password. A widely used password reset tool is the free Petter Nordahl-Hagen program (<http://home.eunet.no/~pnordahl/ntpasswd>). Winternals ERD Commander 2005, one of the tools in Winternals Administrator's Pak (<http://www.winternals.com/Products/AdministratorsPak/#erdcommander2005>) is a popular commercial choice.

- iii) **Password Cracking** : Password cracking method takes a captured password hash and converting it to its plaintext original. For password cracking, an attacker uses tools like extractors for hash guessing, rainbow tables for looking up plaintext passwords, and password sniffers to extract authentication information.
- iv) **Hash guessing** : Some password cracking tools can both extract and crack password hashes, but most password crackers need to have the LM password hash before they can begin the cracking process. The most popular Windows password hash extractor is the Pwdump family of programs [13].
- v) **Rainbow tables**: In this technique attacker is computing all possible passwords and their hashes in a given system and putting the results into a lookup table called a rainbow table. One can purchase very large rainbow tables, which vary in size from hundreds of megabytes to hundreds of gigabytes, or generate your own using Rainbow Crack [14].
- vi) **Password sniffing**: Password crackers can sniff authentication traffic between a client and server and extract password hashes or enough authentication information to begin the cracking process. Tools password crackers are using are ScoopLM (<http://www.securityfriday.com/tools/ScoopLM.html>) and KerbCrack (<http://ntsecurity.nu/toolbox/kerbcrack>),
- vii) **Password Capturing** : In this technique attackers capture passwords simply by installing a keyboard-sniffing Trojan horse or one of the many physical keyboard-logging hardware devices for sale on the Internet.

4.0 Countermeasures.

Many of these attacks can be stopped and detected early. Proper defences require a well planned approach. Only a few of the possible approaches have been discussed in this paper. Following are the recommendations for security improvements, a comprehensive security plan is shown in order to manage security risk.

4.1 Comprehensive Security Plan

Activity	Description
Security Threat / Vulnerability	Each threat is identified as breach, occurrences , speed of recovery, Financial Damage/ loss.
Security Process	Implementation , management, maintenance
Process Improvement	Lessons learned from past incidents
Measurement system	Identify cost required for maintenance, calculate direct and indirect costs.
Security Assessment	Data collection after incident, their effectiveness, cost of

	handling.
Security monitoring	Data record about vulnerabilities, Experience from past incidents.
Awareness	Training to employee for security awareness, reward and recognition system for security improvements suggested by employee.

Table 3 : Security Plan

4.2 Platform Threats and Vulnerabilities

Threat or vulnerability	Definition	Countermeasure
Network port exploits	Leaving standard ports open to the Internet can invite attack.	- Use a firewall on the server. - Also consider using the Secure Sockets Layer (SSL) for stronger security.
Inappropriate service account settings. For database server	The service accounts for Database Server are often granted more access to the platform or network than is necessary.	The service accounts should operate with least privilege, and should have strong passwords.

4.3 Authentication Threats and Vulnerabilities

Threat or vulnerability	Definition	Countermeasure
Weak passwords	Simple passwords are at risk to brute-force or dictionary attacks.	Always use strong, complex passwords.
User accounts not audited	Users often change positions or leave an organization. If the access for a user account is not changed, the system can still be accessed with the previous permissions level.	User accounts should be audited frequently to make sure that appropriate access to database servers and objects is enabled. For more information about how to audit SQL Server access,

4.4 Programming Threats and Vulnerabilities

Threat or vulnerability	Definition	Countermeasures
SQL injection	SQL Injection is a technique often used to attack data driven applications.	Use stored procedures whenever possible. Create and use Views as table sources. Avoid "Select *" statements for performance as well as security.
Embedded passwords	Some applications save connection strings in the program or configuration files.	Do not store passwords or sensitive connection information in a program, the registry, or a configuration file.
Cross Site Scripting	Cross Site Scripting malicious scripts are injected in to the trusted website.	Use a Web Vulnerability Scanner which, crawls your entire website and automatically checks for Cross Site Scripting vulnerabilities.

4.5 Data Access Threats and Vulnerabilities

Threat or vulnerability	Definition	Countermeasures
Encryption in appropriately applied	Encryption hides the data or connection information in DB Server.	Correctly implement DB Server encryption.
Certificates inappropriately applied	Certificates are a mechanism to verify authentication. SQL Server can use certificates for a variety of purposes, from connections to data.	Understand and correctly implement SQL Server certificates.

4.6 Strong passwords -- The use of simple passwords to be one of the main weaknesses attackers looking for. In short, attackers look for default system passwords that have not been changed. Common usernames and passwords also make it harder to audit who did what on a system. Unique usernames and passwords are an essential control in order to identify and tie every user-initiated action to an individual.

4.7 Data encryption - Encrypted data is intrinsically protected because it is unreadable. This is why it is required in so many compliance guidelines and industry standards.

4.8 Security-aware employees - Employees and their workstations are the main targets for attackers. It's important to keep staff informed of the latest attack techniques being used by attacker. Employees should be instructed to report any suspicious activity, emails to security dept.

4.9 Firewall - Firewalls must be used to ensure incoming and outgoing data is being sent to the proper location, over the proper port, using an authorized protocol. Many organizations only configure their firewalls to monitor traffic coming into the network. But to prevent malware sending data back to its controller, egress traffic must also be monitored.


5.0 Conclusion: We believe that there is a genuine need for a client-side tool and a combination of application of both technologies and end user awareness are the only effective ways of defence against e-commerce attacks. Technologies such as application layer firewalls, reverse proxies, Intrusion Detection and Prevention systems coupled with security training program for application developers and programmers will give security enhancements, Having only a layer 3 device protecting critical portions of the network is no longer sufficient. There is a need to use of code review tools and scanners which provide proactive resources that both developers and security professionals can use in analyzing application layer weaknesses.

6.0 References

- [1] Rod Rasmussen, Greg Aaron, "Global Phishing Survey: Trends and Domain Name Use", "Internet Policy Committee, 1H2010 October 2010
- [2] P.S. Keila and D.B. Skillicorn, "Detecting Unusual and Deceptive Communication in Email", External Technical Report, School of Computing Queen's University, Kingston, Ontario, Canada K7L 3N6, ISSN-0836-0227-2005-498, June 8, 2005
- [3] Darshanand Khusial, Ross McKegney, "e-Commerce security: Attacks and preventive strategies", IBM Software Group at the IBM Toronto lab., 13 Apr 2005

- [4] Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel, "The Economic Impact of Cyber-Attacks", CRS Report for Congress, The Library of Congress, Government and Finance Division, April 1, 2004
- [5] Malware statics 2011 : http://en.wikipedia.org/wiki/File:Malware_statics_2011-03-16-en.svg
- [6] P S Lokhande, B B Meshram, " Evaluation of High Performance, Secure Enterprise Content Management System, International Conference on Electronics, Information and Communication Systems Engineering., ICEICE-2010, Jodhpur , Rajsthan, India., March 28th-30th -2011.
- [7] P.S. Lokhande, P.H. Rathod, " Buffer Overflow Attack Detection By Using Different Techniques", 2nd International Conference On "Recent Trends in Business, Management & IT" In association with Department of Commerce & Research Centre University of Pune, 24th April 2011
- [8] Seny Kamara, Sonia Fahmy, Eugene Schultz, Florian Kerschbaum, and Michael Frantzen, "Analysis of Vulnerabilities in Internet Firewalls", Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University 656 Oval Dr., West Lafayette, IN 47907-2039, USA
- [9] Dave Wichers, COO, Aspect Security OWASP Board Member, "OWASP Top 10 – 2010 The Top 10 Most Critical Web Application Security Risks, OWASP Foundation-2010"
- [10] Engin Kirdaa,, Nenad Jovanovicb, Christopher Kruegelc, Giovanni Vigna, "Client-side cross-site scripting protection", Computers and Security, Elsevier, 2009.
- [11] Narn-Yih Lee, Yu-Chung Chiu, "Improved remote authentication scheme with smart card", Elsevier, Computer Standards & Interfaces 27 (2005) 177–180
- [12] Web Link: http://www.thc.org/blob/manhydra/thc_hydra_article_r3.pdf
- [13] Web Link : <http://pr.openwall.net/dl/pwdump/pwdump4.zip>
- [14] Web Link : <http://www.antsight.com/zsl/rainbowcrack>

Authors

<p>P S Lokhande</p> <p>Working as Head Dept of IT at MGM's College of Engineering and Technology, Navimumbai, India. Having 14 years of Teaching and Industry Experience. Published more than 20 paper in various National, International conferences and Journals. His basic area of interest is Web Engineering, E-Commerce, E-Commerce Security, Digital Evidence Collection etc.</p>	
<p>Dr. B.B. Meshram</p> <p>Working as Head Dept of Computer Technology at VJTI (Veer Jijamata Technological Institute) Matunga, Mumbai, India. Guided 50+ PG students , 15+ research Scholars are doing research under him. Working in the field of education since last 20 years. Has more than 100+ paper to his credit at National, International Conferences and Journal.</p>	