Cyber security: the common application threats and attack types

Science, Computer Science

Cyber security also known as computer security is a field of study which deals in protecting of computer systems from either damage or theft. The damage or theft could be either in the form of its hardware or software or may even include loss of electronic data. The field is beginning to grow in terms of its importance because of the boom of Internet and other technologies like wireless networks(which include Bluetooth and WI-FI) and smart devices. Cybersecurity can be defined in a better way as the act or practice of protecting computers, networks and programs from digital attacks. These so called attacks are usually aimed at accessing, changing or destroying sensitive information, stealing money from users; or interrupting a process. These attacks are performed by a hackers known as Black hat hackers. A Black hat hacker is usually a person who commits a crime by illegally breaking into systems and compromising their security. These hackers are often countered by ethical hackers known as white hat hackers. The are also known as penetration testers. They are like an army that fight against cyber crime and their aim is to prevent cyber crime from happening. There is a third category of hackers known as grey hat hackers-They are usually hackers that conduct black hat hacks for white hat hacker reasons.

Elements of cyber security

The helplessness of a person’s interaction with information systems can be easily exploited to launch a cyber attack. A better understanding of the elements of cyber security will make us aware of the loopholes which we have in our system and help us from preventing a malicious attack.

Application Security: Application security starts with the steps taken through an information application. A hacker first sees loopholes in the security protocols and policies of an application and then figures out a way to penetrate the application in-turn hacking into a user’s computer/device.

Take for instance you have an app in your phone which is allowed to read text messages and make phone calls. If the app isn’t protected enough a hacker can easily get into the app and misuse the app and use the app inappropriately. Things could get worse as he is able to read the message on your phone using the app as a medium and could potentially give a threat to you.

The method to tackle threats to application security is to have knowledge about potential threats and improving the security of an application, network or host and embedding security within the software development process.

In context to application security, an asset refers to a resource of value like information within a database or in the file system or system resource. The main challenge over here is to spot the vulnerabilities within the parent system which when becomes exposed to a cyber hacker can be misused or exploited. The risk can be mitigated or in other terms be prevented by weaving the security within the application.

The common application threats and attack types are mentioned below.

i) Input validation related like buffer overflow, cross site coding, , canonicalization , structured query language injection

- A buffer overflow is the term given to an instance which occurs whenever a program or process attempts to write more data to a fixed length block of memory or buffer, than the buffer is allocated to hold. Buffers are areas of memory set which are designated to hold data, often while moving it (the data) from one section of a program to another or between programs. A Hacker could trigger a buffer overflow by giving malformed inputs to a set of programs. This could in turn result in memory errors, incorrect results and crashes in the software or site.
- Cross site coding or XSS is a type of injection technique used by hackers in which he/she injects malicious scripts into (what is otherwise a trusted) website. The hacker who uses this technique is often refered to as an XSS attacker. Most of the time he/she uses an application which is linked to the web to send the malicious code which is usually in the form of a browser side script, to an end user. The hacker or attacker over here can use cross side coding to an unsuspecting user. The end user and his browser has no way to know that the script is malicious because according to the user the script came from a trusted source, The corrupted code can access any cookies, session tokens, or any other sensitive information which is retained by the browser itself and used by that site. These scripts are capable of even rewriting the content of a HTML page.
- Canonicalization attacks are the attacks in which unauthorized access of a file or directory on a webserver machine takes place in a method which involves tampering of file/directory paths a website normally

allows users to enter as a part of its functionality. The so called attack is usually carried out by entering the path of the file in the input field on a webpage or by supplying it as a part of the URL.

Although it may seem that canonicalization isn’t that big a threat, we have to be aware that canonicalization attacks may consequencially lead to loss of confidentiality, integrity and denial of service results if in case the files are deleted by the hacker

- SQL injection technique is a technique which is used to attack data-driven applications or data dependant applications Over here dump SQL statements are inserted into a field of execution. It often referred to as attack vector for websites containing high amount of data. Amidst an SQL injection the attacker/hacker can tamper with existing data , spoof identities and cause repudiation issues such as voiding transactions or changing balances. On a worst case scenario an attacker can destroy data or make it otherwise unavailable, and become administrators of the database server.

ii) Authentication related like brute force assault, network eavesdropping, replaying cookies, dictionary assaults, stealing credentials etc.

- A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data. This is one reason why account holders are often prompted by

sites to have a complicated passphrase consisting of caps and small letter, numbers and special characters. This would make the automated software unable to arrive at your password. Recently many websites have limited the number of attempts to type your password which inturn prevents brute force attack from taking place.

- Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, videoconference or fax transmission. In this technique a hacker intercepts your message and is able to view it with/without your knowledge and is able to misuse the communication which had taken place between two private parties. This is against the law and is a cyber crime.
- A cookie replay attack occurs when an attacker steals a valid cookie of a user, and reuses it to impersonate that user to perform fraudulent or unauthorized transactions/activities. A Cookie is a small file which are stored in a user’s PC. They are designed to hold an information or data regarding a particular client and website, and can be accessed either by the web server or the client computer. Cookies may even contain stored passwords and usernames . This is how the fraudulent activities are performed
- A dictionary attack is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password. This can also be called as the unsmarter method of brute attack